

## **Schedule 1: General Order Form**

**PROCURE IT VERSION 3.2**

---

**General Order Form to the Customer Contract between:**

**The Crown in right of the State of New South Wales  
acting through Department of Customer Service**

**(ABN 81 913 830 179)**

**and**

**Australian Centre for Advanced Computing and  
Communication Pty Ltd trading as AC3 Pty Limited**

**(ABN 27 095 046 923)**

**for the provision of a suite of services known as "Computing  
Integration Services"**

**Contract Number: DICT/693541**

## CUSTOMER

### Item 1 Name of Customer

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Formation (clause 3.4)</b>	
Specify the Customer's full legal name:	The Crown in right of the State of New South Wales acting through Department of Customer Service (ABN 81 913 830 179)

### Item 2 Service Address

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Formation (clause 3.4)</b>	
Specify the Customer's service/delivery address:	Department of Customer Service McKell Building 2-24 Rawson Place Sydney NSW 2000

### Item 3 Customer's Representative

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Representatives (clause 23.1)</b>	
Specify an employee who is the [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

## CONTRACTOR

### Item 4 Name of Contractor

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Formation (clause 3.4)</b>	
Specify the Contractor's full legal name:	Australian Centre for Advanced Computing and Communication t/as AC3 Pty Limited (ABN 27 095 046 923)

### Item 5 Service Address

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Formation (clause 3.4)</b>	
Specify the Contractor's service/delivery address:	AC3 Pty Limited Level 7, 477 Pitt Street Haymarket NSW 2000

## Item 6 Contractor's Representative

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Representatives (clause 23.1)</b>	
Specify an employee who is the [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

## Item 7 Head Agreement

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Formation (clause 3.1)</b>	
Specify the Head Agreement number:	Not applicable
Specify the Head Agreement title:	Not applicable
Specify the Term of the Head Agreement: Start Date: End Date:  If the Term of the Head Agreement has expired the Customer must obtain the Contract Authority's approval to enter into a further Customer Contract, and this approval should be attached to this General Order Form.	Not applicable
<b>Insurance (clause 16.2)</b>	
Specify the insurances required under the Head Agreement:	Not applicable
The default insurance requirement under the Head Agreement is public liability insurance with an indemnity of at least \$10,000,000 in respect of each claim for the period of cover.  Specify any higher limit of cover that is required by the Head Agreement:	Not applicable
The default insurance requirement under the Head Agreement is product liability insurance with an indemnity of at least \$10,000,000 for the total aggregate liability for all claims for the period of cover.  Specify any higher limit that is required by the Head Agreement:	Not applicable
Specify if professional indemnity/errors and omissions insurance was required under the Head Agreement.  If so, the default insurance requirement is for a limit of cover of \$1,000,000 in respect of the total aggregate liability for all claims for the period of cover.  Specify any higher limit that is required by the Head Agreement:	Not applicable

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Workers' compensation insurance in accordance with applicable legislation:	Not applicable
Specify any other type of insurance required under the Head Agreement and the specified amount:	Not applicable
<b>Performance Guarantee (clause 17.1)</b>	
Specify if the Contractor was required to provide a Performance Guarantee under the Head Agreement:	Not applicable

## Item 8 Modules that form part of the Customer Contract

### Formation (clause 3.8(a))

Indicate, by marking with an X, the Modules that apply

Module 1 – Hardware Acquisition and Installation	<input type="checkbox"/>	Module 11 – Telecommunications as a Service	<input type="checkbox"/>
Module 2 – Hardware Maintenance and Support Services	<input type="checkbox"/>	Module 12 – Managed Services	<input checked="" type="checkbox"/>
Module 3 – Licensed Software	<input type="checkbox"/>	Module 13 – Systems Integration	<input type="checkbox"/>
Module 4 – Development Services	<input type="checkbox"/>	Module 13A – Major Project Systems Integration Services	<input type="checkbox"/>
Module 5 – Software Support Services	<input type="checkbox"/>		
Module 6 – Contractor Services	<input type="checkbox"/>		
Module 7 – Professional Services	<input type="checkbox"/>		
Module 8 – Training Services	<input type="checkbox"/>		
Module 9 – Data Migration	<input type="checkbox"/>		
Module 10 – As a Service	<input type="checkbox"/>		

## Item 9 Schedules that form part of the Customer Contract in addition to the General Order Form

### Formation (clause 3.8(b))

Indicate, by marking with an X, the Schedules that apply

Schedule 1 – General Order Form	Applies	Schedule 7 – Statutory Declaration - Subcontractor	<input type="checkbox"/>
Schedule 2 – Agreement Documents	<input checked="" type="checkbox"/>	Schedule 8 – Deed of Confidentiality	<input type="checkbox"/>
Schedule 3 – Service Level Agreement	<input checked="" type="checkbox"/>	Schedule 9 – Performance Guarantee	<input type="checkbox"/>
Schedule 4 – Variation Procedures	<input checked="" type="checkbox"/>	Schedule 10 – Financial Security	<input type="checkbox"/>
Schedule 5 – Escrow Deed	<input type="checkbox"/>	Schedule 11 – Dispute Resolution Procedures	<input checked="" type="checkbox"/>
Schedule 6 – Deed Poll – Approved Agents	<input type="checkbox"/>	Schedule 12 – Project Implementation and Payment Plan	<input checked="" type="checkbox"/>

## Item 10 Contract Period

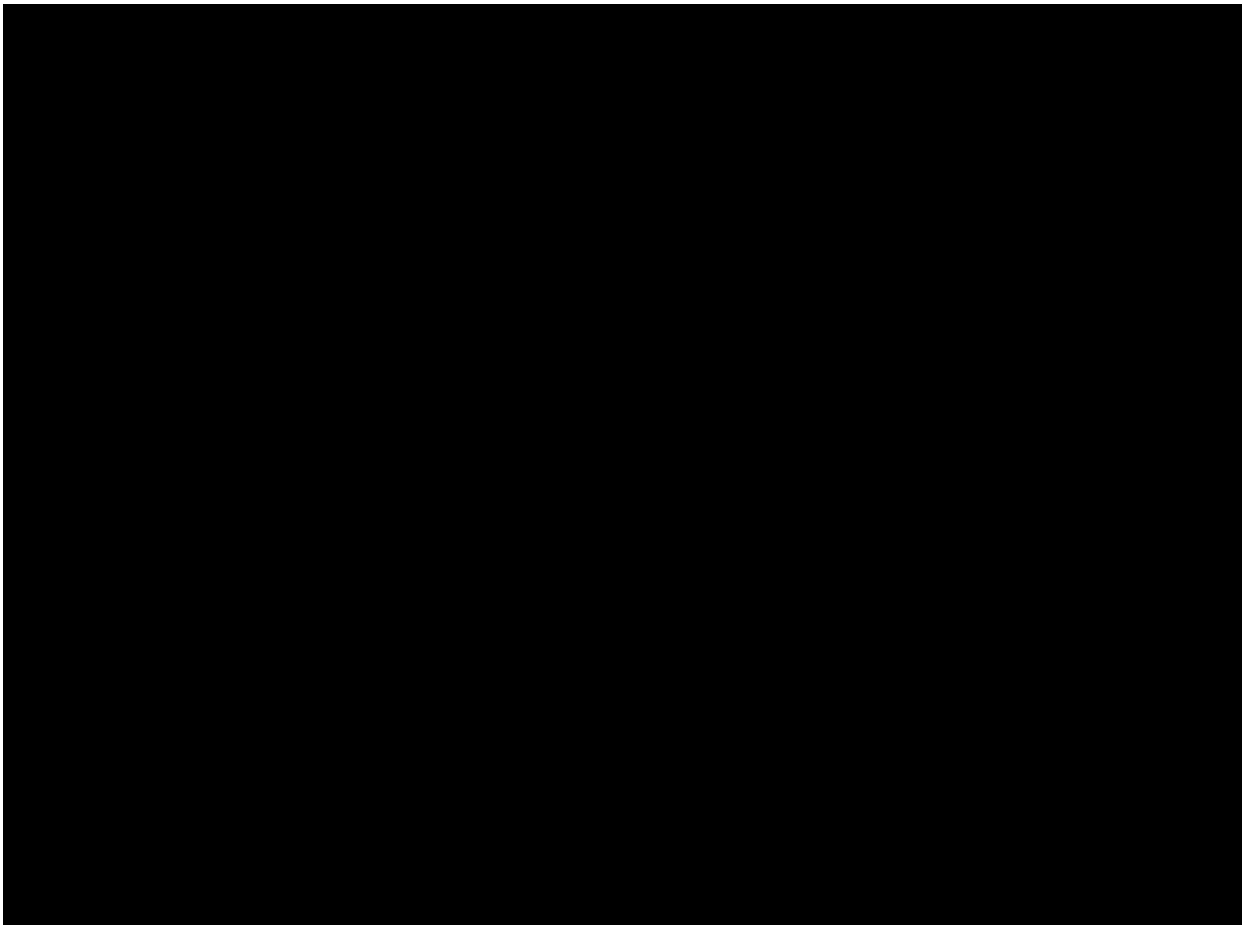
Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Contract Period (Clause 2.4)</b>	
Specify the Commencement Date if it is not the date when the Customer and the Contractor sign the Customer Contract:	The Commencement Date is 1 February 2021.
Specify the end of the Contract Period:	The Contract Period will end on the date that is 3 years after the Commencement Date.
Specify any period of extension of the Contract Period in days/weeks/years:	One-year extension option, followed by a second one-year extension option (both at the Customer's option).

## Item 11 Common Details

For the purposes of the following table, "Monthly Recurring Price" in rows B to H below includes the separate Price for:

- (a) Infrastructure As A Service (Monthly Fee);
- (b) Service Integration and Management (Monthly Fee); and
- (c) Customer Success (Monthly Fee)

as set out in Exhibit 3 (Pricing) to this General Order Form (together the **Ancillary Services Price**). The Parties acknowledge and agree that the Ancillary Services Price is payable from the commencement of Transition Phase 1, in accordance with Exhibit 3 (Pricing) to this General Order Form and the Customer Contract.





**Item 12 Delivery Address**

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Delivery (clause 5.1)	

Contract Number: DICT/693541

Confidential – Department of Customer Service

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Specify the address of the Site where delivery is to be made:	The applicable delivery Site is: Department of Customer Service McKell Building 2-24 Rawson Place Sydney NSW 2000
Specify any delivery instructions:	Not applicable
Specify the hours during which delivery may be made to the Site:	The relevant delivery hours will be Business Hours or as otherwise notified by the Customer from time to time.

### Item 13 Contract Specifications

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Formation (clause 3.4)</b>	
If the Contract Specifications are the User Documentation leave this Item blank. If the Contract Specifications comprise other documents, list those documents in order of priority:	
<b>System (clauses 5.11 and 9.3)</b>	
Specify whether the Products and Services comprise a System.	No

### Item 14 Payment

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Payment (clauses 11.1 and 11.2)</b>	
<b>Invoicing (clauses 11.7 and 11.9)</b>	
Specify the Customer's officer to receive invoices:	
Specify address to which invoices should be sent:	

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Specify the number of days from receipt of a Correctly Rendered Invoice that the Customer must make payment. If this Item is not completed, the Customer must pay the Contractor within 30 days from receipt of a Correctly Rendered Invoice.	The Customer must pay the Contractor within 30 days after receipt of a Correctly Rendered Invoice.
Specify when the Contract Price must be paid: <i>E.g. if the earlier Price is to be paid on delivery, insert "The Contract Price is due on delivery".</i> If payment is to be made on more than one occasion, then consider using a PIPP under Item 20.	As per Item 11.
Specify whether the Contract Price is fixed: <i>E.g. does the unit Price per item vary for inflation or other factors? If so, specify the calculation for Price variations:</i>	The Contract Price is as per Item 11, unless it is varied in accordance with the terms of this Customer Contract.

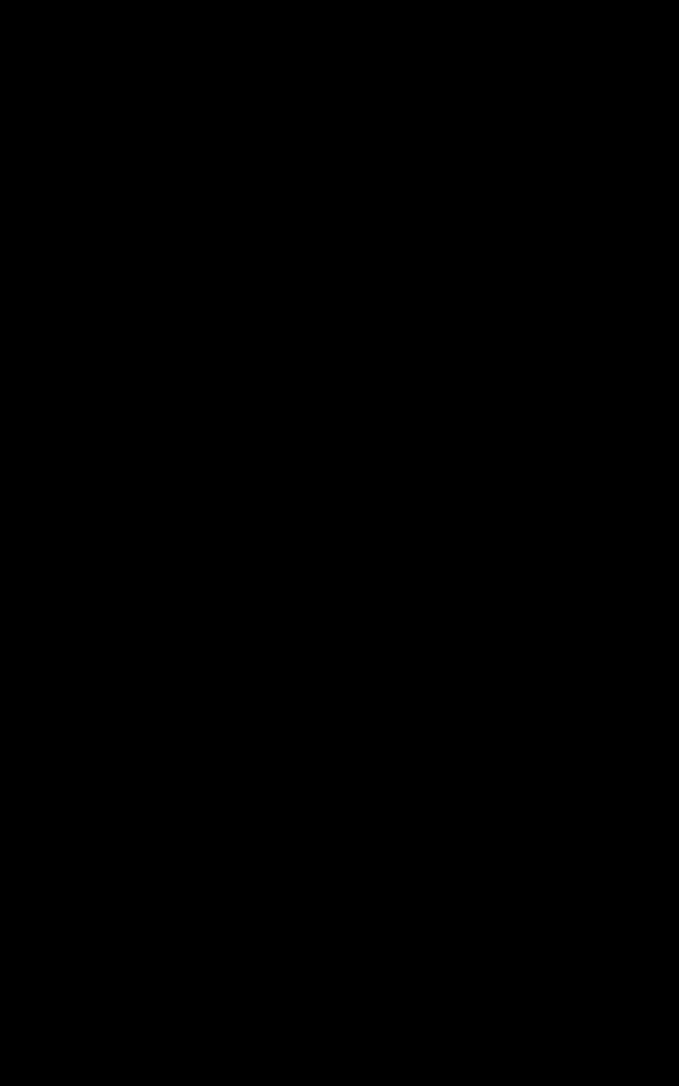
### Item 15 User Documentation

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>User Documentation (clause 5.4(b))</b>	
Specify the Price of any additional copies of the User Documentation:	The Contractor must provide one hard copy of the User Documentation to the Customer and make the User Documentation available to the Customer at all times in electronic format at no cost. No additional Price is payable for additional copies of User Documentation.

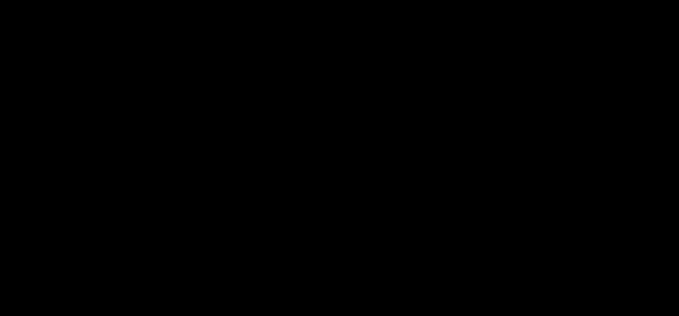
### Item 16 Management Committee

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Management Committee (clause 6.4)</b>	
List the name/s of the Contractor's project manager, officers or other relevant persons who will sit on the management committee:	
<b>Management Committee (clause 6.6)</b>	
Specify the function to be performed by the management committee:	
List the name/s of the Customer's project manager, officers or other relevant persons who will sit on the management committee:	



Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Management Committee (clause 6.8)</b>	
Specify the details, including the contents of the progress report to be submitted to the Customer's project manager:	
Specify any other details:	

**Item 17 Performance Review Procedures**

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Performance Reviews (clause 6.10)</b>	
Specify if a service and performance review/s of the Contractor's performance of the Customer Contract is to apply:	
Specify any specific time intervals for service and performance reviews:	



**Item 18 Site Preparation and Maintenance**

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Site Specifications (clause 6.12)</b>	
Specify: <ul style="list-style-type: none"> <li>• Site location; and</li> <li>• whether a Site Specification is required.</li> </ul>	
<b>Access to Customer’s Site (clause 7.1(b))</b>	
Specify any other requirements in relation to the Site access:	
Specify any requirements for the preparation and maintenance of the Site:	

**Item 19 Implementation Planning Study**

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Implementation Planning Study (clauses 6.14 to 6.16)</b>	
Specify if the Contractor must provide an implementation planning study:	An implementation planning study is not required.
Specify the implementation planning study objectives and time for provision of study:	Not applicable
Date for delivery of the implementation planning study to the Customer:	Not applicable
Specify if the implementation planning study need to undergo Acceptance Tests in accordance with clause 10.1(b):	Not applicable

**Item 20 Project Implementation and Payment Plan (PIPP) and Staged Implementation**

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Project Schedule (clause 6.17)</b>	The Contractor must perform the Services and deliver the Deliverables to: <ul style="list-style-type: none"> <li>(a) achieve Completion of the relevant Milestones by their Agreed Dates as set out in the Customer Contract (and, in respect of the Transition-In Services, the PIPP); and</li> <li>(b) meet any other specified timeframes that are set out in the Customer Contract (and, in respect of the Transition-In Services, the PIPP), including delivery of the Deliverables by the applicable due dates as set out therein.</li> </ul>
<b>Invoicing (clause 11.7)</b>	
Specify if a PIPP has been created. If so, identify the document in this Item and attach as an Annex to this General Order Form:	Yes, the PIPP is attached at Schedule 12 (Project Implementation and Payment Plan) to this General Order Form.

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<i>E.g. the PIPP is in a document "PIPP v1_1 27/10/11" and Annexure 1 to the Customer Contract.</i>	
<b>Staged Implementation (clause 6.20)</b>	
Specify if there is to be Staged Implementation: If so, details of the Deliverables that comprise each Stage must be stated in the PIPP together with the period during which the Customer must give written notice to move to the next Stage (if greater than 10 Business Days):	Not applicable. Staged Implementation does not apply to the Services and Deliverables under this Customer Contract.

### Item 21 Liquidated Damages

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Liquidated Damages (clauses 6.28 to 6.34)</b>	
Specify if Liquidated Damages (LDs) will apply:	Yes, Liquidated Damages will apply in accordance with the PIPP.
Specify the Milestones which are LD Obligations:	As set out in the PIPP
Specify the Due Date for completion of each LD Obligation:	As set out in the PIPP
Specify the calculation and amount of LDs for each LD obligation:	As set out in the PIPP
Specify the maximum number of days LDs are to be paid for each LD obligation:	As set out in the PIPP

### Item 22 Customer Supplied Items (CSI) and Customer Assistance

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Customer Supplied Items (CSI) (clause 6.36)</b>	
Specify each CSI to be provided by the Customer: CSI may be: <ul style="list-style-type: none"> <li>office access, desks etc (specify location, standards, times of access);</li> <li>Hardware or software (specify equipment, capacity, versions of software and dates of availability);</li> <li>VPN access or other remote access (specify capacity and hours available).</li> </ul> <b>[Note: details of any Customer Personnel should be specified in Item 26].</b>	As set out in section 6 of the PIPP.
Specify if any CSI must be covered by support and maintenance contracts including the period of cover, the Contractor's rights of access to any third	As set out in section 6 of the PIPP.

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
party support help desk, the hours and service levels to which support and maintenance must be available to the Contractor:	
Specify the times when each CSI is to be provided:	As set out in section 6 of the PIPP.
Specify any requirements to attach to any CSI: <i>E.g. any standards that the CSI must meet.</i>	Not applicable
Specify if the Contractor must conduct any verification checks of CSI's to ensure they are satisfactory:	Not applicable
If so, specify the verification check process for each CSI: Include: <ul style="list-style-type: none"> <li>• a process to manage satisfactory and unsatisfactory verification checks;</li> <li>• a process to manage 'reissued' CSI's;</li> <li>• a process to manage repeat CSI verification checks;</li> <li>• a process to manage 'draft' or 'incomplete' and 'updated' CSI's;</li> <li>• a process to manage rejected CSI's;</li> <li>• a process to manage previously satisfactory CSI which becomes defective;</li> <li>• a list of required verification check forms and/or registers and a corresponding data entry process;</li> <li>• a list of Customer and Contractor nominee/s for responsibility to undertake verification checks:</li> </ul>	Not applicable
Specify any amount payable by the Contractor to the Customer for any item of CSI:	None payable
<b>Customer Assistance (clause 6.41)</b>	
Specify the instructions, information, data, documents, specifications, plans, drawings and other materials that must be provided by the Customer to the Contractor:	The Customer will use reasonable efforts to provide assistance to the Contractor as set out in, or to be agreed in accordance with, the PIPP and Exhibit 1 (Services) to this General Order Form.

### Item 23 Escrow

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Escrow (clause 6.42)</b>	
Specify if an escrow arrangement is required:	Not applicable
Specify the parties to the escrow arrangement:	Not applicable

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Specify the time for the escrow arrangement to endure:	Not applicable

## Item 24 Business Contingency Plan

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Business Contingency (clauses 6.45 to 6.47)</b>	
Specify if a Business Contingency Plan is required:	Yes, a Business Contingency Plan is required.
Specify when the Business Contingency Plan is required:	The Business Contingency Plan is required from the Commencement Date until the end of the Contract Period.
Specify any information to be included in the Business Contingency Plan including the business contingency services required and the period of the services:	<p>The Contractor must:</p> <ul style="list-style-type: none"> <li>(a) develop a Business Contingency Plan that: <ul style="list-style-type: none"> <li>(i) is consistent with the Customer's business continuity policies;</li> <li>(ii) specifies when the Business Contingency Plan is to be activated;</li> <li>(iii) specifies: <ul style="list-style-type: none"> <li>(A) the steps to be taken to recover one or more of the Services and Deliverables;</li> <li>(B) the Contractor's Personnel, Customer's Personnel and other persons to be involved; and</li> <li>(C) the communications to be implemented, when the Business Contingency Plan is activated;</li> </ul> </li> <li>(iv) specifies the training and testing required before activating the Business Contingency Plan;</li> <li>(v) specifies and addresses all other matters requested by the Customer;</li> <li>(vi) includes procedures to reduce the impact of an incident (including a Force Majeure Event) disrupting the Services and Deliverables; and</li> <li>(vii) is specifically tailored for the Customer;</li> </ul> </li> <li>(b) within 30 days after the Services Commencement Date for the Managed Services under Module 12 (Managed Services), submit that Business Contingency Plan for the Customer's review in accordance with clause 6.45 of Part 2 (Customer Contract); and</li> <li>(c) implement the activities set out in the Business Contingency Plan at the times and in accordance with the procedures set out in the Business Contingency Plan.</li> </ul> <p>The Customer may advise the Contractor of any other required information to be included in the Business Contingency Plan from time to time during the Contract Period.</p>
Specify the periods that the Business Contingency Plan must be reviewed and updated by the Contractor:	Six monthly

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Specify the time periods that the Contractor is to test the operability of the Business Contingency Plan:	Annually

### Item 25A Transfer of Records outside NSW - Customer Data

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Customer Data (clause 7.5)</b>	
<p>Specify whether any State Records will be transferred to the Contractor's possession under the Customer Contract.</p> <p>If yes, Customer to state whether consent is provided to transfer State Records outside the jurisdiction of New South Wales.</p> <p>If consent is granted, Customer to specify:</p> <ul style="list-style-type: none"> <li>the jurisdiction(s) for which consent is granted</li> <li>the conditions on which such consent is granted.</li> </ul> <p><i>[Note: clause 7.5 of the Customer Contract requires that the Contractor must not transfer, take or send Customer Data which is a State Records without the Customer's prior written consent.]</i></p>	<p>From time to time during the Contract Period, the Customer may transfer or provide State Records to the Contractor (or its Personnel) or grant the Contractor (or its Personnel) with access to State Records. Unless expressly authorised by the Customer's Authorised Representative in writing at the time that the relevant State Records are made available to the Contractor:</p> <p>(a) the Customer does not consent to the Contractor (or its Personnel) transferring State Records to, or accessing State Records from, any locations outside the jurisdiction of New South Wales; and</p> <p>(b) the requirements of clause 7.5 of Part 2 (Customer Contract) will apply to any such State Records.</p>

### Item 25B Transfer of Records outside NSW – Personal Information

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Privacy (clause 15)</b>	
<p>Customer to specify whether consent is provided to transfer Personal Information outside the jurisdiction of New South Wales.</p> <p>If consent is granted, Customer to specify:</p> <ul style="list-style-type: none"> <li>the jurisdiction(s) for which consent is granted</li> <li>the conditions on which such consent is granted.</li> </ul> <p><i>[Note: Clause 15.1(h) of the Customer Contract requires that the Contractor must not transfer, take or send Customer Data which is a State Records without the Customer's prior written consent.]</i></p>	<p>Unless expressly authorised by the Customer's Authorised Representative in writing at the time that the relevant Personal Information is made available to the Contractor:</p> <p>(a) the Customer does not consent to the Contractor (or its Personnel) transferring Personal Information to, or accessing Personal Information from, any locations outside the jurisdiction of New South Wales; and</p> <p>(b) the requirements of clause 15.1(h) of Part 2 (Customer Contract) will apply to any such Personal Information.</p>

### Item 25 Secrecy and Security

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Access to Customer's Site (clause 7.11)</b>	

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<p>Specify any secrecy or security requirements that the Contractor and its Personnel must comply with:</p> <p><i>E.g. insert a reference to any document that includes a security requirement.</i></p>	<p>In addition to the requirements of clauses 7.10 to 7.12 of Part 2 (Customer Contract), the Contractor must comply with the following policies (which may be updated from time to time):</p> <ul style="list-style-type: none"> <li>(a) 'NSW Cyber Incident Response Plan';</li> <li>(b) 'NSW Government Cyber Security Policy';</li> <li>(c) 'Department of Customer Service Information Security Policy'; and</li> <li>(d) all other requirements of the Contract Specifications.</li> </ul> <p>The Customer will notify the Contractor of any updates to these policies in writing and in advance.</p>
<p><b>Timeframes for response to a Security Issue</b></p>	
<p>Specify whether Customer agrees to any alternate timeframe for:</p> <ul style="list-style-type: none"> <li>• Notification of actual, alleged or suspected security breach (clause 7.12(a))</li> </ul> <p><b>[Note: default is immediate notification]</b></p> <ul style="list-style-type: none"> <li>• Investigation of Security Issue (clause 7.12(b))</li> </ul> <p><b>[Note: default is within 48 hours from notification]</b></p> <ul style="list-style-type: none"> <li>• Remedy the Security Breach (clause 7.12(c)).</li> </ul> <p><b>[Note: the default is within 24 hours from conclusion of investigation].</b></p> <p>Any alternate timeframes agreed to in this General Order Form must:</p> <ul style="list-style-type: none"> <li>• be approved by the Customer's Chief Information Officer; and</li> <li>• comply with the NSW Government Digital Information Security Policy, NSW Government Information Security Event Reporting Protocol, NSW Government Cloud Policy and all other applicable NSW Government policies;</li> <li>• comply with applicable security standards; and</li> <li>• comply with the Customer's Information Security Management System and other Customer security and policy requirements.</li> </ul>	<p>In addition to the requirements of clauses 7.11 and 7.12 of Part 2 (Customer Contract), if the Contractor becomes aware or suspects that:</p> <ul style="list-style-type: none"> <li>(a) it, or any of its Personnel, is using or disclosing, or has used or disclosed, any Customer Data or any Personal Information in contravention of clauses 7, 14 or 15 of Part 2 (Customer Contract) or any Privacy Laws or data protection laws;</li> <li>(b) there has been actual or attempted unauthorised access to any Customer systems;</li> <li>(c) there has been actual or attempted theft of, unauthorised access to, or unauthorised disclosure of any Customer Data or Personal Information;</li> <li>(d) any Customer Data or any Personal Information has been lost in circumstances where unauthorised access to, or unauthorised disclosure of, that Customer Data or Personal Information may occur or has occurred; or</li> <li>(e) any other breach of any Privacy Laws or data protection laws by the Contractor or any of its Personnel, Subcontractors or Related Companies,</li> </ul> <p>(each a <b>Data Breach</b>), then the Contractor must notify the Customer of that Data Breach immediately upon becoming aware of the Data Breach.</p> <p>Otherwise, default timeframes apply, except to the extent that applicable laws require the Contractor to respond within an earlier timeframe, in which case that earlier timeframe applies.</p>

## Item 26 Customer's Personnel

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<p><b>Personnel General (clause 8.5)</b></p>	
<p>Specify the Customer's Personnel who will be available to work with the Contractor and their roles and responsibilities:</p>	<p>None required</p>

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Also specify the times and duration of their involvement as well as their authority levels:	

### Item 27 Specified Personnel

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Specified Personnel (clause 8.8)</b>	
Specify the identity and roles and responsibilities of any of the Contractor's Specified Personnel:	

### Item 28 Subcontractors

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Agents and Subcontractors (clause 8.17)</b>	
Specify which subcontractors are required to provide a Statutory Declaration - Subcontractor, substantially in the form of Schedule 7:	Not applicable

### Item 29 Quality Standard Accreditation

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Contractor Warranties (clause 9.1(h))</b>	
Specify any quality standard accreditation arrangements the Contractor must hold during the Contract Period:	The Contractor must hold the following quality standard accreditations for the duration of the Contract Period: (a) ISO 9001:2015 – Quality Management Systems; and (b) ISO 27001 Information Security Management Systems.



### Item 30 Contractor's Compliance with Standards, Codes and Laws

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Contractor Warranties (clause 9.1(g))</b>	
Specify any laws (other than Statutory Requirements) the Contractor is to comply with:	The Contractor must comply at all times with: <ul style="list-style-type: none"> <li>(a) the Privacy Laws, as though it was acting as a New South Wales Government Agency;</li> <li>(b) the <i>Work Health and Safety Act 2011</i> (NSW) (and any other applicable work health and safety legislation in any other jurisdiction(s) where the Contractor carries out any activities in relation to this Customer Contract);</li> <li>(c) the <i>Competition and Consumer Act 2010</i> (Cth) (including the Australian Consumer Law set out in Schedule 2 of that Act); and</li> <li>(d) all applicable Commonwealth and NSW anti-bribery, anti-corruption, anti-terrorism financing and anti-money laundering laws and all domestic and international sanctions relating to such laws.</li> </ul>
Specify any codes, policies, guidelines or standards the Contractor is to comply with:	The Contractor must comply with all industry codes of conduct which are applicable to its business, products and services.  Any additional codes, policies, guidelines or standards which are specified after the Commencement Date will be notified to the Contractor by the Customer in writing and in advance.

### Item 31 Customer's Compliance with Standards, Codes and Laws

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Customer Warranties (clause 9.4(h))</b>	
Specify any laws (other than Statutory Requirements) the Customer is to comply with:	Not applicable
Specify any codes, policies, guidelines or standards the Customer is to comply with:	Not applicable

### Item 32 Acceptance Testing

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Part 3 Dictionary (clauses 1.2 to 1.5)</b>	
<b>Acceptance Test Notification Period</b> is the period from the end of the Acceptance Test Period, within which the Customer must provide to the Contractor written notice of the result of the Acceptance Test. Specify this period: If no period is specified, the period is 2 Business Days:	Not applicable – the default position under clause 1.2 of Part 3 (Dictionary) applies
<b>Acceptance Test Data</b> is the data that is provided by the Customer, and agreed by the Contractor that reflects the data the Customer will use in the Deliverable, that is to be used for Acceptance Testing.	As set out in, or to be agreed in accordance with, the PIPP

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Specify the Acceptance Test Data:	
<p><b>Acceptance Test Period</b> is the period for the performance of any Acceptance Tests for any Deliverable.</p> <p>Specify this period:</p> <p>If no period is specified, the period is 10 Business Days from the date of delivery of the Deliverable to the Customer.</p>	Not applicable – the default position under clause 1.5 of Part 3 (Dictionary) applies
<b>Acceptance (clause 10.1)</b>	
<p>For each Deliverable, specify whether each Deliverable is to undergo Acceptance Testing:</p> <p>If not, the Deliverable will be Accepted under clause 10.1(a)</p>	As set out in the PIPP
<p>If a Deliverable is not to undergo Acceptance Tests, specify the period required following delivery of the Deliverable as required by the Order Documents when the Actual Acceptance Date for a Deliverable occurs:</p> <p>If no period is specified, then the period is 2 Business Days.</p>	As set out in the PIPP
<b>Conducting Acceptance Tests (clause 10.3)</b>	
For each Deliverable that is to undergo Acceptance Tests, specify details of the Acceptance Testing requirements:	As set out in, or to be agreed in accordance with, the PIPP
Specify the identification of the Deliverables or part of the Deliverables to be tested:	As set out in, or to be agreed in accordance with, the PIPP
Specify the allocation of each Party's responsibilities in relation to testing, including the Party responsible for conducting the Acceptance Tests:	As set out in, or to be agreed in accordance with, the PIPP
Specify which Party is to provide the test environment, including hardware, software, power, consumables and other resources and when the environment and resources must be ready for use:	As set out in, or to be agreed in accordance with, the PIPP
Specify the methodology and process for conducting Acceptance Tests:	As set out in, or to be agreed in accordance with, the PIPP
Specify the scheduling of Acceptance Tests including the Acceptance Test Period and the Acceptance Test Notification Period:	As set out in, or to be agreed in accordance with, the PIPP
Specify the Acceptance Criteria used to test whether the Deliverable meets the Contract Specification and other requirements of the Customer Contract:	As set out in, or to be agreed in accordance with, the PIPP
Specify the Acceptance Test Data required:	As set out in, or to be agreed in accordance with, the PIPP

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
If an Acceptance Test document has been created that addresses the above points it can be attached to the General Order Form by identifying the document here:	Not applicable

### Item 33 Credit/Debit Card

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Payment (clause 11.3)</b>	
Specify any credit/ debit card or electronic facility that the Customer may use to pay the Contractor:	Not applicable
Specify any fee that is applicable for payment by credit/debit card	Not applicable

### Item 34 Intellectual Property

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Existing Material (clauses 13.7, 13.9 and 13.10)</b>	
Specify any terms and condition applicable for granting a licence for Existing Material owned by a third party:	No terms applicable
If a perpetual and irrevocable licence to use certain Existing Material cannot be provided (for example because it is licensed under subscription for a defined period), specify: <ul style="list-style-type: none"> <li>the duration of the licence to use that Existing Material and/or</li> <li>the terms on which the licence may be revoked.</li> </ul>	Not applicable
Specify any fees to be charged for any licence to use any of Contractor's Existing Materials:	Not applicable
<b>Customer Owned New Material (clause 13.11)</b>	
Specify whether clause 13.11 applies ie. whether the Customer owns any New Material. If so, specify: <ul style="list-style-type: none"> <li>which items of New Material are Customer Owned New Material; and</li> <li>whether the Contractor is granted any licence by the Customer to use the Customer Owned New Material, and if so, what licence terms apply to the Contractor's use of the Customer Owned New Material.</li> </ul> If clause 13.11 does not apply, state "Not applicable".	Clause 13.11 applies to any New Material created. The Contractor is granted a non-exclusive, non-transferrable, royalty free licence to use the New Material to the extent necessary, and for the purposes of, performing its obligations under this Customer Contract.

### Item 35 Confidentiality

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Confidentiality (clause 14.4)</b>	
Specify if the Contractor must arrange for its Subcontractors to execute a Deed of Confidentiality substantially in the form of Schedule 8 – Deed of Confidentiality:	Not applicable

### Item 36 Insurance Requirements

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Insurance (clause 16.7)</b>	
Level of indemnity of public liability insurance in respect of each claim for the period of cover. The default requirement in the Customer Contract is \$10,000,000 <b>[Only specify if a higher limit of cover that is required by the Customer Contract:]</b>	An amount of not less than \$20,000,000 for each and every event.
Level of indemnity of product liability insurance for the total aggregate liability for all claims for the period of cover. The default requirement in the Customer Contract is \$10,000,000 <b>[Only specify if any higher limit of cover that is required by the Customer Contract:]</b>	An amount of not less than \$10,000,000 for each and every event and in the annual aggregate for all events in any one annual policy period.
If Services are being provided under the Customer Contract the default level of indemnity of professional indemnity insurance for the total aggregate liability for all claims for the period of cover is \$1,000,000 <b>[Only specify if a higher limit that is required by the Customer Contract:]</b>	An amount of not less than \$10,000,000 for each and every claim and in the annual aggregate for all claims in any one annual policy period.
Specify any additional insurance that the Contractor is to hold, including the type of insurance, the term of the insurance and the amount of the insurance:	Workers compensation insurance in accordance with applicable workers compensation legislation and awards. Any other insurance required by applicable Statutory Requirements.

### Item 37 Performance Guarantee

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Performance Guarantee (clause 17.2)</b>	
Specify if the Contractor must arrange for a guarantor to enter into a Performance Guarantee:	Not applicable
Specify the date by which the Performance Guarantee must be provided to the Customer. If no date is specified the Contractor must provide the Performance	Not applicable

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
Guarantee to the Customer within 30 days of the Commencement Date.	

### Item 38 Financial Security

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Financial Security (clause 17.4)</b>	
Specify if the Contractor must provide a Financial Security: If so, specify the amount of the Financial Security:	Not applicable
Specify the date by which the Financial Security must be provided to the Customer: If no date is specified, the Contractor must provide the Financial Security within 14 days of the Commencement Date.	Not applicable

### Item 39 Limitation of Liability

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Limitation of Liability (clause 18)</b>	
<p>If the Parties cannot agree the amount that is legally payable under the Customer Contract for the:</p> <ul style="list-style-type: none"> <li>• Non-Recurring Service or Product; and/or</li> <li>• Short Term Recurring Service,</li> </ul> <p>(as applicable) insert the amount that the Parties agree is the best estimate of the Contract Value for the relevant item (the Estimated Contract Price).</p> <p><b>Note: It may be necessary to separately identify the amounts payable under a single Customer Contract into separate amounts that are attributable to each of the different types of Product / Service.</b> (See definition of Contract Value in Part 3)</p>	<p>The Parties acknowledge and agree that Clause 18.1(b)(i) of Part 2 (Customer Contract) is replaced with the following new clause 18.1(b)(i) (and Clause 18.1(b)(iii) of Part 2 (Customer Contract) will not apply where this Clause 18.1(b)(i) applies):</p> <p><i>"(i) any Service, before the date the first amount of the Price for Recurring Services (other than Transition-in Services) is payable under the Customer Contract: 12 times the estimated monthly Price payable for the Recurring Services (other than Transition-in Services) for the first six months after Go Live (as that term is defined in the PIPP)."</i></p> <p>Otherwise, default liability limits for Recurring Services apply, as specified in clause 18.1 of Part 2 (Customer Contract) as amended by clause 5 of Part A, and Part B, of Item 43 (Additional Conditions) of this General Order Form.</p>
<p>If Services are being provided under any of the following Modules:</p> <ul style="list-style-type: none"> <li>• Module 6 – Contractor Services;</li> <li>• Module 7 – Professional Services; or</li> <li>• Module 8 – Training Services,</li> </ul> <p>specify whether the Parties regard the relevant Services as being:</p> <ul style="list-style-type: none"> <li>• the supply of a service of the same type on a periodic basis, and so are to be classified as Recurring Services for the purpose of the limitation of liability; or</li> <li>• provided in respect of a specific project where the Contractor has been engaged by a Customer to produce, create or deliver a specified outcome or solution that may be subject to Acceptance Testing, in which case the Services are to be classified as Non-Recurring Services for the purpose of the limitation of liability.</li> </ul> <p>(See definition of Non-Recurring Services and Recurring Services in Part 3)</p>	<p>Not applicable, as the Services are all being provided under Module 12 (Managed Services).</p>
<b>Details to be included from the Customer Contract</b>	
<p>Specify the alternative cap of liability (clause 18.3):</p>	<p>Not applicable, as the Contract Price does not exceed \$20,000,000 and a Prescribed Use does not apply.</p>

### Item 40 Performance Management Reports

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Reporting (clause 21.1)</b>	

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer		
Specify the reports required, (if any), the time for provision and the agreed format:	The Contractor must provide the reports, containing the content, in the form and at the times as specified in the following table:		
	<b>Name of report</b>	<b>Brief description</b>	<b>Frequency</b>
	Operations Status Report	Provides summary status of Service delivery operations for discussion.	Fortnightly
	Projects Status Report	Provides summary of all Projects.	Monthly
	Transition and Transformation Management Report	Information regarding the status of the Transition (and Transformation) programs of work.	Weekly
	Resourcing Report	Provide details on the Contractor's resourcing	Monthly
	Service Level Report	Report providing Service Level results, including Service Credits.	Monthly
	Commercial and Finance Report	Providing overview of commercial and financial status of the relationship.	Monthly
	Risk and Issues Register	List of risks and issues across all Services and Customer projects undertaken by the Contractor.	Monthly
	Capacity Management Plan and Report	Report providing information to allow management of forecasting, planning and Implementation of current and future business demand of ICT infrastructure and applications.	Monthly
	Balanced Scorecard Summary Report	Provides details of performance and health of the relationship and status of the program covering agreed categories and metrics. Shows quadrants including relationship, customer service, financial and technical.	Quarterly
Continuous Improvement Plan	Plan provides the Executive with information about continuous service improvement opportunities and can be used to ensure that service improvement	After 6 months and then annually thereafter	

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer		
		activities are receiving the necessary support and are resourced sufficiently to implement solutions.	
	Post Incident Report	Information regarding events and activities undertaken to resolve a major incident (Priority 1 or Priority 2) and corrective actions. Incorporates Root Cause Analysis.	As required
	Technology and Innovation Report	An update of the technology and innovation plan.	As required
	Ad Hoc Reports	As determined/mutually agreed by the parties.	As required

#### Item 40A Audit

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Alternative Audit Mechanism (clause 23.11)</b>	
<p>If the default audit provisions of clause 23.5-23.8 are to apply, state "Not Applicable".</p> <p>If an alternative audit mechanism is agreed by the Customer and Contractor, specify the terms of such alternate audit including the Contractor's obligations to be audited.</p> <p><b>Note: Any alternate audit mechanism must address compliance with the Contractor's Customer Data, security and privacy obligations and such other obligations required by the Customer and reasonably agreed by the Contractor.</b></p>	Not applicable – the default audit provisions apply

#### Item 41 Dispute Resolution

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<b>Dispute Resolution (clause 24)</b>	
Specify the threshold amount in AU\$ for issues to be resolved by expert determination under clauses 24.7-24.8.	Default threshold under clause 24.11(a) of Part 2 (Customer Contract) applies
Specify type of issue/s not to be determined by expert determination under clauses 24.7 to 24.8.	Not applicable



## Item 42 Termination for Convenience

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<p><b>Termination for Convenience by the Customer (clause 25.4)</b></p>	
<p>Specify whether an amount is payable under clause 25.4(b) if the Customer exercises its right of termination for convenience under clause 25.3, and if so, specify that amount:</p>	<p>(a) The Customer may at any time terminate the Customer Contract for convenience under clause 25.3 of Part 2 (Customer Contract) by providing at least 90 days' prior Notice in Writing to the Contractor (<b>Termination Notice</b>).</p> <p>(b) If the Customer issues Notice in Writing to terminate the Customer Contract for convenience under clause 25.3 of Part 2 (Customer Contract):</p> <p>(i) the Contractor must:</p> <p>(A) immediately (or at the later time requested by the Customer) commence providing the Transition Out Assistance in accordance with clause 13 of Part A of Item 43 (Additional Conditions) of this General Order Form; and</p> <p>(B) continue to provide the Services and Deliverables in accordance with clause 13.6 of Part A of Item 43 (Additional Conditions) of this General Order Form (<b>BAU Services</b>),</p> <p>from the date of the Termination Notice until the end of the Transition Out Period (or, in each case, until the earlier time requested by the Customer); and</p> <p>(ii) the Transition Out Period will be a minimum of 30 days; and</p> <p>(iii) the Contractor may invoice the Customer (and, if so, the Customer must pay) the following amounts:</p> <p>(A) during the first month after the date of the Termination Notice, the full monthly Price for that month; and</p> <p>(B) for the remaining duration of the Transition Out Period, a reduced portion of the monthly Price as determined in accordance with clause 13.7 of Part A of Item 43 (Additional Conditions) of this General Order Form,</p> <p>in exchange for the Contractor's provision of the Transition Out Assistance and the BAU Services in accordance with clause 13 of Part A of Item 43 (Additional Conditions) of this General Order Form.</p> <p>The amounts specified above are the only compensation payable to the Contractor for any termination for convenience under clause 25.3 of Part 2 (Customer Contract). Once the Customer has paid the amounts specified above, no further compensation is payable for any termination for convenience under clause 25.3.</p>

## Item 43 Additional Conditions

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<p>Specify any Additional Conditions:</p> <p><b>Note: where the Customer Contract is made under a Head Agreement the Customer must obtain the consent of the Contract Authority and the Secretary of the New South Wales Department of Customer Service where an</b></p>	<p>The Additional Conditions are as set out in the Annexure to this General Order Form.</p>

Details to be included from the Customer Contract	Order Details agreed by the Contractor and the Customer
<i>Additional Condition varies any term or condition of the Procure IT Framework including a Protected Clause.</i>	

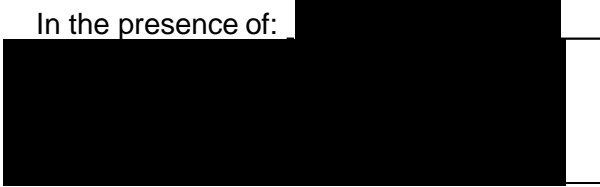
**This General Order Form is part of the Customer Contract and incorporates all Parts, terms and conditions and other documents listed in clause 3.8 as if repeated in full in this General Order Form.**

# SIGNED AS AN AGREEMENT

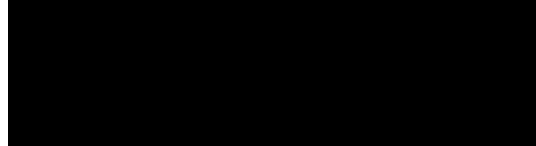
**Signed** for and on behalf of the Crown in right of the State of New South Wales acting through Department of Customer Service (ABN 81 913 830 179)

By  but not so as to incur personal liability

In the presence of:



Signature of Customer



Signature of Witness



Print name

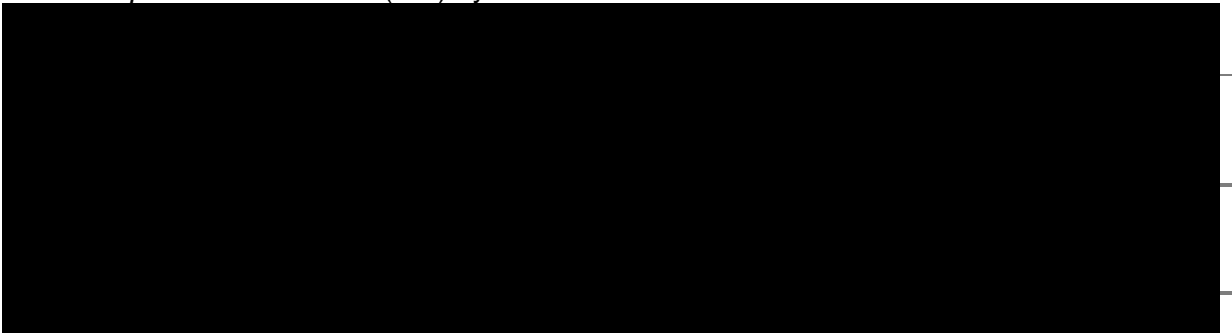
Feb 8, 2021

Feb 8, 2021

Date

Date

**Signed** for and on behalf of Australian Centre for Advanced Computing and Communication Pty Ltd trading as AC3 Pty Limited (ABN 27 095 046 923) in accordance with section 127(1) of the *Corporations Act 2001* (Cth) by:



## ANNEXURE TO SCHEDULE 1 GENERAL ORDER FORM ITEM 43 ADDITIONAL CONDITIONS

### **PART A: AMENDMENTS AND ADDITIONS TO CUSTOMER CONTRACT TERMS**

The clauses contained in this Annexure apply to the Customer Contract and are deemed to be incorporated into Item 43 of the General Order Form as if they are stated in that Item.

#### **1. Delay and Liquidated Damages**

- 1.1 Clauses 6.24 to 6.35 (inclusive) of Part 2 (Customer Contract) are deleted and replaced with "Not Used" and all other references to those clauses in Part 2 (Customer Contract) are considered to be references to the corresponding clause in this Clause 1 of this Item 43.

#### **NOTIFICATION**

- 1.2 Without prejudice to any other obligation of the Contractor under clauses 1.3 to 1.12 of this Item 43, each Party must do all it reasonably can to promptly inform the other of anything that it becomes aware of which is likely to affect the cost, quality or timing of delivery of the Deliverables, and the Parties must then investigate how to avoid or minimise any adverse effect on the Customer Contract.

#### **KEY DATES**

- 1.3 The Contractor shall:
- (a) proceed with the performance of the Services and provision of the Deliverables under the Customer Contract with due expedition and without delay; and
  - (b) ensure that each Milestone is Complete by the Agreed Date.

#### **NOTICE OF DELAY**

- 1.4 Within three Business Days of the Contractor becoming aware of a Delay, it shall give the Customer Notice in Writing of the cause or probable cause of Delay and the estimated Delay.

#### **CLAIM**

- 1.5 The Contractor will be entitled to an extension of time (**EOT**) to an Agreed Date, if and only if, and as conditions precedent to such entitlement:
- (a) a Delay Event occurs so as to delay the Contractor in achieving:
    - (i) prior to the Agreed Date, Completion of a relevant Milestone by the Agreed Date; and
    - (ii) after the Agreed Date, Completion of a relevant Milestone;
  - (b) within 30 days after the earlier of the date when the Contractor became aware or should reasonably have become aware of the cause of the Delay, the Contractor gives the Customer a claim, by Notice in Writing, for an EOT to the Agreed Date, setting out in detail:
    - (i) the cause of the Delay;
    - (ii) the facts of the Delay;
    - (iii) the extent of the Delay and the number of days EOT claimed;

- (iv) the date on which the cause of the Delay first arose; and
  - (v) the steps taken by the Contractor to prevent the occurrence of the Delay and minimise the consequences of the Delay;
- (c) the Contractor has done all things reasonably within its power to minimise the duration and consequences of the Delay;
  - (d) if, when the time for giving the notice in accordance with clause 1.5(b) of this Item 43 arises, the Delay is continuing, the Contractor gives a further Notice in Writing of the Delay to the Customer advising the Customer that the Delay is still continuing every 10 days until the cessation of the Delay; and
  - (e) if clause 1.5(d) of this Item 43 applies, within 10 Business Days of the cessation of the delay, the Contractor gives the Customer a claim, by Notice in Writing, for an EOT to the Agreed Date, setting out in detail the final number of days EOT claimed.

#### ASSESSMENT

- 1.6 If the Delay Event is overlapping with another cause of Delay which is not a Delay Event, then, to the extent that the Delays or part of them are overlapping, the Contractor shall not be entitled to an EOT.
- 1.7 In determining whether the Contractor is entitled to an EOT:
  - (a) the Customer may assess whether the Contractor will be delayed in achieving Completion of the relevant Milestone by the Agreed Date by using all of the information available to it at the time that the determination is made (regardless of when the determination is made) and the Customer is not restricted to considering only that information available at the time of the cause of the Delay or at the time the Contractor's claim for an EOT is submitted; and
  - (b) the Customer shall have regard to whether the Contractor has taken all reasonable steps to prevent the occurrence of the Delay and minimise the consequences of the Delay.
- 1.8 If the Contractor has not strictly complied with the provisions of clauses 1.4 and 1.5 of this Item 43:
  - (a) the Customer is required to provide Notice in Writing to the Contractor that the Contractor is not entitled to an EOT in respect of the relevant Delay;
  - (b) the Customer shall not be liable upon any claim by the Contractor in respect of the Delay Event or the Delay; and
  - (c) the Contractor releases and waives any entitlement it may have to any claim whatsoever against the Customer, including a claim for an adjustment to the contract sum, an EOT, delay damages or any other costs, in respect of the Delay Event or the delay.

#### EXTENSION OF TIME

- 1.9 Within 30 days after receiving the Contractor's claim for an EOT pursuant to clause 1.5(b) or 1.5(e) of this Item 43 (as applicable), the Customer shall give to the Contractor a Notice in Writing setting out the EOT so assessed.
- 1.10 A delay by the Customer or the failure of the Customer to grant an EOT or to grant an EOT within 30 days shall not cause any Agreed Date to be set at large and the EOT claim will be deemed to be rejected.
- 1.11 Notwithstanding that the Contractor is not entitled to or has not claimed an EOT, the Customer may at any time and from time to time, by notice in writing to the Contractor, give Notice in Writing of an EOT. This entitlement to extend is for the benefit of the Customer only, and the Customer is not required to act fairly or take into account the interest of the Contractor in deciding whether or not to exercise this right.

## TERMINATION

1.12 Subject to clauses 1.13 and 1.20 of this Item 43, if the Contractor fails to Complete a Milestone by the Agreed Date, the Customer may issue a Notice in Writing of a breach in respect of such failure, specifying a period during which the Contractor is required to remedy that breach, such period to be the greater of:

- (a) 10 Business Days; or
- (b) such longer period stated in the Notice in Writing,

and if the Contractor has not remedied that failure to Complete the Milestone (by Completing the Milestone) by the end of such period, the Customer may terminate the Customer Contract immediately by Notice in Writing to the Contractor.

1.13 The Customer agrees that clause 1.12 of this Item 43 does not apply to failure to Complete a Milestone by the Agreed Date, where that Milestone is an LD Obligation, during any period in which the Customer may exercise its rights under clause 1.18 of this Item 43.

## LIQUIDATED DAMAGES

1.14 Where the Parties have agreed in Item 21 of the General Order Form that liquidated damages will be payable for the late completion of an LD Obligation, clauses 1.15 to 1.19 of this Item 43 apply.

1.15 If the Contractor fails to achieve an LD Obligation by the applicable Agreed Date, the Contractor will pay the Customer liquidated damages at the rate set out in Item 21 of the General Order Form (**Liquidated Damages**) per day for each day from the Agreed Date to the date on which the Contractor achieves Completion in respect of the Milestone, inclusive. The Liquidated Damages will accrue on a daily basis as a debt due and owing. Notwithstanding the foregoing, if the Contractor has made a claim for an EOT pursuant to clause 1.5(b) of this Item 43 in relation to the relevant LD Obligation, then the applicable Liquidated Damages are not payable until such time as the Customer has given to the Contractor a Notice in Writing setting out the EOT so assessed under clause 1.9 of this Item 43 (or is deemed to have rejected the EOT under clause 1.10 of this item 43), and if the Contractor is granted an EOT, then the Agreed Date will be extended accordingly.

1.16 The Parties agree and acknowledge that the Liquidated Damages are a genuine estimate of the costs to be incurred by the Customer in the event that the Contractor fails to achieve Completion in respect of a Milestone by the Agreed Date and is not out of all proportion to those costs.

1.17 If the Contractor has paid the Customer Liquidated Damages and subsequently the Customer notifies the Contractor of an EOT, then the Customer will reimburse the Contractor the Liquidated Damages paid to the extent of the EOT.

1.18 Subject to clause 1.20 of this Item 43, the Customer may, at any time during the period in which Liquidated Damages are payable under clause 1.15 of this Item 43, issue a Notice in Writing of a breach in respect of the Contractor not completing the LD Obligation by the Agreed Date specifying a period during which the Contractor is required to remedy that breach, such period to be the greater of:

- (a) 10 Business Days;
- (b) the period during which Liquidated Damages are payable for that breach; or
- (c) such longer period stated in the Notice in Writing,

and if the Contractor has not remedied that failure to complete the LD Obligation (by completing the LD Obligation) by the end of such period, the Customer may terminate the Customer Contract immediately by Notice in Writing to the Contractor.

1.19 The Parties agree that where the Contractor has not successfully achieved Completion in respect of a Milestone by the date on which any cap on Liquidated Damages that is set out in Item 21 of the General Order Form is reached (**Relevant Date**), the payment of Liquidated Damages by the

Contractor under clause 1.15 of this Item 43 is without prejudice to the Customer's right to claim damages at large in respect of loss, damage or expense that arise after the Relevant Date out of or in connection with the Contractor not achieving Completion in respect of the Milestone by the Relevant Date.

1.20 If:

- (a) an Action Plan Issue occurs; and
- (b) as a result, the Customer has a right to give a Notice in Writing or terminate the Customer Contract under clauses 1.12 or 1.18 of this Item 43,

then the Customer agrees that it will not terminate this Customer Contract under clauses 1.12 or 1.18 of this Item 43:

- (c) before the date the Contractor provides the Action Plan in respect of that Action Plan Issue to Customer for its review and acceptance (or any earlier date on which the Contractor is required to provide that Action Plan to Customer for its review and acceptance under clause 10 of this Item 43); or
- (d) if the Action Plan in respect of that issue is accepted by the Customer in writing and is being implemented by the Contractor under clause 10.4 of this Item 43, before the date that the implementation of the Action Plan is completed by Contractor (or before the end of any earlier time frame specified in the Action Plan within which Contractor is required or expected to complete the implementation of that Action Plan), unless the Customer, acting reasonably, forms the view that the Contractor will not complete its obligations under the Action Plan by the end of such time frame in a way that remediates the relevant Delay.

## 2. Personnel

### PERSONNEL – GENERAL

2.1 Clause 8 of Part 2 (Customer Contract) is deleted and replaced with "Not Used" and all other references to clause 8 of Part 2 (Customer Contract) are considered to be references to the corresponding clause in this clause 2.

2.2 Neither Party may, without the prior written consent of the other Party, engage, employ or induce or cause a third party to induce the other Party's Personnel engaged in the performance of the Customer Contract to enter into a contract for service or a contract of employment with it.

2.3 The restriction in clause 2.1 of this Item 43 shall apply during the Contract Period and for a period of six months after the end of the Contract Period.

2.4 A general solicitation for employment which is placed in good faith such as a newspaper advertisement shall not constitute a breach of clause 2.1 of this Item 43.

2.5 The Parties agree that the restrictions in clauses 2.1 to 2.4 of this Item 43 are necessary to protect the legitimate interests of each Party.

2.6 The Customer must make available its Personnel to work with the Contractor as stated in the Order Documents including Item 26 of the General Order Form. The Parties will identify such Personnel and their roles in the Order Documents.

2.7 The Customer must use reasonable efforts to ensure that its Personnel who are made available to work with the Contractor have the requisite authority, qualifications, competencies, skills and experience to perform their tasks.

2.8 The Contractor must ensure a safe system of work for any of the Customer's Personnel who the Customer makes available to perform work under the control and direction of the Contractor at the Contractor's premises.

## CONTRACTOR PERSONNEL CHECKS

2.9 Subject to clauses 2.10 and 2.11 of this Item 43, before a member of Contractor's Personnel (**Prospective Person**) is engaged to perform any of the Contractor's obligations under the Customer Contract, the Contractor must, at the Contractor's expense:

- (a) except to the extent that the Customer directs otherwise, within the three week period before the person is engaged to perform any of the Contractor's obligations under the Customer Contract:
  - (i) check the Prospective Person's personal identification from standard photographic identification documentation (that is, photographic identity proof which is approved as official identity proof by the government of the country in which the Prospective Person resides, for example but not limited to passport or driver's licence);
  - (ii) check that the Prospective Person actually resides at the residential address provided;
  - (iii) verify all details of the previous employment of the Prospective Person represented on that Prospective Person's application for employment with the Contractor, either:
    - (A) for the last two forms of employment of the Prospective Person; or
    - (B) if the Prospective Person's last two forms of employment spanned less than three years, for the last three years;
  - (iv) verify references of the Prospective Person relevant to the last two years of employment with that Prospective Person's previous employer(s);
  - (v) verify all details of the highest level of education that the Prospective Person has represented to the Contractor that they have obtained, on their application for employment with the Contractor (including that the relevant certification of the relevant level of education is genuine);
  - (vi) verify that the relevant Prospective Person is not listed on any:
    - (A) global terrorism database; or
    - (B) international or national criminal database (based on the country in which the Prospective Person is engaged to perform the Services and Deliverables),and is not the subject of any Sanctions or listed on the Consolidated List;
  - (vii) verify that a trial is not currently underway against the Prospective Person, which could result in a conviction of that Prospective Person for a Relevant Offence;
  - (viii) for Contractor Personnel who are resident in Australia, perform or procure:
    - (A) a National Police Check of that person from the Criminal Records Branch of the Australian Federal Police (or such other branch or office of the Australian Federal Police or Law enforcement agency performing the functions of the Criminal Records Branch from time to time); and
    - (B) an Eligibility to Work Check,and provide the results to the Customer; and
  - (ix) for Contractor's Personnel who are resident outside Australia (or have resided outside Australia at any point in the 10 years prior to the Commencement Date), use reasonable endeavours to perform or procure a criminal record search of that person from the relevant police force of the jurisdiction where the Contractor Personnel resides (and any jurisdiction in which that Contractor Personnel has



resided at any point in the 10 years prior to the Commencement Date) and provide the results to the Customer,

and re-perform the checks required at clauses 2.9(a)(vi) to 2.9(a)(ix) (inclusive) of this Item 43 in relation to the relevant Contractor Personnel at least once during every two years of the Contract Period; and

- (b) conduct such other investigations as the Customer may reasonably request and must provide the results of those investigations to the Customer.

2.10 If:

- (a) the Customer requires, by Notice in Writing to the Contractor, that a Prospective Person commences the performance of any of the Contractor's obligations under the Customer Contract prior to the relevant checks required under clause 2.9 of this Item 43 (**Relevant Checks**) being finalised, then the Contractor must complete the Relevant Checks as soon as reasonably practicable after (but in any event no later than six weeks after) the Prospective Person has commenced performing the relevant obligations; and
- (b) the Relevant Checks return a non-compliant result, then the Contractor must:
  - (i) immediately remove the relevant Contractor Personnel from the performance of any of the Contractor's obligations under the Customer Contract; and
  - (ii) replace that Contractor Personnel with a person who is acceptable to the Customer within a reasonable time of the Customer's request to do so and without inconvenience or cost to the Customer.

2.11 If a Prospective Person who performs (or who is to perform) any of the Contractor's obligations under the Customer Contract was already employed or engaged by the Contractor before the commencement of the three-week period referred to in clause 2.9(a) of this Item 43 (**Existing Personnel Member**), then instead of performing the Relevant Checks in respect of that Existing Personnel Member in that three-week period as required by clause 2.9 of this Item 43, the Contractor represents and warrants that:

- (a) if the Existing Personnel Member was employed or engaged by the Contractor:
  - (i) within the two years before they commence performing any of the Contractor's obligations under the Customer Contract, then the Relevant Checks were performed in respect of that Existing Personnel Member at or about the time the Contractor employed or engaged them, and before the commencement of the three-week period referred to in clause 2.9(a) of this Item 43; or
  - (ii) two or more years before they commence performing any of the Contractor's obligations under the Customer Contract, then the Relevant Checks were performed in respect of that Existing Personnel Member within the two years before they commence performing any of the Contractor's obligations under the Customer Contract; and
- (b) no Existing Personnel Member in respect of whom the Relevant Checks have not been performed will be engaged to perform any of the Contractor's obligations under the Customer Contract.

2.12 The Contractor acknowledges that:

- (a) the Customer may:
  - (i) carry out the searches referred to in clause 2.9(a) of this Item 43 itself; and
  - (ii) conduct such other investigations as the Customer considers appropriate and the Contractor must provide all such assistance as the Customer may reasonably request; and

- (b) any search or investigation by the Customer in accordance with this clause 2.11 of this Item 43 will not constitute a breach of the Customer Contract nor affect the Contractor's obligations under the Customer Contract.
- 2.13 The Contractor must obtain all necessary consents from Contractor Personnel to enable:
- (a) the Contractor and the Customer to conduct searches or investigations under and within the timeframes specified in clauses 2.9 and 2.11 of this Item 43; and
- (b) the Contractor to provide the results of its searches or investigations to the Customer in accordance with clause 2.9 or clause 2.11 of this Item 43.
- 2.14 If the Contractor is unable to obtain a consent required under clause 2.13 of this Item 43 from a person, then, unless the Customer agrees otherwise in writing, the Contractor must not engage that person to perform the Contractor's obligations under the Customer Contract and the Contractor must provide a replacement for that person who is acceptable to the Customer within a reasonable time of the Customer's request to do so and without inconvenience or cost to the Customer.
- 2.15 The Contractor must notify the Customer and not allow any Contractor Personnel to be engaged in performing the Contractor's obligations under the Customer Contract without the Customer's written consent if:
- (a) a search conducted under clauses 2.9, 2.11 or 2.12 of this Item 43 shows that the person:
- (i) has been convicted of an offence which is or could be a Relevant Offence;
- (ii) is listed on any:
- (A) global terrorism database; or
- (B) international or national criminal database (based on the country in which the Prospective Person is engaged to perform the Services and Deliverables); or
- (iii) is the subject of any Sanctions or listed on the Consolidated List;
- (iv) fails the Eligibility to Work Check; or
- (v) any of the identification, address, prior employment, education or other details provided by the person are false or incorrect;
- (b) the Contractor has reliable evidence that the person has a criminal conviction or has served a custodial sentence and that conviction occurred, or any part of that sentence was served, in the previous 10 years anywhere in the world; or
- (c) the Contractor has reliable information indicating that a trial is currently underway against the person which could result in a conviction of that person for an offence which is or could be a Relevant Offence,
- (each such member of Contractor Personnel being **Prohibited Contractor Personnel**).
- 2.16 If, after the Contractor has engaged a person to perform the Contractor's obligations under the Customer Contract, the Contractor becomes aware of information of the type referred to in clause 2.15 of this Item 43 such that the relevant person is Prohibited Contractor Personnel, then the Contractor must immediately notify the Customer and the Contractor must take such reasonable action as the Customer requests in relation to such person, including replacing that person with a person who is acceptable to the Customer within a reasonable time of the Customer's request to do so. Such replacement must be without inconvenience or cost to the Customer.
- 2.17 If, as a result of any investigation referred to in this clause 2, the Customer is of the reasonable opinion that any member of the Contractor's Personnel is unsuitable to be involved in performing the Contractor's obligations, then the Customer may request the Contractor to remove that person from the performance of the Customer Contract. If the Customer makes such a request, then the

Contractor must provide replacement personnel reasonably acceptable to the Customer within a reasonable time of the Customer's request to do so. Such replacement must be without inconvenience or cost to the Customer.

2.18 The Contractor:

- (a) represents and warrants that, as at the Commencement Date and on every day during the Contract Period:
  - (i) no Contractor Personnel are:
    - (A) the subject of any Sanctions; or
    - (B) listed on the Consolidated List; and
  - (ii) it is not:
    - (A) the subject of any Sanctions;
    - (B) controlled by, one or more persons that are the subject of Sanctions; or
    - (C) located, organised or resident in a country or territory that is the subject or target of Sanctions; and
- (b) must:
  - (i) annually during the Contract Period, within 30 days of the Commencement Date, and each anniversary of the Commencement Date (each, a **Compliance Date**), conduct an assessment of the Contractor's continued compliance with the warranties given by the Contractor under this clause 2.18; and
  - (ii) provide to the Customer, within 30 days of each Compliance Date during the Contract Period, a report which details the results of the assessment referred to in paragraph (i) above.

#### SPECIFIED PERSONNEL

- 2.19 The identity and roles of any Specified Personnel must be stated in Item 27 of the General Order Form.

#### RETENTION / TURNOVER OF PERSONNEL

- 2.20 The Contractor must put in place and maintain an effective retention strategy and use other commercially reasonable efforts to keep the turnover of Contractor Personnel performing the Services to a level comparable with or better than the industry average for large, well-managed professional services companies providing services that are the same as or substantially similar to the Services.
- 2.21 Not used.

#### APPROVED AGENTS AND SUBCONTRACTORS

- 2.22 The Contractor may supply Deliverables to the Customer through Approved Agents.
- 2.23 If a Customer Contract is entered into between the Customer and an Approved Agent, the Contractor is deemed to have entered into a Customer Contract with the Customer.
- 2.24 The Contractor must ensure that its Approved Agents supply the Deliverables only in accordance with the terms of the Customer Contract under which the Approved Agent is to supply the Deliverables.
- 2.25 If requested in writing by the Customer, the Contractor must arrange for its Approved Agents to execute a Deed Poll substantially in the form of Schedule 6 – Deed Poll.

- 2.26 The Contractor must not subcontract the performance or supply of any Services under the Customer Contract without obtaining the prior written consent of the Customer which will not be unreasonably withheld or delayed and which may be given on such conditions as the Customer thinks fit.
- 2.27 Where the Customer believes that any Subcontractor is in breach of its obligations to the Contractor, or its performance of obligations or services is unsatisfactory, so that the Contractor is likely to be in breach of the Customer Contract as a result, the Customer may:
- (a) provide Notice in Writing to the Contractor setting out the details of its concerns;
  - (b) require the Contractor to meet with the Customer within 3 Business Days of the Contractor's receipt of the Notice in Writing to discuss the concerns; and
  - (c) if, following the discussions with the Contractor, the Customer is satisfied that the Contractor will be in breach of the Customer Contract as a result of the performance of the Subcontractor, the Customer may give Notice in Writing that it is withdrawing its consent to allow the Subcontractor to continue to work in connection with the Customer Contract and require the Contractor to procure that the Subcontractor promptly ceases performing any work in connection with the Customer Contract subject to any contrary requirements of the Customer in respect of effecting an orderly transition notified to the Contractor, and in such circumstances, the Contractor agrees that the Customer will have no liability whatsoever to the Contractor for any loss, damage or expense suffered by the Contractor arising out of any termination of, or the continuation of, the relevant subcontract.
- 2.28 The Contractor:
- (a) must ensure that each Subcontractor is aware of all the terms and conditions of the Customer Contract that are relevant to the Subcontractor's performance of its work;
  - (b) is not relieved of its liabilities and obligations arising out of, or in connection with, a Customer Contract by subcontracting any work; and
  - (c) must ensure that the Subcontractor ceases work upon receipt of a Notice in Writing from the Customer of withdrawal of the consent given under clause 2.27(c) of this Item 43.
- 2.29 If stated in Item 28 of the General Order Form, the Contractor must obtain from the Subcontractor a signed statutory declaration substantially in the form of Schedule 7 – Statutory Declaration – Subcontractor.

### 3. Acceptance

#### ACCEPTANCE

- 3.1 Clause 10.1 of Part 2 (Customer Contract) is deleted and all references to Clause 10.1 of Part 2 (Customer Contract) are considered references to clause 3.2 of this Item 43.
- 3.2 The Actual Acceptance Date (**AAD**) for a Deliverable occurs:
- (a) unless it is stated in Item 32 of the General Order Form that the Deliverable is required to undergo Acceptance Testing, 2 Business Days or such other period that is stated in Item 32 of the General Order Form following the delivery of the Deliverable as required in the Order Documents; or
  - (b) where it is stated in Item 32 of the General Order Form that the Deliverable is required to undergo Acceptance Tests, on the sooner of:
    - (i) the date the Customer issues a certificate of acceptance; or
    - (ii) on the date the Customer issues a notice that it conditionally accepts the Deliverable in accordance with clauses 10.10(b) or 10.12(c) of Part 2 (Customer Contract).
- 3.3 Clause 10.13 of Part 2 (Customer Contract) is deleted and replaced with the words "Not used."

### 3.4 Acceptance Testing of documentary Deliverables

- (a) Where a Deliverable is a documentary Deliverable, the following clauses 3.4(b) to 3.4(e) and clause 3.5 of this Item 43 apply to the Acceptance Testing of that documentary Deliverable and clauses 10.3 to 10.16 will not apply. All documentary Deliverables are required to follow the procedure set out in the following clauses 3.4(b) to 3.4(e) of this Item 43, and clause 3.5 of this Item 43 applies to them.
- (b) The Contractor must submit each documentary Deliverable to the Customer for approval on or before the applicable Due Date and before submitting any documentary Deliverable, the Contractor must ensure that the documentary Deliverable meets all applicable Acceptance Criteria and other requirements of the Customer Contract.
- (c) The Customer must, within 10 Business Days (or any other timeframe agreed between the Parties in writing) of receiving a documentary Deliverable, review that documentary Deliverable and notify the Contractor that either:
  - (i) it approves the documentary Deliverable; or
  - (ii) it rejects the documentary Deliverable and requires amendments to the documentary Deliverable.

If, at the end of such 10 Business Day period the Customer has not provided notification to the Contractor in accordance with this paragraph (c), the Contractor must, within a further 2 Business Days, notify the Customer that no notification has been received in relation to the documentary Deliverable, in which case the Customer shall notify the Contractor of the timeframe within which it expects to be able to provide the notification. To the extent that such additional timeframe will cause a Delay, the Contractor is entitled to seek an EOT under clause 1.5 of this Item 43, and the provisions of clauses 1.6 to 1.11 of this Item 43 shall apply.

- (d) If the Customer notifies the Contractor that it requires amendments to a documentary Deliverable under clause 3.4(c)(ii) of this Item 43, the Contractor must, within five Business Days (or any alternative timeframe agreed between the Parties in writing), prepare a revised documentary Deliverable which addresses all of the amendments required by the Customer.
- (e) The Parties must repeat the process set out in this clause 3.4 of this Item 43 until the documentary Deliverable meets all applicable Acceptance Criteria and other requirements of the Customer Contract, unless the Customer terminates that documentary Deliverable in accordance with clause 3.5 of this Item 43.

### 3.5 Termination and refund of documentary Deliverables

- (a) If the Customer rejects a documentary Deliverable on two or more occasions, the Customer may immediately terminate that documentary Deliverable and any other dependent items for that documentary Deliverable (collectively, **Terminated Items**) by Notice in Writing to the Contractor. Such termination will be deemed to be a termination for cause under clause 7.1 of this Item 43.
- (b) If the Customer issues a termination notice under clause 3.5(a) of this Item 43, the Contractor must, within 10 Business Days, refund to the Customer all Prices and other amounts paid by the Customer in connection with the Terminated Items.
- (c) The Customer will not be deemed to have accepted a documentary Deliverable under any circumstances.
- (d) The Customer's rights under this clause 3.5 are cumulative with each other and with any other rights the Customer may have under the Customer Contract or otherwise.

## 4. **Intellectual Property Rights – Changes to Part 2 (Customer Contract)**

- 4.1 Clause 13 (Intellectual Property Rights) of Part 2 (Customer Contract) is deleted and replaced with the following new clause 13:

## **13. Intellectual Property Rights**

### *OWNERSHIP*

13.1 All Intellectual Property Rights in:

- (a) any Existing Material remain vested in the person that owns the Intellectual Property Rights at the Commencement Date (**Owner**); and
- (b) any adaptation, translation or derivative of that Existing Material, vests in, or, is hereby transferred or assigned to the Owner, immediately upon creation.

### *CONTRACTOR OWNED NEW MATERIAL*

13.2 The provisions of clauses 13.3 to 13.5 apply to New Material, unless clause 13.11 applies.

13.3 All Intellectual Property Rights in any New Material vest in, or, are hereby transferred or assigned to, the Contractor, immediately upon creation.

13.4 Immediately on the creation of a Deliverable that incorporates the relevant New Material, the Contractor grants the Customer a non-exclusive, perpetual, irrevocable, royalty free, transferable licence to use, copy, adapt, translate, reproduce and in any way exploit that New Material in connection with, or for the operation, modification, support and/or use of, the Deliverable in which it is incorporated, subject to the restrictions set out in clause 13.5.

13.5 The licence to New Material in clause 13.4:

- (a) does not permit the Customer to disclose the New Material to any other person, except as stated in clauses 13.5(c) to (e);
- (b) does not permit the Customer to manufacture, sell, license, transfer, commercialise or otherwise exploit any of the New Material or any Existing Material except as stated in clauses 13.5(c) to (e);
- (c) permits the Customer to sublicense any of the rights in clause 13.4 without additional charge to any "Public Service agency" or other "government sector agency" (as defined in the Government Sector Employment Act 2013 (NSW)), any NSW Government agency or statutory body representing the Crown (as referenced in section 13A of the Interpretation Act 1987 (NSW)), any other public authority that is constituted by or under an Act of the State of New South Wales or that exercises public functions, and any "public health organisation" (as defined in the Health Services Act 1997 (NSW));
- (d) permits the Customer's subcontractors to access the New Material, without additional charge, for the internal purposes of the Customer provided that, unless otherwise required by the Contractor, the Customer's subcontractor first signs an agreement or undertaking in a form reasonably acceptable to the Contractor that protects the use and disclosure of the New Material in the same manner as stated in the Customer Contract; and
- (e) permits the Customer to sublicense any of the rights in clause 13.4, without additional charge, to a contractor that is providing outsource services to the Customer that include the operation of the New Material, provided that:
  - (i) the New Material is used solely for the internal business purposes of the Customer for the period of the outsource arrangement and the sublicense automatically terminates at the end of the period of the outsource arrangement; and

- (ii) *unless otherwise required by the Contractor, the contractor first signs an agreement or undertaking in a form reasonably acceptable to the Contractor that protects the use and disclosure of the New Material in the same manner as stated in the Customer Contract.*

#### **EXISTING MATERIAL**

- 13.6 *Immediately on the creation of a Deliverable that incorporates the Contractor's Existing Material, the Contractor grants the Customer a non-exclusive, perpetual, irrevocable, royalty-free licence:*
- (a) *if that Existing Material is Licensed Software, to that Existing Material on the terms and conditions of the licence of that Licensed Software under the relevant Module;*
  - (b) *if that Existing Material is an adaptation, translation or derivative of Licensed Software, to that Existing Material on the same terms and conditions as the licence for the Licensed Software stated in clause 13.6(a);*
  - (c) *if that Existing Material is a tool, object library or similar routine that is not included in the Existing Materials stated in clauses 13.6(a) or 13.6(b), to use, reproduce and adapt that Existing Material for the Customer's own internal use in connection with, or for the operation, modification, support and/or use of, that Deliverable;*
  - (d) *if that Existing Material is a Document Deliverable and any adaptation, translation or derivative of that Existing Material, to use that Existing Material for the Customer's internal use; and*
  - (e) *if that Existing Material is an Online Service, the right to use and access that Existing Material on the terms and conditions under the relevant Module.*
- 13.7 *Immediately on the creation of a Deliverable that incorporates Existing Material that is owned by a third party, including third party software, the Contractor grants the Customer a non-exclusive, perpetual, irrevocable, royalty-free licence to that third party Existing Material to:*
- (a) *use, reproduce and adapt that third party Existing Material on the terms and conditions, and for the fees, stated in Item 34 of the General Order Form; or*
  - (b) *if no terms and conditions or fees are stated in Item 34 of the General Order Form; to use, reproduce and adapt that third party Existing Material for the Customer's own internal use in connection with, or for the operation, modification, support and/or use of, that Deliverable.*
- 13.8 *Where the Contractor uses a methodology in providing any Deliverable, the Contractor grants the Customer, immediately on the creation of the relevant Deliverable, a non-exclusive, perpetual, irrevocable, royalty-free licence to use that methodology solely for the purposes of receiving the benefit of the Services under the Customer Contract or assisting the Contractor to perform its obligations under the Customer Contract.*
- 13.9 *Not used.*
- 13.10 *The Contractor may charge for any licence to use any of its Existing Material, provided that any separate fees payable by the Customer for such use are agreed between the Parties prior to the Commencement Date and are stated in Item 34 of the General Order Form.*

#### **CUSTOMER OWNED NEW MATERIAL**

- 13.11 *If it is stated in Item 34 of the General Order Form that this clause 13.11 applies to some or all of the New Materials and subject to clauses 13.13 to 13.15, immediately on the creation of the relevant Deliverable that incorporates the New Material:*
- (a) *any Intellectual Property Rights in the New Material vest in, or are hereby transferred or assigned by the Contractor to, the Customer; and*



- (b) *the Customer may, in its sole discretion and only if stated in the General Order Form, grant the Contractor a:*
- (i) *non-exclusive, perpetual, irrevocable, royalty-free licence in respect of the Intellectual Property Rights in the New Material to use, copy, adapt, translate, manufacture and in any other way exploit the Intellectual Property Rights in the New Material; or*
  - (ii) *licence in respect of the Intellectual Property Rights in the New Material on such terms as are specified in Item 34 of the General Order Form.*

#### **CUSTOMER MATERIAL**

- 13.12 *The Customer grants the Contractor a non-exclusive, non-transferable licence for the Contract Period for the Contractor and its Personnel to use the Customer's Materials to the extent necessary for the Contractor to perform its obligations under the Customer Contract.*

#### **KNOW HOW ETC**

- 13.13 *Subject to the restrictions on the disclosure of Confidential Information, the Contractor will be free to use the ideas, concepts and know-how that are used, developed or created in the course of performing the obligations under the Customer Contract and may be retained by the Contractor's Personnel in intangible form.*

#### **OPEN SOURCE LICENCE**

- 13.14 *The Contractor must not, without the prior written consent of the Customer:*
- (a) *develop or enhance any Deliverable using Open Source Software; or*
  - (b) *insert any Open Source Software into any Deliverable.*
- 13.15 *Where the Customer provides its consent in relation to the use of any Open Source Software under clause 13.14, the Contractor will ensure that the use of that Open Source Software will not:*
- (a) *result in an obligation to disclose, license or otherwise make available any part of the Customer's environment, data or Confidential Information to any third party; or*
  - (b) *diminish the Contractor's obligations under this Customer Contract.*

#### **SOFTWARE PROVIDED BY CUSTOMER**

- 13.16 *The Contractor must comply with, and ensure that its Personnel comply with, the terms of any third party licences in respect of any software or other material which the Customer provides or makes available to the Contractor for the purposes of the performance of the Services (including any such software or material listed as part of the Customer Supplied Items) (such terms being the **Third Party Licence Terms**). The Customer will provide (or otherwise make available) to the Contractor a copy of the applicable Third Party Licence Terms prior to or at the time of providing or making available the relevant software or material to the Contractor.*
- 13.17 *The Contractor must ensure that it and its Personnel do not act, or omit to act, in any way which causes the Customer to breach any provision of the Third Party Licence Terms.*
- 13.18 *The Contractor indemnifies the Customer against all Losses suffered or incurred by the Customer or its Personnel as a result of a breach of clause 13.16 or clause 13.17.*

## **5. Amendments to clause 18 of Part 2 (Customer Contract)**



- 5.1 In each sub-clause of clause 18 in which the word "claim" or "claims" appears, this is changed to "Claim" or "Claims" (as applicable).
- 5.2 In clause 18.1, the words "Contractor's liability in contract (including under an indemnity), tort (including negligence), breach of statutory duty or otherwise in respect of any loss, damage or expense" are deleted and replaced with "total cumulative liability of each Party for anyLoss".
- 5.3 The words "Notwithstanding any other clause in the Customer Contract, " are deleted from clause 18.4 of Part 2 (Customer Contract), and the first letter in the word "neither" is capitalised.
- 5.4 In clause 18.5 of Part 2 (Customer Contract), the words "the Contractor has no financial cap on its legal liability where that liability" are deleted and replaced with "the exclusions and limitations of liability under this clause 18 do not apply to any liability which".
- 5.5 In clauses 18.6 and 18.7 of Part 2 (Customer Contract), the words "loss, damage or expense" are deleted in each instance where they appear and are replaced with "Loss".

## **6. Deletions to Part 2 (Customer Contract)**

- 6.1 Clauses 25.2(b), 25.4(a), 25.6(c) and 25.6(d) of Part 2 (Customer Contract) are deleted and replaced with the words "Not used".

## **7. Substantial Breach**

- 7.1 The Customer may give the Contractor Notice in Writing of termination in respect of all or part of the Customer Contract:
- (a) if the Contractor breaches any term of the Customer Contract which is not capable of remedy;
  - (b) if the Contractor breaches any term of the Customer Contract which is capable of remedy and fails to remedy the breach within 30 days of receiving notice requiring it to do so;
  - (c) if the Contractor breaches any warranty under clause 9.1 of Part 2 (Customer Contract);
  - (d) if the Contractor breaches the same Service Level(s) in each month of any consecutive three month period, or in any three months of any consecutive six month period;
  - (e) if the Contractor or any of its Personnel is guilty of misconduct, or commits any act of fraud or dishonesty in relation to the business of the Customer or the Customer Contract;
  - (f) if the Contractor or any of its Personnel, in the Customer's reasonable opinion, acts in a way that injures, or is likely to injure the business or reputation of the Customer or the New South Wales Government;
  - (g) if in the reasonable opinion of the Customer, there has been, or is likely to be, a substantial failure by the Contractor to carry out any of its obligations under the Customer Contract;
  - (h) if a Step In Issue occurs and the Customer elects (in its sole discretion) to terminate the Customer Contract (in whole or in part) rather than Step In under clause 12.1 of Item 43 (Additional Conditions) of the General Order Form;
  - (i) pursuant to clauses 1.12, 1.18 or 12.4 of Item 43 (Additional Conditions) of the General Order Form;
  - (j) in the circumstances (and manner) specified in clause 3.5 of Item 43 (Additional Conditions) of the General Order Form;
  - (k) where Acceptance Testing is required in order for the Deliverable to achieve AAD (and the obligation to ensure that the Deliverable achieves AAD by a certain date is not an LD Obligation), that Deliverable does not pass its Acceptance Tests on two or more occasions and this results in rejection of that Deliverable by the Customer on those occasions under clause 10.12(e) of Part 2 (Customer Contract);

- (l) where Acceptance Testing is not required in order for a Deliverable to achieve AAD (and the obligation to ensure that the Deliverable achieves AAD by a certain date is not an LD Obligation), the Contractor fails to deliver that Deliverable by its Due Date required under the Customer Contract and fails to remedy that breach within 10 Business Days of receiving notice requiring it to do so;
  - (m) if the Contractor fails to effect and maintain insurance policies as required under clauses 16.1, 16.2, 16.3 or 16.7 of Part 2 (other than to the extent that the Contractor received an exemption under clause 16.8 of Part 2 (Customer Contract));
  - (n) if the Contractor fails to provide a Performance Guarantee as required under clause 17.2 of Part 2 (Customer Contract);
  - (o) if the Contractor fails to provide a Financial Security as required under clause 17.4 of Part 2 (Customer Contract);
  - (p) if a Conflict of Interest exists which in the Customer's reasonable opinion prevents the full and proper performance of the Contract by the Contractor and the Contractor has not complied with clause 20.1(b) of Part 2 (Customer Contract) within a reasonable period; or
  - (q) if there is a change of Control of the Contractor (where Control has the meaning given to that term in section 50AA of the Corporations Act 2001 (Cth)),
- (each, a **Substantial Breach**).

## 8. Wrongful Termination

### WRONGFUL TERMINATION

- 8.1 If the Customer issues a termination Notice in Writing under clause 25.2 of Part 2 (Customer Contract) or clause 7.1 of this Item 43 or otherwise purports to terminate all or part of the Customer Contract for cause, and a court determines that it did not have a right to do so or that the purported termination is otherwise wrongful, the Customer's termination Notice in Writing is deemed to be a termination Notice in Writing for convenience validly given under clause 25.3 of Part 2 (Customer Contract) (even if a requirement for giving that termination Notice in Writing was not complied with and/or the Customer was not entitled to give it).

## 9. General

### SURVIVAL

- 9.1 The provisions of clauses 2.1 to 2.4, 3.5(b), 3.5(d), 8, 12.5, 13 and 14 of this Item 43 shall survive termination or expiry of the Customer Contract.

## 10. ACTION PLANS

### CONTRACTOR TO DEVELOP DRAFT ACTION PLAN

- 10.1 The Contractor is required to develop and implement an Action Plan in the following circumstances:
- (a) a Delay or Failure occurs, in which case the Action Plan must specify the steps that the Contractor will undertake to:
    - (i) overcome the Delay or Failure; and
    - (ii) avoid or minimise any adverse impact on the Customer (including any workaround solutions);
  - (b) a Repeated Incident occurs which has been caused by the Contractor or its Personnel, in which case the Action Plan must specify how the Contractor will remedy the Repeated Incident and avoid the same or similar Incidents occurring subsequently; or

- (c) the Contractor fails to meet any of the Service Levels two or more times in any one Service Level measurement period as specified in the SLA,

(each, an **Action Plan Issue**). If an Action Plan Issue occurs, the Contractor must develop and submit to the Customer a draft Action Plan within three Business Days (or such other time as is agreed between the Parties) of becoming aware of the relevant Action Plan Issue.

#### CONTENTS OF ACTION PLAN

10.2 An Action Plan must specify (in detail satisfactory to the Customer):

- (a) the process for identifying, and where applicable must identify, the cause of the Action Plan Issue which the Action Plan is intended to remedy or prevent;
- (b) if remedy of the Action Plan Issue is possible, the actions that will be implemented by the Contractor to effect that remedy;
- (c) the actions that will be implemented by the Contractor to prevent the same or a substantially similar Action Plan Issue from occurring in the future;
- (d) a timeline for the implementation of the Action Plan;
- (e) any specific content required under clause 10.1 of this Item 43 to be included in the Action Plan; and
- (f) any other content that may reasonably be requested by the Customer from time to time.

#### IMPLEMENTATION OF ACTION PLAN

10.3 Each draft Action Plan is subject to acceptance under clause 3.4 of this Item 43 (regardless of whether or not such document is specified as a Deliverable that is required to undergo Acceptance Testing in Item 32 of the General Order Form).

10.4 Once an Action Plan is accepted by the Customer in writing under clause 3.4 of this Item 43, the Contractor must implement that Action Plan at no cost to the Customer in accordance with the timeframes and other terms specified in that Action Plan.

10.5 The Contractor may only implement an Action Plan:

- (a) if the Customer has approved the Action Plan; and
- (b) in the form approved by the Customer.

### 11. RESOLUTION MANAGER

#### APPOINTMENT OF RESOLUTION MANAGER

11.1 Without limiting any other remedies that the Customer may have under this Customer Contract or at law, if:

- (a) a Significant Failure occurs;
- (b) the Contractor fails:
  - (i) to develop an Action Plan as and when required; or
  - (ii) to implement an Action Plan in accordance with its terms; or
- (c) the Contractor implements an Action Plan and the Action Plan fails to resolve the Action Plan Issue,

the Customer may appoint a resolution manager (**Resolution Manager**).

## ROLE AND AUTHORITY OF RESOLUTION MANAGER

- 11.2 The Resolution Manager will have the ability to issue Directions to the Contractor. Each Direction must specify a reasonable timeframe for compliance with the Direction.
- 11.3 The Contractor must comply with all Directions.

## 12. STEP IN

### STEP IN RIGHTS

- 12.1 If:
- (a) a Significant Failure occurs;
  - (b) the Contractor fails:
    - (i) to develop an Action Plan as and when required; or
    - (ii) to implement an Action Plan in accordance with its terms;
  - (c) the Contractor implements an Action Plan and the Action Plan fails to resolve the Action Plan Issue; or
  - (d) the Contractor fails to comply with a Direction under clause 11 of this Item 43,
- (each, a **Step In Issue**), then the Customer may, by giving Notice in Writing to the Contractor:
- (e) perform the Services and supply the Deliverables affected by that Step In Issue (**Affected Contracted Items**) itself or procure a third party to perform or supply the Affected Contracted Items; and/or
  - (f) take over the implementation of the relevant Action Plan (if applicable) or the rectification of the relevant Step In Issue (or both),
- (each, a **Step In**).

### ACCESS AND CO-OPERATION

- 12.2 If the Customer exercises its right to Step In, the Contractor must co-operate with the Customer and its Personnel and provide all assistance reasonably required by the Customer as soon as possible, including:
- (a) providing access to all relevant equipment, premises and software under the Contractor's control as required by the Customer (or its nominee); and
  - (b) ensuring that the Contractor's Personnel normally engaged in the provision of the Affected Contracted Items are available to the Customer (or its nominee) to provide any assistance which the Customer may reasonably request.

### DURATION OF STEP IN

- 12.3 The Customer's right to Step In under this clause 12 of this Item 43 will end, and the Customer must hand back the responsibility for performing the Affected Contracted Items, when the Contractor is able to demonstrate to the Customer's reasonable satisfaction that:
- (a) the Contractor is capable of resuming provision of the Affected Contracted Items in accordance with the requirements of this Customer Contract; and
  - (b) the Step In Issue giving rise to the right of Step In will not recur.
- 12.4 If the Contractor has not demonstrated its capability in accordance with clause 12.3(a) of this Item 43 within 20 Business Days after a Step In, the Customer may immediately terminate the

Customer Contract (in whole or in part) by Notice in Writing to the Contractor. Such termination will be deemed to be a termination for cause under clause 7.1 of this Item 43.

### COSTS

- 12.5 The Contractor must reimburse the Customer for the following costs (**Step In Costs**) incurred by the Customer in exercising the Step In rights under clause 12.1 of this Item 43:
- (a) any payments the Customer makes to a third party in connection with the provision of the Affected Contracted Items; and
  - (b) the costs and expenses incurred by the Customer as a result of the Customer exercising its right to Step In.
- 12.6 The Customer will continue to pay the Contractor the Price (including that portion which relates to the Affected Contracted Items) during a Step In provided that the Contractor reimburses the Customer for the Step In Costs in accordance with clause 12.5 of this Item 43.

## 13. TRANSITION OUT

### TRANSITION OUT PLAN

- 13.1 Within three months following the Commencement Date or at a time otherwise requested by the Customer, the Parties must negotiate in good faith to agree as quickly as possible a plan (**Transition Out Plan**) for the Transition Out of the Services and Deliverables supplied under the Customer Contract, including:
- (a) the timetable for Transition Out;
  - (b) the Services and Deliverables that the Contractor no longer has to supply;
  - (c) the time and circumstances in which the Contractor will cease supplying those Services and Deliverables; and
  - (d) the time and circumstances in which the Contractor will cease providing any Specified Personnel in respect of the relevant Services and Deliverables.
- 13.2 Unless otherwise agreed by the Parties, the Transition Out Plan should be based on any draft plan for the Transition Out forming part of the Customer Contract as an Order Document or Agreement Document.
- 13.3 If the Customer does not Accept a Transition Out Plan, then within 15 Business Days after commencement of the Transition Out Period, the Contractor must provide the Transition Out Assistance reasonably directed by the Customer at the times reasonably directed by the Customer. The directions issued by the Customer under this clause 13.3 will collectively constitute the Transition Out Plan.

### TRANSITION OUT ASSISTANCE

- 13.4 During the Transition Out Period, the Contractor must perform, and ensure that each of its Personnel performs, all of the services, tasks, functions, activities and responsibilities allocated to the Contractor in the Transition Out Plan and all other assistance required by the Customer to successfully and seamlessly complete Transition Out for the relevant Services and Deliverables, including the following:
- (a) supply of any Deliverables specified in the Transition Out Plan as items the Contractor must supply;
  - (b) provision of any training required by the Customer to permit the Customer or any members of its Personnel to supply the Services and Deliverables to which the Transition Out relates to the satisfaction of the Customer;

- (c) provision of detailed handover by:
    - (i) each member of Specified Personnel;
    - (ii) each other member of the Contractor's Personnel nominated by the Customer; and
    - (iii) including shadowing of those persons in their daily duties by replacement Customer Personnel;
  - (d) provision of reports on the status of the Transition Out and all other reports required by the Customer; and
  - (e) if specified in the Transition Out Plan or otherwise requested by the Customer, the Contractor must, by the due date specified in the Transition Out Plan or by the Customer procure the novation to the Customer or its nominee of:
    - (i) any subcontracts, or the relevant parts of subcontracts (where those subcontracts are severable); and
    - (ii) any licence agreements or agreements for inputs,
  - (f) to the extent that they relate to the Services and Deliverables to which the Transition Out relates.
- 13.5 The Contractor must provide the Transition Out Assistance to the Customer, or any third party appointed by the Customer, to take over the supply of the Services and Deliverables.

#### CONTINUATION OF BUSINESS AS USUAL SERVICES

- 13.6 During the Transition Out Period, for the period in respect of which the Customer continues to pay the Contractor the Price in accordance with the Customer Contract, the Contractor must continue, and to the extent required by the Customer must ensure that each Subcontractor continues, to:
- (a) provide the Services and Deliverables in accordance with the Customer Contract and the Transition Out Plan;
  - (b) allocate the Specified Personnel to the performance of the Services and Deliverables as required by this Customer Contract;
  - (c) maintain sufficient other Personnel to perform the obligations under this clause 13 of this Item 43 and the Transition Out Plan; and
  - (d) maintain all of the existing Personnel (including Specified Personnel) involved in the provision of the Services and Deliverables, and must not remove, replace or reallocate any of those Personnel or reduce the existing Resource Levels without the Customer's written consent,

unless and until specified otherwise in the Transition Out Plan or agreed with the Customer in writing.

#### REDUCTION IN PRICE

- 13.7 During the Transition Out Period, on and from the date that the Transition Out for a particular Service or Deliverable, or part of a Service or Deliverable, has been completed in accordance with the Transition Out Plan (each, a **Transitioned-out Service**):
- (a) the Contractor:
    - (i) acknowledges and agrees that:
      - (A) it must not charge the Customer; and
      - (B) the Customer will not be liable to pay the Contractor, any amounts in relation to that Transitioned-out Service; and

- (ii) must reduce the total Contract Price (and, if applicable, the individual Prices) payable by the Customer proportionately to reflect the Transition Out of that Transitioned-out Service; and
- (b) the Customer will not be required to pay any Price or other amount in respect of any such Transitioned-out Service.

#### PAYMENT OF COSTS FOR TRANSITION OUT ASSISTANCE

- 13.8 The Customer is not liable to pay for Transition Out Assistance to the extent that Transition Out Assistance can be provided by the Contractor using existing Contractor Personnel involved in the provision of the Services and Deliverables.
- 13.9 The Customer is also not liable to pay for any Transition Out Assistance unless the Transition Out Period to which the Transition Out relates was triggered by a termination notice issued by the Customer under clause 25.3 of Part 2 (Customer Contract) or by the Contractor under clause 25.6 of Part 2 (Customer Contract).
- 13.10 Except as provided under clauses 13.8 and 13.9 of this Item 43, the Customer must pay for any additional Personnel required by the Contractor to provide the Transition Out Assistance (that is in addition to those existing Personnel who are used to provide the Services and Deliverables under the Customer Contract) on a time and materials basis in accordance with the agreed rates as set out in the Customer Contract.

### 14. NSW GOVERNMENT CONTRACTING

#### INTERPRETATION

- 14.1 In this clause 14:
  - (a) **Claim** means any claim, demand or proceeding arising out of any cause of action (including breach of contract (including under an indemnity), tort (including negligence) and any other common law, equitable or statutory cause of action); and
  - (b) **Losses** means all liabilities, losses, damages, costs and expenses suffered or incurred by any person, whether arising in contract (including under an indemnity), tort (including negligence), under any statute or under any other common law, equitable or statutory cause of action, and **Loss** has a corresponding meaning.
- 14.2 This clause 14 prevails over any inconsistent clause in the Customer Contract.

#### BENEFIT AND LIABILITY

- 14.3 The Parties acknowledge and agree that the exclusions and limitations of liability that apply to the Customer's liability under this Customer Contract extend to, and apply to, the liability of all Government Agencies collectively in connection with this Customer Contract.
- 14.4 Despite any other provision of the Customer Contract to the contrary:
  - (a) any and all Government Agencies which have been authorised by the Customer to receive the benefit of the Services and Deliverables may make use of the Services and Deliverables provided under the Customer Contract;
  - (b) the Contractor acknowledges that an act or omission of the Contractor, including any breach of the Customer Contract or negligence in relation to the performance or failure to perform the Customer Contract, may result in Loss by a Government Agency;
  - (c) the Customer is not prevented from recovering Losses by the fact that the relevant Losses were suffered by any other Government Agency under or in connection with the Customer Contract, if those Losses would have been capable of being recovered by the Customer from the Contractor had the Customer suffered those Losses itself; and



- (d) those Losses are deemed to be suffered by the Customer for the purposes of the Customer Contract and the Contractor indemnifies the Customer against those Losses suffered by any Government Agency under or in connection with the Customer Contract.
- 14.5 The Customer enters into the Customer Contract, and holds the benefit of any and all rights and remedies granted or available to the Customer under the Customer Contract, for itself in its own right and on trust for each Government Agency which has been authorised by the Customer to receive the benefit of the Services and Deliverables, and the Customer may enforce the benefit of those rights and remedies on behalf of those other Government Agencies for the purposes of:
- (a) each Government Agency obtaining (and being able to enforce through the Customer) any and all rights and remedies granted or available to the Customer under the Customer Contract (including under clause 19 of Part 2 (Customer Contract) and clauses 14.3 and 14.4 of this Item 43); and
- (b) each Government Agency obtaining (and being able to enforce through the Customer) the benefit of any exclusions and limitations on the Customer's liability in the Customer Contract (including under clause 18 of Part 2 (Customer Contract) and clause 14.3 of this Item 43).
- 14.6 As the contracting party to this Customer Contract, the Customer will be responsible for enforcing this Customer Contract, including bringing any Claim for and on behalf of the other Government Agencies.
- 14.7 The Contractor must not (and must procure that its Related Companies and Personnel do not) make any Claim for Losses against any Government Agency other than the Customer in connection with this Customer Contract, and agrees that any Claim by the Contractor in relation to any other Government Agency must be brought by the Contractor directly against the Customer and not against any other Government Agency.

#### EXERCISE OF RIGHTS

- 14.8 The Customer may vary, amend, enforce or otherwise act under this Customer Contract without seeking the approval of the NSW Government or any other Government Agency.
- 14.9 Without limiting this clause 14 of this Item 43, the Customer is entitled to exercise all rights, powers, authorities, discretions and remedies conferred on the Customer under this Customer Contract, or any applicable laws, as if the Customer were the sole beneficiary of the rights and obligations under this Customer Contract.

#### CLAIMS

- 14.10 The Parties acknowledge and agree this clause 14 of this Item 43 does not permit the NSW Government or the Government Agencies to recover twice for the same Loss.

### **PART B – Amendments to Part 3 (Dictionary) of Procure IT Framework**

- 1.1 The following definitions are added to Part 3 (Dictionary) in their appropriate alphabetical locations:

**Action Plan** means a plan prepared by the Contractor under the Customer Contract in accordance with clause 10 of Item 43 of the General Order Form to remedy a deficiency or failure in respect of the Services or Deliverables.

**Action Plan Issue** has the meaning given to that term in clause 10.1 of Item 43 of the General Order Form.

**Agreed Date** means the date by which a Milestone (including an LD Obligation) must be Complete, as specified in the Customer Contract or the PIPP.

**Affected Contracted Items** has the meaning given to that term in clause 12.1(e) of Item 43 of the General Order Form.



**Claim** means any claim, demand or proceeding arising out of any cause of action (including breach of contract (including under an indemnity), tort (including negligence) and any other common law, equitable or statutory cause of action).

**Complete** means, in respect of a Milestone, when the Actual Acceptance Date for all Deliverables forming part of, or associated with, that Milestone has occurred, and **Completion** shall be construed accordingly.

**Consolidated List** means the list of asset freeze targets (both individuals and companies) designated by the United Nations, Australia, European Union and/or United Kingdom under legislation relating to current sanctions regimes.

**Critical Service Level** means a Service Level identified in the SLA as a 'critical service level' for the relevant Services.

**Delay** means anything which will or will probably cause delay to the Contractor's ability to:

- (a) Complete a Milestone by the Agreed Date; or
- (b) perform or complete any other obligation by the date required by the Customer Contract.

**Delay Event** means:

- (a) acts or omissions of the Customer except to the extent that the Customer has acted within the period contained in the Customer Contract, or, where no period is specified, a reasonable time; or
- (b) a Force Majeure Event.

**Directions** means directions for the resolution of a deficiency or failure in respect of the Services or Deliverables and the implementation of the applicable Action Plan, which may include a requirement that the Contractor makes available and provides access to leading subject matter experts (as nominated by the Contractor) within its organisation.

**Eligibility to Work Check** means checks that the Customer may perform, or require to be performed from time to time, to confirm whether a member of the Contractor Personnel is an Australian citizen, permanent resident, or otherwise entitled to work in Australia in the capacity in which they work as a member of Contractor's Personnel.

**Failure** means a failure, problem, issue, concern in relation to, or deficiency in the quality of, any Services or Deliverables.

**Incident** means an event which is not part of the standard operation of a Service and which causes:

- (a) a failure to meet the Service Levels;
- (b) an interruption to, or a reduction in the quality of, that Service; or
- (c) a material impairment of the Contractor's ability to carry out a Service effectively and in compliance with applicable Statutory Requirements.

**Key Position** means a key position that is, or that is required to be, filled and performed by the Specified Personnel at all times during the Contract Period, as specified in Item 27 of the General Order Form.

**Losses** means all liabilities, losses, damages, costs and expenses suffered or incurred by any person, whether arising in contract (including under an indemnity), tort (including negligence), under any statute or under any other common law, equitable or statutory cause of action, and **Loss** has a corresponding meaning.

**Prospective Person** has the meaning given to that term in clause 2.9 of Item 43 of the General Order Form.

**Relevant Offence** means any offence which:

- (a) involves an element of dishonesty or violence;

- (b) involves behaviour which is, in the reasonable opinion of the Customer, inconsistent with the inherent requirements of the roles which the relevant person will be required to perform; or
- (c) is an offence which the Customer reasonably considers is of a nature that if a person who has been convicted of it were to perform the Contractor's obligations under the Agreement, would reflect adversely on the reputation of the Customer or expose the Customer to adverse public comment.

**Repeated Incident** means an Incident which is the same as or similar to an Incident which has occurred previously during the Contract Period.

**Resolution Manager** has the meaning given to that term in clause 11.1 of Item 43 of the General Order Form.

**Resource Levels** has the meaning given to that term in clause **Error! Reference source not found.** of Item 43 of the General Order Form.

**Sanctions** means any sanction administered by the:

- (a) Department of Foreign Affairs and Trade of the Commonwealth of Australia;
- (b) Office of Foreign Assets Control of the U.S. Department of the Treasury;
- (c) U.S. State Department; or
- (d) any other agency of the Commonwealth of Australia, U.S. Government, the United Nations, the European Union or Her Majesty's Treasury.

**Significant Failure** for a Service means any one or more of the following:

- (a) one or more failures to meet any Critical Service Level in any month, or such other measurement period as may be specified in the SLA;
- (b) a breach of the security of any of the Services which resulted in a person being in a position to commit an act which has the potential to have a significant adverse impact on the business, operations or reputation of the Customer or the New South Wales Government;
- (c) any other breach of the Customer Contract by the Contractor which has a significant adverse impact on a critical part of the Customer's business or operations; and
- (d) any other failure, problem or issue which is specified as such in the Customer Contract.

**Step In** has the meaning given to that term in clause 12.1 of Item 43 of the General Order Form.

**Step In Costs** has the meaning given to that term in clause 12.5 of Item 43 of the General Order Form.

**Step In Issue** has the meaning given to that term in clause 12.1 of Item 43 of the General Order Form.

**Transition Out** means the transfer of responsibility for provision of Services and Deliverables supplied under the Customer Contract from the Contractor to the Customer (or a third party designated by the Customer).

**Transition Out Assistance** means all of the services, tasks, functions, activities and responsibilities allocated to the Contractor in the Transition Out Plan or otherwise required to be supplied or performed by the Contractor under clause 13.4 of Item 43 of the General Order Form.

**Transition Out Period** for Services and Deliverables supplied under the Customer Contract means the period commencing on the earlier of:

- (a) the date a Notice in Writing of termination of the Customer Contract is issued; and
- (b) the date specified in the Customer Contract as the date on which the Transition Out Period is to commence for the relevant Services and/or Deliverables,

and continuing until the earlier of:

- (c) the date on which Transition Out for the relevant Services and/or Deliverables is completed; and
- (d) the date on which the Customer notifies the Contractor in writing that the Customer wishes to end the Transition Out Assistance for the relevant Services or Deliverables.

**Transition Out Plan** has the meaning given to that term in clause 13.1 of Item 43 of the General Order Form.

**Transitioned-out Service** has the meaning given to that term in clause 13.7 of Item 43 of the General Order Form.

- 1.2 The following definitions in Part 3 (Dictionary) are deleted and replaced with the new definitions set out below:

**1.24 Consequential Loss** means any loss, damage or expense recoverable at law:

- (a) which is suffered by a Party as a result of a breach of this Customer Contract by the other Party that cannot reasonably be considered to arise naturally from that breach; or
- (b) which is a loss of opportunity, goodwill, profits, anticipated savings or business.

**1.52 Force Majeure Event** means a circumstance beyond the reasonable control of a Party that results in that Party being unable to perform an obligation on time and includes:

- (a) natural events like fire, flood or earthquake;
- (b) national emergency;
- (c) terrorist acts (including Cyberterrorism) and acts of vandalism; or
- (d) war,

but in each case only if and to the extent that that Party is without fault in causing the event, and the event, or its effects, could not have been prevented by reasonable precautions including:

- (e) invoking any relevant disaster recovery plan;
- (f) appropriate workload management practices; and
- (g) any other prudent back-up or recovery procedures.

**1.66 LD Obligation** means an obligation that is stated in Item 21 of the General Order Form as being an obligation for which the late completion by the Contractor may require the payment of liquidated damages in accordance with clauses 1.15 to 1.19 of Item 43 of the General Order Form.

**1.118 Substantial Breach** has the meaning given to that term in clause 7 of Item 43 of the General Order Form.

- 1.3 The definition of "**Due Date**" in clause 1.44 of Part 3 (Dictionary) is deleted and replaced with "Not Used".

**Exhibits to Schedule 1 (General Order Form)**



Contract Number: DICT/693541

Confidential – Department of Customer Service

ME\_179973450\_2

## Exhibit 1 to General Order Form: Services

### 1. Overview

- 1.1 This Exhibit 1 is governed by and forms part of the Customer Contract. Unless otherwise defined in this Exhibit 1, capitalised terms in this Exhibit 1 shall have the meanings given to those terms in the Customer Contract.
- 1.2 This Exhibit 1 provides Contract Specifications for the following Services:
- (a) multi-cloud management services, including but not limited to:
    - (i) leveraging the Customer's existing cloud management platform to enable the delivery of computing integration services (as further detailed in section 3);
    - (ii) proactive and reactive system operations services (as further detailed in section 4); and
    - (iii) development operations services for engineering support of automated software delivery pipelines in public cloud environments (as further detailed in section 5);
  - (b) computing integration services (the scope of which is further detailed in section 6), including but not limited to:
    - (i) management of infrastructure as a service across public cloud, private cloud and on-premises environments (as further detailed in section 7);
    - (ii) management of backup as a service including management of multiple backup platforms (as further detailed in section 8);
    - (iii) management of storage as a service (as further detailed in section 9);
    - (iv) delivery of cloud optimisation solutions to reduce current and future costs (as further detailed in section 10);
    - (v) delivery of data engineering services (as further detailed in section 11);
    - (vi) configuration of specific security postures as required by the Customer and participation in the Customer's overarching security environment (as further detailed in section 12); and
    - (vii) management and operation of system integrity activities (as further detailed in section 13); and
    - (viii) The service brief for each individual service under management which provides definition of service inclusions and conditions will be reviewed and agreed during Transition-In.
  - (c) Citrix cloud transformation project delivery Services, which may be requested by the Customer and will be performed by the Contractor subject to the Parties agreeing and entering into a Change Request in respect of those Services.
- 1.3 The Contractor (also referred to in this document as “**AC3**”) will perform the Services detailed in sections 1.2(a) and 1.2(b) (**Computing Integration Services**, being the Managed Services the Contractor is to perform under Module 12 of this Customer Contract) from 'Go Live' (as that term is defined in the PIPP) for the remainder of the Contract Period.
- 1.4 Not used.

- 1.5 The Computing Integration Services encompass all activities and tasks related to the lifecycle support and management of the Customer's cloud environment, including to:
- (a) plan for and design Computing Integration Services;
  - (b) build and implement Computing Integration Services;
  - (c) support, maintain, deliver and manage Computing Integration Services; and
  - (d) retire Computing Integration Services,
- as required and directed by the Customer. The Contractor will work with the Customer, in accordance with Transition-In obligations as described both in the PIPP and the Module 12 Order Form, as to the methodology, schedule and deliverables required for the setup and agreement of supporting processes for ongoing Services.
- 1.6 The Contractor will supply all Services in accordance with the requirements and recommendations of:
- (a) ITIL, ISO 27001 Information Security Management Systems and ISO 9001:2015 (Quality Management Systems) practice; and
  - (b) all applicable legislation, regulations, policies, guidelines and standards, including as outlined in Exhibit 2 (Requirements) to the General Order Form.
- 1.7 In addition, the Contractor will maintain compliance with any changes in legislation, regulatory requirements and industry and quality standards.
- 1.8 The Contractor will:
- (a) implement measures to minimise disruption to the Customer's operations during maintenance work; and
  - (b) perform any Services that may cause disruption at times likely to cause the least possible disruption to the Customer and its business.

## 2. General Scope of Services

- 2.1 The Contractor will provide the Services as set out in this Exhibit 1 during the Service Hours (as that term is defined in the Schedule 3 (Service Level Agreement), i.e. between 7:30am and 5:30pm on Business Days).
- 2.2 There is a level of resourcing required to meet the Service Levels outlined in Exhibit 1 of Schedule 3 (Service Level Agreement) at Go-Live. This will be measured across the Stabilisation Period (as defined in Schedule 3 (Service Level Agreement)).
- 2.3 As at the Commencement Date, the Contractor has determined the level of resourcing required to meet the Contract Specifications, Service Levels and other requirements under the Customer Contract (**Appropriate Resourcing**). The Contractor will further measure the Appropriate Resourcing during the Stabilisation Period (as defined in Schedule 3 (Service Level Agreement)) and adjust it as necessary to enable the Contractor to meet the Contract Specifications, Service Levels and other requirements under the Customer Contract. If the Customer (or any of its third party suppliers or service providers) makes a change to its environment, applications, servers or server numbers, systems, services or processes which has the effect of reducing the level of resourcing required to meet the Contract Specifications, Service Levels and other requirements under the Customer Contract (**Customer Efficiency**), then:

- (a) the Contractor must promptly reduce the Appropriate Resourcing to reflect the Customer Efficiency (**Resource Reduction**); and
  - (b) to the extent that the Resource Reduction lowers the cost to the Contractor of performing the Services the Contractor must:
    - (i) pass on any and all such cost savings to the Customer as a reduced fee; and
    - (ii) promptly following the Resource Reduction occurring, propose a Change Request (to take effect on and from the date of the Resource Reduction) to pass on such cost savings to the Customer as a reduced fee.
- 2.4** In the event that the Customer requires assistance from the Contractor outside the Service Hours outlined in section 2.1 (or where an emergency requires such assistance to occur outside of these Service Hours), additional charges will apply on a time and material basis in accordance with the Contractor's standard rates (as set out in Appendix A (Rate Card) to this Exhibit 1). Such time and material charges will not be payable by the Customer (and must not be invoiced by the Contractor) unless:
- (a) those charges have been approved by the Customer in writing in advance in relation to the relevant circumstances of assistance (with approval required for each specific instance of assistance); and
  - (b) the Contractor has provided the Customer with reasonable evidence (such as timesheets) to verify its charges.
- 2.5** The Contractor will nominate a single point of contact for the arrangement of out of hours support as outlined in section 2.4.
- 2.6** The Contractor will nominate a service delivery manager responsible for scheduling and attending onsite face-to-face service review meetings and providing a specific focus on Service Level management and Service improvement plans.
- 2.7** The Contractor will nominate a dedicated Technical Account Manager with appropriate cloud administrator/engineer experience, who understands the lifecycle of cloud infrastructure management to cost optimisation.
- 2.8** If at any point the Contractor recognises or otherwise becomes aware of a gap in the Customer's service management capability, the Contractor will advise the Customer and present options including tooling to help support the environment and address this gap.
- 2.9** The Contractor will work with the Customer to identify opportunities for service improvement and to ensure that improvement initiatives and ideas are generated from both a Customer and Contractor perspective. These initiatives should deliver a more efficient service, improve the delivery of service objectives, reduce the cost of the service and/or increase Customer satisfaction.
- 2.10** The Contractor will identify opportunities to transform siloed service management environments by introducing a unified management approach and consolidating Services to a single platform wherever possible and at the Customer's direction.
- 2.11** In the event that a Service Request (as defined in Schedule 3 (Service Level Agreement)) falls outside the scope of the included Services, the Contractor must contact the Customer to discuss requirements and agree to the scope. The Contractor must then advise the Customer of the estimated Price (based on rates as set out in Appendix A (Rate Card) to this Exhibit 1) to complete that Service Request and confirm the availability of resources prior to commencing work. Both Customer and Contractor will agree in writing the scope and Price for the applicable Service Request prior to work commencing, and no Price will be payable by the Customer (and the Contractor must not invoice the Customer) in respect of such work unless the scope and

Price of the relevant work have been approved by the Customer in writing in advance of work commencing.

**2.12** The Contractor's overall solution will provide

- (a) a unified management interface via the Customer's cloud management platform;
- (b) in-depth reporting and data extraction capabilities via the Customer's cloud management platform;
- (c) an onshore support model with at least 80% of resources based in Australia (and predominantly in NSW);
- (d) mixture of dedicated and leveraged resources across all Services;
- (e) deployment and configuration standardisation through automated blueprint deployment of workloads;
- (f) tagging of workloads on an agency and business unit level, which may assist with providing financial information to cross-charge business units or agencies;
- (g) the extension of the Customer's current operating model and SIAM ecosystem and capability to recommend improvements through operational efficiencies; and
- (h) a leveraging of existing toolsets to provide an outcome and optional tools to cover gaps where necessary.

**2.13** The Contractor will provide service management activities including but not limited to:

- (a) proactive support, including but not limited to:
  - (i) health checks and log monitoring;
  - (ii) monitoring traffic levels for unusual activity;
  - (iii) capacity management; and
  - (iv) management of security zones
- (b) reactive support, including but not limited to:
  - (i) Incident management and resolution;
  - (ii) Problem management and resolution;
  - (iii) vendor liaison; and
  - (iv) support for hardware under valid vendor maintenance arrangement (and support on best efforts basis for hardware outside vendor maintenance arrangement)
- (c) service delivery, including but not limited to:
  - (i) ITIL process alignment;
  - (ii) Service level reporting;
  - (iii) monthly Incident and Problem reporting; and



- (iv) provision of a yearly firewall rules report for the firewall devices under the Contractor's management;
- (d) Vendor best practice, including but not limited to maintaining device firmware to a vendor-supported release; and

### 3. Cloud Management Platform

- 3.1 The Contractor will manage public and private cloud virtual machines using the Customer's chosen cloud management platform.
- 3.2 The Contractor will be accountable for delivery to identified outcomes working within the parameters provided by the Customer through the cloud management platform tool.
- 3.3 Notwithstanding the Customer's rights in respect of Step-in under clause 12 of Item 43 (Additional Conditions) of the General Order Form, the Contractor will provide the Customer with the ability to run and manage the environment where required by the Customer, including by providing the required level of access to any Contractor provided tools utilised in the Customer's environment. This specific request must be authorised in writing by Chief Technology Officer or someone of equivalent management level.
- 3.4 The Contractor will leverage the cloud management platform, cloud native tools and traditional computing integration tools (such as database administration tools) to enable the delivery of the Services.
- 3.5 The Contractor may bring and utilise additional tools, but:
  - (a) any such tool must integrate with the Customer's cloud management platform tool;
  - (b) any use of Contractor's own tools must not detract from the processes implemented by the Customer's cloud management platform; and
  - (c) the Customer must have the required level of access to these tools for the purpose set out in section 3.3.
- 3.6 The Contractors' tools must support the following environments:
  - (a) AWS;
  - (b) Azure;
  - (c) VMware;
  - (d) Oracle; and
  - (e) any others that could be reasonably expected by the Customer.
- 3.7 The Contractor will work within the Customer's chosen cloud management platform solution and collaborate with the Customer at the Customer's direction to leverage the key pillars that the platform contributes to the environment:
  - (a) Visibility to discover and maintain accurate inventory across the technical landscape, including:
    - (i) discovery; and
    - (ii) service mapping;

- (b) Real-time identification of service health issues while pinpointing the root-cause of service Incidents or failures, including:
    - (i) event management;
    - (ii) operational intelligence; and
  - (c) use of Cloud Management and Cloud Insights capabilities to provide optimisation and management across the cloud environment.
- 3.8** The Contractor will align closely with the Customer's cloud management team to ensure the technical landscape is covered in full by cloud management platform discovery agents as the environment evolves and that the CMDB fully represents all technical resources within the environment.
- 3.9** The Contractor will work with the Customer to closely monitor and manage credentials to support CMDB data population across both cloud based and on-premises infrastructure.
- 3.10** The Contractor will contribute to Service Map Design to ensure service maps maintain the correct business context through relationships, dependencies, and components that make up that service. The Contractor will (at the Customer's direction) collaborate with the Customer's cloud management team to provide event management services. The Customer will configure all components within the Customer's ServiceNow environment including Cloud Management, Cloud Catalogue, Event Management, Discovery, Service Mapping, Asset Management, IT Service Management and the ServiceNow Integration to the Contractor (the Customer side of the integration) to allow for a centralised and holistic view of the health of all services.
- 3.11** The Contractor will provide guidance and insight in supporting the Customer's journey to mature its capabilities and tools (including its chosen cloud management platform) over the duration of the Contract Period.
- 3.12** The Contractor will utilise the out-of-the-box Cloud User Portal as commissioned and configured by the Customer, which may be used to perform the following actions:
- (a) monitor Customer's quota, costs, budget, life cycle events, stack health and Requests;
  - (b) request stacks from the service catalogue and track Service Requests;
  - (c) request life cycle operations for stacks and resources (for example stop, start or de-provision); and
  - (d) create and track Incidents.
- 3.13** The Customer will deliver and manage the cloud admin portal to allow for the management, design, governance, operation and analysis of cloud resources from a unified base.
- 3.14** The Customer may request additional assistance in relation to the design, delivery and maturity of ServiceNow solutions on an ad hoc basis. If additional ServiceNow configuration support is to be required, this is considered a Service Request and is subject to section 2.11.

## 4. System Operations

- 4.1** The Contractor will provide a comprehensive range of proactive and reactive support and workload management services across Customer's on-premises and private cloud server fleet.
- 4.2** The Contractor will manage all operating system instances (**OSIs**) across the environment, regardless of the platform.

- 4.3 The Contractor will utilise server management to provide:
- (a) regular and emergency patching of operating systems;
  - (b) maintenance of desired security posture;
  - (c) operating system configuration; and
  - (d) optimisation in line with industry best practices.
- 4.4 The Contractor will align with the Customer's Change control processes, ensuring that no Change is implemented in the Customer's environment without an approved Customer Change request.
- 4.5 The Contractor will provide reporting of progress and efficiency metrics to the Customer, ensuring full transparency of all system operations activities.
- 4.6 The Contractor will assist in the fulfillment of provisioning Service Requests through the maintenance of provisioning templates on a per-platform basis and the configuration assurance and patching of newly provisioned instances.
- 4.7 The Contractor will utilise a centralised patching infrastructure to provide the Customer with the following:
- (a) reduced complexity of patch deployment across various infrastructures;
  - (b) increased coverage of operating systems that can be centrally patched under a unified and auditable Change control process; and
  - (c) eliminating the need for maintaining multiple Windows Server Update Services and Satellite environments across infrastructure platforms.
- 4.8 The Contractor will perform moves, adds, changes and deletions for ad hoc automated macro provisioning of new OSIs each month.
- 4.9 The Customer may engage the Contractor to fulfil Large Scale provisioning requests (where **Large Scale** refers to activities that are to be funded and defined by the Customer as a project and require more than forty (40) hours of Contractor effort), provided that any such requested engagement is to be considered a Service Request and is subject to section 2.11.
- 4.10 The Contractor will provide cloud operations support, including but not limited to:
- (a) responding to infrastructure monitoring alerts and resolving Incidents to ensure system uptime meets Customer requirements;
  - (b) coordinating with Customer to remediate issues detected in the public cloud to enhance efficiency;
  - (c) collaborating with the Customer's architecture and cloud management teams in the development and management of infrastructure automation scripts, templates and integrations with development operations tools;
  - (d) collaborating with the Customer's network services team to complete network connections or configurations (e.g. provisioning new environment);
  - (e) collaborating with the Customer in the configuration of in-scope cloud services such as:
    - (i) Domain Name System (DNS);
    - (ii) direct/express route links;

- (iii) peering;
  - (iv) security groups;
  - (v) load balancer;
  - (vi) application firewalls;
  - (vii) certificate management; and
  - (viii) any other configurations required to enable a new application service
- (f) providing support to the Customer in optimising or troubleshooting cloud-based workloads or applications;
  - (g) installing, configuring and managing workloads with different combinations of operating systems;
  - (h) ongoing configuration management of the in-scope cloud services;
  - (i) ensuring all cloud infrastructure components meet the Customer's performance and security standards;
  - (j) monitoring cloud native security tools to ensure the security posture of in-scope managed elements, including:
    - (i) ensuring cloud native security tools are configured to forward events to the Customers designated SOC; and
    - (ii) working to resolve issues raised by the Customers designated SOC
  - (k) collaborating with the Customer to investigate and remediate infrastructure issues reported by Security monitoring tools; and
  - (l) selecting the optimal cloud services based on data and security requirements

## 5. Development Operations

- 5.1 The Contractor will provide engineering support of fast-moving automated software delivery pipelines in public cloud environments.
- 5.2 The Contractor will (at the Customer's direction) assist the Customer in the design, deployment and management of public cloud software delivery pipelines and applications by:
  - (a) focusing on best practice and utilising an iterative approach that ensures flexibility and innovation; and
  - (b) augmenting the Customer's environment with resources that advise on and provide modern approaches, ensuring the Customer's continuous incremental improvement.
- 5.3 The Contractor will participate in regular (at a frequency to be determined by the Customer) meetings and workshops to review, design, track and govern work undertaken by the Contractor in development operations.
- 5.4 The Contractor will design and deploy instrumentation, monitoring and alerting of pipeline design and management of platforms

- 5.5 The Contractor will design and manage containerised environments using industry-leading toolsets for efficient and reliable communication, governance and systems of record.
- 5.6 The Contractor will adhere to agile project management practices, tailored to the Customer's environment to deliver development operations services.
- 5.7 The Contractor will create and manage development activity/requirements backlog.
- 5.8 The Contractor will provide control of and insight to the Customer as to how the environment is being developed and maintained by employing tools and processes that deliver effective technological design, responsible deployment methods and efficient governance.
- 5.9 The Contractor will uplift the Customer's environment to a high standard of automation using infrastructure as code and full monitoring and alerting capabilities in order to mature focus on proactive improvement opportunities.
- 5.10 The Contractor's development operations team also has a significant cloud optimisation focus as detailed in section 10.17.
- 5.11 The Contractor will use infrastructure as code provisioning orchestrated by ServiceNow ITOM for newly established infrastructure and for all reusable components for public cloud management, including performing:
  - (a) infrastructure as code catalogue template definition and maintenance;
  - (b) maintaining and rolling out infrastructure changes (through infrastructure as code); and
  - (c) optimisation of public cloud workloads as outlined in section 10.

## 6. Computing Integration Services Scope

- 6.1 The Contractor will undertake actions across the multiple managed environments as directed by the Customer.
- 6.2 The Contractor will undertake actions across the multiple cloud platforms and on-premises environments, delivering to the Customer its goals of:
  - (a) performance optimisation;
  - (b) improved cost management;
  - (c) automated macro provisioning;
  - (d) cloud security; and
  - (e) capacity management.
- 6.3 The Contractor will engineer and operate the solutions as an integrated package.
- 6.4 The Contractor will manage and conduct operational tasks above the abstraction layer for the entire centralised computing environment.
- 6.5 The Contractor will deliver computing integration Services to support and manage the Customer's cloud services offerings:
  - (a) infrastructure as a service (**IaaS**);
  - (b) storage as a service (**STaaS**);

- (c) back-up as a service (**BUaaS**); and
  - (d) any future cloud service offerings that the Customer may seek to introduce.
- 6.6** The Contractor must be able to absorb new services, upon mutual agreement, with its associated requirements and continue to manage the cloud service offerings outlined in section 6.5 as the Customer develops new services and retires existing services.
- 6.7** The Contractor will contribute to the creation of a bi-directional integration between the Customer and Contractor's ITSM modules (configuration in Contractor environment only) to enable the routing of Incidents, Problems, Service Requests and Change Requests. This integration will be uplifted by the Contractor and Customer over time as the environment matures to ensure both the Customer and the Contractor can maintain consistent engagement and high responsiveness.
- (a) The Contractor will contribute to the Customer's Cloud Centre of Excellence by: collaborating with the Customer's architects to organise the in-scope cloud services in an optimal end state;
  - (b) contributing to the Customer's architectural forum in the optimal design/reference architecture for in-scope cloud services (including but not limited to addressing requirements relating to deployment, security, cost-effectiveness, high availability and process improvement);
  - (c) facilitating the transition of the Customer's architectural requirements to future processes;
  - (d) providing regular reports to the Customer on the health, cost initiatives and overall state of cloud infrastructure;
  - (e) collaborating with the Customer's cloud management and architecture teams to develop an appropriate cloud cost model;
  - (f) ongoing monitoring of overall costs of in scope cloud services in light of cost reduction initiatives; and
  - (g) ensuring compliance with all applicable Customer policies and procedures.
- 6.8** The Contractor will manage the Customer's operating system and database licence positions for the physical servers and virtual machines and provide licence optimisation services.
- 6.9** The Contractor will contribute to the Customer's IT Service Desk known errors database and knowledge articles as directed by the Customer.
- 6.10** The Contractor may be required to provide private clouds, consulting expertise for planning and execution of migration activities and/or consulting services to build platform and cloud specific automations and workflows to enhance and extend the capabilities of the Customer's chosen cloud management platform. If these requests fall outside the scope of the Services as described in this Exhibit 1, such a request will be a Service Request subject to section 2.11.

## **7. Infrastructure as a Service**

- 7.1** The Contractor will provision new instances (and retire existing instances) as directed by the Customer.
- 7.2** The Contractor will build and maintain operating system images and templates for deployment on each infrastructure platform:
- (a) according to the N-2 pattern;

- (b) with quarterly image updates applied for each system; and
  - (c) with security related and critical hotfixes and patches applied within 48 hours of release in accordance with the Customer's relevant security and release policies.
- 7.3** The Contractor will provide OSI provisioning using image templates and cloud management platform automation.
- 7.4** The Contractor will provide ongoing operating system level support and management, including but not limited to:
  - (a) full support for all vendor backed operating system editions and versions up to the vendor's end of life support dates;
  - (b) visibility of the pending end of life status for all managed operating system instances and assistance with management of end of life events including advice and expertise in assisting the development of migration and upgrade roadmaps; and
  - (c) support beyond vendor end of life dates on a best efforts basis.
- 7.5** The Contractor will provide OSI performance optimisation and best practice alignment, including but not limited to:
  - (a) right-sizing recommendations as part of regular service delivery reporting; and
  - (b) system optimisation and right-sizing activities in alignment with the Customer's relevant change control policies.
- 7.6** The Contractor will provide backup client installation and configuration for
  - (a) virtual machine image-level backups;
  - (b) agent-based backups; and
  - (c) advanced agent-based backups,as detailed in section 8.
- 7.7** The Contractor will perform restores at the virtual machine or file-level actioned through Service Request and in accordance with the Customer's Change control policies and procedures.
  - (a) in accordance with the Customer's recovery point objective and recovery time objective as defined in Appendix C of Exhibit 2 (Requirements) to the General Order Form; and
  - (b) within response time service levels as outlined in Exhibit 1 to Schedule 3 (Service Level Agreement),as detailed in section 8.
- 7.8** The Contractor will manage and support:
  - (a) the node infrastructure in the Customer's data centres, including procuring additional nodes before capacity is reached (this process is automated in public cloud environments);
  - (b) the VMWARE elastic sky X hosts and host clusters in the data centre (this process is automated in public cloud environments);
  - (c) the database clusters in the Customer's data centres;

- (d) DNS in the Customer's data centres;
- (e) Dynamic Host Configuration Protocol (DHCP) in the Customer's data centres; and
- (f) centralised digital certificates including issuing new certificates, renewing certificates and securing storage of the keys in a key store (this process is automated in public cloud environments).

- 7.9** The Contractor will develop and manage gold images for all virtual machine types within the Customer environment, including but not limited to the operating system, end-point protection, monitoring tools, backup software and group policy.
- 7.10** The Contractor will, if requested by the Customer, be responsible for provisioning and decommissioning of virtual machines. Decommissioning physical servers, provided that if this request falls outside the scope of the Services as described in this Exhibit 1, will be a Service Request subject to section 2.11.
- 7.11** The Contractor will ensure all vendor virtual machine service level agreements are met.
- 7.12** The Contractor will provide day to day oversight of its relationship with partners and third parties within the Customer's environment and will promptly address any issues or gaps

## 8. Backup as a Service

- 8.1** As part of the management of the BUaaS services, the Contractor will provide:
- (a) file system backup and recovery services;
  - (b) database backup and restore;
  - (c) image level backups and recovery of virtual machines;
  - (d) the ability to add, remove and/or modify clients from backup services;
  - (e) ad hoc backups as requested by the Customer from time to time; and
  - (f) ad hoc restore from backup of selected production services including physical servers, virtual machines, applications and databases.
- 8.2** The Contractor will provide image based backup, agent based backup and advanced agent based backup as per the service plans outlined in Appendix C of Exhibit 2 (Requirements) to the General Order Form.
- 8.3** The Contractor will perform service activation, agent installation and configuration as well as any other tasks required to enable functionality of the backup toolset.
- 8.4** The Contractor will monitor, alarm and respond to backup failure events with protection activities.
- 8.5** In the event a backup does not complete within the backup window (**Backup Failure**), the Contractor will re-run the backup process in alignment with related services and in accordance with the Customer's requirements as outlined in Exhibit 2 (Requirements) to the General Order Form unless otherwise directed by the Customer.
- 8.6** The Contractor will deploy and configure backup agents to newly provisioned virtual machines.
- 8.7** As part of the restoration services, the Contractor will:



- (a) plan, establish and test restore procedures required to restore files and directories in accordance with Customer requirements;
- (b) plan, establish and test the recovery procedures required to re-establish the functionality of systems managed by the Contractor in accordance with the Customer requirements (in the event of a failure);
- (c) provide individual file and directory restores in accordance with pre-defined and established Customer processes and procedures;
- (d) provide system restores for the purpose of recovering a system or solving a problem on a system, including where this requires the restoration of the operating system, restoration of any applications and/or the recovery of data from the last known best available backup; and
- (e) restore an improperly functioning virtual machine, including creating a new virtual machine instance and retaining the old virtual machine and relevant storage volumes for 14 days or as otherwise directed by the Customer to safeguard against unintentional data loss.

**8.8** The Contractor will provide BUaaS reporting (in addition to all other operational and compliance reporting outlined in Item 40 of the General Order Form and elsewhere in the Customer Contract), including but not limited to:

- (a) performance success and failure reports;
- (b) time to complete backup reports;
- (c) amount of data backed up;
- (d) number of retention points available;
- (e) number of re-run jobs; and
- (f) any other relevant reporting which can reasonably be requested by the Customer.

**8.9** The Contractor will provide backup monitoring and management Services, including but not limited to:

- (a) maintaining the backup and restore infrastructure to meet the Customer's backup and recovery objectives;
- (b) performing backup administration responsibilities consisting of the installation and configuration of components, scheduling of backups and monitoring of the successful completion of scheduled backups;
- (c) assisting database and application support staff in verifying that database or application backup and restore capabilities are functional, including working with Customer resources to periodically test backup and restore processes;
- (d) testing backup and restore processes twice a year and generating a report as a result of the testing; and
- (e) monitoring and managing alerts configured by global policy and logged by email and through simple network management protocol traps.

**8.10** The Contractor will be able to cater for backup retention period changes and continue with the process of secure disposal of backup media once set retention periods are reached.

- 8.11 The Contractor will provide licence and consumables management for the Customer's existing back up platforms including procuring additional licences, hardware, consumables and third-party services as approved by the Customer when existing stock runs low.
- 8.12 The Customer may request additional assistance in relation to backup platform optimisation and consolidation. If additional platform optimisation support services are to be required, this is to be considered a Service Request and is subject to section 2.11.
- 8.13 The Customer may request additional customisations for retention cycles. If this is requested, it is to be considered a Service Request and is subject to section 2.11.

## 9. Storage as a Service

9.1 As part of the management of the STaaS services, the Contractor will:

- (a) deliver storage utilising the Customer's storage platforms and arrangements;
- (b) perform all storage operations in accordance with vendor OEM standards;
- (c) manage the assignment of volumes;
- (d) provide provisioning and reclamation services;
- (e) provide monitoring services;
- (f) provide storage replication services;
- (g) provide quota management; and
- (h) monitor performance for storage area networks (SAN) and network attached storage devices (NAS).

9.2 As part of the delivery of the provisioning and reclamation Services, the Contractor will:

- (a) review storage requests and action or advise as appropriate;
- (b) deallocate and reclaim storage and perform required clean-up of unused files;
- (c) connect new hosts;
- (d) manage encryption keys for all encrypted storage implementations;
- (e) develop, publish and perform processes for managing the file system structures, access, and data life cycles and update documentation as required;
- (f) update and/or interface with billing and operational systems; and
- (g) provide accurate and timely monthly reporting.

9.3 As part of the delivery of the performance management Services, the Contractor will:

- (a) analyse workload profile and create performance baseline;
- (b) analyse the workload changes and make recommendations in the relevant monthly report;
- (c) provide data for planning of additional workloads as required;

- (d) provide recommendations to prevent performance issues as required; and
- (e) review performance alerts and take required actions, and report to the Customer in the relevant monthly report.

**9.4** As part of the delivery of the capacity and optimisation Services, the Contractor will:

- (a) provide patch management monitoring and identify and implement the storage vendor's hardware and software patches, security patches and service releases in accordance with OEM requirements. Updates will be implemented during the standard patching window in accordance with the Customer's approved Change management processes, or otherwise at the Customer's direction;
- (b) monitor storage growth, manage the buffer and report on capacity impacts to meet the requirements of the Customer;
- (c) provide a flexible solution which enables the storage capacity to grow as the Customer requires (whilst supporting the committed Customer-directed minimum capacity volume with sufficient buffer to support general demand);
- (d) maintain a capacity-based high water mark of 80% of total available storage capacity (or as otherwise directed by the Customer) for volume increases;
- (e) actively respond to unexpected storage demands in accordance with the quarterly Customer forward storage consumption projection;
- (f) optimise allocated storage and reclaim as required, delivering an optimisation saving if change is non-outrage related and obtaining approval via Customer's change advisory board where an outage may be required to optimise and reclaim storage; and
- (g) manage a 20%-30% threshold for headroom or as otherwise directed by the Customer to maintain an optimal storage operating environment.

**9.5** As part of the delivery of the STaaS services, the Contractor will manage storage security by:

- (a) providing access management for the storage platform in accordance with the Customer's requirements;
- (b) using zoning and secure port authentication and enforcing settings for the fabric;
- (c) ensuring that file-sharing is controlled by system and user security systems, network file services through the NAS; and
- (d) providing data at rest encryption.

**9.6** The Contractor will use and implement (where appropriate) software and technology capable of delivering:

- (a) encryption and security capabilities;
- (b) storage optimisation;
- (c) deduplication management and optimisation capabilities;
- (d) compression;
- (e) custom block sizes (facilitating Customer non-standard requests); and
- (f) additional storage protocols when requested by the Customer.

## 10. Optimisation

- 10.1 The Contractor will commercially optimise the environment to manage workload so as to be executed in the most cost-effective manner (for portal and transient load enabled applications).
- 10.2 The Contractor is required to adhere to the principles (including boundaries and constraints) set by the Customer's cloud management team as to how the Contractor can provision, operate and optimise the infrastructure.
- 10.3 The Contractor will provide regular updates on performance and cost metrics based on utilisation.
- 10.4 The Contractor shall collaborate with the Customer to define and implement key reports or report views in the Customer's cloud management platform environment to aid in, and facilitate cost optimisation and standardised optimisation reporting.
- 10.5 The Contractor will provide financial management of the cloud.
- 10.6 The Contractor will configure the cloud services to optimise the usage with an objective to provide the performance appropriate for the task.
- 10.7 The Contractor will configure the cloud services to optimise the usage with an objective that it is provided in a cost-effective way that leverages the fees structure for the applicable cloud through demonstrable and repeatable processes.
- 10.8 The Contractor as part of its development operations services (as detailed in section 5) will, for applications other than those that have software defined infrastructure, undertake the predictive and reactive tasks to configure and reconfigure the environment within and across tenancies for an optimal outcome. For applications that support portability, the reconfiguration could be across multiple clouds, including, for example, baseload operating on premises or in a private cloud with a fixed cost and peak activities 'bursting' into the identified public clouds. Where such Customer requests are identified as Large Scale programs of work (as defined in section 4.9), they are to be considered a Service Requests and are subject to section 2.11.
- 10.9 The Contractor will provide the Customer with regular reports on optimisations achieved as well as to any constraints, exceptions or failures to meet the requirements of the Customer.
- 10.10 The Contractor will provide the Customer with reports and/or dashboards detailing trend analysis in key reportable metrics (or otherwise at the Customer's direction).
- 10.11 The Contractor will provide an integrated approach, utilising both technology metrics and subject matter expertise to interpret and act on findings and automated system recommendations, delivered under agile methodology.
- 10.12 The Contractor will reduce current and future cloud costs by leveraging five cost pillars across all workloads, architectures and cloud types:
  - (a) 'right-sizing' by ensuring that provisioning matches needs and decommissioning unused resources;
  - (b) leveraging the right pricing model to optimise costs based on the nature of the workload;
  - (c) increase elasticity, optimising costs to meet dynamic Customer needs and turning resources off when they are not needed;
  - (d) optimising storage for Customer data while maintaining level of performance and availability; and

- (e) measuring, monitoring and improving service to ensure the full economic potential of the public cloud is utilised at any stage.
- 10.13** The Contractor will collaborate with the Customer to institute a process to consolidate and optimise the use of backup software licenses across the Customer's chosen backup platforms.
- 10.14** The Contractor will collaborate with the Customer to:
- (a) institute a process to validate and update the backup retention periods;
  - (b) institute compliance implementation and management (including but not limited to guardrails, policies and encryption);
  - (c) drive the triaging of tickets on moves, adds and changes;
  - (d) institute a process to consolidate and optimise the use of operating system licences across the fleet of physical servers and virtual machines;
  - (e) institute a process to optimise the capacity, usage and procurement of the node infrastructure in the Customer's data centres;
  - (f) centralise the process of provisioning and decommissioning of virtual machines;
  - (g) centralise the management of digital certificates;
  - (h) institute a process to regularly audit the secure disposal of backup when the duration of the set retention periods have been reached;
  - (i) regularly review the current procedures and processes, with a view to automate where possible;
  - (j) institute a regular process to audit all Contractor staff remote and physical access to the infrastructure;
  - (k) establish an optimal engagement model to manage and support infrastructure in areas of conflicting responsibilities;
  - (l) facilitate the ad-hoc requests for project resourcing and/or delivery of a project; and
  - (m) facilitate the ad-hoc requests to quote on resourcing and delivery of infrastructure initiatives.
- 10.15** The Contractor will extend optimisation efforts beyond public cloud services into existing private cloud infrastructure, seeking to drive intelligent decision making to migrate (or relocate) workloads and individual applications into public cloud infrastructure.
- 10.16** The Contractor will adhere to the following cloud optimisation methodology unless otherwise directed by the Customer:
- (a) identify optimisation opportunities by evaluating workload metrics in terms of both cost and performance, utilising insights from the Customer's cloud management platform and cloud native tooling where relevant;
  - (b) evaluate optimisation opportunities by forming an optimisation pathway for individual applications or complete workloads, drafting optimised state recommendations whilst adhering to relevant governance and architectural review board circulation and approval as determined by the Customer's Cloud Centre of Excellence; and

- (c) implementing the approved recommendations and implementing optimisation roadmap work items.

- 10.17 The Contractor's development operations team will be flexible in time allocation as optimisation options and business requirements fluctuate, and are responsible for both cloud optimisation and cloud management. In relation to the cloud optimisation function, the team will focus on public cloud process optimisation and infrastructure re-engineering by means of right-sizing, scaling and scheduling to improve performance and resiliency and lower cost.
- 10.18 The Contractor may be required to utilise the CloudHealth or CloudSaver tools to enhance the existing financial management and optimisation capability. If this is requested by the Customer, this will be considered a Service Request and is subject to section 2.11, provided that the applicable charges payable for this will be the price stated for this in per Exhibit 3 (Pricing) to the General Order Form.

## 11. Data Engineering

- 11.1 The Contractor will operate the systems within the environment (including the public cloud and private cloud), engineering the data across the entire environment.
- 11.2 The Contractor will ensure that data is held in the right locations and accessible for the applications that need them.
- 11.3 The Contractor will work with the Customer to ensure networking between data points is configured correctly and accessible.
- 11.4 The Contractor will enable seamless flow of data and transactions across systems in hybrid environments.
- 11.5 The Contractor will provide regular reports showing that the data is secure, being backed up, and that disaster recovery (DR) and business continuity planning (BCP) on the data is available in compliance with the Customer's relevant policies and direction.
- 11.6 The Contractor will provide database patch and upgrade management for in-scope production services.
- 11.7 The Contractor will monitor database performance and fine tune as directed by the Customer.
- 11.8 The Contractor will facilitate ad hoc database support requests, including but not limited to the creation of new databases, creation of new tables and indexing.
- 11.9 The Contractor may be required to provide database administration Services on an ad hoc basis. If this is requested by the Customer, it is considered a Service Request and is subject to [section 2.11](#).
- 11.10 The Contractor will have the capability to provide immediate database support on a 24x7 basis during major Incidents. If this is requested by the Customer, it is considered a Service Request and is subject to section 2.11.

## 12. Security

- 12.1 The Contractor will operate the systems within the environment, providing common access and common security posture.
- 12.2 The Contractor will configure the systems for the identified security posture during deployments and reconfiguring through optimisation activities.

- 12.3 The Contractor will harden the virtual machines, following the Customer's security requirements and policies.
- 12.4 The Contractor will undertake specific cloud related security activities as defined by the Customer's security strategy and as directed by the Customer's cloud management team.
- 12.5 The Contractor will submit and comply with the Customer's security policies and direction.
- 12.6 The Contractor will participate in the Customer's audit and compliance activities as required and directed by the Customer.
- 12.7 The Contractor will undertake patch management in accordance with the Customer's patching schedule that covers all Customer environments, workloads and appliances in scope.
- 12.8 The Contractor will apply emergency patches outside the regular patching window at the direction of the Customer (including infrastructure, database, and appliance patching in addition to operating system patching).
- 12.9 The Contractor is required to have the Customer's monitoring and security tools on any infrastructure or service that they place on the Customer's network for management or other purposes.
- 12.10 The Contractor will provide virtual patching at the Customer's direction.
- 12.11 The Contractor will provision infrastructure with the security baseline as directed by the Customer's security policies and processes.
- 12.12 The Contractor will establish privileged access management for the operating environments and leverage existing mechanisms and processes where appropriate. The Contractor will define and implement access models in accordance with the Customer's security policies.
- 12.13 The Contractor will monitor the IaaS environment using cloud native tools and the Customer's chosen monitoring/alarming tool. The Contractor may be asked to provide a LogicMonitor centralised monitoring platform to enhance the Customer's monitoring capabilities, and if so this is considered a Service Request and is subject to section 2.11.
- 12.14 The Contractor will provide three categories of security optimisation Services:
  - (a) proactive or emergency security optimisation as part of a cooperative effort with the Customer's resources during a security Incident;
  - (b) continuous security optimisation forms part of the cloud optimisation focus and includes but is not limited to performing recommended security configuration updates on public cloud or private cloud that do not impact on production; and
  - (c) governed security optimisation makes up larger security best practice implementations that may impact production and runtime systems and require architectural review board consideration and approval.

## 13. System Integrity Activities

- 13.1 The Contractor will undertake monitoring, tasks and configurations to ensure the resilience of the configuration and individual failures.
- 13.2 The Contractor will undertake backup and restoration activities, ensuring the integrity of the Customer's data sets.

- 13.3** The Contractor will undertake activities to ensure that the services can be recovered in the event that a physical data centre becomes unavailable for any reason.
- 13.4** The Contractor will back up and maintain a versioned copy of text based hardware device configurations via SSH. This will be performed on a regular schedule as well as on an ad hoc basis prior to and immediately following controlled Change implementation activities and at the Customer's direction.
- 13.5** The Contractor will provide monitoring and maintenance Services for physical equipment within the on-premises environment, including but not limited to measurement and tracking of performance, capacity and breakage.
- 13.6** The Contractor will provide breakfix management Services for physical equipment within the on-premises environment.
- 13.7** The Contractor will provide physical engineering and operation Services, including but not limited to racking, patching, power up and power down.
- 13.8** The Contractor will provide storage and backup Services for the on-premises infrastructure, including but not limited to:
- (a) physical storage, including storage arrays and storage network devices;
  - (b) NAS devices;
  - (c) backup systems including tape drives and libraries, media agent systems, cloud attached storage gateways and backup-to-disk storage devices; and
  - (d) support and management of array-to-array replication for DR purposes
- 13.9** The Contractor will provide physical compute Services for the on-premises infrastructure, including but not limited to:
- (a) vendor relationship management and support for physical compute hardware;
  - (b) Hypervisor operation and management for all virtual machines across the environment;
  - (c) operating system management for physical servers;
  - (d) remote management of physical compute and operating systems located at branch sites;
  - (e) facilities management for the Customer's data centre sites (for the Customer's Silverwater and Unanderra sites and remote hands scheduled preventative and reactive support for the Bathurst site); and
  - (f) the option to leverage LogicMonitor platform for monitoring gaps (subject to section 12.13)
- 13.10** The Contractor will provide event monitoring, support, capacity management, backup and break-fix Services for:
- (a) the underlying compute and storage infrastructure in the on-premises environment;
  - (b) the Hypervisor infrastructure across public cloud, private cloud and on-premises environments;
  - (c) physical servers and virtual machine infrastructure including operating systems, CPU's, GPU's and storage;



- (d) databases and database clusters including providing ongoing performance tuning; and
  - (e) the node infrastructure (for on-premises and private cloud environments only)
- 13.11** The Contractor will provide business as usual patch management and firmware upgrades on the fleet of physical servers and virtual machines, including the prioritisation of emergency patches when the need arises or at the Customer's direction.
- 13.12** The Contractor will provide business as usual database version releases and upgrades.
- 13.13** The Contractor will provide audit Services for:
- (a) physical data centres, physical servers and virtual machines hosting the in-scope production Services;
  - (b) services with high availability capabilities including sourcing/examining the relevant BCP documents;
  - (c) services with operating disaster recovery (**DR**) and the location of DR, including examining the DR plan; and
  - (d) the operating system and database licences installed on the production and non-production servers including confirming the date of licence expiry (for on-premises and private cloud hosted services only).
- 13.14** The Contractor will collaborate with the Customer to link asset and business owners and cost centres to the in-scope production and non-production servers.
- 13.15** The Contractor will support the Customer's DR capability for:
- (a) the on-premises database infrastructure layer;
  - (b) the OSIs within the on-premises environment;
  - (c) the virtualised machine hardware layer within the on-premises environment;
  - (d) the Hypervisor layer within the on-premises environment; and
  - (e) any storage and backup platforms operating within the on-premises environment.
- 13.16** The Contractor is required to deliver DR services above the abstraction layer (Hypervisor) for the entire centralised computing environment. The Contractor is not required to deliver DR services at or below the abstraction layer (Hypervisor) for private or public clouds.
- 13.17** The Contractor will conduct a DR workshop with the Customer to provide a forum for a review of the Customer's existing DR and BCP policies and strategies, to ensure alignment of Contractor procedures with Customer's existing governance.
- 13.18** The Contractor will be required to participate in ad hoc DR testing at the direction of the Customer. If this is requested by the Customer, it is to be provided at the price as per the calculation methodology in Exhibit 3 (Pricing) to the General Order Form and is subject to section 2.11.

## **14. Citrix On-Premises Management and Cloud Transformation**

- 14.1** If requested by the Customer, the Contractor will perform the activities and Services set out in this section 14, subject to the Parties agreeing and entering into a Change Request in respect of those activities and Services. To avoid doubt, sections 14.2 to 14.15 do not apply unless and until such Change Request is executed by the Parties.
- 14.2** The Contractor will deliver end-to-end Citrix management capabilities, including but not limited to:
- (a) daily checks of environments, system patching, capacity management and performance reporting;
  - (b) reactive support such as Incident management and Problem management and resolution;
  - (c) service delivery including ITIL process alignment and monthly Incident and Problem reporting; and
  - (d) vendor best practice including Citrix vendor support services, quarterly health checks and yearly current state documentation updates and environment audit.
- 14.3** The Contractor will also provide granular Citrix management Services such as:
- (a) management of the existing Citrix NetScaler pair, including:
    - (i) NetScaler appliance management;
    - (ii) NetScaler networking for routing, traffic management, security and SSL; and
    - (iii) NetScaler application delivery including virtual servers, monitors, pools and profiles
  - (b) management of Citrix virtual applications and desktops, including:
    - (i) overall platform management for supporting components such as SQL Database, licensing, delivery controllers and virtual delivery agents;
    - (ii) identity framework including unified access to Citrix applications;
    - (iii) application delivery management;
    - (iv) session and user profile management; and
    - (v) gold image management.
- 14.4** The Contractor will perform a current state assessment of current Citrix environment, mapping out the delivery architecture and how virtual delivery agents deliver desktop and applications to users.
- 14.5** The Contractor will undertake the management of the current on-premises deployment of Citrix.
- 14.6** The Contractor will undertake activities in regard to planning and conducting the transformation from the on-premises deployment of Citrix to a virtualised cloud platform as directed by the Customer.
- 14.7** The Contractor will take into account all required security and governance requirements as well as deliver operations effectively with minimal cost by way of elasticity and infrastructure on demand when delivering the Citrix cloud transformation.
- 14.8** The Contractor will enable and automate capabilities to scale-out and scale-in Citrix cloud based on demand (including both schedule-based scaling and load-based scaling) in order to reduce costs.

- 14.9** The Contractor will fine-tune the virtual delivery agents to be used for application delivery to be compatible with Citrix cloud and extract templates that will be used for base images. This will form the basis of the identity, application delivery, security, performance and availability model in delivering Citrix cloud Services.
- 14.10** The Contractor will prepare the base tenancy in Citrix cloud, including the purchase of relevant products and services, establishing the identity and security model as well as any single sign on requirements and the deployment of relevant servers and agents.
- 14.11** The Contractor will undertake a pilot migration to deliver the Services to a subset of users to perform user acceptance testing at the Customer's discretion.
- 14.12** The Contractor will review usage behaviour and in parallel adjust performance metrics, elasticity and availability parameters so that the platform does not consume unnecessary resources as well as ensure user performance is not impacted by the transition to the cloud.
- 14.13** The Contractor will consider and perform decommissioning tasks required to clean up the existing on-premise environment after transition at the Customer's direction.
- 14.14** The Contractor will provide consolidation of the Citrix licences.
- 14.15** The Contractor's Citrix cloud solution will:
- (a) increase agility with the ability to spin up virtual desktops rapidly based on Customer demand;
  - (b) reduce costs as the management overheads are removed as well as provide the ability to pay for virtual desktops on-demand based on usage; and
  - (c) provide better stability and reliability by outsourcing the support of the underlying virtual desktop infrastructure and management infrastructure to the vendor.

## **15. Customer Responsibilities and Exclusions**

- 15.1** The Customer is responsible for the following:
- (a) ensuring all transitioned platforms and systems are under current vendor support agreements, in a satisfactory operational state, and meet all requirements for DR capabilities. The Customer agrees that if any remediation is required to those platforms or systems (as a result of them not being in such an operational state or meeting those requirements), the Contractor will propose a Change Request for the performance of such remediation work, and the Contractor's obligations under the Customer Contract to meet any Service Levels applicable to such components will be suspended until such remediation is implemented. End-of-life equipment (ie. equipment which is outside of the warranty / repair period of the equipment OEM) will be managed by the Contractor on a 'best efforts' basis and to the extent that a Service Level failure is caused by an issue or defect with that end of life equipment, no Service Credits will apply;
  - (b) the Customer's anti-virus and security management including Identity and Access Management for the existing platforms and systems;
  - (c) the Customer's or its customer(s)' management windows server roles other than DNS and DHCP where these are in scope for the Contractor should they be in use in any transitioned environment. This includes but is not limited to the following roles:
    - BitLocker Drive Encryption (on OS drive - data drives are supported)
    - Internet Storage Name Server
    - Peer Name Resolution Protocol

- Storage Manager for SANs
  - Windows Internet Name Service
  - Wireless LAN Service
- (d) development of custom dashboarding and reporting on the Customer ServiceNow platform;
  - (e) ensuring all required reporting is currently in place for all IaaS, BUaaS and STaaS components, and that these reports meet the Customer's current requirements;
  - (f) installation of all necessary applications to the Citrix Desktop provisioned by the Contractor (noting that this applies only if Citrix management services (as detailed in section 14) are requested by the Customer and an agreed Change Request is executed);
  - (g) providing all Citrix Desktop customisation and test plans where available and on a best endeavours basis (noting that this applies only if Citrix management services (as detailed in section 14) are requested by the Customer and an agreed Change Request is executed);
  - (h) the Customer Application packaging, compatibility testing and remediation of the published applications against Windows Server 2016 and the Citrix XenApp environment;
  - (i) configuration automation and orchestration within the Customer's cloud management platform;
  - (j) implementing Software Asset Management for licensing in the Customer ServiceNow instance(s);
  - (k) configuring the CMP Service Catalogue to support provisioning requirements;
  - (l) configuring all components within the Customer ServiceNow including Cloud Management, Cloud Catalogue, Event Management, Discovery, Service Mapping, Asset Management, and ServiceNow Integration to the Contractor (Customer side of the integration);
  - (m) ensuring DR capabilities are fit for purpose and meet the Customer's current RTO and RPO requirements. No remediation has been factored into the solution. The Customer agrees that if any remediation is required to the Customer's DR capabilities on the basis that they are not fit for purpose or do not meet such requirements, the Contractor will propose a Change Request for such remediation work, and until such remediation is implemented, to the extent that a Service Level failure is caused by an issue or defect with the relevant DR capabilities, no Service Credits will apply;
  - (n) providing any updated security requirements and the Customer will also communicate to the Contractor any changes to the supported Operating System;
  - (o) performing User Acceptance Testing that validates the functionality and usability of Virtual Machines post deployment. (the Contractor will perform Post-Validation Testing that validates the technical deployment prior);
  - (p) using its best endeavours to ensure all hardware support contracts are kept current and all hardware is covered under maintenance, and details of renewal are communicated to the Contractor promptly where available;
  - (q) the overall architecture;
  - (r) management of Application layer on all servers;
  - (s) providing network, security and application management;

- (t) post transition, notifying the Contractor of proposed changes to core processes in the Customer ServiceNow that may impact the ServiceNow to ServiceNow Integration to protect the integrity of the integration and support operational delivery;
- (u) when ServiceNow Upgrades are executed, engaging the Contractor through the upgrade process to ensure solutions are not jeopardised or impacted during the upgrade process;
- (v) ensuring that not more than 5% of the Linux/Unix systems in the Customer's environment will require manual patching. If the scope needs to be increased this will incur a corresponding uplift in pricing for the manual patching service; and
- (w) triaging and escalating through the Customer SOC any alerts that are generated from the public cloud security services (Azure Security Centre, AWS Security Hub).

**15.2** The Contractor is not required to provide the following:

- (a) identity and access management for infrastructure;
- (b) private cloud underlying network, compute and storage infrastructure (unless otherwise directed by the Customer under section 6.10);
- (c) application support and application release management;
- (d) business continuity planning;
- (e) onboarding and offboarding of Contractor resources access to in-scope infrastructure and service management tools;
- (f) administration of physical access for Contractor resources to physical data centre sites;
- (g) cybersecurity management (including vulnerability management);
- (h) security induction including data centre site induction;
- (i) onboarding Customer resources to Citrix cloud environment;
- (j) offboarding Customer resources from legacy Citrix on-premises environment;
- (k) desktop support of the Citrix client;
- (l) financial or physical ownership of the Customer's data centre sites;
- (m) consolidation of Customer's data centre sites; and
- (n) ServiceNow configuration unless otherwise directed by the Customer as a Service Request under section 2.11.

**15.3** The Contractor will perform, prior to or during the Stabilisation Period (as defined in Schedule 3 (Service Level Agreement)), an assessment of the current state of the in-scope Customer environment. If the Parties agree that a deficiency or problem with the environment discovered in the course of such assessment will prevent the Contractor from meeting any applicable Service Level (**Environment Issue**), then the Customer will:

- (a) request the Contractor to propose a Change Request for any remediation work to resolve the Environment Issue; or

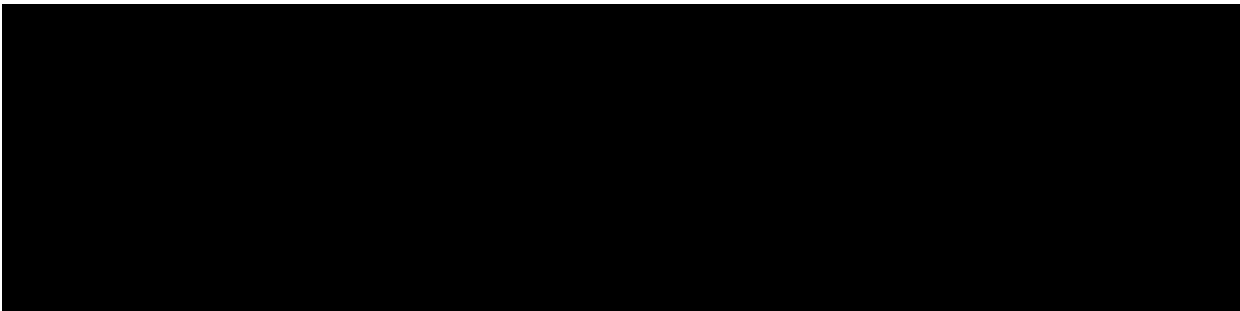
- (b) adjust the relevant Service Level to a level that can be met by the Contractor, notwithstanding the Environment Issue; or
- (c) waive the Contractor's obligation to meet the relevant Service Level.

## Appendix A – Rate Card

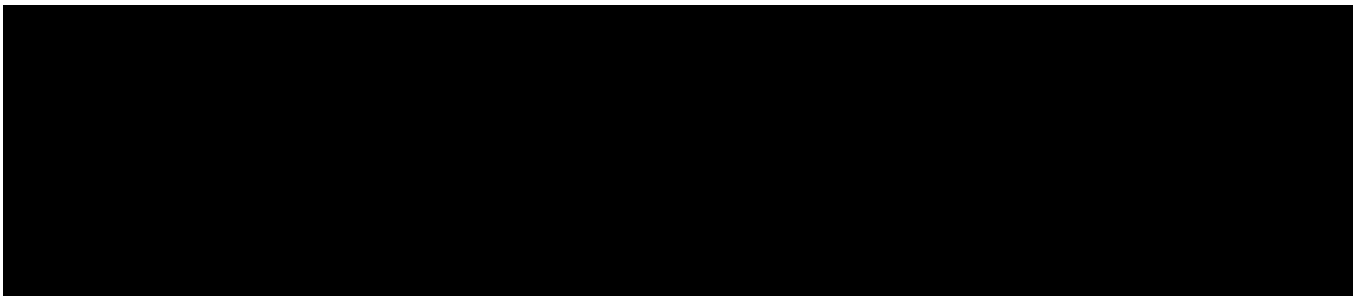
### Standard Rates



### Surcharges



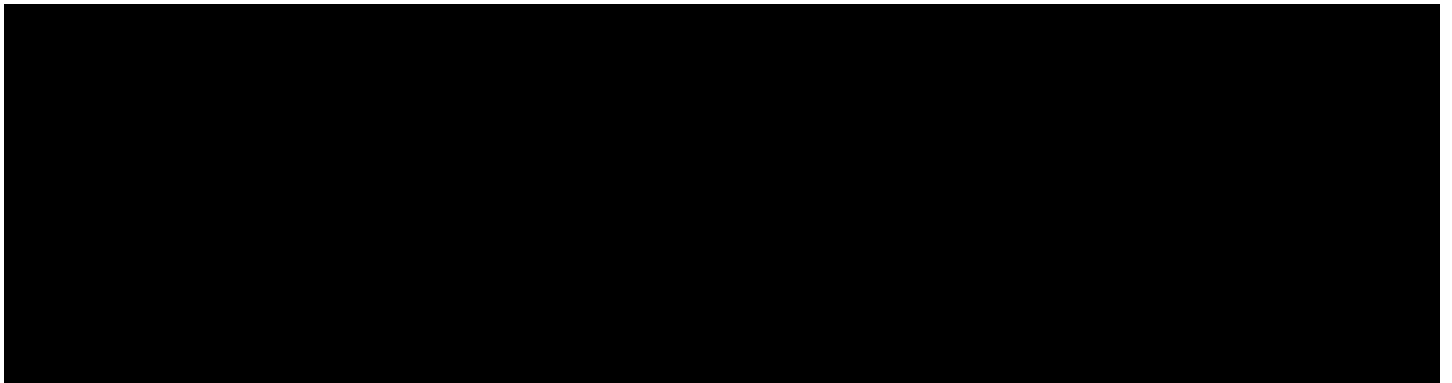
### Minimum Job Times



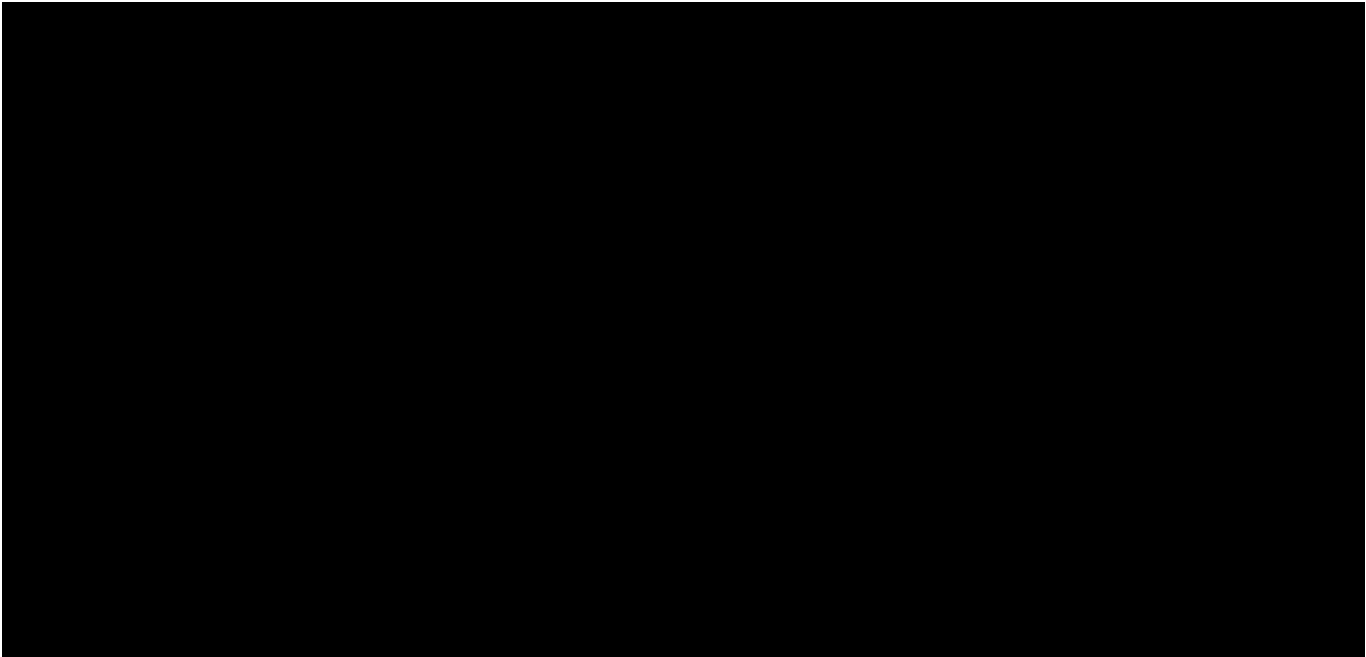
# Exhibit 2A: Computing Integration Services Requirements

<b>Document number:</b> DICT/693541	<b>Date:</b> 16 June 2020
-------------------------------------	---------------------------

## Contact details

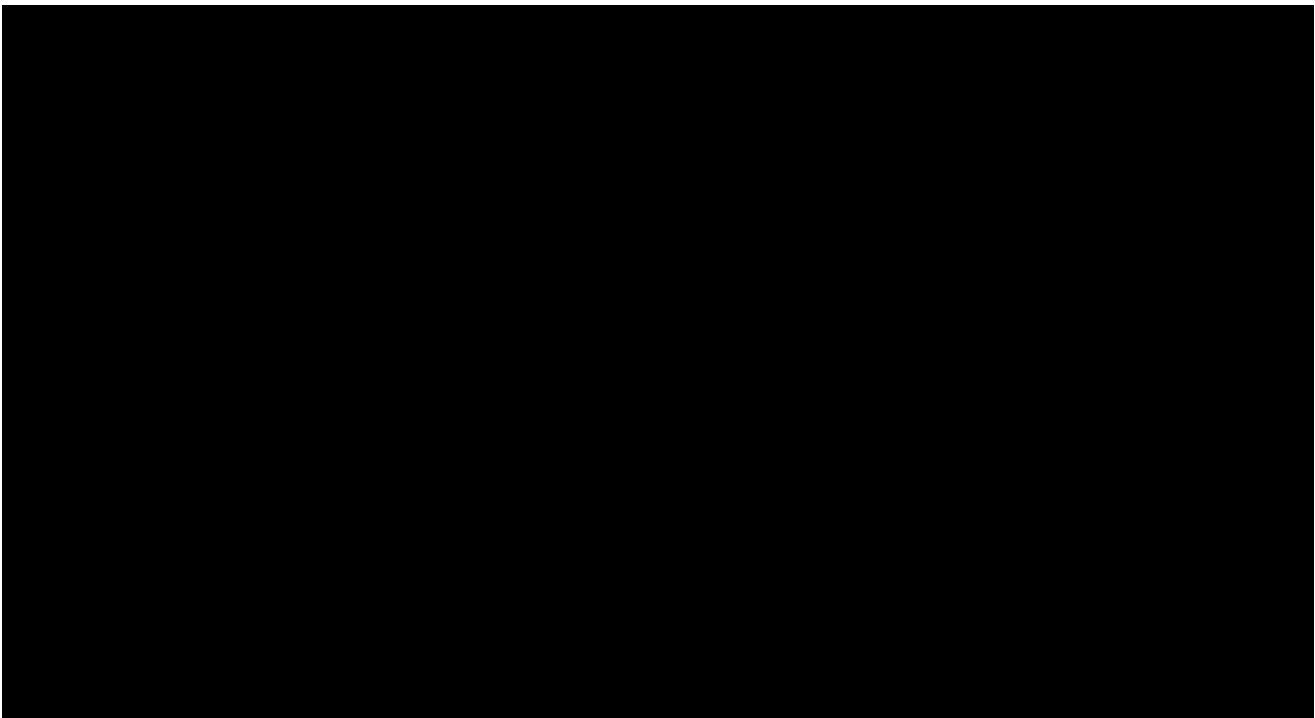






**Revision record**

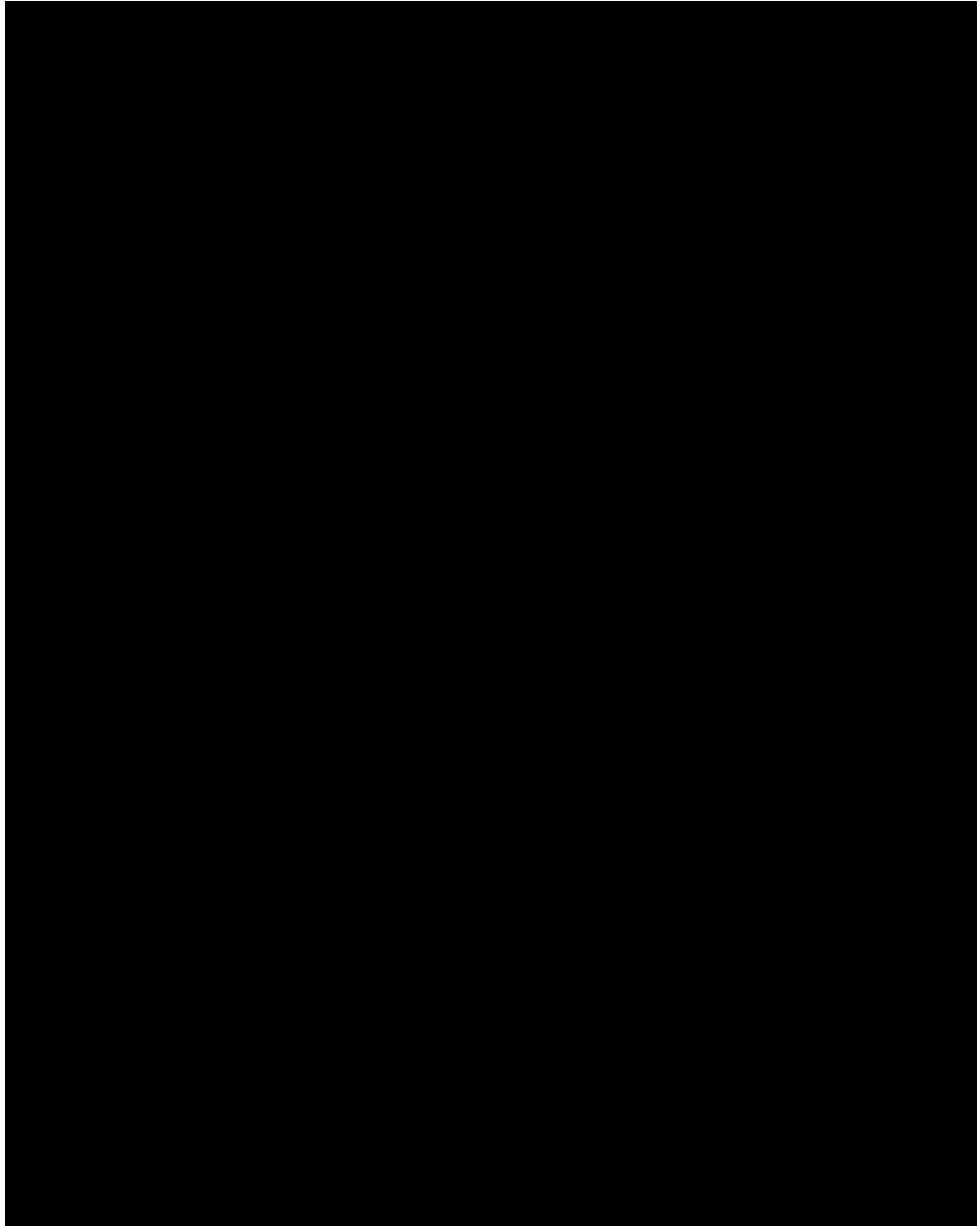
Please note significant document changes with a version increment of 1.0. Minor administrative changes, where the meaning or intention of the document is not altered should increase by an increment of 0.1.

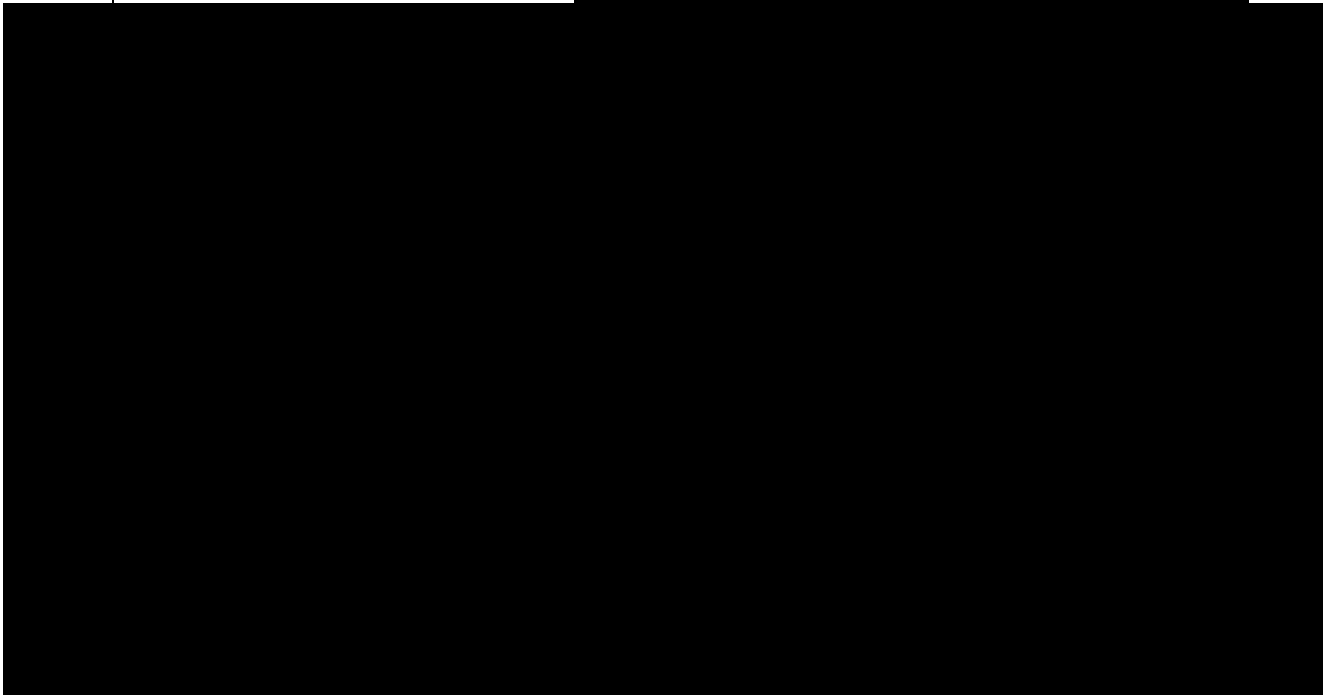
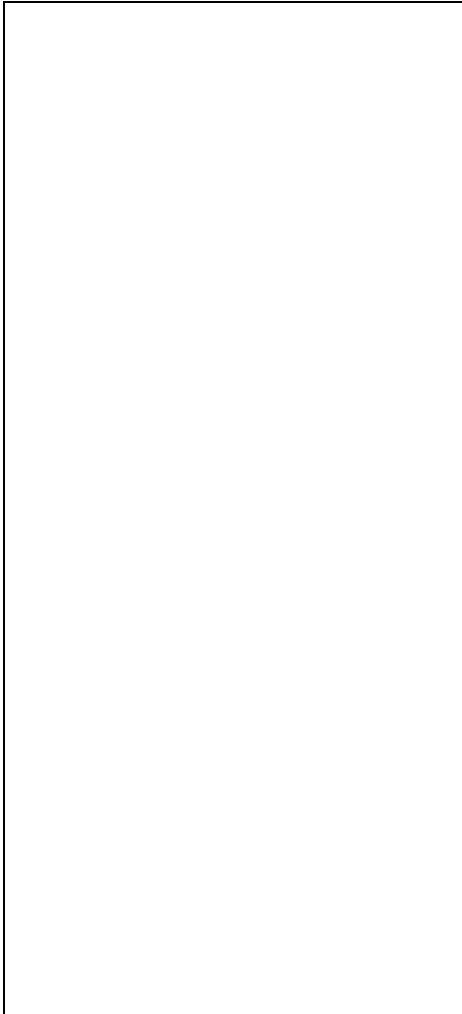


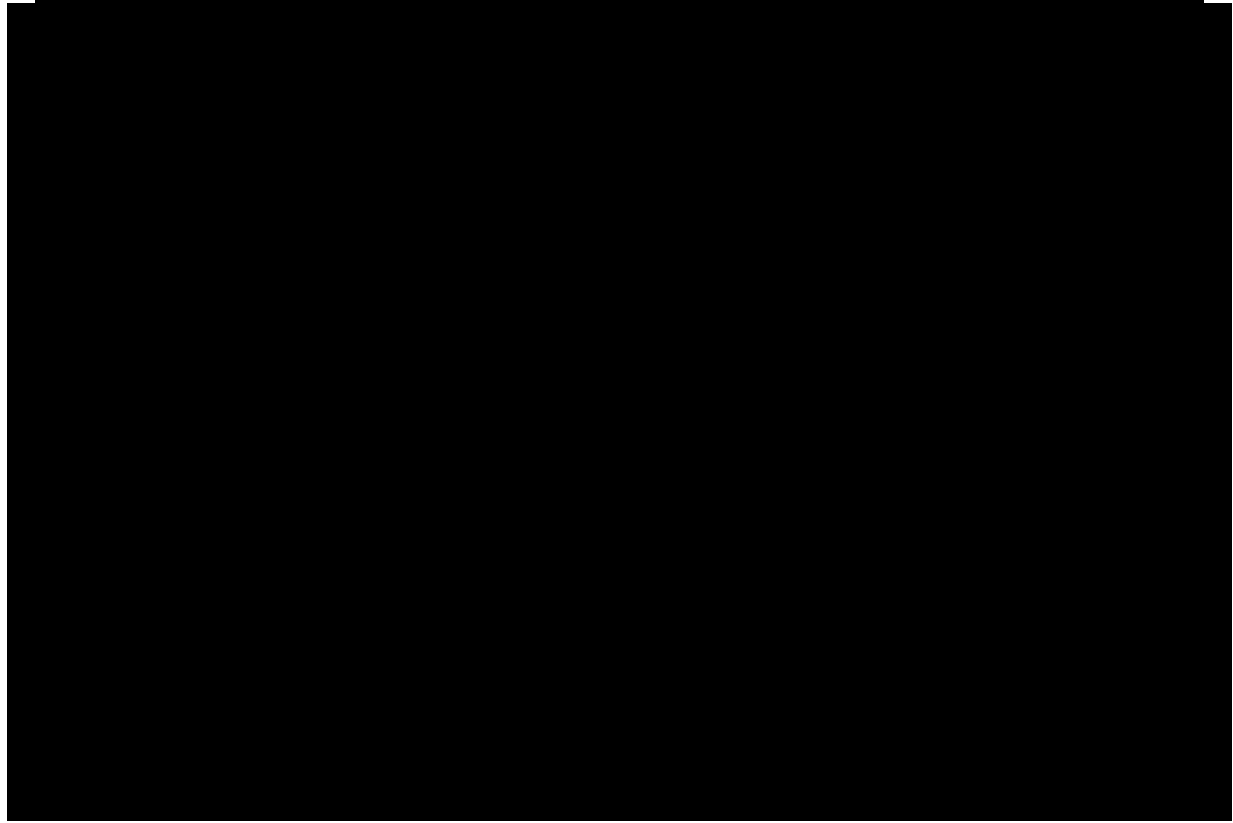
# Table of Contents

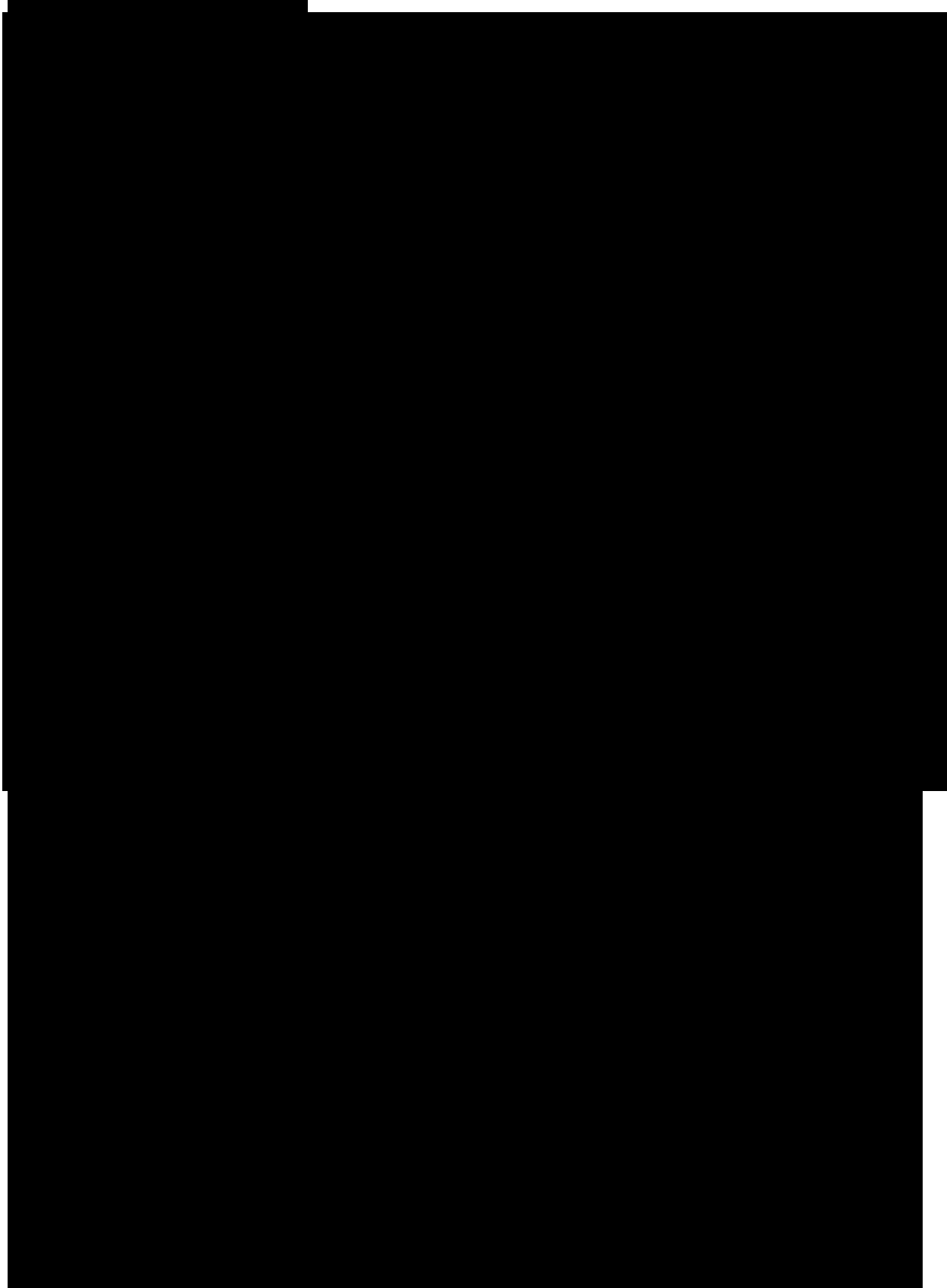
<b>Glossary</b>	<b>4</b>
<b>1. Introduction</b>	<b>9</b>
1.1 Background	9
1.2 Future Approach	9
<b>2. Computing Integration Services Definition</b>	<b>11</b>
<b>3. Current State</b>	<b>13</b>
3.1 Current Consumers of Infrastructure Services / Platforms	13
3.2 Current Environments	13
3.3 Current Device Count	16
3.4 Current Storage Volumes	23
3.5 Current Cloud Services	23
3.6 Current Computing Integration Services	24
<b>4. Future State</b>	<b>26</b>
<b>5. Requirements</b>	<b>28</b>
5.1 Additional On-Premises Infrastructure Support	32

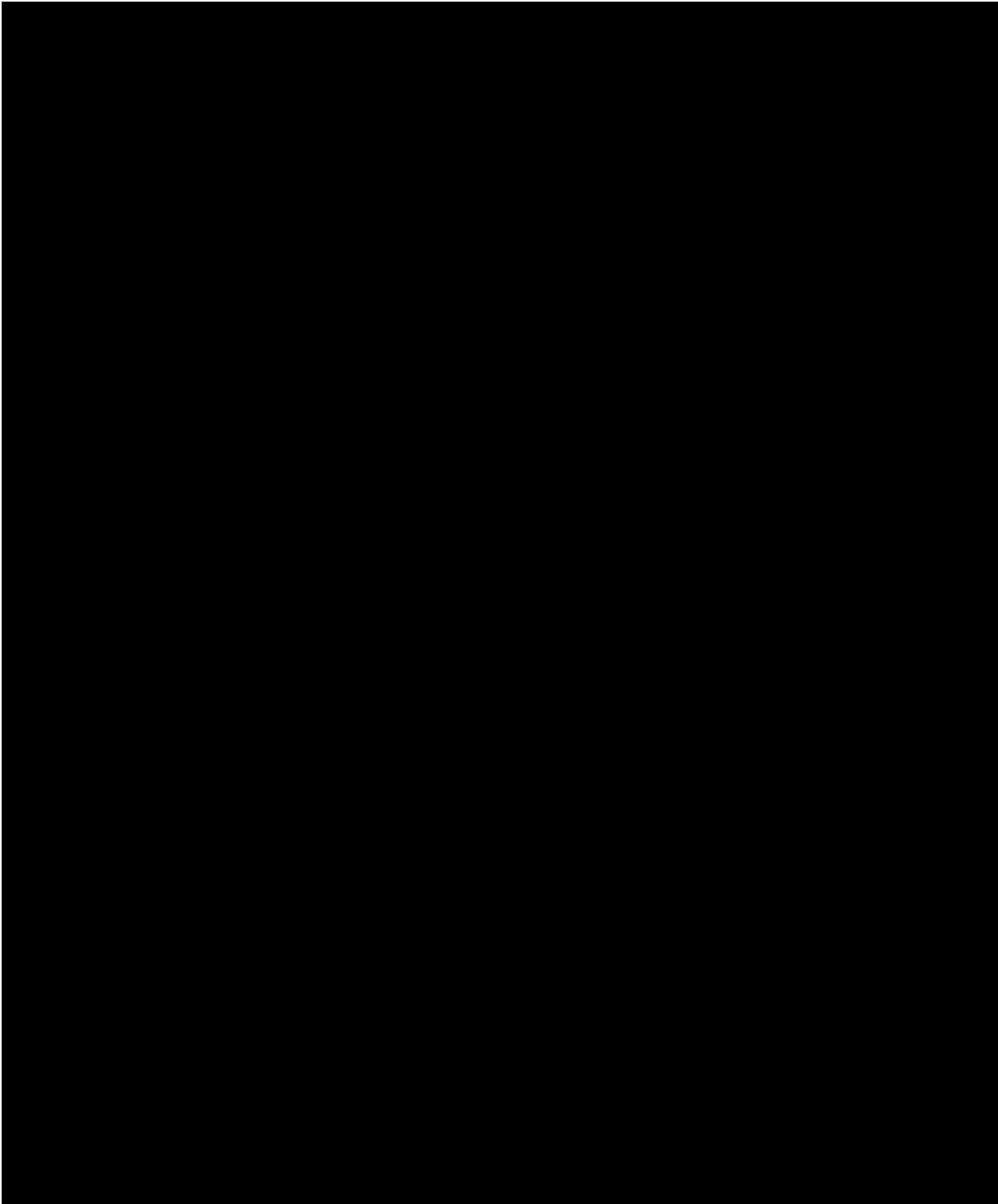
# Glossary











# 1. Introduction

The purpose of this Requirements document is to detail the requirements that will be used in the development of the RFQ document set for the outsourcing of Computing Integration Services (including additional on-premise infrastructure support).

Responses to any RFQ published for the outsourcing of Computing Integration Services (CIS) shall be evaluated against the requirements detailed within this document.

## 1.1 Background

There is a disaggregation of applications and data from single locations to services from many sources: Multiple providers across Private Cloud, Public Cloud, and On-Premises environments. The CTO is aggregating agencies to a single unified architecture.

There is limited interoperability between interfaces and tools are different for each

## 1.2 Future Approach

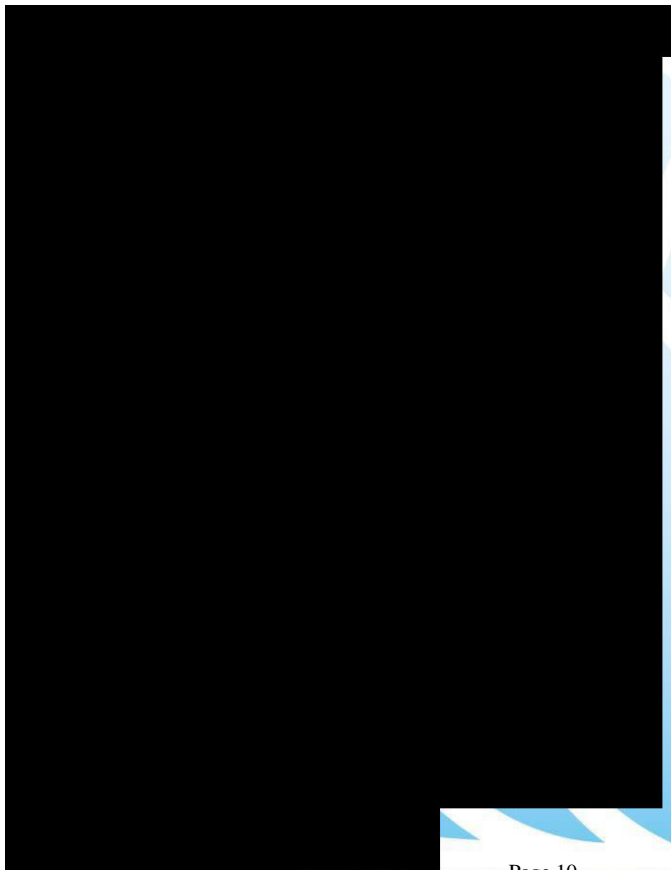
The State's intended future approach to address the issues identified above is to:-

- have the DCS Cloud Management Manager Cloud Services, determine constraints) as to how the CIS provide the infrastructure.
- have the CM Team configure the Cloud Management Platform (CMP) to be in alignment with the governance,



integrated cloud environment designed by the DCS Cloud Centre of Excellence (CCE) and ,

- utilise the CMP tool to facilitate the management of the multiple cloud instances (public, private and hybrid) and the delivery of services such as performance optimisation, cost management, automated macro provisioning and cloud security.
- utilise the CMP to direct the actions and activities of the Supplier who will provision, operate and optimise the State's infrastructure, whilst working within the boundaries and constraints set for them.



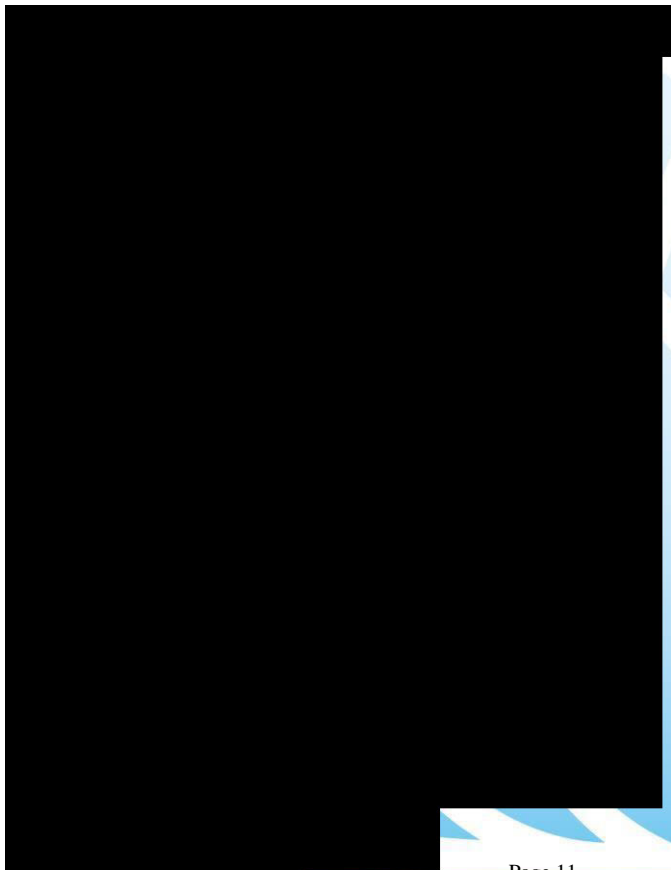
## 2. Computing Integration Services Definition

Computing Integration Services encompasses SysOps and DevOps activities that both operate the environment and present it as a single comprehensive environment to business users.

Computing Integration Services comprises a number of aspects required for the management and optimisation of all centrally served environments. These include environments operating within and across multiple clouds, including private clouds, as well as on-premises environments.

It manages the use of the cloud by the application or service. It does not include the management of the underlying infrastructure that the cloud is provisioned from.

It includes additional on-premise infrastructure support.





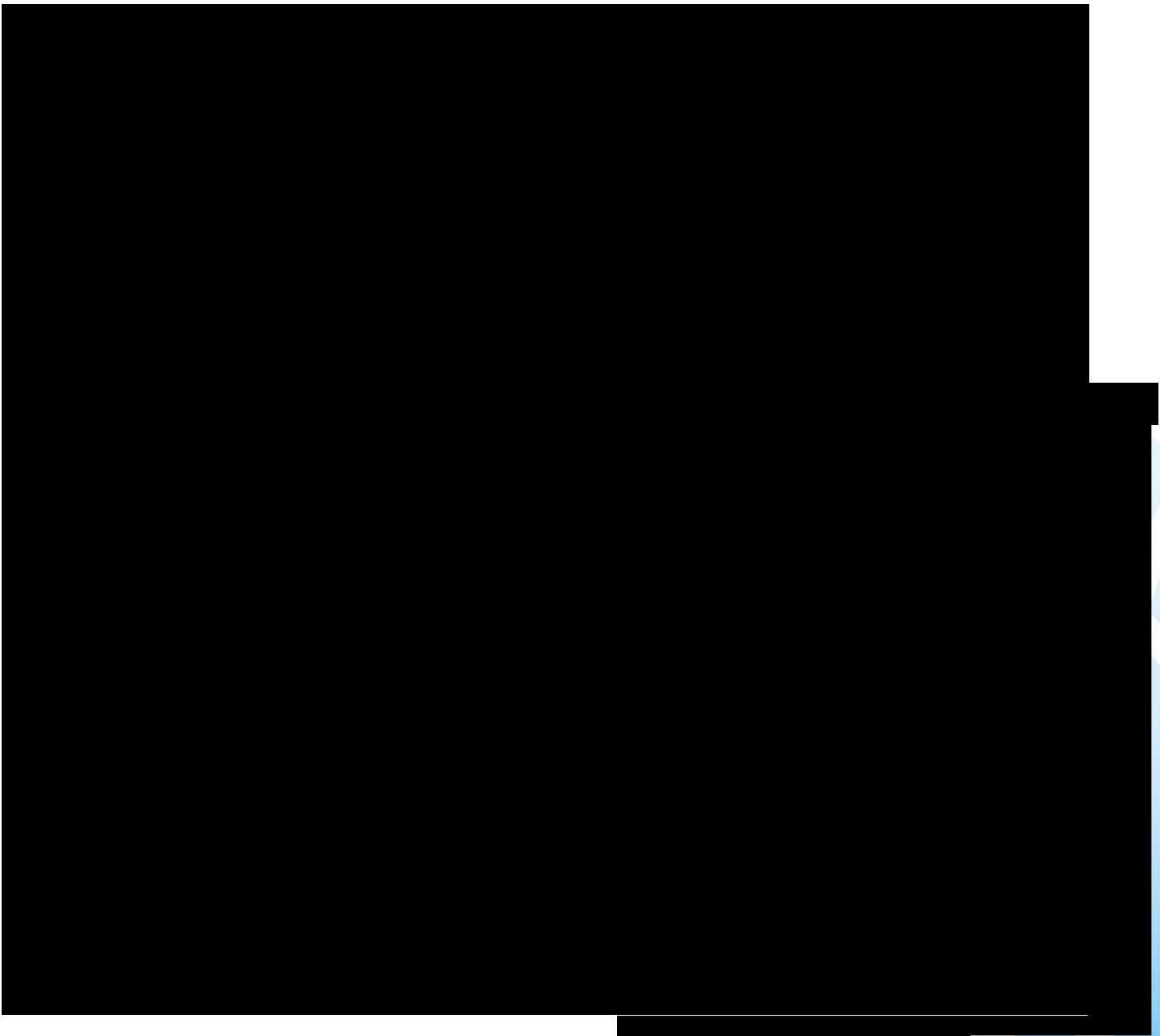
<b>CIS Component</b>	<b>Description</b>
<b>Optimisation</b>	<ol style="list-style-type: none"><li>1. The cloud services are configured to optimise the usage with an objective that would provide the performance appropriate for the task, and it is provided in a cost-effective way that leverages the fees structure for the applicable cloud.</li><li>2. For applications that have software defined infrastructure these activities are largely automated. For other applications the predictive and reactive tasks and jobs undertaken to configure / reconfigure the environment within and across tenancies for an optimal outcome.</li><li>3. For applications that support portability, the reconfiguring could be across multiple clouds (e.g. baseload operating on “on prem” or in a private cloud with a largely fixed cost, with peak activities “bursting” into the identified public clouds)</li></ol>
<b>Data Engineering</b>	Ensuring that data is held in the right locations and accessible for the applications that need them. The extent of this activity is determined by the extent to which data should be accessible to all applications and the level of portability of each application.
<b>Security</b>	<ol style="list-style-type: none"><li>1. Configuring for the identified security posture during deployments and reconfiguring through Optimisation activities.</li><li>2. Specific cloud related security activities as defined by the security strategy and directed by the SOC.</li></ol>
<b>System Integrity Activities</b>	Undertake monitoring, tasks and configurations the ensure that: <ol style="list-style-type: none"><li>1. Ensuring the resilience of the configuration, and individual failures.</li><li>2. Backup and restoration and ensuring the integrity of this.</li><li>3. Ensuring that the services can be recovered in the event that a physical data centre becomes unavailable for whatever reasons</li></ol>

## 3. Current State

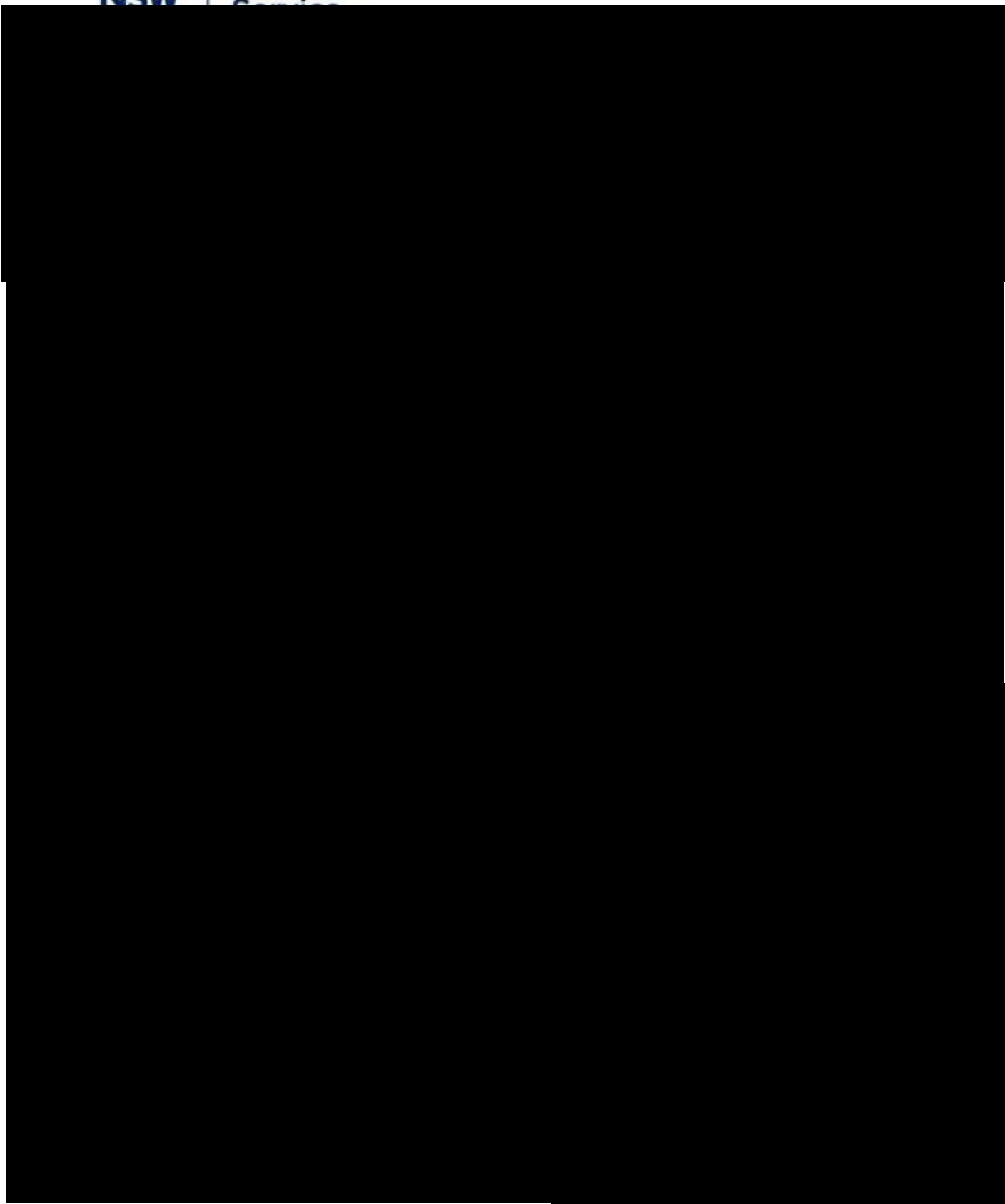
### 3.1 Current Consumers of Infrastructure Services / Platforms

DCS and GovConnect Agencies

### 3.2 Current Environments







### 3.3 Current Device Count

change.

S

D



[Redacted content]

[Redacted content]

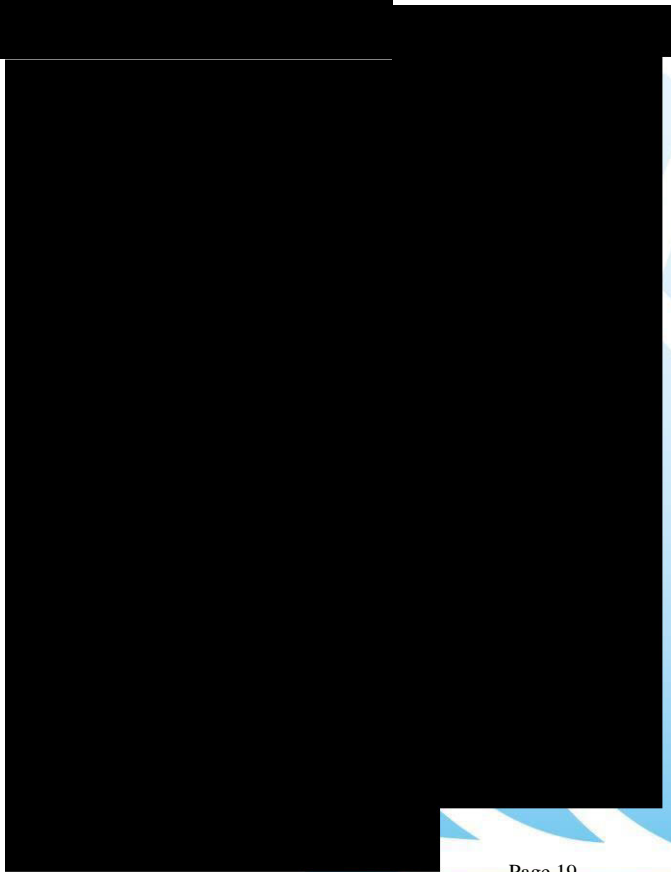
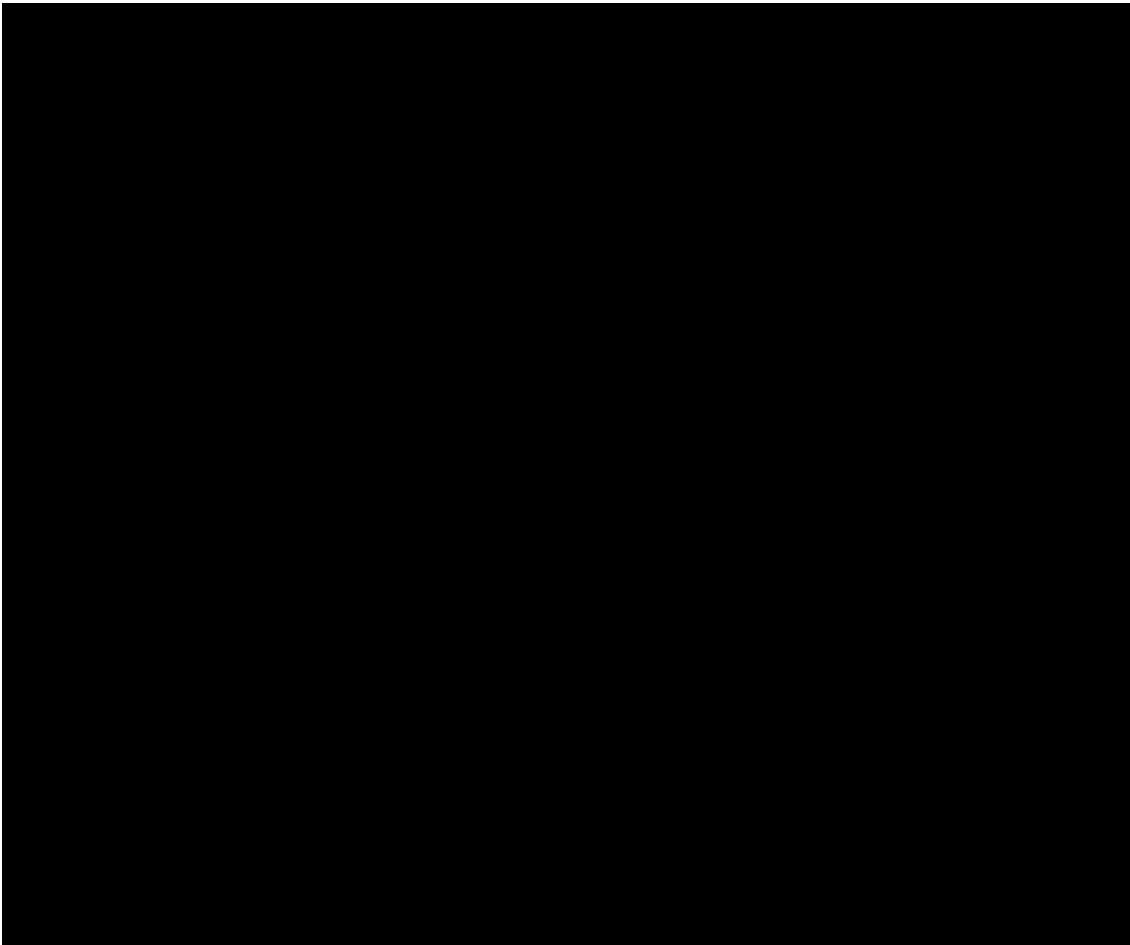
[Redacted content]





[Redacted content]

[Redacted content]





[Redacted content]



[Redacted]

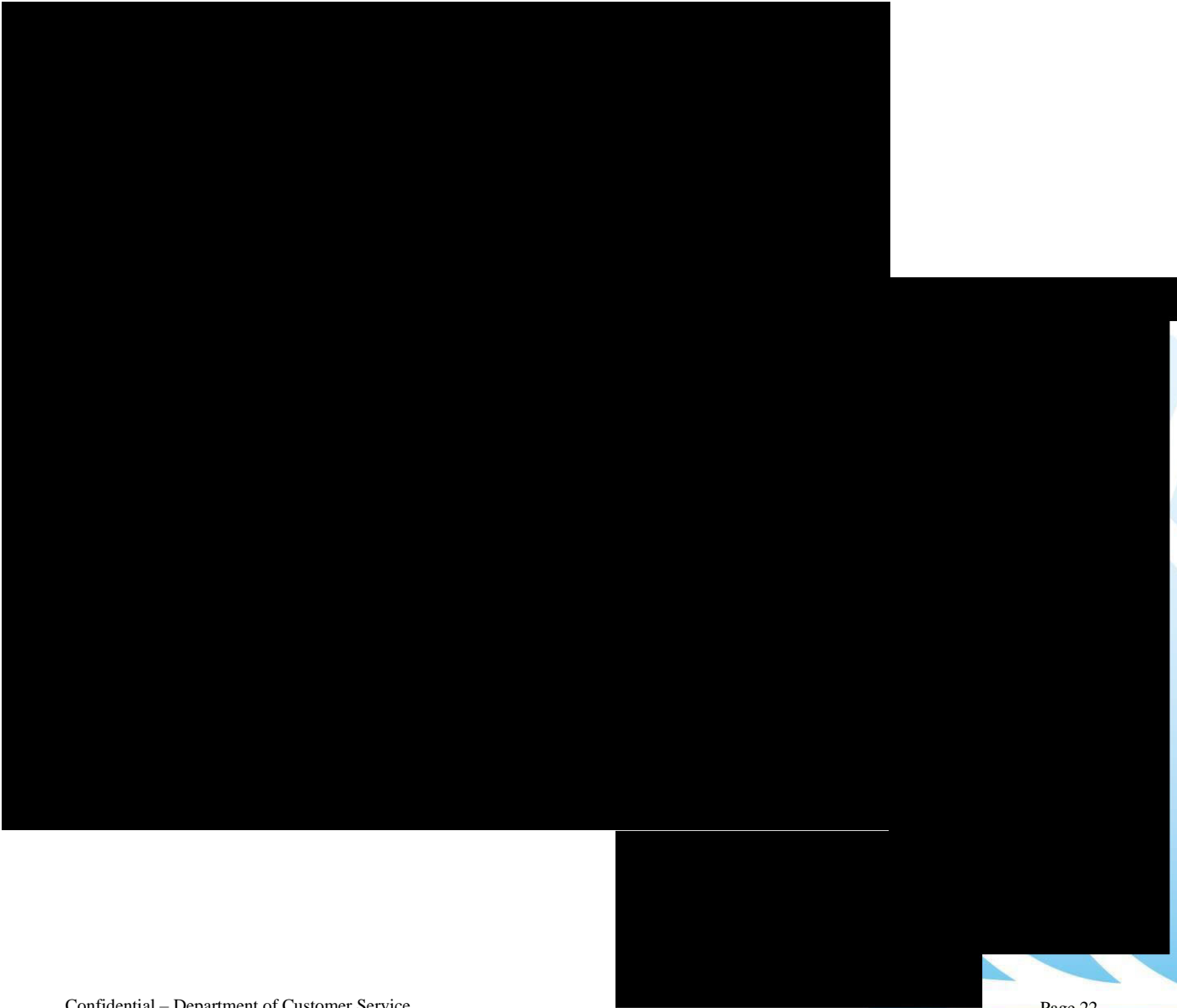
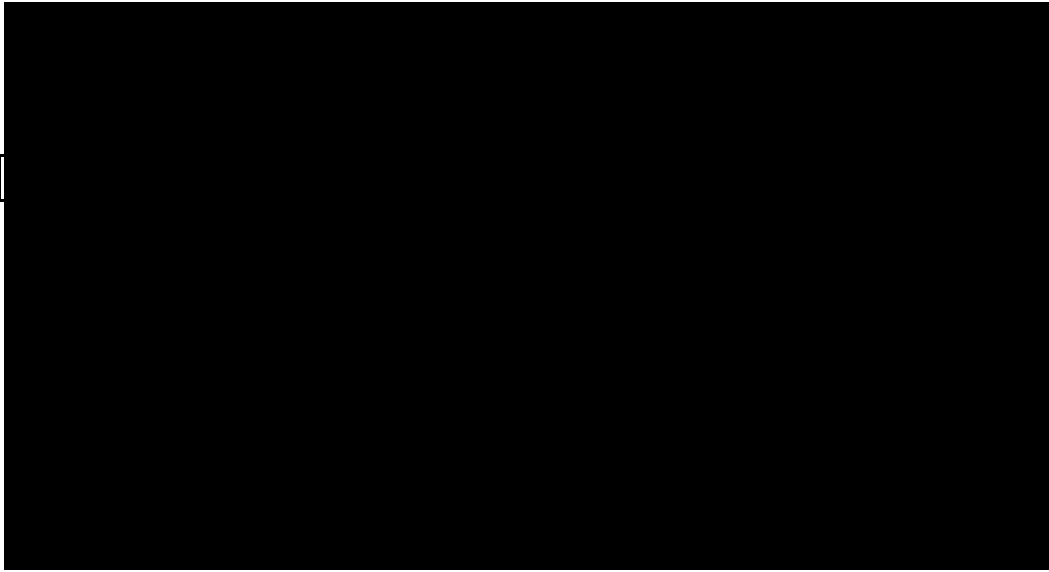
[Redacted]

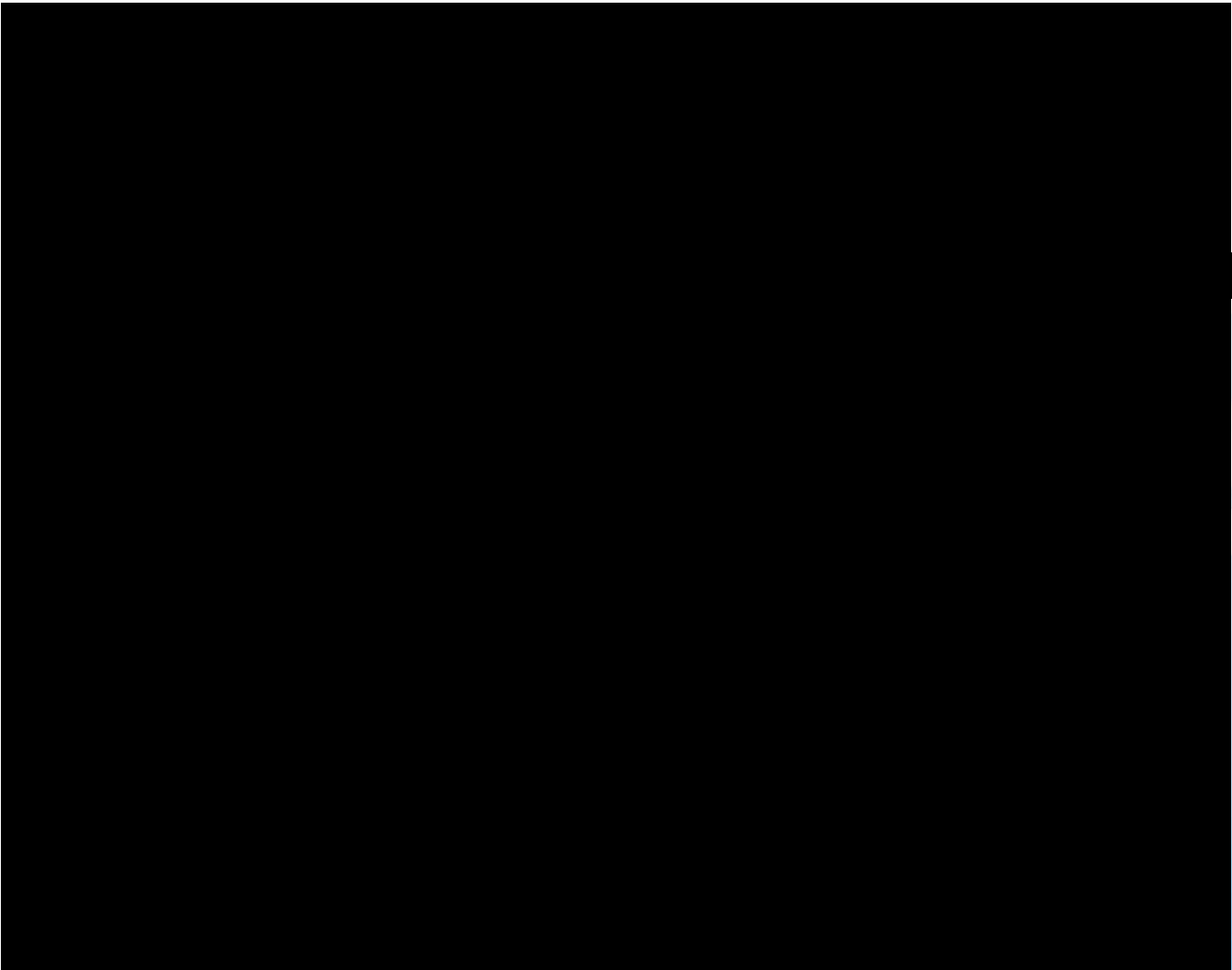
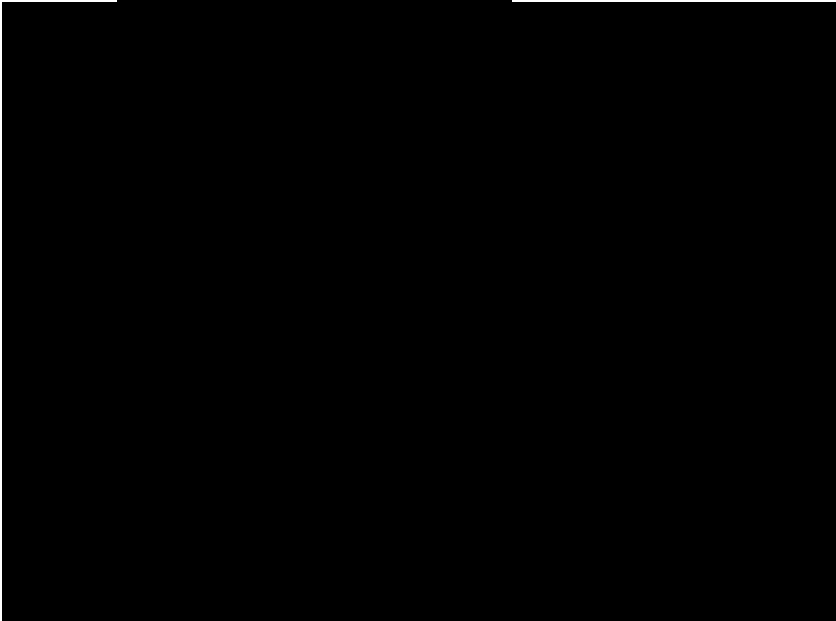
[Redacted]

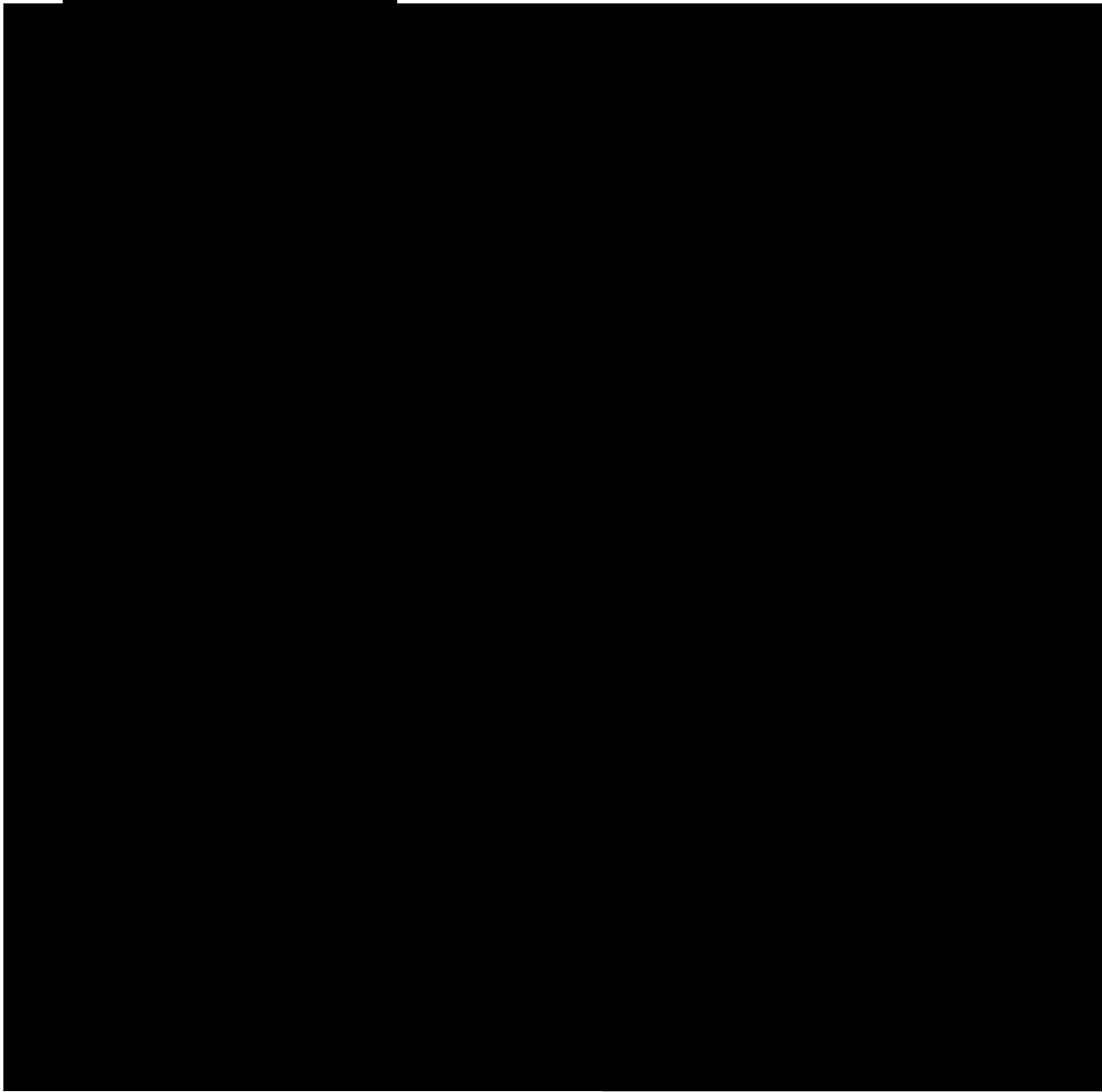
[Redacted]

[Redacted]

[Redacted]

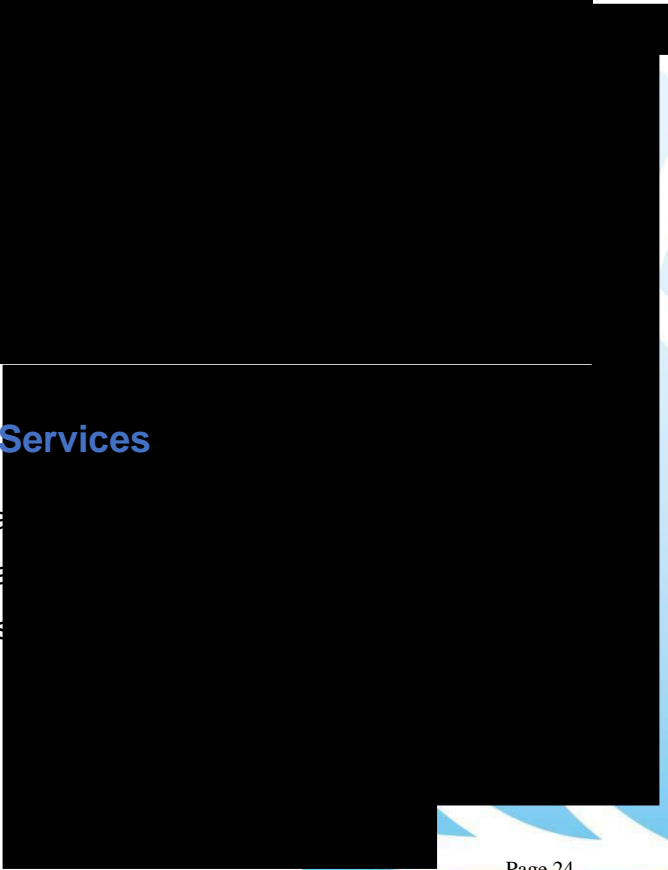






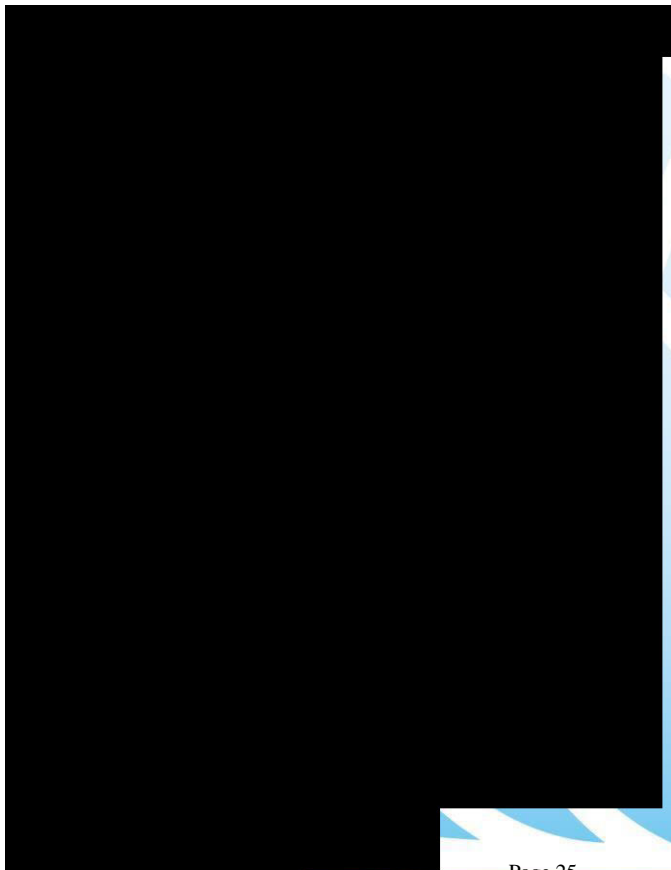
### 3.6 Current Computing Integration Services

Currently IT administrators work to manage cloud and on-premises resources and data across multiple and distinct entities with a process that is prone to human opportunity for error.



SysOps and DevOps activities, in support of the multiple cloud and on-premises environments utilised to deliver the cloud services of IaaS, SaaS, and BUaaS, are not conducted in a manner that sees the environments presented as a single comprehensive environment to business users.

Current practices do not benefit from Computing Integration Services that are enabled by through a CMP.





## 4. Future State

The actions undertaken by the supplier of Computing Integration Services will be done in an integrated fashion across all facets of the services with the view that they will be accountable for delivery to identified outcomes working within the parameters provided by the state through the CMP to:-

- Operate the systems within the integrated environment (public Cloud, Private Cloud or otherwise) providing common access, common security posture and engineer the data across the entire environment.
- Commercially optimise the environment to manage workload so as to be executed in the most cost-effective manner (for portal and transient load enabled applications).
- Leverage the CMP, Cloud native tools, and other traditional CIS tools e.g. DBA tools.

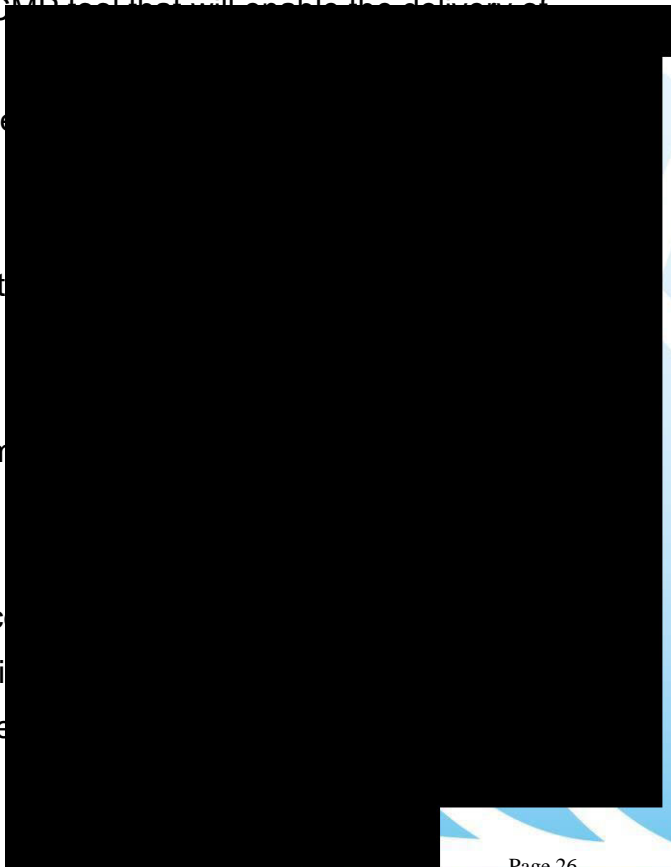
ServiceNow – ITOM will be the State's CMP tool that will enable the delivery of Computing Integration Services.

Discovery will be undertaken with selected ITOM

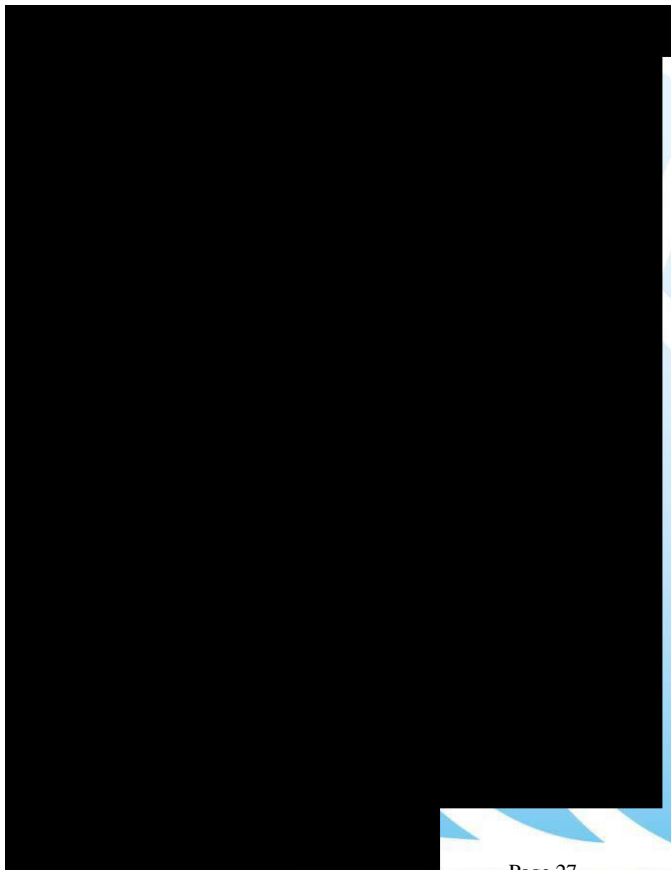
The CMP tool will be managed by the State Manager Cloud Services.

The future state incorporates a transform Citrix to Citrix Cloud.

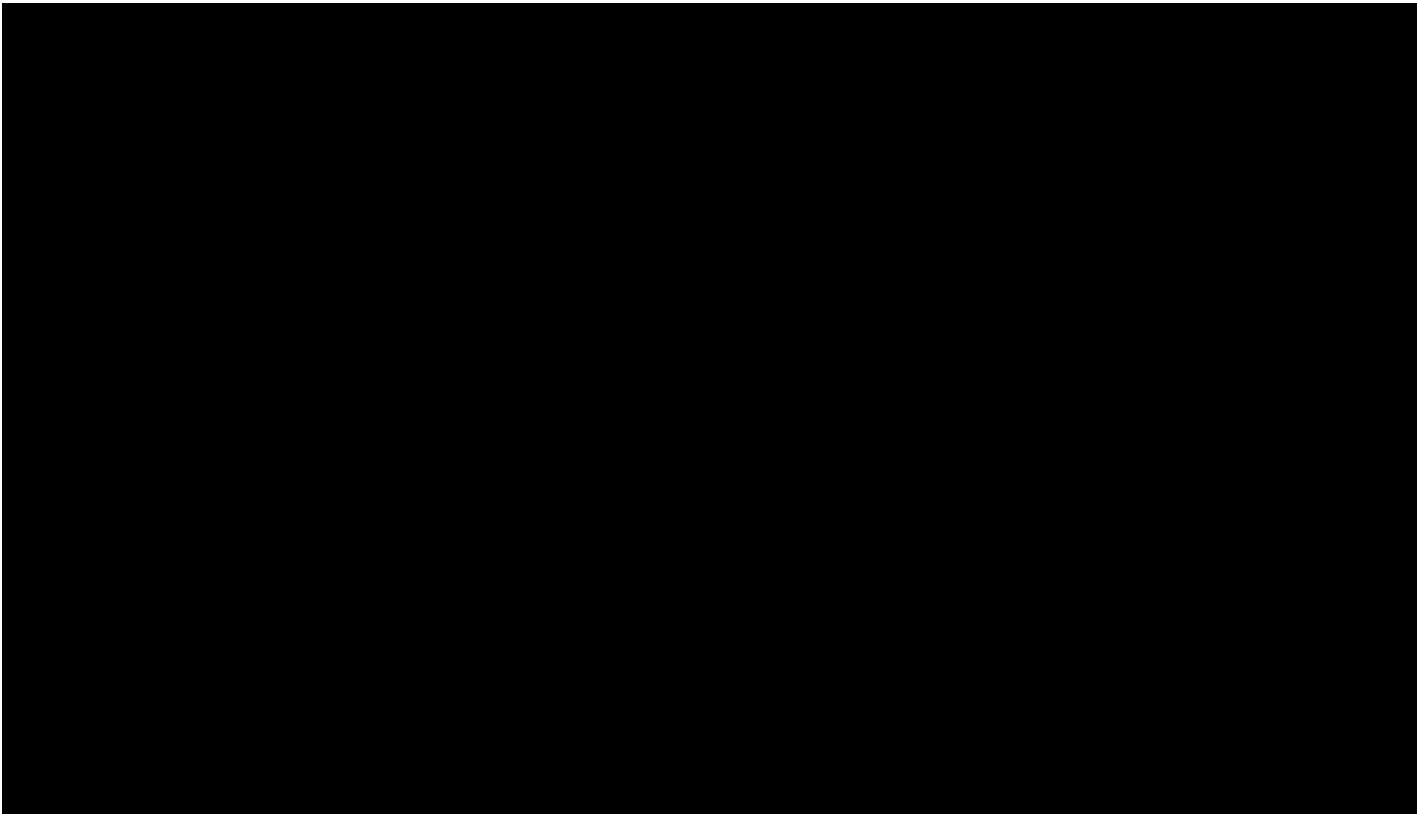
The Transition-In of these services will occur in a DCS environment followed by other DCS environments. Spatial being the key environments to be



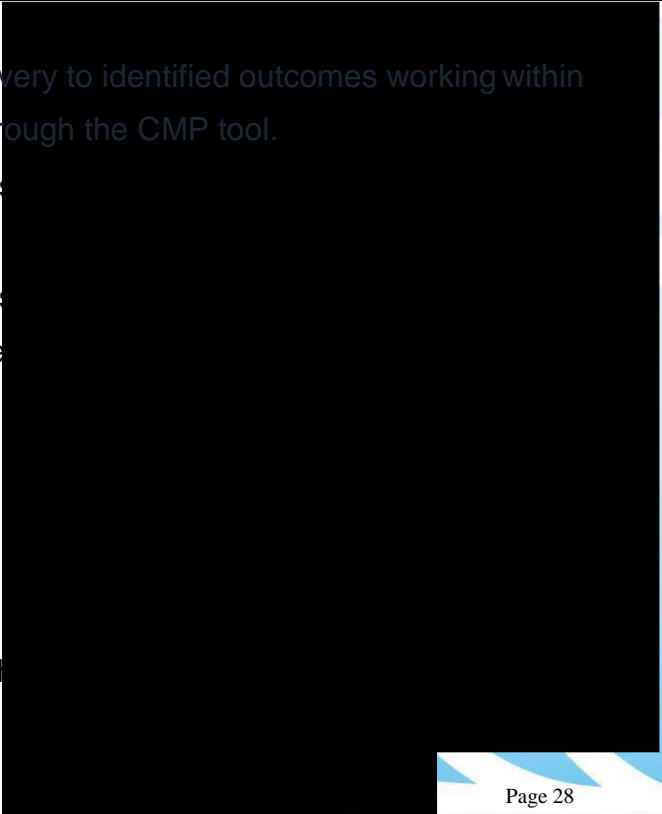
The Strategy with respect to other DCS environments is to transition these into the GovConnect environment.



## 5. Requirements



- The Supplier will be accountable for delivery to identified outcomes working within the parameters provided by the State through the CMP tool.
- The Supplier will undertake actions across the State directed by the State.
- The Supplier will undertake actions across premises environments, delivering to the
  - performance optimisation;
  - improved cost management;
  - automated macro provisioning,
  - cloud security, and
  - capacity management
- The Supplier will engineer and operate the



- The Supplier will manage and conduct operational tasks above the abstraction layer for the entire centralised computing environment.
- The Supplier will leverage the CMP, Cloud native tools, traditional CIS tools e.g. DBA tools to enable the delivery of CIS.
- The Supplier may bring and utilise their own/additional tools, but any such tool must integrate with the State's CMP tool, that any use of their own tools must not detract from the processes implemented by the State's CMP, and the State must have access to these tools .
- The Supplier will align with the State's Change Control processes.
- The Supplier tools must support the following environments:-
  - AWS
  - Azure
  - VMware
  - Others (e.g. Oracle)
- The Supplier will deliver CIS to support and manage the State's Cloud Services offerings:-
  - Infrastructure as a Service (IaaS), (Application as a Service (AppaaS))
  - Storage as a Service (STaaS),(AppaaS)
  - Back-up as a Service (BUaaS) .(AppaaS)
  - Any future cloud service offerings
- The Supplier will provision new instances of CIS as requested by the State.
- The Supplier will provide reporting of production CIS utilization.
- The Supplier must provide regular updates on utilization.
- The Supplier will provide financial management of CIS.
- The Supplier must provide the State with access to the environment and manage the environment.

- The Supplier shall undertake the management of the current on-premises deployment of Citrix.
- The Supplier shall undertake activities in regard to planning and conducting the transformation from the on-premises deployment of Citrix, to a virtualised cloud platform as directed by the State.
- The Supplier is required to deliver DR services above the abstraction layer (Hypervisor) for the entire centralised computing environment. The Supplier is not required to deliver DR services at or below the abstraction layer (Hypervisor) for Private or Public clouds.

### Optimisation

- The Supplier will configure the cloud services to optimise the usage with an objective that they would provide the performance appropriate for the task.
- The Supplier will configure the cloud services to optimise the usage with an objective that it is provided in a cost-effective way that leverages the fees structure for the applicable cloud through demons [REDACTED]
- The Supplier will, for applications other than [REDACTED] infrastructure, undertake the predictive and reactive tasks and jobs to configure / reconfigure the environment within and across tenancies for an optimal outcome. (For applications that support portability, the reconfiguring could be across multiple clouds. e.g. baseload operating on “on prem” or in a private cloud with a largely fixed cost, with peak activities “bursting” into the identified public clouds)
- The Supplier will provide the State with [REDACTED] well as to any constraints or exceptions.
- The Supplier will provide the State with [REDACTED] analysis.

### Data Engineering

- The Supplier will operate the systems within the environment (public Cloud, Private Cloud or otherwise) engineering the data across the entire environment.
- The Supplier will ensure that data is held in the right locations and accessible for the applications that need them.
- The Supplier will enable seamless flow of data and transactions across systems in hybrid environments
- The Supplier will provide regular reports showing that the data is secure, being backed up, and that Disaster Recovery (DR) / Business Continuity Planning (BCP) on the data is available in compliance with the State's policies and direction.

### Security

- The Supplier will operate the systems within the environment (public Cloud, Private Cloud or otherwise) providing common access, and common security posture.
- The Supplier will configure the systems for the identified security posture during deployments and reconfiguring through [REDACTED]
- The Supplier will undertake specific cloud related security activities as defined by the security strategy and directed by the [REDACTED]
- The Supplier will submit and comply with [REDACTED]
- The Supplier will participate in the State's [REDACTED] required and directed by the State.
- The Supplier will apply emergency patches [REDACTED] (Includes infrastructure, database, and application system patching).

### System Integrity Activities

- The Supplier will undertake monitoring, tasks and configurations to ensure the resilience of the configuration, and individual failures. [REDACTED]

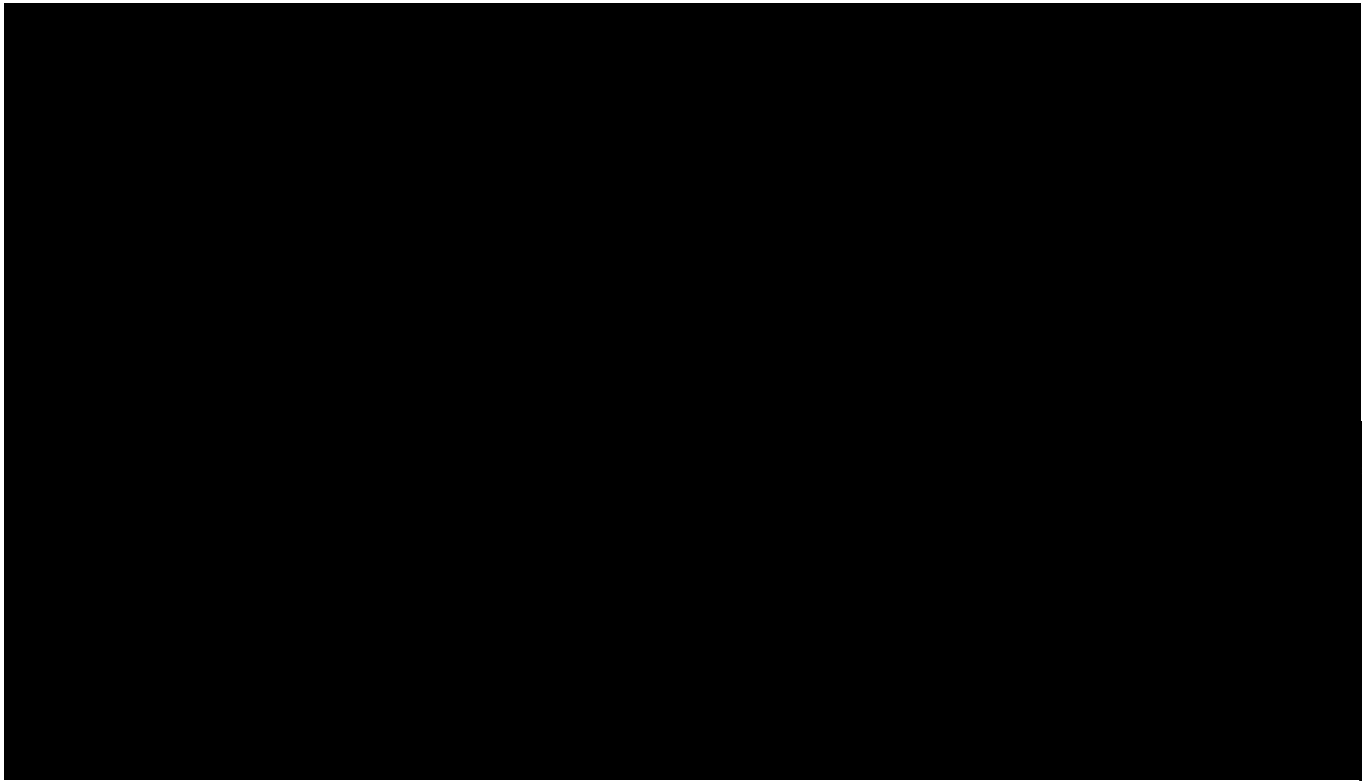
- The Supplier will undertake backup and restoration activities, ensuring the integrity of these data sets.
- The Supplier will undertake activities to ensure that the services can be recovered in the event that a physical data centre becomes unavailable for whatever reasons
- The Supplier will provide the following services in support and management of the BUaaS offering:-
  - a) File System Backup and Recovery Service
  - b) Database Backup and Restore
  - c) Image Level Backups and Recovery of Virtual Machines.
  - d) The ability to Add/Remove/Modify Clients from Backup Services.
  - e) Ad Hoc Backups
- The Supplier will provide the following services in support and management of the STaaS offering:-
  - a) Performing all storage operations in accordance with existing Vendor OEM standards.
  - b) Managing the assignment of volumes.
  - c) Provisioning.
  - d) Monitoring.
  - e) Storage replication.
  - f) Quota management, and
  - g) Performance monitoring for Storage / Attached Storage (NAS) devices.

## 5.1 Additional On-Premises Infrastructure Support

- The Supplier will manage and conduct a range of operational and support activities for The “On Prem” environment at the abstraction layer (Hypervisor) and below, including:



- Hypervisor (VMWare) to provide virtualise the network, compute and storage.
- Monitoring and maintenance often physical equipment (for performance, capacity and breakage).
- Break/fix management.
- Physical engineering / operation (racking / patching / power up / down etc.).
- The Supplier is required to deliver DR services at and below the abstraction layer (Hypervisor) for “On-Prem” environments.





**Appendix A: IaaS**

Begins on next page



# 1. IaaS Description

## 1.1. Services provided by the Supplier

The Infrastructure As A Service (IaaS) is hosted in two data centres GovDC (Silverwater and Unanderra) in which the Supplier will provide and manage resources within the data centre environments.

This solution, includes dedicated services and shared Infrastructure as a Service (IaaS), and is architected around the principle that all data is sensitive and needs to be protected from unauthorised access.

Physical devices are used to create virtualised operating systems that are available for subscription. When a Customer subscribes to this service “compute, network and storage resources” are reserved and available for use. These resources are reserved for the Customer for the duration of the subscription and billed monthly.

The Supplier establishes each virtual server instance from the agreed operating system listing in a Supplier managed facility provisioned in a single data centre to deliver services as per the agreed service level. The Supplier also provides the capability for High Availability, and virtual server replication by providing IaaS instances in two geographical diverse data centres.

For resourcing pertaining to the IaaS environment, the Supplier provides:

- Compute, network and storage capacity as ordered by the Customer

The Supplier allocates and provides access for operating system instances as selected by the Customer.

The Supplier :

- Allocates and provisions the operating system instance for the Customer (hosted environment).
- Allocates the required Storage for the system partition.
- Performs all Server virtualisation activities (from create, manage, monitor, migrate and optimise) as agreed with the Customer.

### 1.1.1. Operating System

Appendix A sets out the operating system software supported by the Supplier.

For each operating system instance the Customer:

- May install components including specific software applications on the operating system instance.
- Will be responsible for providing ongoing licence management of each operating system instance, except where provided by the Supplier (e.g. Microsoft Server) and all Customer components except as such services may be provided by Supplier under a separate Fee-for-Service Option.
- Appendix D sets out the Software Ownership



Custom configurations available on request.

### **Platform Resilience:**

High availability within the data centre is configured as follows

- All Hosts (the underlying infra/hypervisor level) are configured as HA (High Availability) on Hyper-V and n-x (VMware)
- Network, all switches are redundant and multi pathed at hypervisor level.
- Guest Virtual Servers can be configured for HA upon request

Note: This does not include application network failover. This is only applicable if there is a DR plan in place for virtual server with hosted applications

### **Bronze Level Virtual Server (Operating System Only)**

The Supplier establishes a virtual server and storage capacity in a Supplier-managed facility as per the table for operating system virtual server instances, which are then logically provisioned according to Customer demand.

### **Silver Level Virtual Server (Operating System Only)**

In addition to the Bronze Level IaaS inclusions, the Silver Level IaaS offering provides data backup. This backup will be retained as per the backup and retention procedure as described in the Operations Manual.

### Gold Level Virtual Server (Operating System Only)

In addition to the Silver Level IaaS inclusions, the Gold Level IaaS offering provides High Availability (HA) capability in the design as an active-standby model, HA is at the operating system layer and does not include application HA.

### Platinum Level Virtual Server (Operating System Only)

In addition to the Silver Level IaaS inclusions, the Platinum IaaS offering provides High Availability (HA) capability in the design as an active-active model at the OS layer across Silverwater and Unanderra. HA is at the operating system layer and does not include application HA.

Constructs:

Bronze (Single Site)	Virtual Machine	Small Medium Large Extra Large Custom
	Storage allocated to the VM	Tier 2
	Backup Storage (consumed Tier 4)	None Basic Standard
Silver (Single Site)	Virtual Machine	Small Medium Large Extra Large Custom
	Storage (allocated to the VM)	Tier 2
	Backup Storage (consumed Tier 4 and 5)	Basic Standard Advanced
Gold (Active-Passive Virtual Server Replication)	Virtual Machine	Small Medium Large Extra Large

		Custom
	Storage (allocated to the VM)	Tier 2
	Backup Storage (consumed Tier 4 and 5)	Basic Standard Advanced
	Passive Virtual Machine (VM and Storage)	Small Medium Large Extra Large Custom
	Storage allocated to passive VM	Tier2
Platinum (Active-Active Virtual Replication)	Virtual Machine	Small Medium Large Extra Large Custom
	Storage (allocated to the VM)	Tier2
	Backup Storage (consumed Tier 4 and 5)	Basic Standard Advanced
	Passive Virtual Machine (VM and Storage)	Small Medium Large Extra Large Custom
	Storage allocated to Passive secondary VM	Tier 2

### 1.1.3. Storage

Storage for Virtual Services is provided in accordance with the Storage as a Service requirements.

#### 1.1.4. Backup

System and data backups have two distinct purpose. The primary purpose is recovering data that has been lost, accidentally deleted, corrupted or made inaccessible.

The secondary purpose is to recover data from an earlier time, according to a user-defined data retention policy, configured within a backup application for how long copies of data are required.

All services are supplied out of the NSW Government GovDC environments with all offsite storage located within NSW

The Service provides a comprehensive Backup and Recovery Services for Enterprise Servers within the IaaS platform. The backup services are detailed below.

The Backup service features are outlined in the BUaaS requirements.

#### 1.1.5. Network

The Supplier's virtual network is to be logically isolated and will be created to allow secure connectivity to the State's on premise data centers. Virtual networks also allow the Customer to take advantage of the Supplier's infrastructure while providing connectivity to data and applications on premises.

### 1.2. Supplier Supported Components

- a) Infrastructure including virtual machine and operating system;
- b) Network;
- c) Monitoring up to an including the operating system level;
- d) Operating system patching.;
- e) Anti-virus;
- f) Anti-malware; and
- g) Storage.

### 1.3. N-X Services

Except as set out in this paragraph 1.3, the Supplier must provide the Services as set out in paragraphs 1.1 and 1.2 of this document where there is compatibility with the VMWare Hypervisor:

- a) If an operating system becomes N-X:
  - (i) and there is a Managed Third Party Agreement for support in place, the Supplier will provide the Services described in paragraphs 1.1 and 1.2 of this document;
  - (ii) and Managed Third Party Agreement for support is not available, the Supplier will provide up to 8 hours of remediation for an operating system issue. Any additional effort required to remediate the operating system will be subject to a Service Request

### 1.4. Other Services provided by the Supplier

The following list describes the other Service and includes the actions taken by the Supplier in the support of the Service described elsewhere in this document to the Customers:

- a) Comply with approved change and release management policies for server image management.
- b) Develop new server images as agreed between the Supplier and the State.
- c) Maintain the standard image(s) in accordance with the agreed image update schedule.
- d) Notify the State of planned operating system upgrades, that relates to the N, N-1 and N-2 topology.
- e) Others- for example- Produce and maintain design and configuration documentation

### **1.5. The State's Required Inputs:**

- a) Provide advice of any updated security requirements to the Supplier.
- b) Maintain the relevant Microsoft agreement for productivity software as agreed, for example SQL licensing.
- c) Advise the Customer of N, N-1 and N-2 topology changes when advised by Supplier
- d) Provide the VMWare Hypervisor Software licenses.

### **1.6. Customer Required Inputs:**

- a) The Customer is responsible for all Customer provided software including selection, creation, design, licensing, installation, capacity, performance, accuracy, maintenance, testing, as well as requesting backup and support within the requirements specification.
- b) Customer applications must remain compatible to run on operating systems that are at least N-2 (current version minus 2).
- c) Applications supplied by the State or Customers must be maintained at a level that is supported by operating system level N-2. If an operating system becomes N-X, the Supplier will provide the support described in paragraph 1.3 of this document and the Customer must provide operating system licenses for non-Microsoft products.

### **1.7. Optional Services:**

The following Services can be provided under an agreed Statement of Work:

- a) Tailored operating environments
- b) Tailoring of Applications provided by the State or Customers, which are not supported by Operating System N-2 (for example the Supplier will provide a consulting service to the CA or Customers and provide a quote for supporting environments with legacy applications, which may include segmenting the environment from the core network to maintain a secure computing environment)
- c) Disaster Recovery Services can be provided on a Statement of Work, these Services could incorporate the following:
  - DRaaS Assessment
  - DRaaS Implementation
  - DRaaS Ongoing Maintenance
  - DRaaS Disaster 'Event' Recovery

The first part of the Disaster Recovery offering is to perform a "Disaster Recovery Assessment" to evaluate the scope of Disaster Recovery in parallel to understand what can and cannot be delivered. The second part is to craft the roadmap with remediation services and implement the DRaaS solution based on the outcome of the Disaster Recover Assessment. The third part is to update the DR documentation and provide regular tests, to maintain compliance. The fourth part is to recover the services after a disaster event has been declared.

### **1.8. Reports and Deliverables**

As agreed with customer and includes:-

Virtual Server Reporting

- IOPS Performance Reporting (per Tier)

- Capacity reporting
- Optimisation of services – actions/recommendations

## Appendix A – Operating System Software Supported

Standard Images	Microsoft Windows Server Supports .NET
	Microsoft SQL Server
Linux	OpenSUSE
	Red Hat
	Ubuntu
	SUSE Linux Enterprise Server



## Appendix B – Windows Server roles Supported

Windows Server 2012 R2 and later versions are supported for the following roles unless explicitly noted otherwise. The following list will be updated as new roles are confirmed

Windows Server Roles	Active Directory Domain Services
	Active Directory Federation Services
	Active Directory Lightweight Directory Services
	Application Server
	DNS Server
	File Services
	Network Policy and Access Services
	Print and Document Services
	Remote Access (Web Application Proxy)
	Remote Desktop Services
	Web Server (IIS)
	Windows Server Update Services

## Appendix C – Windows Server roles unsupported

Windows Server Roles	BitLocker Drive Encryption (on the operating system hard disk; may be used on data disks)
	Windows Server Failover Clustering, except for SQL Server Always On Availability Groups
	Internet Storage Name Server
	Multipath I/O
	Peer Name Resolution Protocol
	Storage Manager for SANs
	Windows Internet Name Service
	Wireless LAN Service

## Appendix D – Software Licenses Ownership Matrix

Hosted Platform	Hypervisor & License	VM OS & License
N-2	Supplier	Supplier
Legacy	Customer	Customer

**Appendix B: STaaS**

Begins on next page



# 1. STaaS.

## 1.1 Service Description

STaaS delivers a consumption-based storage model for NSW Government.

This Service is an on-premise private solution which supports GovConnectNSW from the GovDC Silverwater and Unanderra data centres. It uses dedicated services hosted on shared infrastructure and is architected around the principle that all of the State's and its Customer's Data is sensitive and needs to be protected from unauthorised access.

The solution comprises the following storage service categories, each category has been designed to cater for different levels of performance and purposes. The below categories supply Customers with various storage performance, pricing and choice options, which will give customers the ability to right size and select volume and storage orders based on application requirements.

The following service tiers available:-

<b>Storage Service Categories*</b>	<b>Performance Characteristics</b>
High Performance	High performance transactional storage designed to meet the requirements of high-speed applications
General Workload	Medium performance storage provides general purpose storage for file services (and any non-high transactional types of service) to support mission critical application data or large capacity requirements.
Backup & Long Term Retention Storage (LTS) Target	Low performance and high capacity storage that is ideal for backup targets, storing long term data and backups, unstructured data, object storage, etc

## 1.2 Service – Storage Options

The storage options available are set out in the table below.

<b>Tier</b>	<b>Service</b>	<b>Performance Characteristics</b>
MS Tier 1	High Performance	High performance transactional storage designed to meet the requirements of high-speed applications
MS Tier 2	General Workload – Mission Critical	Medium performance storage provides general purpose storage for file services (and any non-high transactional types of service) for mission critical application data.
MS Tier 3	General Workload – Large Capacity	Medium performance storage provides general purpose storage for file services (and any non-high transactional types of service) for large capacity requirements solutions.
MS Tier 4	Backup Target	Low performance and high capacity storage that is ideal for backup targets, long term data retention with low access requirements such as archives.
MS Tier 5	Long Term Retention Storage (LTS)	Low performance, archiving, long term backups, object storage, unstructured data for long term retention (LTR and policies)

This service:-

- a) Delivers storage tiers consumable by storage units (one storage unit is 1GB)
- b) Operates seamlessly in the GovConnect environment.

### 1.3 Host Connectivity

The service supports storage connectivity for:-

- Fibre Channel (FC)
- Network File System (NFS) and/or
- Common Internet File System (CIFS)
- Internet Small Computer Systems Interface (iSCSI)

### 1.4 Data Replication

Asynchronous and Synchronous Replication is to be available between GovDCs (Silverwater and Unanderra) and be available upon request.

### 1.4.1 Storage Replication Type

<b>Storage Service Type</b>
No Replication
Local Replication (Native/Recover point) eg single data centres
Remote Replication (Recover point) eg multiple data centres

### 1.4.2 Replication Capabilities per Tier

Storage platform replication capabilities exist. This capability enables Customers to plan and execute Application and Data Discovery processes across Silverwater and Unanderra Data Centres. The following table describes the STaaS characteristics of the service.

Tier	Asynchronous Replication	Synchronous Replication	Storage Array Replication	Host Base Replication	Local HA	Remote HA
High Performance	Yes	TBC	TBC	Yes	TBC	TBC
General Workload	Yes	Yes	Yes	Yes	Yes	Yes
Backup Workload	N/A i.e. Backup is in 1 direction	N/A i.e. Backup is in 1 direction	N/A i.e. Backup is in 1 direction	N/A i.e. Backup is in 1 direction	Yes	Yes
Long Term Storage	N/A i.e. Backup is in 1 direction	N/A i.e. Backup is in 1 direction	N/A i.e. Backup is in 1 direction	N/A i.e. Backup is in 1 direction	Yes	Yes

## 1.5 Supplier Service Management

The services provided by the supplier in support and management of the services include:-

- a) Delivering storage
- b) Performing all storage operations in accordance with existing Vendor OEM standards.
- c) Managing the assignment of volumes.
- d) Provisioning.
- e) Monitoring.

- f) Storage replication.
- g) Quota management, and
- h) Performance monitoring for Storage Area Networks (SAN) and Network Attached Storage (NAS) devices.

#### **1.5.1 Provisioning / Reclamation**

- a) Review storage requests and action or advise as appropriate.
- b) Deallocate and reclaim storage and perform required clean-up of unused files.
- c) Connect new hosts.
- d) Manage encryption keys for all encrypted storage implementations.
- e) Develop, publish and perform processes for managing the file system structures, access, and data life cycles and update documentation as required.
- f) Update and/or interface with billing and operational systems.
- g) monthly reporting

#### **1.5.2 Performance Management**

- a) Analyse workload profile & create performance baseline.
- b) Analyse the workload changes and make recommendations in the relevant monthly report.
- c) Provide data for planning of additional workloads as required.
- d) Provide recommendations to prevent performance issues as required.
- e) Review performance alerts and take required actions, and report to the customer in the relevant monthly report.

#### **1.5.3 Capacity & Optimisation Management**

- a) Patch management monitoring, identify and implement the storage vendor's hardware and software patches, security patches and service



releases in accordance with Original Equipment Manufacturer (OEM) requirements/recommendations. Updates will be implemented during the standard patching window or as agreed with the customer and approved change management processes.

- b) Monitor storage growth and manage the buffer and report on capacity impacts to meet customer demands.
- c) The storage capacity will be able to grow as required by the customer. The supplier's solution is to have flexibility to expand, however there is a committed Minimum Capacity Volume with buffering to support general demand.
- d) Capacity-based water mark for volume increases within the supplier's solution is notionally set to 80% of total available storage capacity at any given point in time (custom requirements may set as required).
- e) Customers will be engaged quarterly to supply a formal 'customer forward storage consumption projection'. This forecast will assist the supplier to actively respond to unexpected storage demands.
- f) If the volume requested is significantly greater than Customer forecasted projections, customers may be required to wait up to 40 Business Days to allow the service to provision additional storage.
- g) Optimise allocated storage and reclaim as required (on monthly basis service will deliver optimisation saving if change is non-outage related, and request approval via CAB where outage may be required to optimise and reclaim storage)
- h) Threshold management with 20-30% headroom will be the service target (case by case consumption available of headroom is possible, but a risk based approach may be taken at the discretion of the State.

#### **1.5.4 Storage Security Management**

- a) Access Management for the storage platform is in accordance with the State's compliance requirements.
- b) The fabric is secured by the use of zoning and secure port authentication. This is a mode of operation that is controlled by the fabric switching and

routing services. The storage platforms will enforce the settings for the Fabric (a Storage Proprietary Network and Protocol)

- c) File-sharing is controlled by system and user security systems, NFS (Network File Services) through the NAS (Network Attached Storage) service.
- d) Data at rest encryption will be provided for Storage under this Service.

### **1.5.5 Miscellaneous**

This service includes the use and implementation of appropriate software / technology capable of delivering:

- a) Encryption and security capabilities.
- b) Storage Optimisation
- c) Deduplication management & optimisation capabilities
- d) Compression
- e) Custom block sizes (non standard can be requested)
- f) Additional Storage Protocols can be requested.

## **1.6 Reporting**

As agreed with Customer.

## **1.7 Support Hours**

As agreed with Customer.

**Appendix C: BUaaS**

Begins on next page



## 1. BUaaS Description

This BUaaS service is designed to protect the Infrastructure and the Virtual Machines in the event of short term data loss. It enables the recovery of the Servers and Virtual Machines within the Infrastructure.

System and Data backups have two distinct purposes. The primary purpose is recovering data that has been lost, accidentally deleted, corrupted or made inaccessible.

The secondary purpose is to recover data from an earlier time, according to a user-defined data retention policy, configured within a backup application for how long copies of data are required.

BUaaS is not to be classified as Archiving & records management to meet statutory regulations under the NSW Government Data and Archiving Act.

### 1.1. Services provided by the Supplier

All services are supplied out of the NSW Government GovDC environments with all offsite storage located within NSW.

#### 1.1.1. Back Up as a Service

The service provides a comprehensive backup and recovery services for Enterprise Servers on infrastructure hosted by the Supplier (IaaS), the State or Third Parties. The backup services are detailed below.

The Supplier provides:

- File System Backup and Recovery Service
- Database Backup and Restore
- Image Level Backups and Recovery of Virtual Machines.
- The ability to Add/Remove/Modify Clients from Backup Services.
- Ad Hoc Backups – Backup management team may be required to perform ad hoc backups. These additional backups will be undertaken with consideration of the existing backup schedule and must be non-intrusive to the regular backup schedule.

#### 1.1.2. Service Plan

Services Plans summarises the proposed Recovery Point Objective (RPO) / Recovery Time Objective (RTO), the protection schedule, the number of backup copies and the retention of backup data. Customised retention cycles are available to meet client needs beyond the standard retention data protection service levels, refer Optional Services below.

- **Recovery Point Objective (RPO)** – This is defined as the roll-back point that will be experienced as a result of the recovery.
- **Recovery Time Objective (RTO)** – This is defined as the amount of time elapsed between failure event and restoration.
- **Data Retention Period** – This defines the policies for data to meet business requirements. Once the data retention period has been reached the data is then migrated to a Long-term backup or deleted. This will be defined by the Customer.

### 1.1.2.1. Image Based Back Up

Image Based backup and recovery is an integrated solution that offers the ability for virtual machines and all associated storage files to be recovered. This allows for server to be recovered after catastrophic failure without the need to reinstall operating systems and applications followed by lengthy data restoration.

- a. A full backup of the whole Virtual Machine (VM) and associated Storage files
- b. Daily within a 14 day cycle.
- c. RPO: Last successful backup within 24 hours
- d. RTO: Last successful backup within 24 hours
- e. Recovery Initiation: Within 4 hours of the Service Request being raised.
- f. Data Retention period: 14 days
- g. Long Term Retention – Not Available
- h. Copies: 2 (Local DC and Secondary DC)
- i. Restoration of the whole VM
- j. Exclusions: Restoration of individual files.

### 1.1.2.2. Agent Based Back Up

While Image Based Recovery offers possible speed on recovering servers in instances of catastrophic failure often a finer grained recovery option is required to recover specific files over longer time intervals.

- a. A full backup of the VM (Agent Based).
- b. Daily within a 7 day cycle.
- c. RPO: Last successful backup within 24 hours
- d. RTO: Last successful backup within 18 hours
- e. Recovery Initiation: Within 2 hours of the Service Request being raised.
- f. Data Retention period: 14 days
- g. Long Term Retention – 13 months or 36 months or 84 months (RTO/RPO do not apply). Any other retention periods are optional services
  1. On Premise (at alternate Data Centre to the Virtual Machine)
  2. Off Premise (Azure)
- h. Copies: 2 (Local DC and Secondary DC)
- i. Restoration at a more granular file level
- j. Retention periods align with the current periods that are provided under the Managed Services. Long term Retention is an option where a checkpoint of the data will be transferred according to the Long-Term retention option selected which is a more appropriate and cost effective storage solution.

### 1.1.2.3. Advanced Agent Based Back Up

Is a service for mission-critical or business-critical application that require quicker Recovery Time Objectives (RTO) and minimal data loss.

- a. A full backup of the VM (Agent Base)

- b. Twice Daily, 7 days a week, 365 days a year (6am and 6pm)
- c. RPO: 12 hours
- d. RTO: 12 hours
- e. Recovery Initiation: Within 1 hour of the Service Request being raised
- f. Retention: 30 days
- g. Long Term Retention – 13 months or 36 months or 84 months (RTO/RPO do not apply). Any other retention periods are optional services.
  - 1. On Premise(at alternate Data Centre to the Virtual Machine)
  - 2. Off Premise (Azure)
- h. Copies: 2 (Local DC and Secondary DC)
- i. Restoration at a more granular file level within the timeframes detailed below.
- j. Retention periods align with the current periods that are provided under the Managed Services. Long term Retention is an option where a checkpoint of the data will be transferred according to the Long-Term retention option selected which is a more appropriate and cost-effective storage solution.

### 1.1.3. **Optional Services**

The additional optional service outlined below can be provided as an extension to the Services described in section 1.1.2.1, 1.1.2.2 and 1.1.2.3.

These Services can be priced on the receipt of a statement of requirements managed through the normal request for change process.

- Data Encryption at rest. Additional customisations for retention cycles can be requested.

## 1.2. **Service Operations**

The following additional operations are performed to establish and operate the Backup as a Service infrastructure:

- perform service activation, agent installation & configuration of the backup toolset;
- monitor, alarm and respond to failure events with protection activities.

## 1.3. **Backup Failure**

A backup failure is defined as a backup that does not complete within the backup window or the backup starts but fails to finish. When a backup process for a server fails, the backup process will be re-run in alignment with the related Services unless otherwise requested by the Customer.

## 1.4. **Restore Method**

The Supplier performs file restorations and recovery functions as part of these Services. Requests for file restores must be made via the Service Request process in advance except in the case of Priority 1 event emergencies.

The Supplier will:

- Plan, establish, and test the restore procedures required to restore files and directories,

in accordance with the customer requirements.

- Plan, establish, and test the recovery procedures required to re-establish the functionality of systems managed by the Supplier in accordance with Customer requirements, in the event of a failure.
- Provide individual file and directory restores in accordance with the pre-defined and established processes and procedures as detailed in CONOPS.
- Provide system restores for the purpose of recovering a system or solving a problem on a system, this may involve the restoration of the operating system, restoration of any applications, and the recovery of data from the last known best available backup.
- Restore principle for a “broken” VM.
  - A new VM instance will be created and the old retained
  - Old VM will be retained for 14 days (unless agreed otherwise)

## 1.5. Reporting

Reporting is a core element of BUaaS and is intended to provide the Customer with a range of information pertaining to the health and performance of the subscribed services.

Monthly Service reports are made available to the Customer and the standard set of reports include:

- Performance success and failure reports
- Time to complete backup reports
- Amount of data backed up
- Number of retention points available
- Number of re-run jobs

## 1.6. Backup Windows

The following table outlines the default backup window that can be selected:

Job Type	Pattern
Daily	between 9:00 PM to 5:00 AM Monday to Sunday
Twice Daily	Start at 6am and 6pm.
Weekly	between Friday 9:00 PM and Sunday 5:00 AM
End-of-Month	The weekend of the first Sunday between Friday 9:00 PM and Sunday 5:00 AM
Continuous	As per RPO/RTO

## **1.7. Monitoring and Management**

The Backup monitoring and management consist of the following:

- Maintaining the backup and restore Infrastructure to meet the backup and recovery objectives as specified in the Service Level Agreement.
- Perform backup administration responsibilities consisting of the installation and configuration of components, scheduling of backups, monitoring of the successful completion of scheduled backups.
- Assist database and application support staff in verifying that database or application backup and restore functions are functional. This consists of working with the support staff to periodically test backup and restore processes.
- Test backup and restore processes twice a year, a report will be generated as a result of the testing.
- Alerts will be configured by a global policy. Alerts will be logged by email and through SNMP Traps.

## **1.8. Service Description Exclusion**

The following services are not included in the BUaaS.

- Business Continuity Planning (BCP) & Disaster Recovery (DR) Services – although backup may be considered an element of both BCP and DR. This service scope is limited to backup only.
- Archiving – Data backups are copies of data used as a recovery mechanism to restore data in the event it is corrupted or destroyed. In contrast, data archives protect and provide access to older information not used in everyday operations, but may have to be accessed occasionally. This service scope does not include archiving.
- Guest OS Support – Guest OS support will continue as provided by delivery teams and no additional cost items are required.
- Workloads not supported– incompatible backup workloads will be identified and excluded from this service.
- Remote Site Backup – Remote or Branch Sites are excluded from this service.
- Desktop – End User Backup – End User end point devices are excluded from this service.
- Exchange – Exchange and Mailbox backups are not part of this scope.

## **1.9. Customer Required Inputs:**

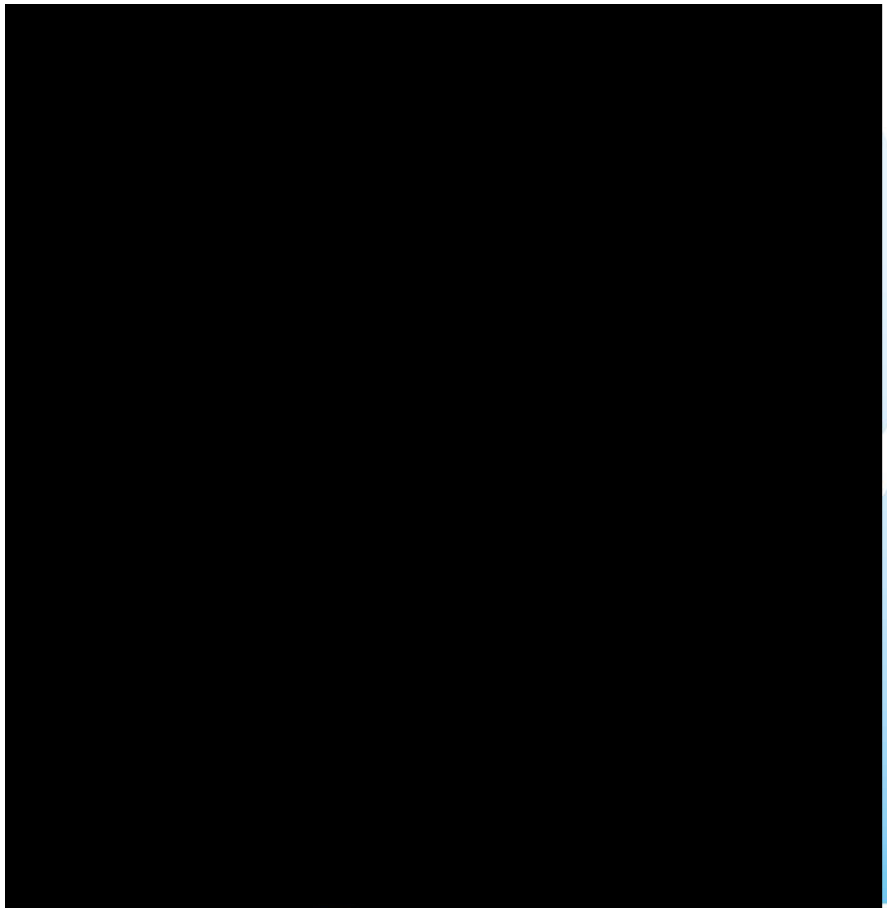
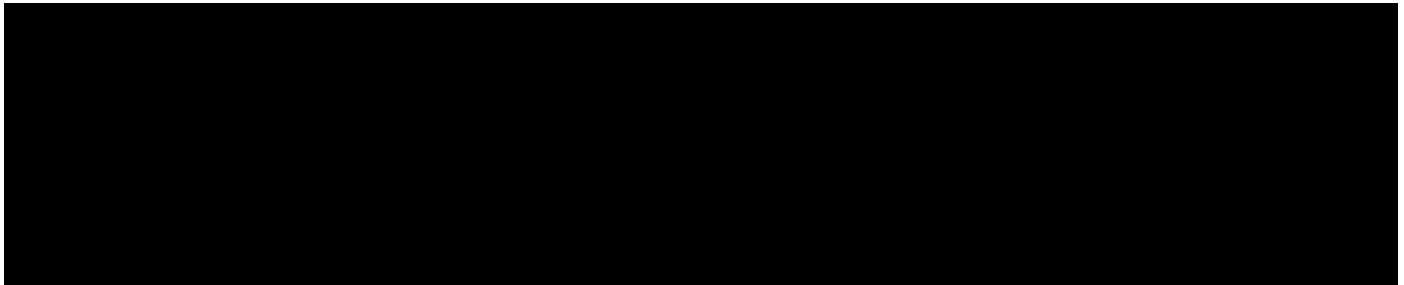
- a) The Customer is required to select the Service Plan and the window for scheduled back up for each VM.

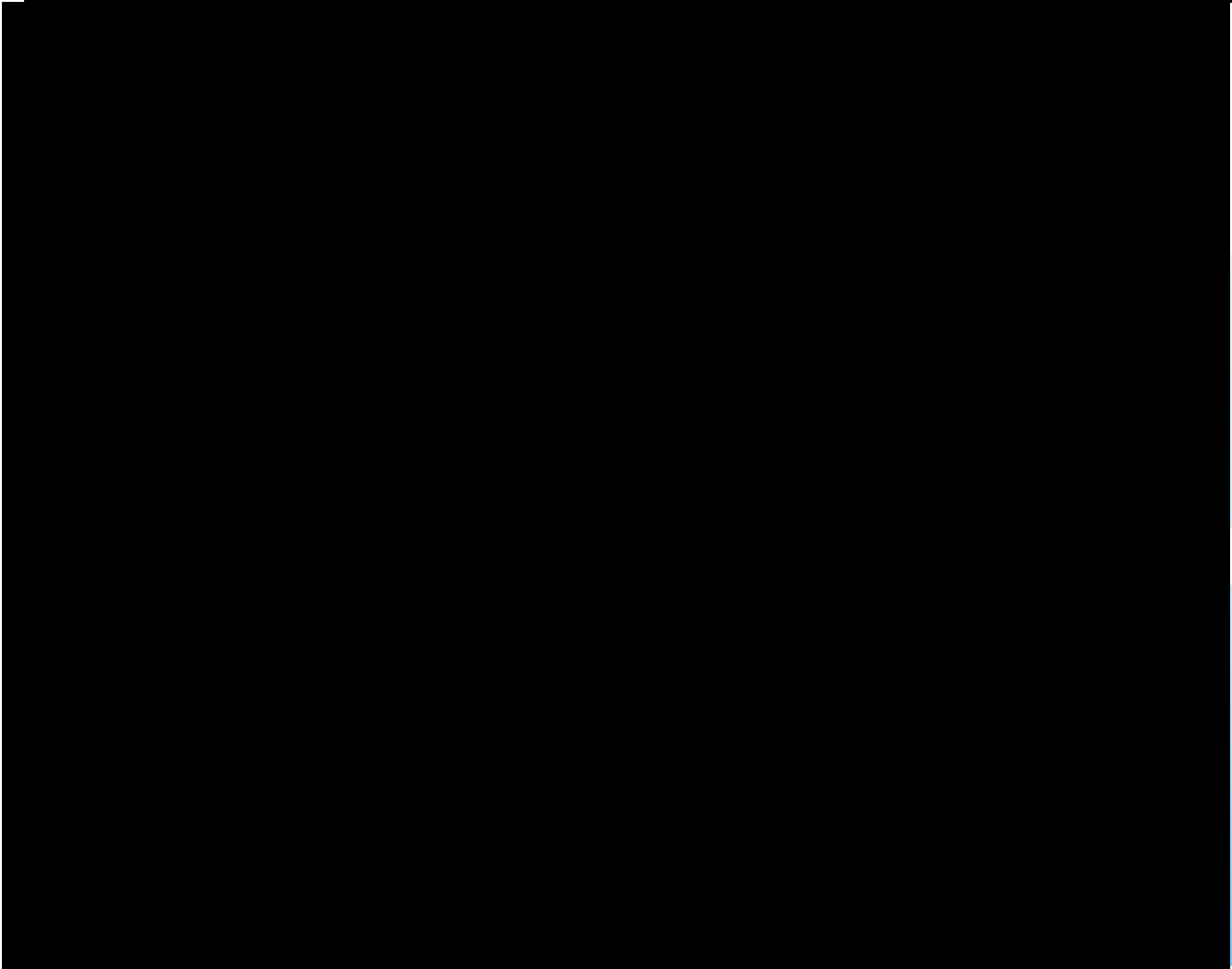
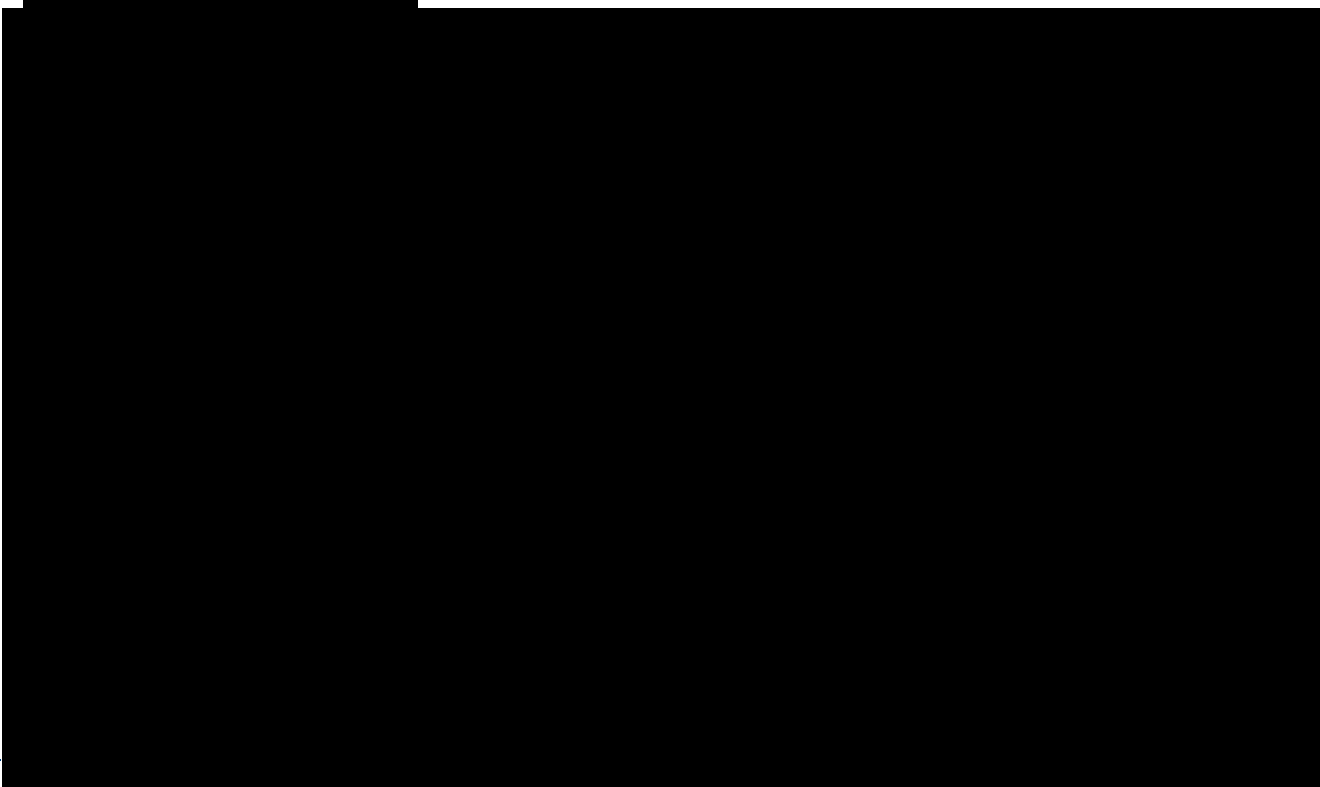


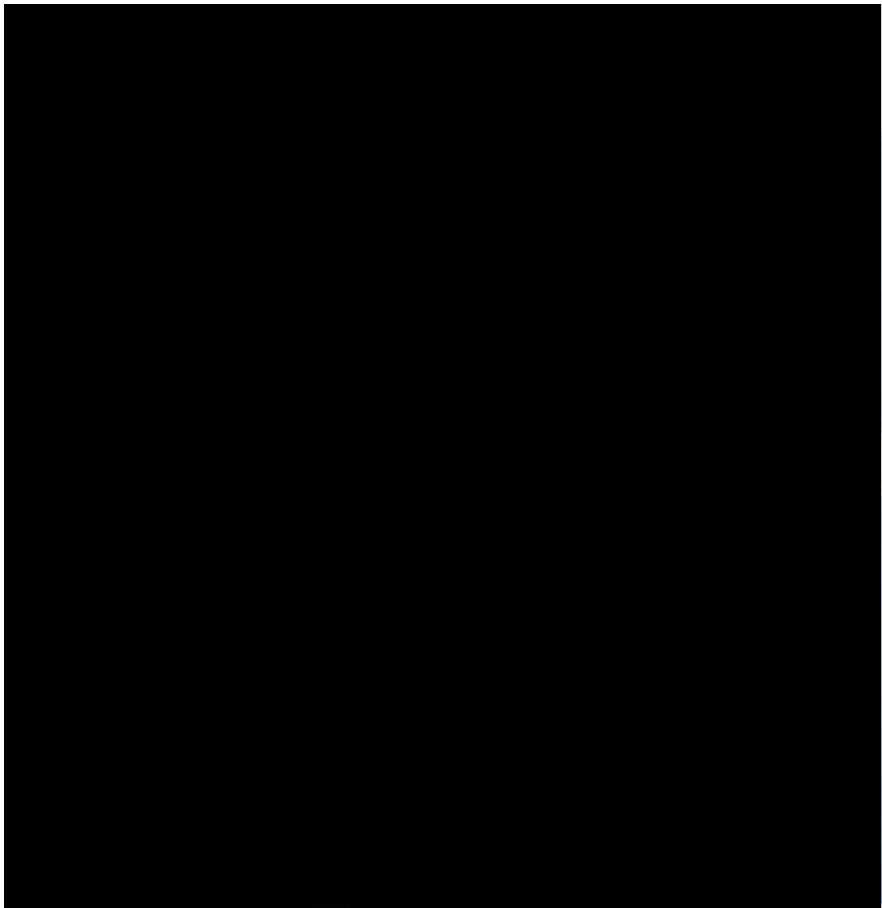
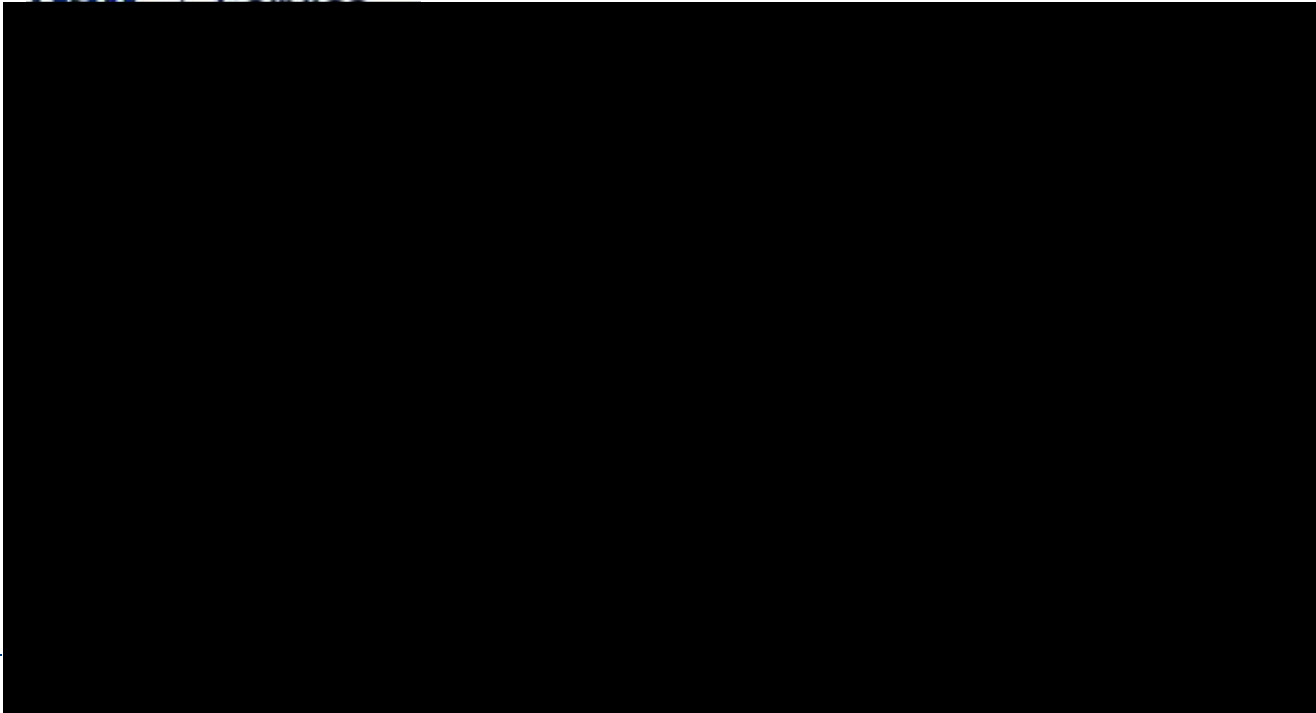
# Exhibit 2B: DCS CIS Outsourcing Scope/Functional Requirements

<b>Document number:</b> DICT/693541	<b>Date:</b> 21 August 2020
-------------------------------------	-----------------------------

## Contact details







# Table of Contents

1.	<b>Executive Summary</b>	5
2.	<b>Introduction</b>	7
3.	<b>Proposed Transition Phases</b>	8
4.	<b>Outsourcing In-scope</b>	9
4.1	Production Services	9
4.2	IT Audit and Discovery	10
4.3	Production Services with High Availability (HA) capabilities	10
4.4	Disaster Recovery Services	10
4.5	Hosting Infrastructure Support/Management	11
4.6	Contributing to the DCS Cloud Centre of Excellence	12
4.7	Storage Services (excluding the underlying cloud compute storage)	13
4.8	Backup/Restore	
4.9	DBA Support	
4.10	CITRIX Service	
4.11	Service Manager	
4.12	Optimisation	
4.13	Integration	
5.	<b>Outsourcing Out-of-Scope</b>	
6.	<b>Appendix A – DCS SIAM</b>	
7.	<b>Appendix B – CIS Outsourcing</b>	

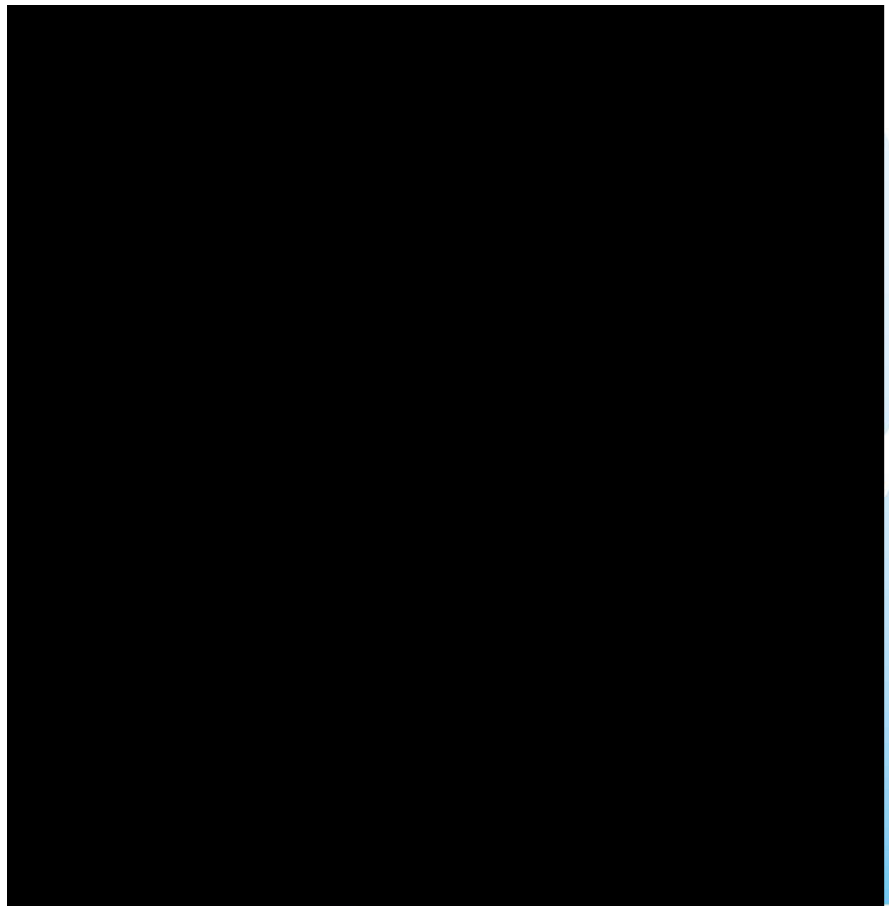
# 1. Executive Summary

Please refer to Appendix B for the CIS Outsourcing Context Diagram

## In-scope for outsourcing:

- Event monitoring, support, capacity management, backup and attending break-fix for:
  - Underlying compute and storage infrastructure (on-premise only)
  - Hypervisor infrastructure (public/private cloud, on-premise)
  - Physical servers, VM's infrastructure including operating systems, CPU's, GPU's, storage
  - Databases and database clusters including ongoing performance tuning
  - Node infrastructure (on-premise and private cloud only)
- BAU patch management and firmware upgrades of the fleet of physical servers and VM's including the prioritisation of emergency patches when the need arises
- BAU database versioning
- Development/management of VM types including V
- Provisioning new VM
- Application Service(s) participation in DR te
- Optimisation:
  - Right sizing o
  - Managing op
  - Managing dat
  - Managing CI
  - Managing bac
  - Managing dig
  - expired and s
- Service management

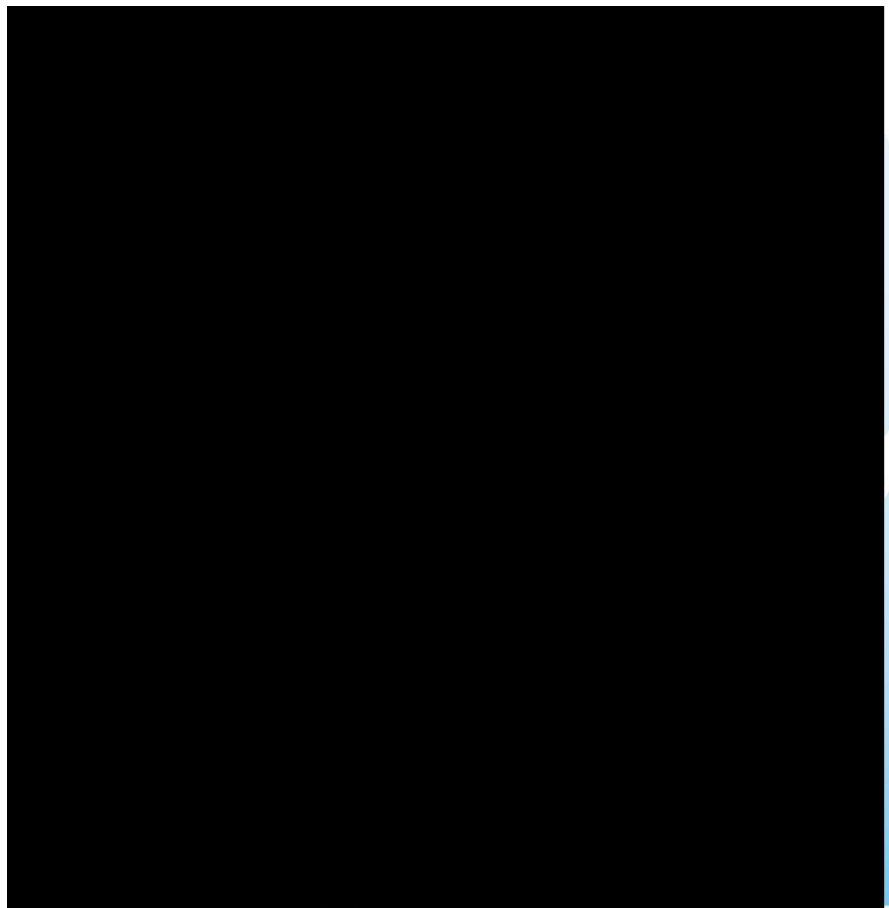
- Scoping/Planning/executing the transition and consolidation of the DCS and BRD CITRIX on-premise service to a virtualised CITRIX environment in the Azure public cloud



## 2. Introduction

This document is to be read in conjunction with the Computer Integration Services requirements document that has been put to market as an RFQ end of June 2020 and associated addenda.

The purpose of this document is to provide the shortlisted CIS vendor candidates greater clarity as to their scope of work in this outsourcing partnership. Hence, in using this document the vendors should be able to provide a firm quote on the ensuing outsourcing work.







## 4. Outsourcing In-scope

### 4.1 Production Services

1. On-Premise infrastructure support/management @ GovDC1 hosting GovConnect services (currently Unisys managed)
2. On-Premise infrastructure support/management @ GovDC1, GovDC2 and Bathurst sites hosting Revenue NSW and Spatial services (currently DCS IT Operations managed)
3. Azure public cloud infrastructure support/management hosting the BRD services including SIRA and Safework services (currently DCS Cloud Team managed)
4. AWS public cloud infrastructure support/management (excluding the underlying Cloud compute, network and storage infrastructure) hosting the GovConnect services (currently Unisys managed)
5. NTT private cloud infrastructure support/management (excluding the underlying private cloud compute, network and storage infrastructure @ GovDC1 hosting GovConnect services (currently NTT managed)
6. OutcomeX private cloud infrastructure support/management (excluding the underlying private cloud compute, network and storage infrastructure) hosting SNSW Genesys services (currently OutcomeX managed)
7. AC3 private cloud infrastructure support/management (excluding the underlying private cloud compute, network and storage infrastructure) hosting SNSW services, excluding Genesys (currently AC3 managed)

**Note:**

- a. All the GovConnect services are expected to be fully migrated by the commencement of the project.
- b. Support/management of the infrastructure and the sites listed above, at the vendor field staff managed.
- c. Must continue support/management of the infrastructure and the sites listed above.

- d. Must be able to absorb the support/maintenance of new production services in the in-scope data centres as they are enabled
- e. Ownership and support of underlying infrastructure of the NTT, OutcomeX and AC3 private clouds, shall remain with the incumbent vendors (i.e. compute, network and storage infrastructure)

## 4.2 IT Audit and Discovery

- 8. Work with incumbent vendors and DCS IT Operations to accept handover of the support/management of the in-scope production services
- 9. Audit the physical data centres, physical servers and VM's hosting the in-scope production services
- 10. Audit the services with HA capabilities including sourcing/examining the relevant BCP documents
- 11. Audit the services with operating DR, where DR is located and examining the DR plan
- 12. Audit the operating system and database licences installed on the production/non-production servers including the date of licence expiry (for on-prem/private cloud hosted services only)
- 13. Link asset owners/business units to production/non-product

## 4.3 Production Services with High Availability (HA) capabilities

- 14. All production services

**Note:**

- a. Must continue support
- b. Must be able to absorb HA capabilities in the

## 4.4 Disaster Recovery Services

- 15. All operating disaster recovery services outlined above (N.B. Az not located at GovDC2)

**Note:**

- a. Must continue supporting/maintaining the current DR services
- b. Must be able to absorb the support/maintenance of new DR services in the in-scope data centres as they are enabled
- c. Must be able to participate in an ad-hoc basis the cluster and agency disaster recovery exercises, when required

#### 4.5 Hosting Infrastructure Support/Management

- 16. Managing/supporting the node infrastructure in the data centre including procuring additional nodes before capacity is reached (N.B. automated on public cloud)
- 17. Managing/supporting the VMWARE ESX hosts and host clusters in the data centre i.e. hypervisor infrastructure layer (N.B. automated on public cloud)
- 18. Managing/supporting the on-premise data centre(s) hypervisor and the underlying compute and storage infrastructure (N.B. underlying network infrastructure is out of scope)
- 19. Managing/supporting the database cluster(s) in the in-scope data centre(s)
- 20. DNS (Domain Name System) management in the data centre (N.B. on public cloud this is done via AWS route 53/Azure DNS)
- 21. DHCP (Dynamic Host Configuration Protocol) management in the data centre
- 22. Centralised digital certificates management i.e. issuing new certificates, managing a key store
- 23. Develop then maintain network security system, end-point protection
- 24. Cloud Operations Support
  - a. Respond to infrastructure issues, system uptime and performance
  - b. Coordinate with cloud providers for in-scope public cloud services
  - c. Collaborate with development/maintenance teams for infrastructure and integration work

- d. Collaborate with the DCS Managed Network Services team in completing network connections or configurations for the VPC's/VNet (e.g. provisioning new environment)
- e. Collaborate with the DCS Managed Network Services and Cloud Management team(s) in the configuration of in-scope cloud services such as DNS, Direct/Express route links, peering, security groups, load balancer, application firewalls, certificate management, etc (e.g. enabling new application service)
- f. Provide support to DCS team(s) in optimising or troubleshooting the cloud-based workloads or application(s)
- g. Installing, configuring and managing workloads with different combinations of operating systems
- h. Ongoing configuration management of the in-scope cloud services (e.g. additional monitoring dashboard, alerts, password vault, etc)
- i. Ensure all cloud infrastructure components meeting DCS performance and security standards
- j. Monitoring the AWS Security Hub and AZURE Security Centre to ensure high data security
- k. Collaborate with DCS Security Operations team to identify and remediate infrastructure security issues
- l. Selecting the optimal end-state for cloud infrastructure based on requirements (e.g. security, performance, cost, etc)

**Note:**

- a. Access to the in-scope cloud services to be provided to CIS vendor staff, DCS Security Operations team and DCS Managed Network Services team
- b. All documentation produced as part of this project to be stored in a DCS managed storage location

## 4.6 Contributing to the DCS Cloud Centre of Excellence

- 25. Collaborate with the DCS Managed Network Services team in completing network connections or configurations for the VPC's/VNet (e.g. provisioning new environment)

26. Contribute to the DCS Architectural forum in the optimal design/reference architecture for the in-scope cloud services (i.e. addressing requirements relating to deployment, security, cost-effectiveness, high availability, process improvement, etc)
27. Facilitating the transition of DCS architectural requirements to future processes i.e. tasks and activities
28. Provide regular reports to DCS Cloud Management team (i.e. daily/weekly/monthly on the health, cost optimisation initiatives and overall state of the cloud infrastructure)
29. Collaborate with the DCS Cloud Management/Architecture teams to develop an appropriate cloud cost model i.e. cloud service usage costs vs cost control procedures
30. Ongoing monitoring of overall costs of the in-scope cloud services vs cost reduction initiatives
31. Ensuring the order of compliance (e.g. tagging/naming standards)

**Note:**

- a. It is mandatory that the new CIS vendor assign a dedicated Cloud Operations Administrator or Engineer to manage the lifecycle of cloud infrastructure throughout the delivery of this project and the delivery framework
- b. 80% of the DCS work

#### 4.7 Storage Services (excluding the underlying cloud compute storage)

32. All storage services (i.e. the hosting of the in-scope
33. Procuring additional storage
34. Surrendering surplus storage (sizing)

## 4.8 Backup/Restore Services (excluding the underlying cloud compute storage)

35. Backup of the production services (above) in line with current standard operating procedures

**Note:**

- a. Must continue maintaining the current backup processes/services including the management of offline backups
- b. Must be able to absorb new services with its associated backup requirements
- c. Must be able to cater for backup retention period changes
- d. Must continue with the process of secure disposal of backup media once set retention periods are reached

36. Facilitate requests for ad-hoc restore from backup of selected production services (above) including physical servers, VM's, application, database

37. Facilitate requests for ad-hoc backup of selected production/non-production environments

38. Commvault and Veeam when stock run low

## 4.9 DBA Support

39. Database upgrades and production services

40. Monitoring database performance

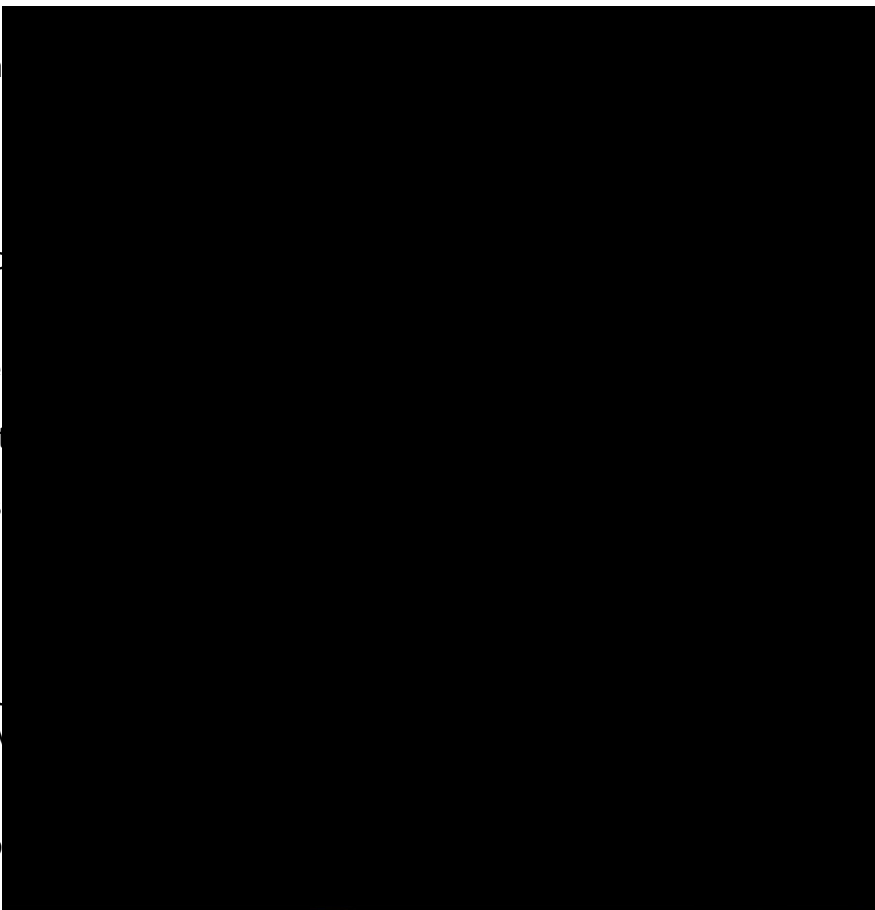
41. Immediate DBA support

42. Facilitate ad-hoc DBA support etc

## 4.10 CITRIX Service

43. Scoping/Planning/execution of CITRIX on-premise services to cloud

44. Support/management of



45. Decommissioning the DCS CITRIX on-premise service (approximately 30 servers)

46. Consolidation of the CITRIX licences

**Note:** The DCS Cloud Management Team has commenced work to transition the BRD CITRIX on-premise service to a virtualised CITRIX environment in the Azure public cloud. The expectation is that the CIS vendor will collaborate then takeover to complete the remaining work

## 4.11 Service Management

47. DCS ServiceNow ITOM

- a. System health and availability monitoring
- b. Infrastructure discovery (including service map)
- c. Cloud management platform

48. DCS ServiceNow ITIL

- a. Change impact evaluation
- b. Incident diagnosis
- c. True service level

49. DCS ServiceNow ITAM

- a. Managing DCS physical servers
- b. Licence optimisation
- c. Operational and

50. DCS ServiceNow CMD

- a. Create/update C

51. Incident Management

- a. Align with Service

52. Problem management

- a. Align with Service

53. Change management

- a. Align with DCS CAB/Change Management processes

54. Request management (currently via DCS portal)

- a. Actioning request(s) for provisioning new VM's and/or physical servers
- b. Actioning request(s) for decommissioning redundant VM's and/or physical servers

55. IT Service Desk

- a. Contribute to the DCS known errors database
- b. Contribute to the DCS knowledge articles

## 4.12 Optimisation

56. Collaborate with the DCS Cloud Management Team to:

- a. Institute a regular process of right sizing the CPU and storage of the in-scope VM's (public/private cloud only)
- b. Institute a process for managing licences (i.e. Con
- c. Institute a process
- d. Drive cost management reserve instances
- e. Drive operational
- f. Institute compliance policies, encryption
- g. Drive the triaging
- h. Establish the rele listed above (i.e.

57. Collaborate with the DC

- a. Institute a regular BA servers and VM's



- b. Institute a process to consolidate/optimize the use of operating system licences across the fleet of physical servers and VM's (i.e. Windows, Red Hat, Oracle, SQL, etc)
- c. Institute a process to optimize the capacity/usage/procurement of the node infrastructure in the in-scope data centres (with the exception of the public cloud) – ref 16
- d. Centralise the process of provisioning/decommissioning VM's in the in-scope data centres – ref 54
- e. Centralise the management of digital certificates - ref 22
- f. Institute a process to regularly demonstrate that the databases of in-scope services are stored in an encrypted manner, at rest in Australia
- g. Institute a process to regularly audit the secure disposal of backup when the duration of the set retention periods have been reached
- h. Regular review of the current procedures and processes, with a view to automate where possible
- i. Establish the relevant SLA's and regular reporting associated with the items listed above (i.e. a-g)

#### 4.13 Integration

58. Collaborate with the DC

- a. Integrate the CIS ve
- b. Integrate the CIS ve  
41 & 42
- c. Integrate the CIS ve
- d. Integrate the CIS ve  
43
- e. Facilitate the popula  
physical and VM ser
- f. Deliver regular finan
  - i. CIS vendor o  
e.g. Cabcharg

- ii. CIS vendor ad-hoc labour costs/time spent and any add-ons e.g. Cabcharge
  - iii. Procurement costs in supporting/operating the in-scope services i.e. operating system licences, node infrastructure, digital certificates, etc
- g. Establish the relevant SLA's and regular reporting associated with the items listed above (i.e. a-f)

59. Collaborate with the DCS IAM & Automation Team to:

- a. Institute a regular process to audit all the CIS vendor staff remote and physical access to the in-scope infrastructure

60. Collaborate with the DCS Managed Network Services Team to:

- a. Establish an optimal engagement model to manage/support the in-scope infrastructure in areas of conflicting responsibilities e.g. network connections or configurations for the VPC's/VNet

61. Collaborate with the DCS PMO/Infrastructure Services to:

- a. Highlight opportunities for optimisation, integration, process improvement and information management for the in-scope infrastructure
- b. Contribute to the
- c. Facilitate the ad- of entire project(s)
- d. Facilitate the ad- infrastructure init

**Note:** The new CIS vendor projects/initiatives. DCS from another vendor

## 5. Outsourcing Out-of-Scope

### Production Services

1. Identity and Access Management to the in-scope infrastructure (DCS IAM & Automation)
2. Private cloud underlying network, compute and storage infrastructure (incumbent vendors)
3. Application support and application release management (DCS Application Support or equivalents)
4. Business Continuity Planning

### Security

5. Onboarding/offboarding CIS vendor staff account access to the in-scope infrastructure and service management tools (DCS IAM & Automation)
6. Administration of the physical access for the CIS vendor field services staff to the physical data centre sites (DCS IAM & Automation)
7. Cybersecurity including vulnerability assessments (DCS inflight projects)
8. Security induction to in-scope infrastructure (DCS IAM & Automation)

### CITRIX Service

9. DCS staff onboarding to the CITRIX environment
10. DCS staff offboarding from the CITRIX environment
11. Desktop support of the CITRIX environment

### Data Centres

12. Financial or physical ownership of data centres
13. Work to consolidate the in-scope data centres

## 6. Appendix A – DCS SIAM Requirements

The DCS SIAM (Service Integration and Management) framework will be implemented in 4 iterations - outlined below. The new CIS vendor is required to meet the requirements for iteration 1 & 2 as part of initial onboarding.

### Iteration 1:

- Event Management
- Incident Management
- Request Fulfilment Management (Including Access Management)
- Problem Management

### Iteration 2:

- Service Asset and Configuration Management
- Release and Deployment Management
- Change Management
- Knowledge Management
- Collaboration Framework
- Continual Improvement

### Iteration 3:

- Service Level Management
- Service Catalogue
- IT Security Management

### Iteration 4:

- Capacity / Availability Management
- IT Service Continuity Management
- Business Relationship Management

Within the State's SIAM ecosystem there is a requirement for flexibility, participation, cooperation and collaboration. This requirement addresses cultural, tooling, data and tool ownership, and integration needs of the DCS Service Integration and Managed environment are as follows:

### **Cultural requirements:**

- Service providers must acknowledge that the service integrator is the voice of the customer and has the autonomy to direct and make decisions and govern without being undermined.
- Service providers must engage in a Fix first, argue later approach; when there is an issue affecting service, the service providers need to work together with the Service Integrator to address and resolve rather than assign blame or pass issues around.
- Service providers must focus on creating and maintaining an environment focused on business outcomes and the customer, not individual service provider's contracts and agreements.
- Service providers must be actively engaged in Process Forums and Working Groups as needed with duly authorised and suitably skilled participation.
- Service providers must support operating under a 'code of conduct' or 'rules of the club' agreement, with input from all parties in the SIAM ecosystem. These govern behaviours on a day to day basis on how staff will behave in meetings, they will maintain professional and make effective contributions.
- Service providers must or agreed between parties they will work together
- The service integrator agreements (OLAs) to be helping them to understand ecosystem and when co

### **Tooling Requirements**

Service Providers will be (ServiceNow) which is granted sufficient access SIAM operating model.

Service Providers will r the following ways in o

- **Event Management:** It forward on event and m

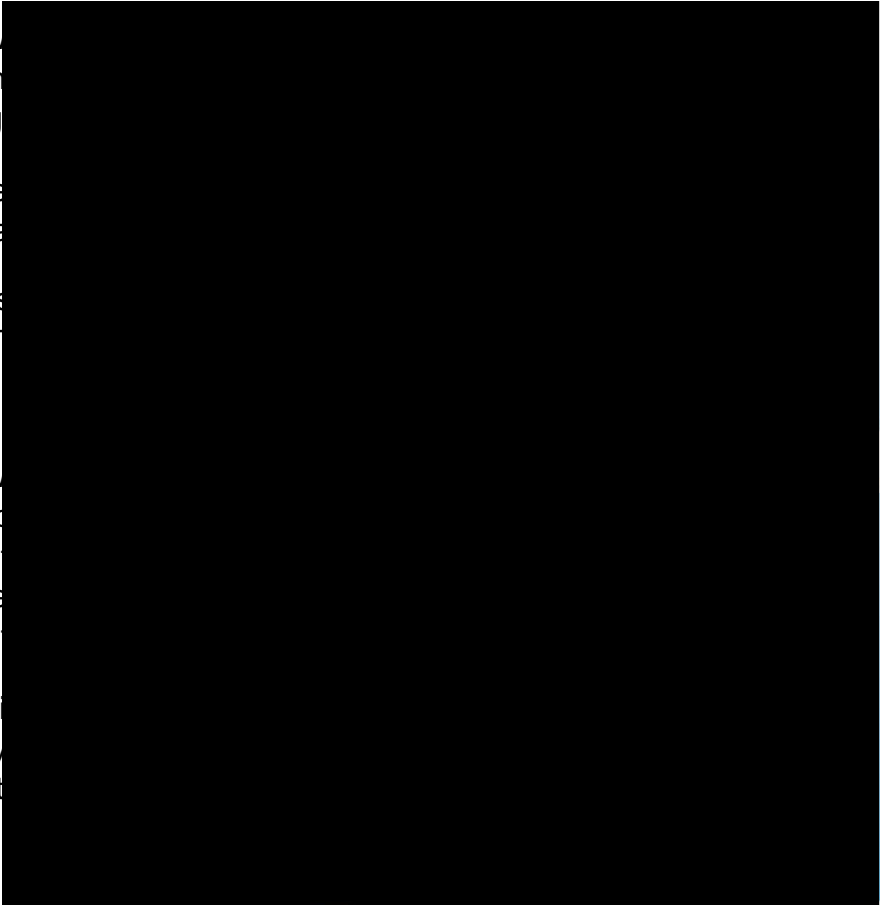
- **Incident Management:** Service providers should access the common tool for incident management
- **Request Management:** Service providers should access the common tool for Request fulfillment
- **Knowledge Management:** Service providers should access to a common Known Error Database (KEDB) in order to populate known errors and workarounds
- **Problem Management:** Service providers should actively engage in problem management activities coordinated by the Service Integrator impacting or dependant of the services they provide
- **Data management:** Service Providers are responsible for maintaining the data with the IT Service Management Platform as it relates to the services they are providing and the processes they participate in.

**Data and Tool ownership and usage:**

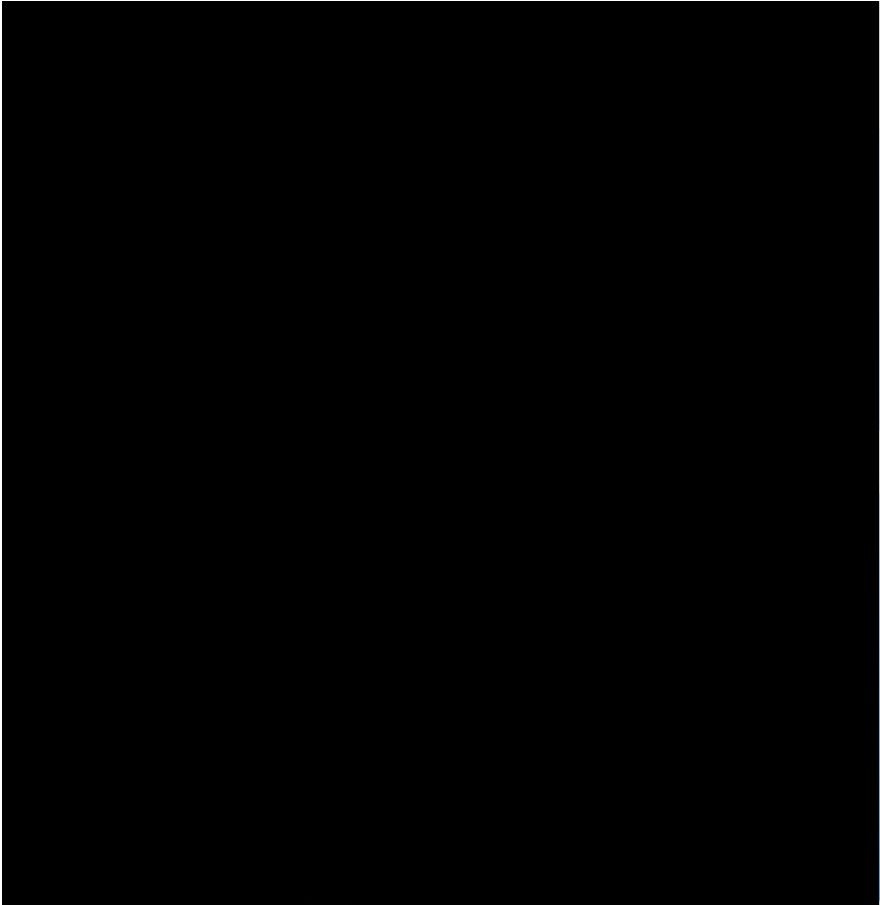
- The IT Service Management platform, which includes all the tools required to support the SIAM process model and the function of the Service Provider, are owned by the DCS (Retained Capabilities). DCS provide the Service Integrator and the Service Providers access to the IT Service Management platform so they can perform their roles and actively participate in the SIAM operating model.
- Each Service Provider will have their own set of tools and processes required with the SIAM model. If additional tools or processes are required, this can be agreed with DCS.
- At the termination of the contract, all data and tools owned by the Service Provider within the IT Service Management platform will be removed.
- Any licences and tools owned by the Service Provider for the purpose they were intended for will be returned to the Service Provider.

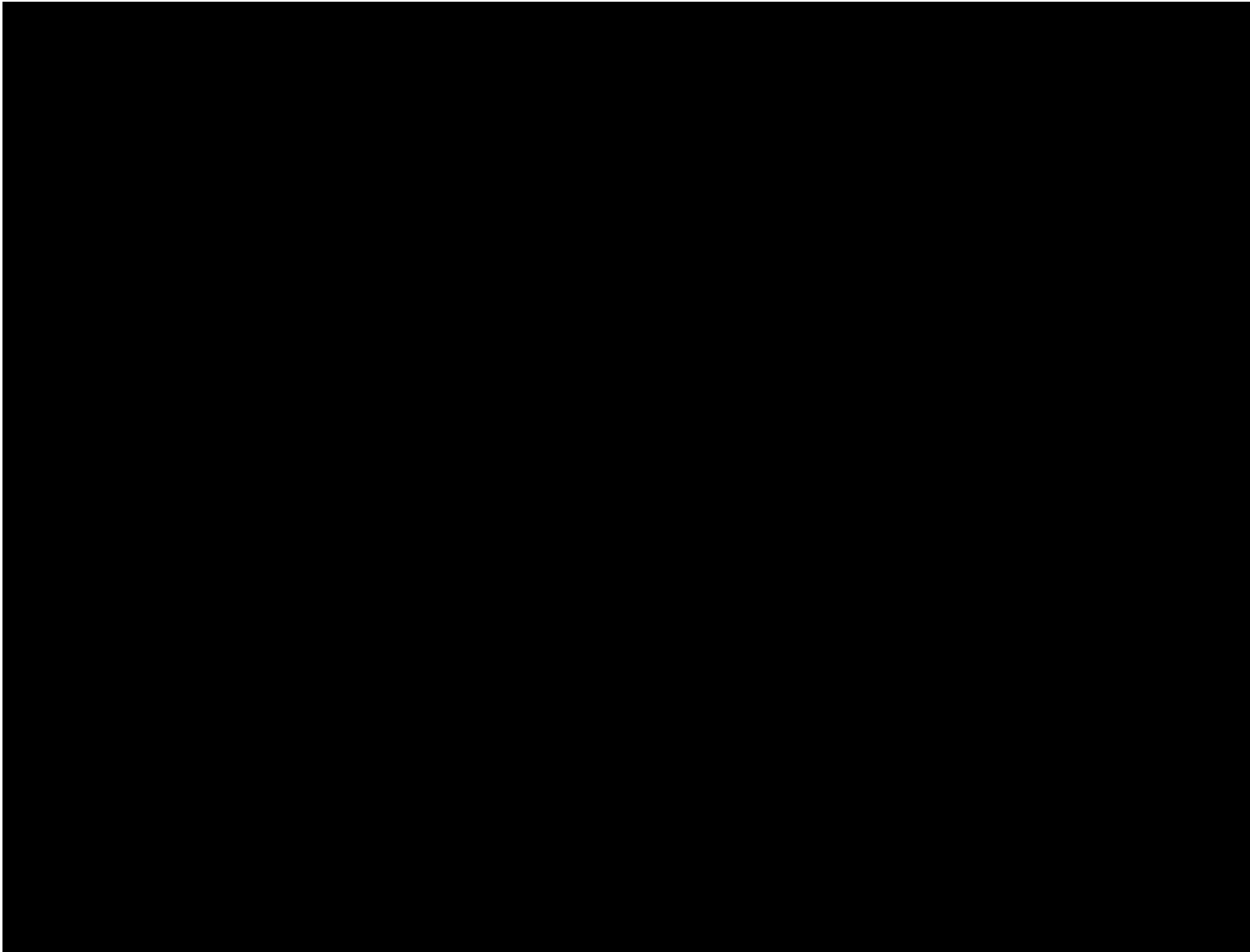
**Integration Approach:**

- The Service Integrator will develop integration models for each of the processes. If a Service Provider does not wish to use the integration model, if approved by DCS, the Synchronisation model will be used.
- The Service Provider will be responsible for maintaining the Data Synchronisation and the ability to change management



- The Service Integrator, in consultation with DCS, will review the Service provider Data Synchronisation model and determine if the approach is suitable to maintain the integrity of data within the IT Service Management platform



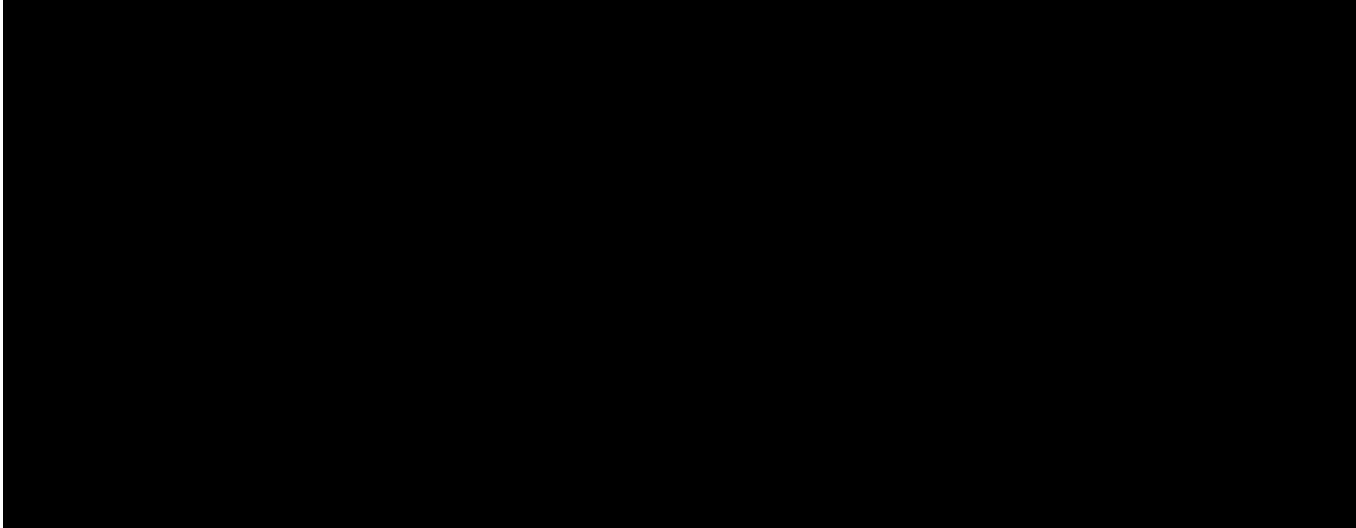


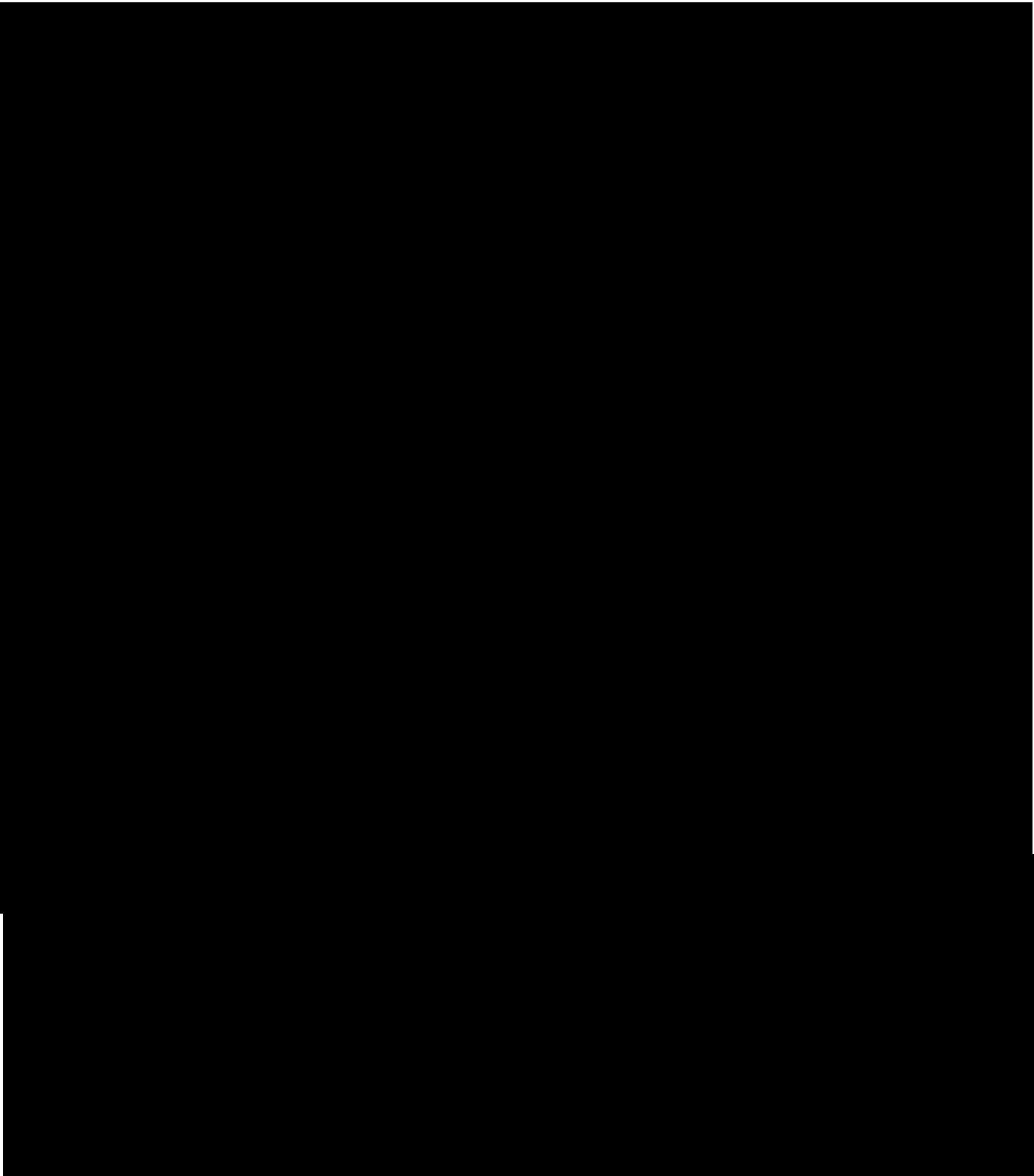


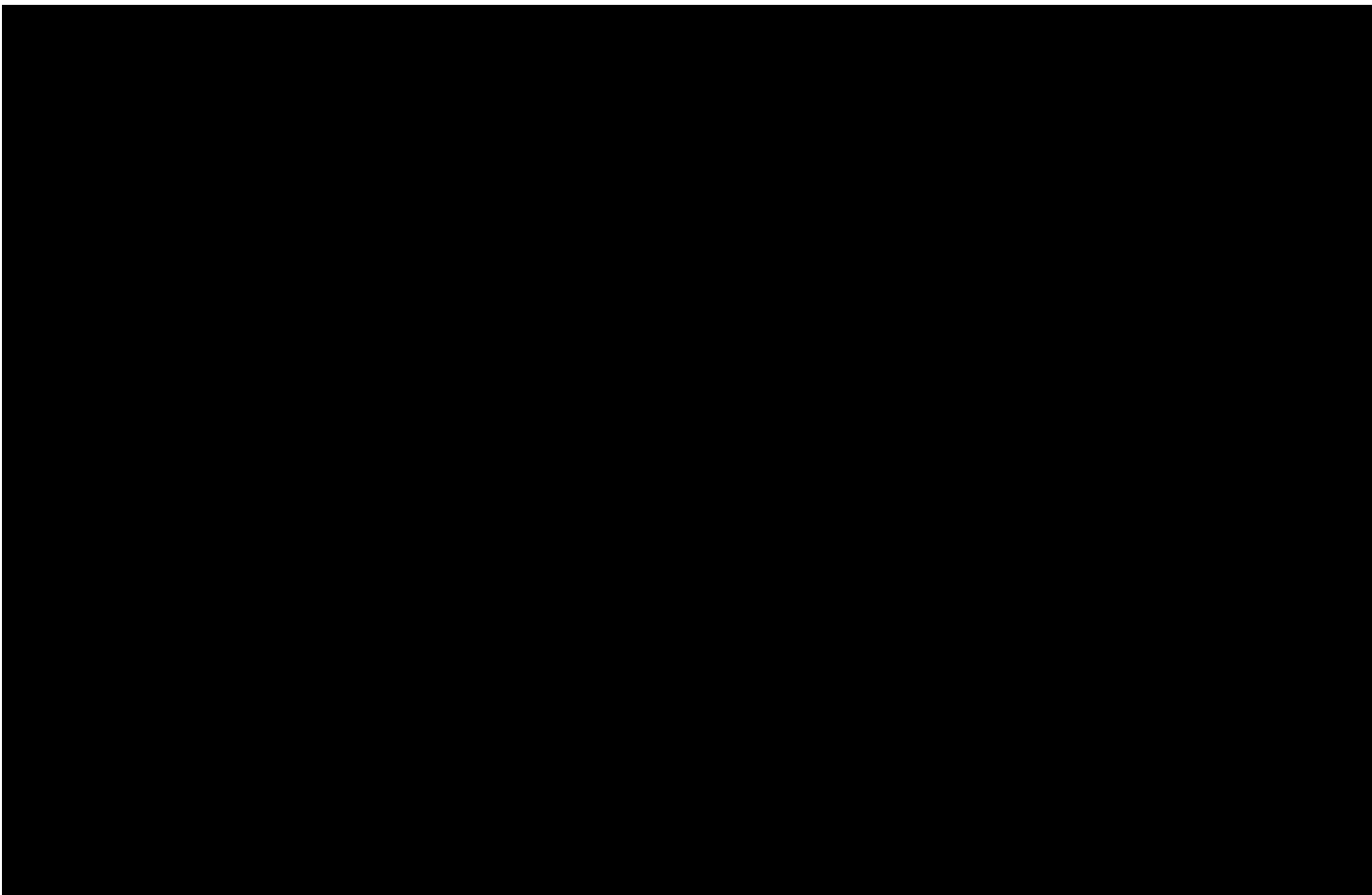
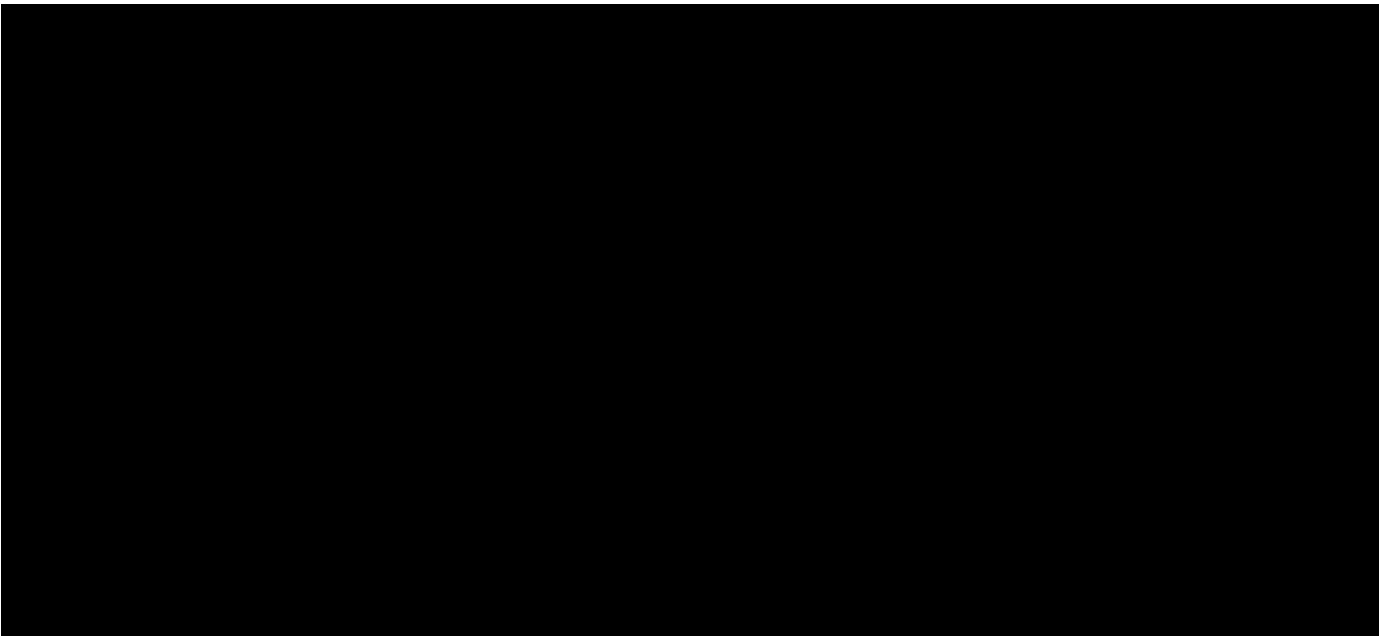


[REDACTED]

[REDACTED]







# **Exhibit 4 to the General Order Form**

## **Risk and Resilience Framework**

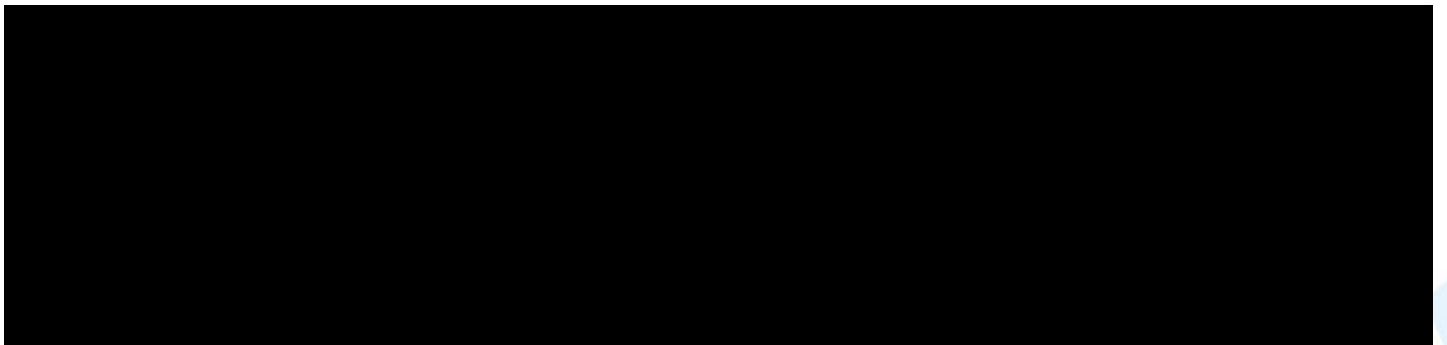
[See the following pages]



# Risk and Resilience Framework

Document number: DR1643	Version number: 6.0
Date: December 2015	

## Contact details



# Table of Contents

<b>Risk and Resilience Framework</b>	<b>1</b>
<b>1. Risk and Resilience Framework</b>	<b>4</b>
1.1 Framework Intent	4
1.2 Risk and Resilience Framework Objectives	4
1.3 Scope	5
1.4 Approach and Methodology	5
1.5 Responsibility	5
1.6 Control Assurance	9
1.7 Risk and Resilience Maturity Evaluation	9
1.8 Benchmarking	9
<b>2. Risk and Resilience Requirements</b>	<b>10</b>
2.1 Requirement 1: Establish the Context	10
2.1.1 Types of Risk	11
2.1.2 Risks Associated with Changes	12
2.1.3 Risks Associated with Major Projects	12
2.1.4 Learning from Successes and Failures	13
2.2 Requirement 2: Identifying Risks	13
2.2.1 Identify the Risk	13
2.2.2 Identify the Causes	13
2.2.3 Identify the Impacts	13
2.3 Requirement 3: Analyse the Risk	14
2.3.1 Risk Rating	14
2.3.2 Risk Controls and Effectiveness	14
2.4 Requirement 4: Evaluating Risk	23
2.5 Requirement 5: Treating Risks	25



2.6	Requirement 6: Monitoring and Reviewing Risks	26
2.6.1	Recording Risks	26
2.6.2	Risk Register Review	27
2.7	Requirement 7: Communication and Consultation Plan	28
2.7.1	DFSI Risk Network	28
2.7.2	Training Strategy	28
<b>3.</b>	<b>Glossary of Terms</b>	<b>29</b>
<b>4.</b>	<b>Related Policies and Documents</b>	<b>32</b>
<b>5.</b>	<b>Document Control</b>	<b>33</b>
5.1	Document Approval	33
5.2	Document Version Control	33
5.3	Review Date	33
<b>Table 1</b>	<b>Responsibilities</b>	<b>6</b>
<b>Table 2</b>	<b>Control Effectiveness</b>	<b>15</b>
<b>Table 3</b>	<b>Consequence Criteria</b>	<b>16</b>
<b>Table 4</b>	<b>Likelihood Rating</b>	<b>22</b>
<b>Table 5</b>	<b>Risk Rating Matrix</b>	<b>23</b>
<b>Table 6</b>	<b>Residual Risk Rating Review Requirements</b>	<b>24</b>

# 1. Risk and Resilience Framework

## 1.1 Framework Intent

The effective management of risk is central to the continued efficient management of the Department of Finance, Services and Innovation (DFSI). Risk management is an integral part of good management practice and an essential element of good corporate governance.

Risk management is part of the DFSI culture, and it is embedded into the DFSI operating philosophy, practices and business processes rather than being viewed or practised as a separate activity.

The Risk and Resilience Framework (the Framework) forms the basis of how risk management is to be conducted throughout DFSI. Divisions and Related Entities are to use the Framework as either their risk framework or as the basis of a framework for their particular requirements. Changes to this framework by Divisions or Related Entities must be discussed with and approved by the DFSI Director Risk Services.

All managers and staff (including temporary staff) are responsible for the management of risk in accordance with the DFSI Risk and Resilience Policy.

## 1.2 Risk and Resilience Framework Objectives

DFSI has established the Framework for the management of risk across all parts of the organisation. DFSI has adopted the definition of risk used in AS/NZ ISO 31000:2009:

### **“The effect of uncertainty on objectives”**

Risk can be applied in a strategic context including positive and negative impacts. The Framework enables risk management to be embedded across DFSI, through a strategic decision making process, for the purpose of evaluating and managing the negative uncertainties the organisation faces.

The aim is to ensure that:

- the Secretary, the DFSI Executive Team and all managers can confidently make informed business decisions
- change opportunities and initiatives can be pursued with greater speed, robustness and confidence for the benefit DFSI and its stakeholders
- there is greater certainty in achieving strategic objectives

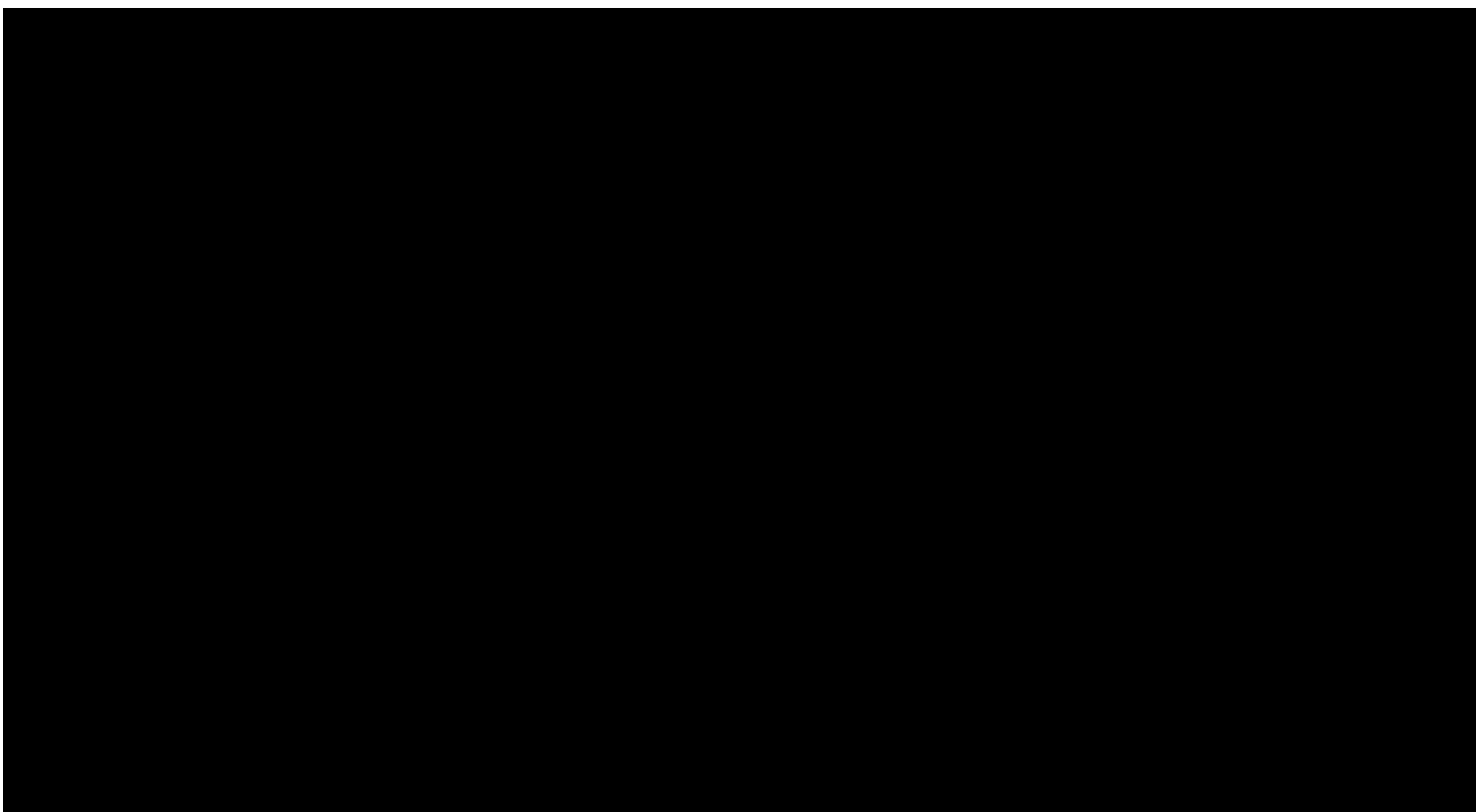
- daily decisions at the operating level are made within the context of DFSI's capacity to accept risk
- the organisation manages the risk of intangible assets – reputation, regulatory, intellectual and knowledge capital, processes and systems – just as fully as it manages physical and financial assets.

This means that risk management is linked with strategic and business planning, initiative planning, value drivers and the performance measurement process.

### **1.3 Scope**

The Framework covers DFSI, and all DFSI Divisions, Related Entities and Business Units.

### **1.4 Approach and Methodology**



### **1.5 Responsibility**

As an integral part of DFSI management systems, covering all aspects of the business, the custody of this Framework rests with the Secretary who is responsible for ensuring the Framework is implemented, tested, maintained and updated. The Secretary is assisted in this process by the DFSI Director Risk Services. In practice, however, ownership of the Framework rests with the entire DFSI Executive.

Accountability is central to an effective risk and resilience framework. Table 1 Responsibilities identifies the key responsibilities in regard to risk management throughout DFSI.

**Table 1 Responsibilities**

<b>DFSI Risk and Resilience Framework Responsibilities</b>	
<b>Secretary</b>	<p>The Secretary is responsible for:</p> <ul style="list-style-type: none"> <li>• governance</li> <li>• risk management</li> <li>• legal compliance.</li> </ul>
<p><b>Audit and Risk Committees (ARC)</b></p> <ol style="list-style-type: none"> <li>1) DFSI Principal Led Shared Arrangement ARC</li> <li>2) Property and Housing Group Collaborative Shared Arrangement ARC</li> <li>3) State Insurance Regulatory Authority ARC</li> </ol>	<p>Audit and Risk Committees oversee the operation of the DFSI Risk and Resilience Policy and Framework, and assesses their adequacy. The Committees monitor the internal policies for identifying and determining the risks to which DFSI is exposed:</p> <ul style="list-style-type: none"> <li>• whether management has in place a current and appropriate enterprise risk management process, and associated procedures for effective identification and management of DFSI's financial and business risks, including fraud and corruption</li> <li>• whether a sound and effective approach has been followed in developing strategic risk management plans for major projects or undertakings</li> <li>• the impact of DFSI's risk management process on its control environment and insurance arrangements.</li> </ul> <p>This is done in accordance with Treasury Policy <i>Internal Audit and Risk Management for the NSW Public Sector</i> (TPP 15-03).</p>
<b>DFSI Executive Team</b>	<p>Members of the DFSI Executive Team are responsible for the management and monitoring of the identified risks across DFSI and the effective implementation of the DFSI Risk and Resilience Policy.</p> <p>Key requirements are:</p> <ul style="list-style-type: none"> <li>• ensuring the completion, accuracy and updating of risk management plans</li> <li>• championing risk management</li> <li>• monitoring and reviewing the risks for completeness, continued relevance, and effectiveness of risk controls and treatment plans while taking into account changing circumstances</li> <li>• members of the DFSI Executive Team may be assigned strategic risks to manage, and they may delegate responsibility for monitoring controls and/or treatment plans to managers and/or specialist staff where appropriate</li> <li>• advising other agencies who have shared risk with DFSI when the residual risk rating determined by DFSI is rated as high or extreme.</li> </ul>

<b>DFSI Risk and Resilience Framework Responsibilities</b>	
<b>Divisional Executive Teams</b>	<p>Members of the Divisional Executive Team are responsible for the monitoring of the identified risks within their area of responsibility. Key requirements are:</p> <ul style="list-style-type: none"> <li>ensuring the completion and updating of their area of responsibility's risk management plans</li> <li>championing risk management within their area of responsibility</li> <li>monitoring and reviewing their area of responsibility's risks for completeness, continued relevance, effectiveness of risk controls and treatment plans, taking into account changing circumstances.</li> </ul>
<b>DFSI Director Risk Services</b>	<p>The DFSI Director Risk Services is responsible for managing DFSI's enterprise risk management function including:</p> <ul style="list-style-type: none"> <li>frameworks for risk management</li> <li>business continuity</li> <li>legal compliance</li> <li>audit and risk committees</li> <li>governance and</li> <li>insurance.</li> </ul> <p>The DFSI Director Risk Services is also responsible for:</p> <ul style="list-style-type: none"> <li>providing expert advice and assistance on risk management to the Executive, Divisions, Related Entities, Business Units and project teams</li> <li>reporting regularly on Enterprise Risk Management and strategic risks to the Executive and Audit and Risk Committees</li> <li>managing the online risk management system including provision of specialist support to DFSI in the use of the system</li> <li>ensuring that each head of authority provides an annual attestation that the entity complies with TPP 15-03.</li> <li>Ensure that there is communication to other agencies where a risk which is shared with DFSI is rated as being high or extreme at the residual rating</li> </ul>
<b>Related Entities / Business Unit Managers</b>	<p>Related Entity / Business Unit Managers are responsible for the management of the risks within their area of responsibility. Key requirements are:</p> <ul style="list-style-type: none"> <li>completing and updating the Related Entity / Business Unit risk registers, including risks associated with outsourced activities</li> <li>monitoring and reviewing the risks within the Related Entity / Business Unit for completeness, continued relevance, and effectiveness of risk controls and treatment plans while taking into account changing circumstances</li> <li>may be assigned operational risks to manage, and they may delegate responsibility for monitoring controls and/or treatment plans to managers and/or specialist staff where appropriate.</li> </ul>

<b>DFSI Risk and Resilience Framework Responsibilities</b>	
<b>Risk Champions</b>	<p>The Risk Champions are nominated managers from the Divisions, Related Entities and Business Units. Each representative is responsible for:</p> <ul style="list-style-type: none"> <li>• providing feedback and assistance to the DFSI Director Risk Services in the implementation and maintenance of risk management within their area of responsibility</li> <li>• embedding risk management processes into key business processes, including strategic and business plan development</li> <li>• coordinating reporting within their area of responsibility</li> <li>• participating in the DFSI Risk Network.</li> </ul>
<b>Internal Audit</b>	<p>Internal Audit reviews the efficiency, effectiveness and compliance of priority programs/processes as well as the adequacy of internal controls. It is responsible for:</p> <ul style="list-style-type: none"> <li>• directing internal audit activity which relates to the critical controls for high-level corporate and strategic risks within the business</li> <li>• independently reviews selected controls as part of the Internal Audit plan to provide assurance that key controls are in place and effective.</li> </ul>
<b>Strategic, Program and Performance Management Office (SPPMO)</b>	<p>The SPPMO is responsible for:</p> <ul style="list-style-type: none"> <li>• monitoring risks at the program level, including interdependencies between major projects, and advise the DFSI Executive Team as required</li> <li>• assisting major project sponsors and managers to manage risk effectively and efficiently.</li> </ul>
<b>Risk Owners</b>	<p>Risk Owners are responsible for:</p> <ul style="list-style-type: none"> <li>• ensuring that the assessments of their risks are up-to-date and are properly recorded and managed in the appropriate risk register/s using the online risk management system</li> <li>• conducting periodic assurance reviews to check that the controls that they are relying on are in place, effective and for possible improvements</li> <li>• monitoring the progress and effectiveness of any treatment plans that are in place to further reduce the risk rating.</li> </ul>
<b>Risk Control Owners</b>	<p>Risk Control Owners are responsible for:</p> <ul style="list-style-type: none"> <li>• ensuring that the risk control/s they are responsible for are effective</li> <li>• conducting periodic assurance to check that the controls they are relying on are in place and effective</li> <li>• reviewing controls to identify cost-effective improvements.</li> </ul>

<b>DFSI Risk and Resilience Framework Responsibilities</b>	
<b>Risk Treatment Owners</b>	<p>Risk Treatment Plan Owners are responsible for ensuring that:</p> <ul style="list-style-type: none"> <li>• risk treatment plans allocated to them are completed by an agreed date</li> <li>• the risk owner is advised of the progress of the treatment plan, particularly if there are delays or issues.</li> </ul>
<b>All Staff</b>	All staff are required to understand and act on their responsibility to report new risks or increases in risk in a timely way.

## 1.6 Control Assurance

The Risk and Resilience Framework is largely self-regulating. Control assurance is principally through the use of control self-assessment, practised by risk and control owners. Control assurance is focused on validating this measure in terms of both the adequacy and effectiveness of controls. See also section 2.3.2 Risk Controls and Effectiveness. Where it is required, Internal Audit will review specific controls as part of the annual Internal Audit program.

## 1.7 Risk and Resilience Maturity Evaluation

A formal system has been implemented to measure and report risk and resilience maturity and its improvement over time in DFSI. The evaluation is conducted using a protocol in TPP 15-03 to provide the Audit and Risk Committees with an accurate representation of the maturity across DFSI and within Divisions, Related Entities and Business Units.

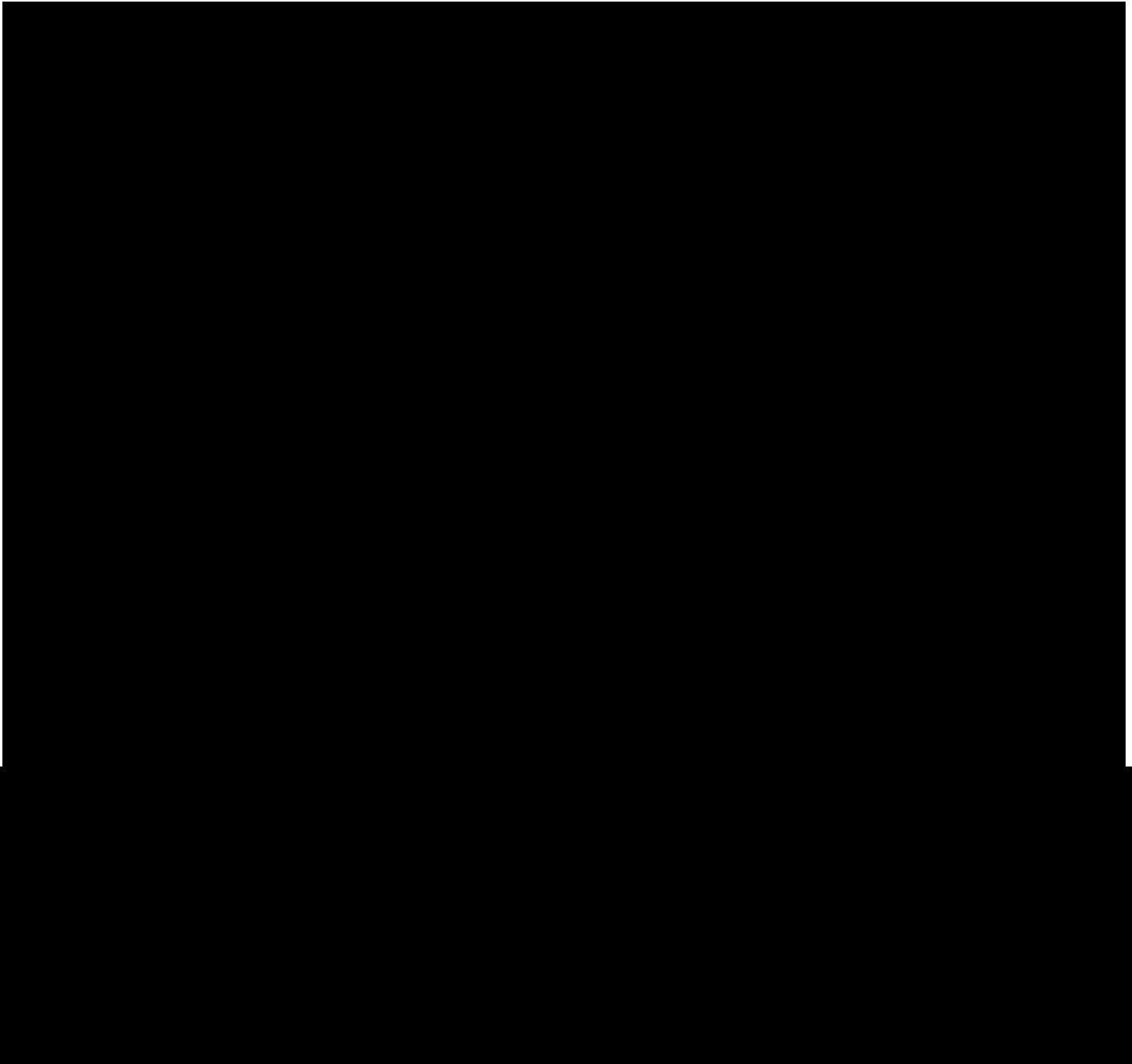
An annual maturity evaluation plan has been developed by DFSI's Risk Services Branch to ensure that DFSI and all Divisions, Related Entities, Business Units and projects are regularly evaluated.

## 1.8 Benchmarking

This Framework is based on a distillation of current best practice. Once the Framework becomes established, it is important that occasional benchmarking take place to maintain the Framework's currency.

## 2. Risk and Resilience Requirements

Figure 1 Risk and Resilience Requirements (below) shows the general structure of the Framework DFSI has deployed. The figure shows seven key requirements. This is how, on a day-to-day basis, DFSI is managing risk.





## **2.1.1 Types of Risk**

### **a) Strategic Risks**

Strategic risks relate directly to an organisation's strategic planning and management processes. Strategic risks are those which could significantly impact on the achievement of the organisation's vision and strategic objectives as documented in the DFSI Corporate Plan.

These are high-level risks which require identification, treatment, monitoring and management by the DFSI Executive Team. Each strategic risk has a nominated DFSI Executive Team member as the Risk Owner, who manages the risk and reports as required to the Secretary.

The DFSI Executive Team conducts formal reviews of strategic risks at least every three months, including the progress of risk controls and treatment plans. These reviews also involve identifying any new or emerging risks that might affect the achievement of strategic and business plan objectives and budgets.

### **b) Operational Risks**

Operational risks generally require oversight by the Divisional Executive Team, or by the relevant program or project steering committee.

Operational risks are those which may have a significant impact on achieving the:

- organisation's strategic objectives (as documented in the strategic plan) from the perspective of the actions undertaken by a particular Division, Related Entity, Business Unit or project
- individual programs or project management objectives.

Each operational risk has a nominated Risk Owner who manages the risk and reports as required to the responsible Divisional Executive Team member. In some instances, these risks may require escalation to the DFSI Executive Team.

All Divisions, Related Entities, Business Units and projects conduct formal reviews of operational risks at least every three months, including the progress of risk controls and treatment plans. The reviews also involve identifying any new or emerging risks that might affect the achievement of plan objectives and budgets of the respective Division, Related Entity, Business Unit or project.

## 2.1.2 Risks Associated with Changes

A change, event or decision is significant if it could potentially have a material adverse impact on the achievement of the DFSI objectives or could lead to a breach of legal, fiduciary or contractual requirements.

The rigour of the risk assessment is determined by the following considerations for:

- simple risks where the consequences are likely to be insignificant or moderate, a simple form of risk assessment that can be applied by most managers, after training, is used
- complex risks with the potential for significant adverse consequences, a more rigorous approach is used that is facilitated by a person with experience in the area of the potential consequences (i.e. Legal, Risk, Finance, HR, ICT Systems, Information Security, Procurement, WHS).

Wherever practicable, a change, event or decision driven risk assessment process is integrated and embedded in applicable DFSI processes and procedures.

## 2.1.3 Risks Associated with Major Projects

Major projects<sup>1</sup> will normally constitute significant change, so they require application of this framework process and compliance with the Strategic Program and Performance Management Office (SPPMO) requirements. A major project should have significant risks managed at the DFSI Executive Team or Division / Related Entity / Business Unit area level depending on DFSI's exposure.

In particular:

- all major projects are planned using a suitable risk assessment to focus their execution plan on the major sources of uncertainty – the risks
- the financial justification and business case for the project are subjected to suitable risk assessment
- the project risk management plan is to be reviewed at least at each phase of the project life cycle:
  - pre-project
  - project initiation
  - project delivery

---

<sup>1</sup> Levels 3-5 as determined by the DFSI Enterprise Performance and Portfolio Management Decision Support Tool.

- project close - for lessons learned, and for passing any remaining risks to business as usual management
- and if major changes are made to the business case, scope, timeframe or budget.

During the project delivery phase of a project the critical controls should be subjected to assurance in accordance with section 2.3.2.

#### **2.1.4 Learning from Successes and Failures**

After any significant event or change, a suitable analysis should be conducted to learn from both successes and failures. The learning should be recorded and action should be taken to ensure that the causes are treated such that subsequent issues are prevented and successes are repeated.

Wherever practicable, post-event or post-change analysis are integrated and embedded in applicable DFSI processes and procedures.

## **2.2 Requirement 2: Identifying Risks**

### **2.2.1 Identify the Risk**

A list of risks is identified, based on those risk events that might prevent, degrade, or delay the achievement of DFSI's business objectives. Key areas to consider when identifying risks to the business objectives include people, clients, customers, service delivery, financial, regulatory, external events (e.g. natural disasters, man-made disasters, and security), ICT, health and safety, government requirements, fraud and stakeholders.

### **2.2.2 Identify the Causes**

It is important that the potential causes of each risk are identified and recorded. In some cases, a cause may become a risk where it is considered that it requires its own controls and possibly its own risk treatment plan. As an example, a cause of the strategic risk '*Fraud or corruption*' could be '*risk and benefits register not kept up to date and requirements not understood*'. This cause may also need to be dealt with as a risk at the operational level (Division / Related Entity / Business Unit), as it requires its own controls and treatments to manage.

### **2.2.3 Identify the Impacts**

It is also important to identify the potential impacts of a risk, particularly when determining the consequence and risk rating. It is quite possible for the impacts to occur in a number of areas of Table 3 Consequence Criteria, but also several times within an area of consequence. For example, an impact of risk around '*Fraud or corruption*' may be rated highest as a '*regulatory non-compliance*' consequence but the impacts on the organisation

could include 'a reputation, financial, media interest/reporting, client/stakeholder negative feedback, etc'.

## 2.3 Requirement 3: Analyse the Risk

To analyse a risk to determine its severity, a risk matrix is used to identify the highest impact consequence with the likelihood of it happening.

A consequence rating is chosen from Table 3 on the basis of the highest potential adverse impact on DFSI and its stakeholders. Where there is more than one type of consequence possible, the one that gives the most severe adverse consequences is chosen as the basis for the rating.

Once the risk has been identified, a likelihood rating is chosen from Table 4 on the basis of the corresponding likelihood that DFSI and its stakeholders could be affected.

### 2.3.1 Risk Rating

The risk rating is the outcome of the combination of consequence and likelihood using Table 5. To determine the overall risk rating, (expressed as Extreme, High, Medium and Low), the consequence and likelihood are combined in the risk matrix. The final overall risk rating is reviewed by the appropriate manager, based on the DFSI risk appetite and reporting requirements.

The risk ratings are expressed as follows:

- the **inherent risk** is the rating of the risk **before** existing controls and its effectiveness are taken into account
- the **residual risk** is the rating of the risk **after** existing controls and its effectiveness are included in the assessment
- the **target risk** is the rating of the risk **after** any treatment plan outcomes, are applied to the residual risk rating.

### 2.3.2 Risk Controls and Effectiveness

Any controls listed as a mitigating factor must then be assessed for their control effectiveness when determining the residual risk. This determines how the residual risk is rated compared to the inherent risk rating. Refer to Table 2 Control Effectiveness for ratings and explanations.

The assessment of control effectiveness requires a robust and defensible assessment of controls. A quantitative assessment technique can be used to determine the adequacy of existing controls to mitigate a particular risk.

For example, a control to mitigate the risk of *'Fraud or corruption'* occurring, could be *'gift and benefits register in place'*, but as an example, the control may only be rated *'needs improvement'* on Table 2: Control Effectiveness. The reason for the control effectiveness being rated as *'needs improvement'* may be because a survey of staff has been undertaken which indicates that whilst there is a gifts and benefits register in place, the *'requirement to complete the gift register is not understood by all staff, particularly temporary staff'*. As a result, the control is determined to be weak and does not adequately mitigate the risk. In this example the recommended action would be that management implements further controls/actions to manage the risk and improve the standard of control effectiveness.

**Table 2 Control Effectiveness**

Control Effectiveness	Internal Audit Rating	Guide
Effective	5	Controls are well designed for the risk, are largely preventative and address the root causes The controls are effective and reliable
Mainly Effective	4	Well controlled with some control weaknesses / areas for improvement identified
Adequate	3	Reasonable level of controls, however, some control weaknesses of concern identified
Needs Improvement	2	Adequate level of control in some areas, however, significant control weaknesses in a number of areas
Non-Effective	1	Poorly controlled. Significant weaknesses in internal controls <u>OR</u> The controls that can be put in place are very limited due to the type of risk (beyond control of DFSI)

### Table 3 Consequence Criteria

The following table is a generic table for use within DFSI Divisions, Related Entities, Business Units or projects. Variations to this generic table in Divisions', Related Entities', Business Units' or projects' risk frameworks can occur; however, any variation to the consequence table needs to be reviewed and agreed with the DFSI Director Risk Services.

DFSI Risk Consequence Table					
Scale	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Criteria	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten DFSI's ability to achieve organisational objectives.	Significant threat to DFSI's functions and ability to fulfil its purpose and organisational objectives.
Budget, Revenue and Capital Spend <sup>2</sup>	Negligible increased costs by, whichever is lowest, <\$100K or <2% of full year total expenses budget Revenue leakage <3% of total revenue budget Capital under or over-spend <3%	Minor increased costs by whichever is lowest \$100K to <\$500k or 2% to <5% of full year total expenses budget, with minor impacts Revenue leakage 3% to <10% of total revenue budget Capital under or over-spend 3% to <10%	Moderate increased costs by, whichever is lowest, > \$500K to <\$5m or >5% to 8% of full year total expenses budget, with significant impacts Revenue leakage >10% to <15% of total revenue budget Capital under or over-spend >10% to <15%	Major increased costs by, whichever is lowest, \$5m to <\$10m, or 8% to <12% of full year total expenses budget, with major DFSI wide impact Revenue leakage 15% to <20% of total revenue budget. Capital under or over-spend >15% to <20%	Severe increased costs by, whichever is lowest, \$10m+ or 12%+ of full year total expenses budget, with severe DFSI wide impact Revenue leakage 20%+ of total revenue budget Capital under or over-spend 20%+

<sup>2</sup> Consequence criteria for Budget, Revenue and Capital Spend are to be reviewed annually and adjusted as required by the CFO.

<b>DFSI Risk Consequence Table</b>					
<b>Scale</b>	<b>Negligible (1)</b>	<b>Minor (2)</b>	<b>Moderate (3)</b>	<b>Major (4)</b>	<b>Severe (5)</b>
<b>Criteria</b>	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten DFSI's ability to achieve organisational objectives.	Significant threat to DFSI's functions and ability to fulfil its purpose and organisational objectives.
<b>Reputation, Stakeholders and Clients</b>	No media attention No loss of client or stakeholder confidence Negligible impact on reputation	Minor level adverse publicity in local media and no broader media reporting May create some short-term, temporary concern amongst clients or stakeholders Readily controlled negative impact on reputation	Limited adverse publicity May create temporary loss of credibility to clients or stakeholders Ministerial enquiries Verbal advice required to Minister's office or Treasury	State-wide and/or national adverse publicity Lead and/or major story in media, with potential for lasting damage to reputation of DFSI Serious loss of credibility with clients, Ministers office and key stakeholders Written advice and follow up with Treasury or Minister's office	Repeated lead and/or major story in media Prolonged negative ministerial attention Critical long-term loss of credibility with clients, Ministers office and key stakeholders Royal Commission inquiry, or Major ICAC investigation/hearing, or adverse and published Auditor General findings
<b>Our People</b>	Very limited/transient staff engagement problems No threat to critical skills or business knowledge Little or no effect on operations	Minor staff engagement problems Short-term loss of skills and business knowledge, effect absorbed within routine operations	Key person loss Loss of a critical skill, or some loss of skills and corporate knowledge with programs/strategies compromised Some industrial disputes	Loss of critical skills and key people, programs/strategies cannot be delivered Capacity to attract quality staff is compromised Major industrial disputes	Significant loss of critical skills, key people and business knowledge, programs/strategies are not delivered Significant long-term industrial disputes involving multiple unions/large staff numbers

<b>DFSI Risk Consequence Table</b>					
<b>Scale</b>	<b>Negligible (1)</b>	<b>Minor (2)</b>	<b>Moderate (3)</b>	<b>Major (4)</b>	<b>Severe (5)</b>
<b>Criteria</b>	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten DFSI's ability to achieve organisational objectives.	Significant threat to DFSI's functions and ability to fulfil its purpose and organisational objectives.
<b>Service Delivery Internal</b>	Minimal disruption to services Short infrequent disruptions to IT Services (<4 hours)	Some disruption to services provided by a business unit(s) or at a site IT Services not available for <1 day	Disruption to services provided by an operational unit or site, and affecting other operational units IT Services not available for >1 day and <3 days	Key DFSI operations / service provision disrupted Access to a Divisional office or several building levels/floors denied >3 days and <5 days IT services not available DFSI wide for >3 working day and <5 working days	Total shut down of operations and or access to premises denied >5 day IT Services not available DFSI wide for >5 days



<b>DFSI Risk Consequence Table</b>					
<b>Scale</b>	<b>Negligible (1)</b>	<b>Minor (2)</b>	<b>Moderate (3)</b>	<b>Major (4)</b>	<b>Severe (5)</b>
<b>Criteria</b>	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten DFSI's ability to achieve organisational objectives.	Significant threat to DFSI's functions and ability to fulfil its purpose and organisational objectives.
<b>Service Delivery External</b>	Minimal or no impact on service delivery or operations	Minor disruption to service delivery and operations (1 to 2 hours)	Moderate disruption to operations due to restricted supply or services, requiring some alternate arrangements by management  Client group dissatisfaction	Major disruption to operations due to significant loss of supply or services  Some alternate arrangements difficult or unavailable  Medium/short-term loss of business capability  Major community or client dissatisfaction and high levels of complaints	Long-term loss of business capability  Very significant and long-term disruption to supply or services  Very few or no alternate arrangements available  Significant level of community, client and executive dissatisfaction  Significant Ministerial and/or Secretary intervention and dissatisfaction

<b>DFSI Risk Consequence Table</b>					
<b>Scale</b>	<b>Negligible (1)</b>	<b>Minor (2)</b>	<b>Moderate (3)</b>	<b>Major (4)</b>	<b>Severe (5)</b>
<b>Criteria</b>	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten DFSI's ability to achieve organisational objectives.	Significant threat to DFSI's functions and ability to fulfil its purpose and organisational objectives.
<b>Regulatory (Compliance, Legislation and Environment)</b>	Minor non-compliance with minimal impact on operational business processes  Rare legislative non-compliance, little or no effect on business operations  Negligible impact on local environment	Regulatory non-compliance requiring local staff effort to rectify  Isolated legislative non-compliance, effect managed at operational level  Minimal impact on local environment	Regulatory non-compliance requiring management effort to rectify  Control failures resulting in frequent legislative non-compliance  Significant effect on DFSI business operations requiring changes to business processes  Some impact on local environment	Regulatory non-compliance resulting in notification by a regulating authority  Grossly negligent breach of legislation  Formal investigations, disciplinary action, ministerial involvement  Substantial impact on local and surrounding environments	Significant non-compliance which may result in fine to agency and/or prosecution  Widespread serious or wilful breach  Prosecutions, dismissals and Parliamentary scrutiny  Severe impact on local and surrounding environments
<b>Work, Health and Safety (Our people and the public)</b>	Minor injury, first aid treatment, minimal or no lost work time	Moderate injury, medical treatment and lost work time resulting in compensation claim	Serious injury resulting in hospitalisation and/or significant compensation or public liability claim	Potential for multiple injuries  Dangerous occurrence requiring notification to WorkCover	Catastrophic event involving multiple injuries or fatalities and/or dangerous occurrence from extensive/catastrophic damage to property and infrastructure

<b>DFSI Risk Consequence Table</b>					
<b>Scale</b>	<b>Negligible (1)</b>	<b>Minor (2)</b>	<b>Moderate (3)</b>	<b>Major (4)</b>	<b>Severe (5)</b>
<b>Criteria</b>	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten DFSI's ability to achieve organisational objectives.	Significant threat to DFSI's functions and ability to fulfil its purpose and organisational objectives.
<b>Major Projects (For use by Strategic Program and Performance Management Office Major Projects)</b>	<p>No threat to overall timeframe</p> <p>Negligible cost increase &lt;5%</p> <p>Scope increase/decrease barely noticeable</p> <p>Quality degradation barely noticeable</p> <p>Insignificant impact on benefits</p>	<p>Delay &lt;5% of original timeframe</p> <p>&lt;5% cost increase or &lt;\$100k, whichever is less</p> <p>Minor areas of scope affected</p> <p>Objective achieved but slight reduction in quality</p> <p>5% to &lt;10% benefits not delivered</p>	<p>Delay 5% to &lt;10% of original timeframe</p> <p>5% to &lt;10% cost increase or \$100k to &lt;\$250k, whichever is less</p> <p>Major areas of scope affected</p> <p>Objective achieved but quality reduced significantly</p> <p>10% to &lt;20% benefits not delivered</p>	<p>Delay 10% to &lt;20% of original timeframe</p> <p>10% to &lt;20% cost increase or \$250k to &lt;\$500k, whichever is less</p> <p>Scope increase/decrease unacceptable</p> <p>Quality reduction unacceptable with major impact on objectives</p> <p>20% to &lt;30% benefits not delivered</p>	<p>Delay 20%+ of original timeframe</p> <p>20%+ cost increase or \$500k+, whichever is less</p> <p>Product or services does not meet key requirements</p> <p>Quality issues lead to non-achievement of objectives and outcomes are not delivered</p> <p>30%+ benefits not delivered</p>

**Table 4 Likelihood Rating**

The following table is a generic table for use within DFSI, and includes control effectiveness in the rating.

Likelihood Rating	Description	Frequency	Probability
Almost Certain (5)	<p>The event will almost certainly occur within next twelve months</p> <ul style="list-style-type: none"> <li>• Complex process with non-effective / no controls in place</li> <li>• Impacting factors are outside of DFSI control</li> </ul>	Risk event could occur up to several times within the next twelve months or during project life, whichever is shorter.	>95%
Likely (4)	<p>The event is likely to occur within next twelve months</p> <ul style="list-style-type: none"> <li>• Previous audits/reports/reviews indicate a level of non-compliance</li> <li>• Controls are inadequate to mitigate the risk and require improvement</li> <li>• Impacting factors are outside of DFSI control</li> </ul>	Risk event is likely to occur once in the next twelve months or during project life, whichever is shorter.	70% to <95%
Possible (3)	<p>The event could occur in some circumstances</p> <ul style="list-style-type: none"> <li>• Previous audits/reports/reviews indicate a level of non-compliance</li> <li>• Controls are reasonable/adequate to mitigate the risk but may still require improvement</li> <li>• Some impacting factors may be outside of DFSI control</li> </ul>	Risk event may occur during the next twelve months or during project life, whichever is shorter.	30% to <70%
Unlikely (2)	<p>The event is not expected to occur during normal operations.</p> <ul style="list-style-type: none"> <li>• The event may occur but is unlikely to occur within next twelve months</li> <li>• Process is non-complex</li> <li>• Controls are in place and are mostly effective</li> </ul>	Risk event is unlikely to occur in the next twelve months or during project life, whichever is shorter.	5% to <30%
Rare (1)	<p>The event may occur only in exceptional circumstances.</p> <ul style="list-style-type: none"> <li>• No previous incidence of non-compliance</li> <li>• Controls are effective and are being monitored regularly</li> </ul>	Risk event is not expected to occur for some time or during project life, whichever is shorter.	<5%

## 2.4 Requirement 4: Evaluating Risk

The results of risk analysis are subjected to risk evaluation to make decisions about whether further treatment is required, which risks need treatment, treatment priorities and whether the risk must be escalated to the next level of management for review (refer to Table 6 Residual Risk Rating Review Requirements).

Generally, a risk review involves four distinct steps, these being:

- comparison with similar risks
- escalation to the next level of management for review and acceptance, and then reporting and managing by an appropriate manager
- where required, the development of treatment plans to further reduce the residual risk rating
- regular review as required by the residual risk rating.

**Table 6 Residual Risk Rating Review Requirements**

<b>Residual Risk Rating</b>	<b>Impact</b>	<b>Reporting and Review Requirements</b>	<b>Authority for Continued Tolerance of Risk or Changing Review Frequency</b>
<b>Extreme</b>	<p>Extreme adverse effect on DFSI</p> <p>Immediate Secretary / DFSI Executive Team action required</p>	<p>Reported immediately to the next level of management, then reviewed weekly until resolved or the risk rating changes to "high"</p> <p>Treatment action plans are required to reduce the risk rating</p>	Secretary
<b>High</b>	<p>Potential for high adverse effect on DFSI</p> <p>Action required by DFSI Executive Team member</p>	<p>Reviewed by the next level of management when initially rated and then every month unless approved by the appropriate authority and then to be reviewed no less than quarterly</p> <p>Treatment action plans should be considered to reduce the risk rating further</p> <p>Consideration of escalation of the risk to the Secretary; or to be managed at Division level</p>	Responsible DFSI Executive Team member
<b>Medium</b>	<p>Potential for medium adverse effect on DFSI</p> <p>Action required by responsible manager</p>	<p>Reviewed by the next level of management when initially rated and then every three months</p> <p>Treatment action plans could be used to reduce the risk rating further</p>	Responsible Manager
<b>Low</b>	<p>Low potential for adverse effect on DFSI</p>	<p>Ongoing control as part of a business as usual management, review no less than every six months</p>	Risk Owner

The decision to tolerate a risk and continue the exposure should be based on a consideration of the:

- cost-effectiveness to further treat the risk
- willingness of DFIS to tolerate risks of that type and risk rating
- need to escalate the risk to the next level of management to manage.

Low risks may be accepted with minimal further treatment. They are to be monitored and reviewed periodically to ensure they remain tolerable.

## 2.5 Requirement 5: Treating Risks

Risk treatment is the activity of selecting and implementing appropriate treatment measures to modify and reduce the risk. Risk treatment includes, as its major element, risk controls and includes the treatment options below. Any system of risk treatment should provide efficient and effective internal controls. Additional treatments, in the form of treatment plans may be required if the residual risk rating is unacceptable, refer to Table 6 Residual Risk Rating Review Requirements.

Treatment options, which are not necessarily mutually exclusive or appropriate in all circumstances, should be considered in the order below:

- (1) **Risk avoidance:** to avoid a risk with a detrimental consequence by deciding not to proceed with the activity likely to create risk (where this is practicable).
- (2) **Changing the likelihood of the risk:** to enhance the likelihood of beneficial outcomes and reduce the likelihood of negative outcomes.
- (3) **Changing the consequences:** to increase the gains and reduce the losses, this may include emergency response, business continuity plans and disaster recovery plans.
- (4) **Risk transfer:** this may include taking the appropriate insurances or the requirement for a warranty as part of a contract.
- (5) **Risk tolerance without further treatment:** this involves an explicit decision to accept the risk.

Selecting the most appropriate treatment option involves comparing the cost of implementing each option against the benefits derived from it. In general, the cost of treating risks will need to be commensurate with the benefits obtained. Divisions and Entities are to determine if costs for treatment of risks can be met from within their budgets or if a corporate or Treasury funding request is required.

A number of treatment options should be considered and applied, either individually or in combination. Decisions should take account of the need to consider carefully rare but severe risks that may warrant risk treatment actions that are not justifiable on strictly economic grounds. Legal, reputational and reporting requirements may require more detailed analysis.

Additional risk treatments to reduce the residual risk rating may be resolved into either a treatment plan or a number of specific treatment plans and these are to be allocated to nominated individuals who are accountable for their completion. Once treatment plans have been completed they may, if appropriate as ongoing mitigation for a risk, become a control.

## 2.6 Requirement 6: Monitoring and Reviewing Risks

The DFSI Executive Team reviews all Strategic Risks on a quarterly basis, which includes:

- a risk management report for all DFSI risks rated 'extreme' and 'high'
- any significant changes in the risk profile (including emerging risks) since the last report and the reasons for the changes
- any other specific risk issues or concerns.

The DFSI Director Risk Services reports to the DFSI Executive Team every quarter on the following:

- all strategic risks
- any emerging strategic-level risks
- all risks that are rated 'extreme' or 'high'
- progress of the risk and resilience implementation within DFSI including any issues or concerns.

The DFSI Director Risk Services reports to the DFSI Audit and Risk Committee, and other Audit and Risk Committees as agreed, on:

- all strategic risks rated 'High' or 'Extreme'
- emerging risks
- risk and resilience program implementation progress.

Divisional / Related Entities / Business Unit risk champions (or nominated managers) need to ensure that prior to reports being provided to the DFSI Executive, DFSI Director Risk Services or Audit and Risk Committees that:

- risk, control and treatment owners have updated their risk, control, treatment plan in the risk register
- the Divisional / Related Entity / Business Unit risks register has been reviewed and approved by the relevant DFSI or Divisional Executive Team member or manager.

### 2.6.1 Recording Risks

All risks are to be recorded in risk registers. The outputs from each stage of the risk management process will be recorded appropriately and specifically. The DFSI Risk Services Branch will develop risk resources which align to ISO 31000:2009 *Risk*



*Management Principles and Guidelines* and best practice principles to assist Divisions / Related Entities / Business Units to develop consistent process for the capture and recording of risk and this information will be available via a 'knowledge bank' on the DFSI intranet.

These registers contain information about the relied-upon controls in terms of a description of the control and the control owner. Risk treatment plans are to be recorded in the appropriate section. The reports generated from the risk registers are defined as strategic, operational or project risk management plans.

Risk management plans are to contain for each risk, the:

- risk owner
- causes
- impacts
- inherent risk (*risk rating before controls are considered*)
- existing controls being relied upon, including the:
  - outline of the control in-place
  - name of the control owner for each control
  - review requirements.
- residual risk rating (*risk rating after controls and their effectiveness are considered*)
- treatment plans (if required) containing for each plan:
  - an outline of the treatment plan, the owner and expected completion date
  - the target risk rating (*risk rating after treatment plans are completed*).

## **2.6.2 Risk Register Review**

Risk owners are to regularly review their risks, ensure that control owners and, where applicable, treatment plan owners are monitoring and reporting on their control and/or treatment plans.

Before reports are made to the DFSI Executive Team, DFSI Director Risk Services and Audit and Risk Committees, Divisions / Related Entities / Business Units are to ensure that risk registers, controls and treatment plans are up-to-date.

## 2.7 Requirement 7: Communication and Consultation Plan

The DFSI Risk Services Branch provides a risk management communication plan to provide general information for staff and specific information for those users of risk management within DFSI. The communication plan includes how information from users is to be obtained to ensure feedback is included in the ongoing review of risk management.

### 2.7.1 DFSI Risk Network

Division / Related Entity / Business Unit risk champions for risk management across the organisation meet informally as a risk network to share learning, mentor development and to assist with communicating risk management across their respective areas.

Information is shared within the risk network electronically and during individual or risk network meetings. A system is provided to manage the information flow and capture learning from the group. Further details on the risk champion's responsibilities are available in section 1.5.

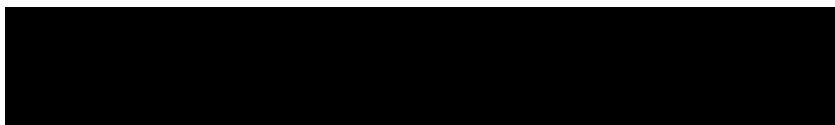
### 2.7.2 Training Strategy

Training of all relevant managers and staff (those identified as being users of the system) about the risk management processes and the online risk management system is a major element of the implementation of the Framework. A training plan has been prepared that covers:

- awareness briefings for all relevant managers and staff
- competency training for both the DFSI and Divisional Executive Team members and nominated persons from Divisions, Related Entities, Business Units and projects on the risk and resilience documentation and the online risk management system
- periodic re-training and continuing professional development for nominated managers and/or project managers.

After the initial training program, regular refresher and new-starter training are conducted on a regular basis to ensure that existing users and new users are familiar with risk management within DFSI.

The DFSI Principal Officer Risk is responsible for administering the training plan.



### 3. Glossary of Terms

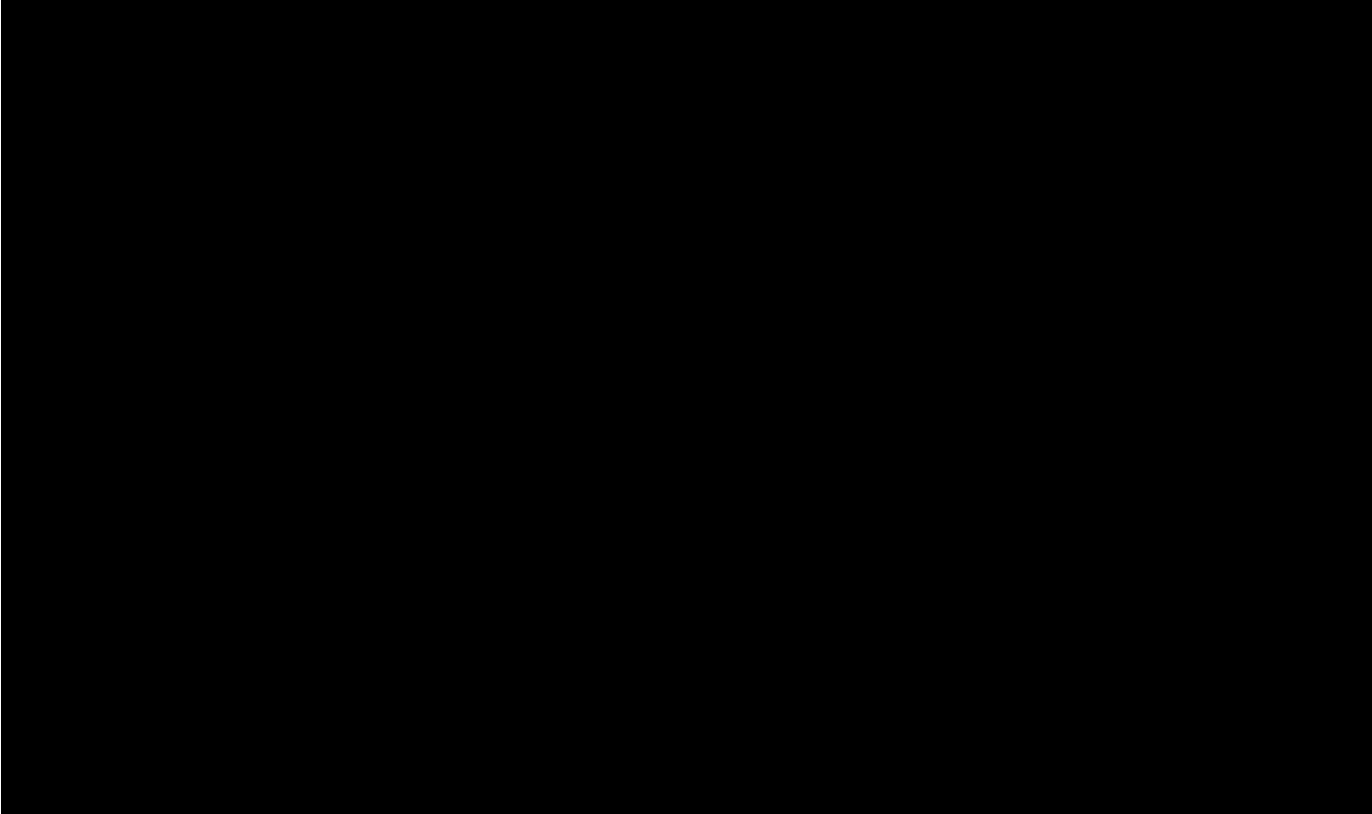
The following definitions are used throughout DFSI. All staff and contractors working for DFSI are to use these definitions. The definitions are consistent with ASNZS/ISO 31000:2009.

Term	Definition
Cause	Something that gives rise to or creates a risk.
Consequence	Positive or negative impact on an objective.
Control	Currently existing processes, policy, procedures or other actions that act to minimise negative risks and/or enhance opportunities.
Control Assessment	The periodic and systematic review of processes to ensure that controls are still effective and appropriate.
Control Effectiveness	A quantitative assessment of actual level of control that is currently present and effective compared with that which is reasonably achievable for a particular risk.
Control Owner	The person nominated as accountable for the assurance of the control to ensure that both the design and the operation of the control are effective.
ICT Risk Management	Information Communication Technology (ICT). The NSW Digital Information Security Policy mandates a risk-based approach to securing information, based on the ISO 27001 standard. DFSI has implemented a framework in line with the policy, with ICT risks being managed through an Information Security Management System (ISMS).
Inherent Risk	Initial assessment of the consequence and likelihood of the risk. Does <u>not</u> take into account the impact of existing controls or their effectiveness.
Issue	An issue is when something has gone or is going wrong and will affect the organisation.
Likelihood	The chance of something happening. May be defined, measured or determined objectively or subjectively and described verbally or mathematically.
Operational Risk	Risks associated with business-as-usual activities at the Division / Business Unit / Related Entity level that is normally managed within that area, unless the level of risk requires a review by the DFSI Executive and/or Secretary.
Project Risk	A risk which may significantly affect the likelihood of a projects being completed to planned time, quality and/or budget.
Risk Rating	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

<b>Term</b>	<b>Definition</b>
Residual Risk	Risk rating remaining after controls are in place and effectiveness reviewed.
Resilience	Adaptive capacity of an organisation in a complex and changing environment.
Risk	Effect of uncertainty on objectives. (This may be a positive or negative impact)
Risk Appetite	The level of risk exposure and type of risk which is considered tolerable and justifiable should it be realised.
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk.
Risk Assessment	The overall process of identifying, analysing and evaluating risks and its controls. May involve qualitative or quantitative assessment.
Risk Avoidance	Decision not to be involved in, or to withdraw from, an activity based on the level of risk.
Risk Management	The culture, processes, coordinated activities and structures that are directed to realising potential opportunities or managing adverse effects. It includes communicating, consulting, establishing context, identifying, analysing, evaluating, treating, monitoring and reviewing risks.
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation.
Risk Management Plan	A plan which takes the Risk Register further, considering DFSI's appetite for the risk, any gaps between existing controls and appetite, and proposing treatments for any remaining risks, which are assigned to owners, given deadlines and monitored.
Risk Matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood.
Risk Owner	The person with the accountability and authority for managing the risk and any associated risk controls or treatment plans.
Risk Register	Record of information about identified risks and management.
Risk Tolerance	The amount of risk the organisation is willing to accept based on the level of residual risk and effectiveness of controls.
Risk Treatment	Actions planned and undertaken to deal with any gaps between existing controls and the agreed appetite for the risk.
Risk Treatment Plan	Documents the risk treatment actions to be taken; includes details of separate tasks to address any gaps between existing controls, (see Table 6 Residual Risk Rating Review Requirements), and the risk appetite.

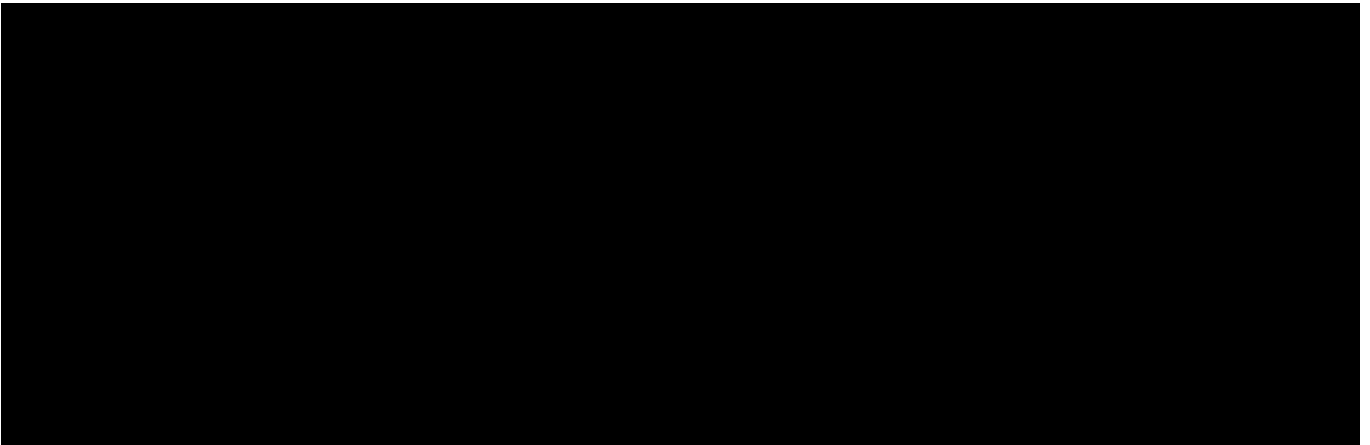
Term	Definition
Shared Risk	Is a risk which is shared with another DFSI Division/Entity and/or another external government agency/service provider/s; where both parties have a responsibility for the mitigation activities to manage/reduce the level of risk.
Strategic Risk	Internally or externally generated forces that may have a significant impact on the achievement of the DFSI strategic objectives and is managed by a DFSI Executive Team member.
Target Risk	The risk rating after any treatment plan outcomes are added to the residual risk assessment.
Treatment Owner	The person nominated as accountable for the completion of a risk treatment action plan.

# 4. Related Policies and Documents

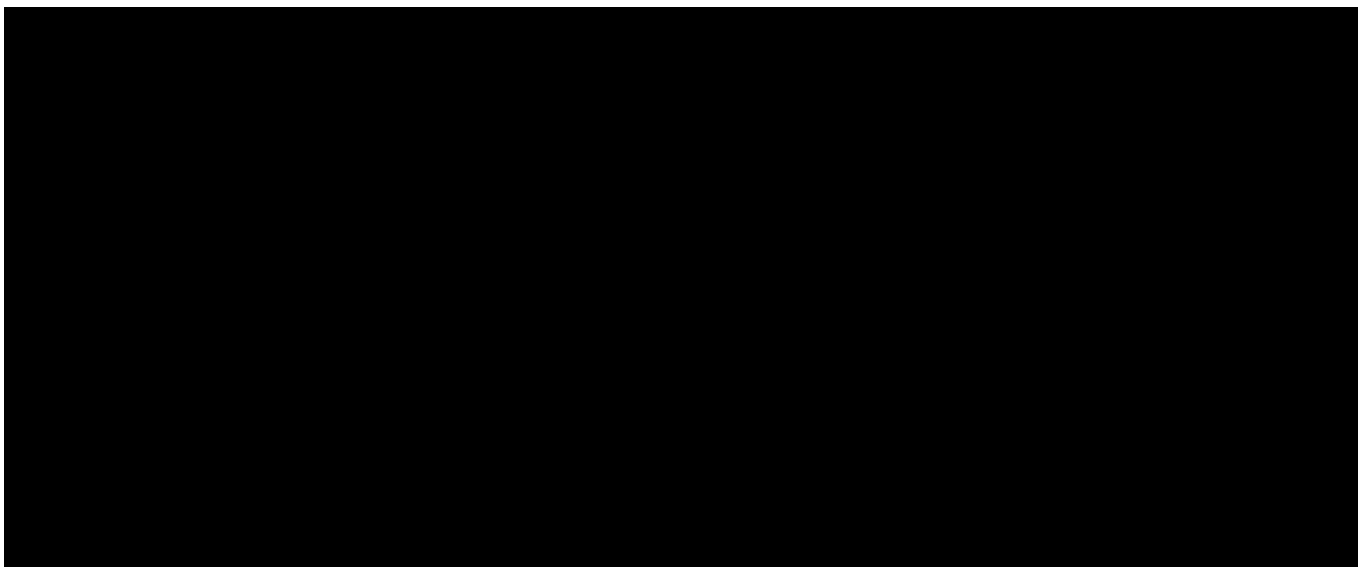


## 5. Document Control

### 5.1 Document Approval



### 5.2 Document Version Control



### 5.3 Review Date

This policy will be reviewed in November 2016.

It may be reviewed earlier in response to post-implementation feedback from Business Units.





## Schedule 3: Service Level Agreement

### 1. Definitions and Interpretation

1.1 In this Service Level Agreement (SLA), unless the contrary intention appears:

- (a) **"Affected Period"** has the meaning given to that term in clause 4.1 of this SLA.
- (b) **"AST"** or **"Agreed Service Time"** means the period in each month during which the Customer requires the full functionality of a service to be available for use in accordance with its specifications, being 24 hours a day, 7 days a week, excluding any part of that period that is Excusable Downtime.
- (c) **"Change"** has the meaning given to that term in the ITIL.
- (d) **"Change Management Policy"** means the Change management policy and any other Change policy, process and procedures notified by the Customer to the Contractor from time to time.
- (e) **"Change Request"** or **"Request for Change"** has the meaning given to that term in the ITIL. For the purposes of this SLA only, any Change Request referred to in this SLA (including its Exhibit 1 and Exhibit 2) does not constitute a Change Request as defined in the Dictionary in Part 3 of the Procure IT Framework and as referred to in Part 2 of the Customer Contract.
- (f) **"CI"** or **"Configuration Items"** has the meaning given to that term in the ITIL.
- (g) **"Circumventable Event"** has the meaning given to that term in clause 4.2 of this SLA.
- (h) **"CMDB"** or **"Configuration Management Database"** has the meaning given to that term in the ITIL.
- (i) **"CSL"** or **"Critical Service Level"** means a Service Level for which Service Credits may be payable if the Contractor fails to meet that Service Level, being a Service Level that is identified as a "CSL" in the Service Levels Matrix.
- (j) **"DT"** or **"Downtime"** means the period in a month during which the full functionality of a service is not available for use in accordance with its specifications, excluding any part of that period that is Excusable Downtime.
- (k) **"Effective Rollback Plan"** means a list of steps, actions and process required to effectively undo a Change and restore a system or environment to the same state it was prior to the implementation of said Change.
- (l) **"Event"** has the meaning given to that term in the ITIL.
- (m) **"Excusable Downtime"** means:
  - (i) any period of planned outage in respect of the relevant service that has been agreed by the parties in writing; and

- (ii) any Affected Period that is to be disregarded in calculating the relevant Service Level for the service in accordance with clause 4.4 of this SLA.
- (n) "**Excusable Event**" has the meaning given to that term in clause 4.1 of this SLA.
- (o) "**Extreme Risk**" means a Security Vulnerability that has been (or should have been) classified as 'extreme' risk under clauses 3.27, 3.28 or 3.30 of this SLA, except if it is subsequently validly reclassified as 'high', 'medium' or 'low' risk under clauses 3.28 or 3.30 of this SLA.
- (p) "**Failure Period**" has the meaning given to that term in clause 7.2 of this SLA.
- (q) "**High Risk**" means a Security Vulnerability that has been (or should have been) classified as 'high' risk under clauses 3.27, 3.28 or 3.30 of this SLA, except if it is subsequently validly reclassified as 'extreme', 'medium' or 'low' risk under clauses 3.28 or 3.30 of this SLA.
- (r) "**Go Live**" has the meaning given to that term in the PIPP.
- (s) "**Incident**" has the meaning given in the Information Technology Infrastructure Library (ITIL).
- (t) "**ITIL**" means the Information Technology Infrastructure Library v3.
- (u) "**KPI**" or "**Key Performance Indicator**" means a Service Level for which no Service Credits are payable if the Contractor fails to meet that Service Level, being a Service Level that is identified as a "KPI" in the Service Levels Matrix. For the avoidance of doubt, the Contractor must still perform the Services to meet the KPI Service Levels and report on its performance of the Services against the KPI Service Levels.
- (v) "**Low Risk**" means a Security Vulnerability that has been (or should have been) classified as 'low' risk under clauses 3.27, 3.28 or 3.30 of this SLA, except if it is subsequently validly reclassified as 'extreme', 'high' or 'medium' risk under clauses 3.28 or 3.30 of this SLA.
- (w) "**Major Incident**" has the meaning given to that term in the ITIL.
- (x) "**Medium Risk**" means a Security Vulnerability that has been (or should have been) classified as 'medium' risk under clauses 3.27, 3.28 or 3.30 of this SLA, except if it is subsequently validly reclassified as 'extreme', 'high' or 'low' risk under clauses 3.28 or 3.30 of this SLA.
- (y) "**P1**", "**P2**", "**P3**" and "**P4**" refer to the corresponding priority levels the Customer allocates to Incidents from time to time in accordance with Customer's matrix of Incident priority levels, as set out in Exhibit 3 (Priority Levels) of this SLA (as those priority levels may be updated, replaced or superseded by the Customer from time to time by Notice in Writing to the Contractor).
- (z) "**Performance Management Framework**" means the combination of both the Service Management Service Levels and the Service Level Matrix as outlined in clause 2.1 of this SLA.

- (aa) "**Period of Calculation**" means, in respect of a Service Level, the period during which the Contractor's performance against that Service Level is measured, as specified in the Exhibit 2 to this SLA.
- (bb) "**Problem**" has the meaning given to that term in the ITIL.
- (cc) "**Problem Record**" has the meaning given to that term in the ITIL.
- (dd) "**Release**" has the meaning given in the ITIL.
- (ee) "**Resolution**", of a Security Vulnerability, means that the Security Vulnerability is patched or otherwise remediated, in each case so that the Security Vulnerability ceases to exist (or, if that is not possible, so that the risk associated with that Security Vulnerability is appropriately addressed to the satisfaction of the Customer) and no other Security Vulnerability has been created or expanded as a consequence of that patching or remediation. "**Resolve**" has a corresponding meaning.
- (ff) "**Security Vulnerability**" means any weakness, flaw, error, threat or other vulnerability in the Customer's systems, applications, firmware or infrastructure, including any circumstances that could facilitate (or that could be leveraged to facilitate) unauthorised access to, use of or Changes to any part of the Customer's environment or any data stored in or transmitted through that environment.
- (gg) "**Security Updates**" means all types of updates, patches, upgrades, new Releases and other improvements and modifications released in connection with anti-virus deployment and/or for the purposes of addressing or mitigating a Security Vulnerability.
- (hh) "**Service Credit**" means the service credits awarded against (and payable by) the Contractor for a failure to meet the Critical Service Levels in accordance with clause 6.5 of this SLA.
- (ii) "**Service Desk**" has the meaning given to that term in the ITIL.
- (jj) "**Service Hours**" has the meaning given to that term in clause 3.14 of this SLA.
- (kk) "**Service Integrator**" means the Customer's Personnel dedicated to service integration and service management.
- (ll) "**Service Levels**" means the minimum performance levels to be achieved by the Contractor and Deliverables, as specified in this SLA, and include CSLs, KPIs and SMSLs.
- (mm) "**Service Levels Matrix**" means the table set out in clause 6.4 of this ServiceLevel Agreement and extrapolated in Exhibit 2 to this SLA.
- (nn) "**Service Management Service Levels**" or "**SMSLs**" means the metrics outlined in Table 1 and extrapolated in Exhibit 2 to this SLA.
- (oo) "**Service Recovery Action**" means a permanent resolution or a workaround to be performed by the Contractor in order to restore a Service. The resolution or workaround may be part of a complex Incident restoration activity that is to be performed by multiple

service providers. The Service Recovery Action refers to the specific action assigned to the Contractor to support this restoration activity.

- (pp) **"Service Request"** or **"Request for Service"** has the meaning given to that term in the ITIL.
- (qq) **"SP"** or **"Service Provider"** has the same meaning as the Contractor in this SLA.
- (rr) **"Start Time"**, in respect of a Security Vulnerability, means the earliest of the following:
  - (i) when the Contractor is informed of or otherwise becomes aware of the Security Vulnerability;
  - (ii) when the Security Vulnerability is publicly disclosed;
  - (iii) when the Security Vulnerability is disclosed to a subscription-based database or any other service for information technology security professionals; and
  - (iv) when a Security Update is released to address the Security Vulnerability.
- (ss) **"Tiers"** means, in respect of an application, the tiers to be agreed between the Parties during the Transition In Period in accordance with Exhibit 1 to this SLA.

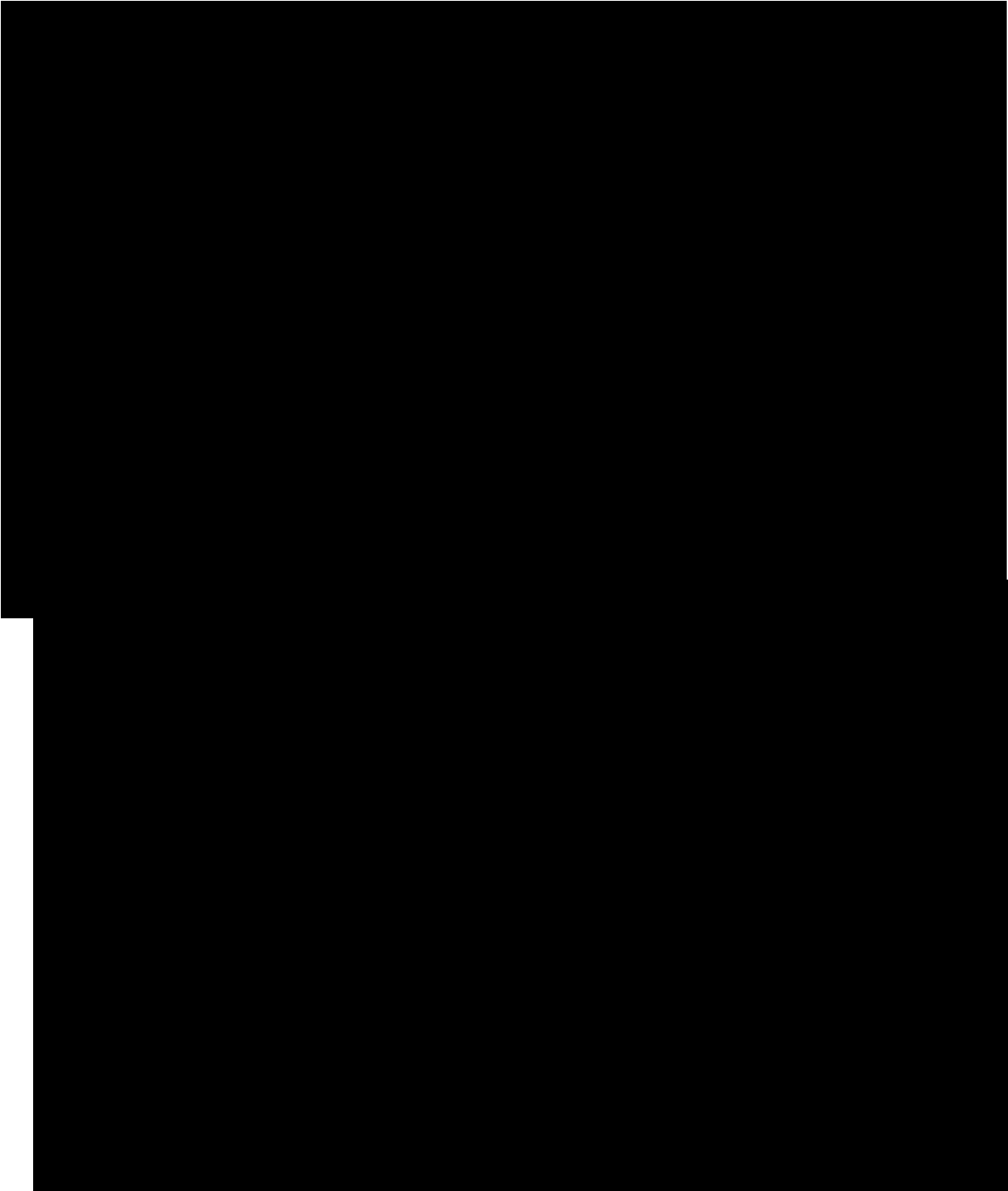
**1.2** Any terms defined in Module 12 (Managed Services), including **"Managed Services"**, **"Services"**, **"Transition In Period"**, **"Transition In Plan"** and **"Transition In Services"**, have the meanings given to those terms in Module 12.

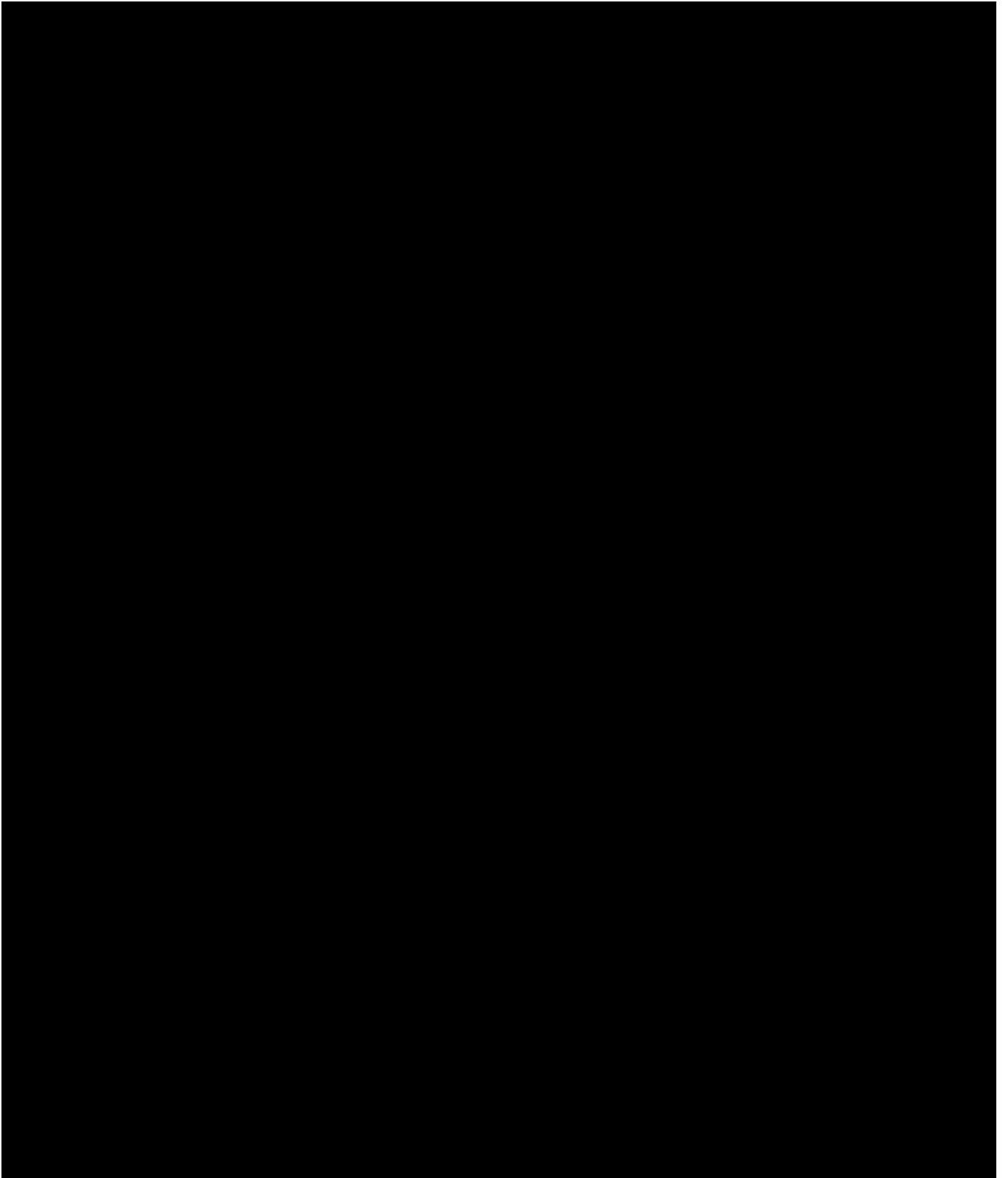
**1.3** Other capitalised words and expressions used in this SLA are defined in the Dictionary in Part 3 of the Procure IT Framework (as amended by Item 43 (Additional Conditions) of the General Order Form).

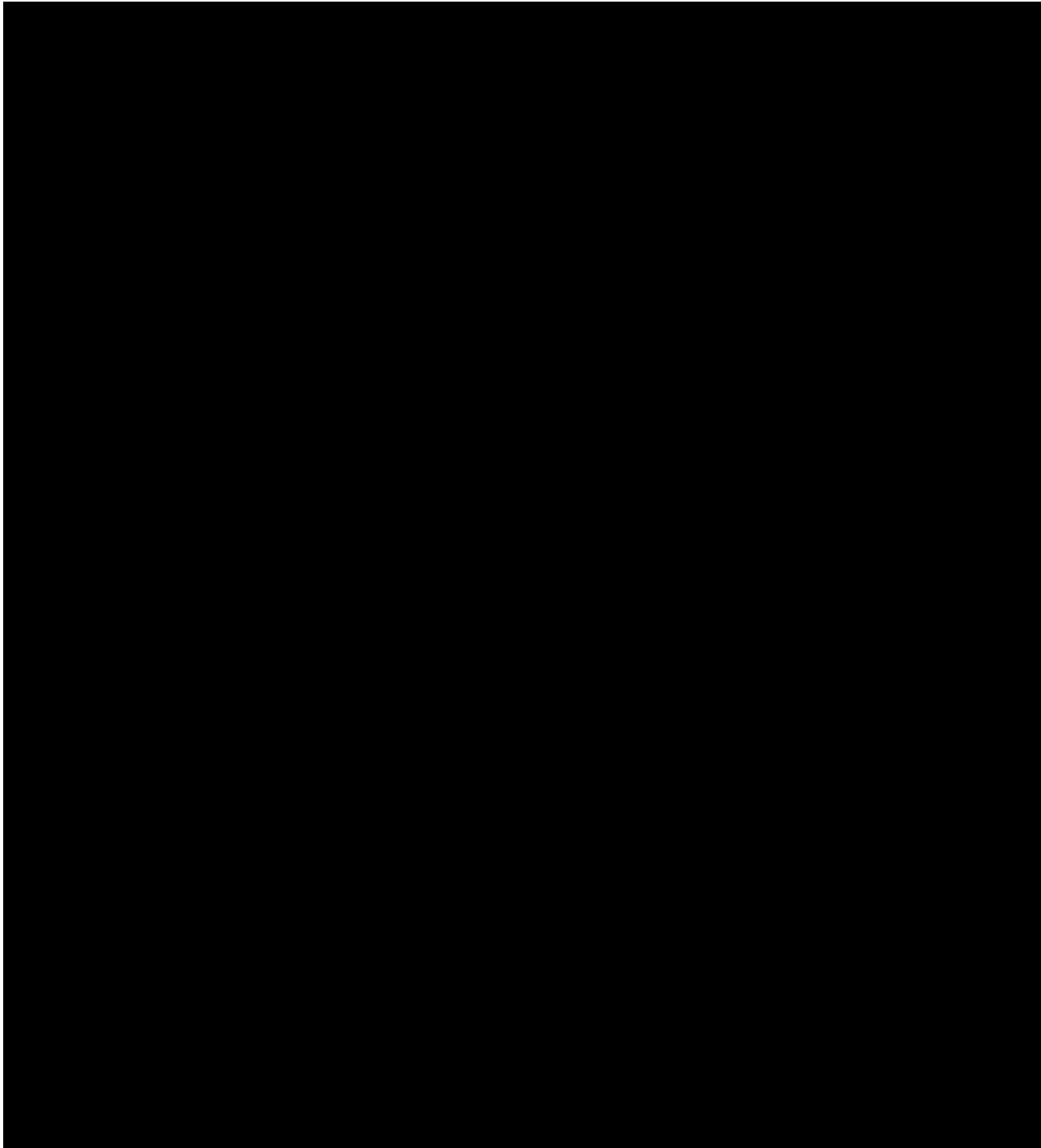
## **2. Performance Management Framework**

**2.1** The Customer seeks to establish a Performance Management Framework comprising of a multi-tiered system of overlapping Service Management Service Levels and a Service Level Matrix (including both Critical Service Levels and Key Performance Indicators), as illustrated in Diagram 1 below, which is designed to:

- (a) guarantee a minimum level of performance outcomes for end-point users,
- (b) incentivise collaboration between all internal and third party service providers within the Customer's environment, and
- (c) achieve the seamless integration of internal and third party service providers so as to provide end-point users a cohesive and efficient experience.







- 2.4** Further details of the above metrics are included in Exhibit 2 to this SLA.
- 2.5** Performance against all of these metrics will be monitored and reported on by the Service Integrator and both monitoring and reporting tasks will be performed in ServiceNow (unless otherwise specified).

- 2.6 The Contractor may also be required to provide access to other records or tools to allow the metrics to be effectively monitored as reasonably requested by the Service Integrator.
- 2.7 Each Service Management Service Level contains both a 'Minimum' and 'Expected' performance level benchmark within Exhibit 2 to this SLA, which indicates the expectations of the Customer with respect to the provision of Services within the integrated service offering provided to end users.
- 2.8 The Contractor must meet or exceed the 'Minimum' and 'Expected' performance levels outlined in the Service Management Service Levels within Exhibit 2 to this SLA.
- 2.9 For each Service Management Service Level, performance below the 'Minimum Performance Level' is contrary to the expectations of the Customer and requires the Contractor to undertake the actions outlined in clause 5.7 of this SLA. A failure by the Contractor to do so is considered a Substantial Breach for the purposes of clause 8.1 of the Item 43 Additional Conditions attached to the General Order Form.

### 3. General

#### PURPOSE OF SLA AND DELIVERY OF SERVICES

- 3.1 This SLA provides a mutual understanding of the Service Level expectations of the Parties and defines a benchmark for measuring the performance of the Services.
- 3.2 A further objective of this SLA is to drive continuous improvement and customer satisfaction in respect of the Services, as well as provide the Customer with a method for active management of the Customer Contract.
- 3.3 The SLA framework also provides a lever with which the Customer can manage risks associated with the delivery of Services to the agreed level of quality and value.
- 3.4 The Contractor must deliver Services in accordance with the relevant ITIL framework disciplines and the Customer's Service Level management policies and processes (as amended and notified to the Contractor from time to time).

#### DURATION OF SLA

- 3.5 This SLA applies to all Services and will commence, for each of the Services, upon the completion of Transition-In for those Services and the occurrence of Go Live for those Services (as defined in Schedule 12 (PIPP)).
- 3.6 The Service Levels set out in this SLA will apply for the duration of the Contract Period, unless otherwise specified by the Customer by Notice in Writing to the Contractor.
- 3.7 In the period commencing on the occurrence of Go Live for the Services (as defined in Schedule 12 (PIPP)) and ending two (2) calendar months thereafter (**Stabilisation Period**), the Parties agree that:
  - (a) the Contractor will measure and report on its performance against the Service



Levels in accordance with clause 6.1 of this SLA; but

- (b) no Service Credits will be payable by the Contractor in respect of any failure to meet a CSL during the Stabilisation Period.

#### REVIEW OF SLA

- 3.8 The Parties will review this SLA and the Contractor's performance of the Services against the Service Levels every 6 months from the date the Service Levels first apply to a Service pursuant to clause 3.5 above. Any agreed changes to the SLA arising out of such review will be documented and the Parties will update this SLA accordingly.

#### NOTIFICATION PROCEDURE

- 3.9 Any Problems or issues in relation to the Contractor's performance of the Services and its ability to meet the Service Levels must be included as an element of monthly Service Level reporting, as described in clause 3.13 below.
- 3.10 The Contractor shall provide a single point of contact for the prompt resolution of all Incidents and failures in relation to the quality of Services, regardless of whether such Incidents or failures were caused by Contractor.

#### DISPUTE PROCEDURE

- 3.11 If there is any dispute arising out of or in connection with this SLA and/or the performance of the Services in accordance with the Service Levels, the Parties will deal with that that dispute in accordance with clause 24 of Part 2 (Customer Contract).

#### ESCALATION PROCEDURE

- 3.12 The Parties will escalate any issues that arise from time to time in accordance with the following table:

	Officer (1)
Level 1	<b>Customer:</b> Service Level Agreement Manager Name and Contact Details: <i>To be agreed between the Parties during the Transition In Period</i>  <b>Contractor:</b> Service Level Agreement Manager Name and Contact Details: <i>To be agreed between the Parties during the Transition In Period</i>
Level 2	<b>Customer:</b> <i>To be agreed between the Parties during the Transition In Period</i> <b>Contractor:</b> <i>To be agreed between the Parties during the Transition In Period</i>
Level 3	<b>Customer:</b> <i>To be agreed between the Parties during the Transition In Period</i>

	<b>Contractor:</b> <i>To be agreed between the Parties during the Transition In Period</i>
--	--

### Table 1 Escalation levels

- (1) If the Parties' respective escalation points (including the relevant officers' titles, names and contact details) have not been nominated and set out in the above Table 2 of this SLA as at the Commencement Date of this Customer Contract, the Parties must nominate and agree on their respective escalation points for the above table (including those officers' titles, names and contact details) during the Transition In Period and prior to the Go Live Date.

## REPORTING AND ANALYSIS

- 3.13** The Contractor is required to produce and deliver a Service Level Report to the Customer on a monthly basis in accordance with the requirements of this SLA and Item 40 of the General Order Form.

## HOURS OF OPERATION

- 3.14** Services must be performed by the Contractor between 07:30 and 17:30 on Business Days in Sydney, New South Wales (**Service Hours**), except on a public holiday in New South Wales, subject to the Customer's requirements for support outside of these hours, as agreed with the Contractor and documented in the Customer Contract.

## CHANGES TO SERVICE LEVELS

- 3.15** The Customer may request additional Service Levels by giving the Contractor three (3) months' Notice in Writing (or a lesser period where agreed by the Contractor) at the end of which period the Parties will, acting reasonably, document the agreed changes and update this SLA accordingly.
- 3.16** Additional Service Levels will be negotiated from time to time during the Contract Period in good faith and will be based on baseline data from relevant service environment (where feasible) and best industry practices.
- 3.17** The Customer may also:
- (a) reclassify a Service Level (changing from KPI to CSL or vice versa); or
  - (b) change the Service Credit percentage applicable to one or more CSLs (as set out in the Service Levels Matrix),

by giving the Contractor Notice in Writing, and the Parties will update this SLA accordingly. Such reclassification or change will take effect on and from the start of the next Period of Calculation.

## TRANSITION IN

- 3.18** The Contractor must perform the Transition In Services (as defined in Module 12) in accordance with Module 12 and the Module 12 Order Form.
- 3.19** The Customer's existing computing integration services environment is comprised of a number of siloed cloud service providers, each undertaking independent ancillary tasks to support their own

service offering.

**3.20** Consequently, the focus of the Transition In Services (as defined in Module 12) is for the Contractor to perform discovery, training and knowledge acquisition activities in order to empower the Contractor to function as a single integrated service provider for all cloud and on premises services.

**3.21** At the completion of the Transition In Services (as defined in Module 12), the Contractor and its associated resources (including any third parties or Subcontractors) must have sufficient capability, expertise and understanding of the service environment so as to provide all required Services in accordance with the Service Levels as outlined in this SLA.

#### **MANAGEMENT AND CONSULTING**

**3.22** The Contractor is required to manage relationships with third parties, external vendors and Subcontractors as necessary to provide the Services in accordance with the Customer Contract.

#### **SERVICE REVIEW AND PLANNING FOR THE FUTURE**

**3.23** See clause 6.10 of Part 2 (Customer Contract). The items for review could include without limitation:

- Service provided during the review period*
- Major incidents during the review period*
- Problems that remain outstanding*
- Review of Contract Variation requests and progress for enhancements*
- Review of any Contract Variation plan*
- Future events or business developments that will affect the Service*
- Review any potential changes required to the SLA*
- Agree items for submission to the executive decision making*
- Review schedules for Services provided*

#### **RISK MANAGEMENT AND PROBLEM PREVENTION**

**3.24** The Contractor is required to update and maintain a risk register on a monthly basis as per Item 40 of the General Order Form.

**3.25** Risks are to be identified, catalogued, mitigated and controlled as outlined in Exhibit 1 (Risk and Resilience Framework) annexed to Schedule 12 (PIPP).

#### **SECURITY VULNERABILITY IDENTIFICATION AND CLASSIFICATION**

**3.26** The Contractor must use its best efforts to proactively identify all Security Vulnerabilities that may

pose a risk to the Customer from time to time (whether the risk is extreme, high, medium or low).

- 3.27** Promptly after a Security Vulnerability is identified, the Contractor must classify its risk level as 'extreme', 'high', 'medium' or 'low' in accordance with:
- (a) Table 5 – Risk Rating Matrix in Exhibit 1 (Risk and Resilience Framework) annexed to the PIPP;
  - (b) the Customer's applicable policies and procedures from time to time; and
  - (c) the following requirements:
    - (i) Notwithstanding paragraphs (a) and (b) above, a Security Vulnerability must be classified as 'extreme' if:
      - (A) the Security Vulnerability facilitates remote code execution, is in the public domain and is being actively used;
      - (B) critical business systems may be affected; and
      - (C) one or more of such systems are internet-connected without appropriate mitigating controls in place to address the Security Vulnerability.
    - (ii) Subject to the requirements of paragraphs (a) and (b) above, a Security Vulnerability may be classified as 'extreme' or 'high' (but no lower) if the circumstances described in paragraphs (i)(A) and (i)(B) above exist in respect of that Security Vulnerability, but paragraph (i)(C) above does not apply, and all systems that maybe affected by it are in a protected enclave with strong access controls.
- 3.28** If further information becomes available about an identified Security Vulnerability, the Contractor must reclassify the risk level of the Security Vulnerability in accordance with clause 3.27, taking into account that further information. However, notwithstanding any other provision of the Customer Contract, any such reclassification may not result in the Security Vulnerability having a lower risk level than that previously assessed by the Customer (if any) under clause 3.30 below.
- 3.29** Promptly following its classification (and any reclassification under clause 3.28 above), the Contractor must notify the Customer of the risk level of a Security Vulnerability.
- 3.30** If the Customer disagrees with any classification or reclassification of a Security Vulnerability, the Customer may, acting reasonably, itself reclassify the risk level of the Security Vulnerability as 'extreme', 'high', 'medium' or 'low' in accordance with clauses 3.27(a) to (c) above, by giving notice to the Contractor.
- 3.31** If a Security Vulnerability is reclassified by the Customer or the Contractor, then, for the purposes of assessing the Contractor's performance against CSL5 in clause 6.4 below only, the risk level of the reclassified Security Vulnerability will be deemed to be that of the last reclassification that was based solely on information that was available before the Security Vulnerability was Resolved by

the Contractor.

### QUALITY MANAGEMENT

- 3.32** The Contractor agrees to maintain, and ensure its Related Companies and Subcontractors maintain, a quality assurance plan for the scope of Services being delivered throughout the Contract Period.
- 3.33** The Customer may audit the quality assurance plan of the Contractor, its Related Companies and Subcontractors and the Contractor agrees to comply, and ensure its Related Companies and Subcontractors comply, with any reasonable direction of the Customer to improve any aspect of the quality assurance plan.

### DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

- 3.34** The Contractor is required to create and maintain a Business Contingency Plan as per Item 24 of the General Order Form

### SECURITY

- 3.35** The Contractor will implement a standard roll on/roll off process which includes an acknowledgement of the need to protect the confidentiality of the Customer's Confidential Information and Customer Data. This acknowledgment will be regarded as an internal Contractor record, but must be made available for audit if required by the Customer.
- 3.36** The Contractor acknowledges that the security of Customer Data is fundamental to the business of the Customer and that any security breach may directly affect the Customer's:
- (a) duties to its Personnel or to citizens; and
  - (b) obligations under the *Privacy and Personal Information Protection Act 1998* (NSW) and other Statutory Requirements applicable to the Customer.
- 3.37** Subject to Items 25A and 25B of the General Order Form, the Customer Data must remain in Australia and must be accessed only by staff of the Contractor in Australia and remotely as authorised by the Customer to access the Customer Data remotely for support and maintenance purposes. Such remote access must only be strictly in accordance with a protocol agreed between the Parties or otherwise agreed in writing. Agreed protocols will be used in relation to support (including information contained in the incident management system) which would include the ability to resolve Incidents, Problems or issues.
- 3.38** Where appropriate to the Services being performed, the Contractor will ensure that appropriate security frameworks, standards and compliance consistent with the ISO 27001 standard are in place for the Contractor and any Subcontractors.

### TRANSITION OUT

- 3.39** As per Box 3 of the Module 12 Order Form.

## 4. Exemptions

- 4.1 If the Contractor fails to meet a Service Level and such failure is directly caused by:
- (c) a Force Majeure Event (to the extent that the Contractor is relieved from meeting or exceeding the Service Level due to that Force Majeure Event under clause 26.9 of Part 2 (Customer Contract)); or
  - (d) the Customer's breach of the Customer Contract,

(each an **Excusable Event**), then subject to clauses 4.2 and 4.3 below, the Contractor may request the Customer to excuse it from the period of its Service Level failure that was caused (and to the extent caused) by the Excusable Event (**Affected Period**).

- 4.2 Without expanding on the Excusable Events available under clause 4.1, an event or circumstance that leads to a failure to meet a Service Level will not be regarded as an Excusable Event to the extent that such event or circumstances was caused or contributed to by a fault of the Contractor or its Personnel or the event or circumstances, or their effects, could have been:

- (a) prevented or limited by adopting or implementing reasonable precautions including reasonable business continuity or relevant disaster recovery practices (including industry standard redundancy, regular preventative maintenance, capacity planning, regular backups and off-site tape storage, uninterrupted power supplies); or
- (b) circumvented by the Contractor using alternative sources, appropriate workarounds or workload management practices or other means or any other prudent backup or recovery procedures,

(each a **Circumventable Event**).

- 4.3 If the Contractor is seeking to rely on clause 4.1 above, then it must promptly notify the Customer in its post Incident review of the details of the relevant Excusable Event and its impact on the Services and Service Levels, the Affected Period and extent that the Services were (or it anticipates that they will continue to be) impacted by the Excusable Event.
- 4.4 If the Customer agrees to the Contractor's request for relief from a Service Level failure on account of an Excusable Event (which is not a Circumventable Event) under clause 4.1 above, then the relevant Affected Period will be disregarded for the purpose of calculating the Contractor's performance of the relevant Service Level for the relevant month.

## 5. Responsibilities

- 5.1 The Customer will promptly notify Contractor as soon as an Incident or request arises that requires Contractor's attention and will provide sufficient details and documentation relating to the Incident or request as required, and the Contractor will itself perform monitoring for Incidents and other issues with the applications. The Contractor will take appropriate action to resolve the Incident or request as part of the Services.
- 5.2 If an Incident or request is identified by the Contractor's monitoring tools or the Contractor is otherwise informed, or becomes aware, of an Incident or request by means other than ServiceNow, the Contractor must record that Incident or request into ServiceNow as soon as reasonably practicable.

- 5.3 The Customer will provide the Contractor with an internal service desk or tracking number through integration.
- 5.4 The Customer will provide formal approval and sign-off before Changes are made to a production environment.
- 5.5 Where necessary to deliver the Services, the Customer will provide the Contractor with access to third party service providers and/or vendors who support dependent services networks, to the extent that such access is specified as a Customer Supplied Item in Item 22 of the General Order Form.
- 5.6 Without limiting its obligations under this SLA and the Customer Contract, the Contractor will:
- (a) consult as necessary with the Customer in order to provide the Customer with such information relevant to the Services and Service Levels as the Customer reasonably requires concerning the current and anticipated future performance of the Services and Service Levels;
  - (b) cooperate with all procedures reasonably implemented by the Customer in relation to the Services and Service Levels; and
  - (c) implement such recommendations as may be reasonably made by the Customer in order to ensure the Services continue to comply with the requirements of the Customer Contract and this SLA.
- 5.7 If, at any time the Contractor fails to meet a Service Level, it will promptly:
- (a) investigate the underlying cause of the failure;
  - (b) prepare and supply to the Customer a report on the failure;
  - (c) take whatever action is reasonably necessary to minimise the impact of the failure;
  - (d) correct the failure as soon as practicable;
  - (e) keep the Customer advised as to the progress being made in rectifying any circumstances which caused the failure; and
  - (f) if required pursuant to Item 43 (Additional Conditions) of the General Order Form, develop and implement an Action Plan to remedy the cause of that Service Level failure.

## 6. Performance Measurement

- 6.1 The Contractor's performance against Service Levels must be measured, tracked and reported by the Contractor (or the Service Integrator where it is specified as having 'Measurement Responsibility' in Exhibit 2 to this SLA) based on objective data, and may be validated and assessed by the Customer on a monthly basis, as per the reporting requirements set out in Item 40 of the General Order Form.
- 6.2 The Contractor (where it is specified as having 'Measurement Responsibility' in Exhibit 2 to this

SLA) must implement and maintain measuring and monitoring tools and procedures that:

- (a) measure the Contractor's performance against the Service Levels;
- (b) permit reporting at a level of detail sufficient to determine compliance with the Service Levels; and
- (c) are approved by the Customer.

**6.3** Where the Contractor is specified as having 'Measurement Responsibility' in Exhibit 2 to this SLA, if the Contractor fails to measure its performance against a particular Service Levels performance for the relevant measurement period and as a result it is not possible to confirm whether the Service Level has been achieved, then, unless such failure to measure was previously agreed in writing by the Customer, the Contractor shall be deemed to have failed to meet the relevant Service Level(s) and the applicable rights and remedies of the Customer under the Customer Contract, this SLA and at law shall apply.

**6.4** All Service Levels have been categorized into SMSLs, CSLs and KPIs as set out in table:

**Service Levels Matrix**

Service/ Responsibility	Classification	Service Level	Service Credit Percentage	Measurement	Period of Calculation
Availability of Services and Data	CSL1	Total Availability $\geq$ 99.9%	3%	[Total availability % = ((AST – DT)/AST) x 100]	Monthly
Reliability of Services	KPI1	1 $\leq$ P1 Incident 2 $\leq$ P2 Incidents	N/A	Number of Incidents by Incident priority	Monthly
Incident Resolution Time	KPI2	90% Incidents within: P1 - 4 hours P2 - 8 hours	N/A	% of Incidents resolved within specified time, by priority level	Monthly
Service Request Resolution Time	CSL2	95% of Tier A Service Requests completed within 1 hour 95% of Tier B Service Requests completed within 1 business day 95% of Tier C Service Requests completed within 3 business days	3%	% of total Service Requests resolved within specified time frame.  Service Request Tiers are outlined in Exhibit 1 to this SLA.	Monthly
Change Process – Unauthorised Changes	CSL3	0 Unauthorised Changes	3%	Number of unauthorised Changes made by Contractor	Monthly



Service/ Responsibility	Classification	Service Level	Service Credit Percentage	Measurement	Period of Calculation
Reporting Management	KPI3	1 ≤ Late Report	N/A	Number of reports submitted to the Customer more than 5 Business Days after agreed upon date.	As required by reporting cycle of relevant report outlined in Item 40 of the General Order Form.
Compliance with Security and ICT Policies	KPI4	≤ 1 non-compliance		Number of non-compliance Events	Monthly
Back up as a Service/ Recovery	KPI5	98%		[Total of all data backups completed on time during the Period of Calculation / total of all data backups scheduled in the Period of Calculation] * 100	Monthly
Change Management Quality	KPI6	≤ 1 P1 Incidents ≤ 2 P2 Incidents	N/A	Number of Incidents caused by the introduction of Changes.	Monthly
		0 Incidents (P1, P2, P3 or P4) not covered by an Effective Rollback Plan.			
Optimisation and Efficiency	CSL4	To be agreed by the Parties during the Transition Period	3%	To be agreed by the Parties during the Transition Period	To be agreed by the Parties during the Transition Period
Threat Protection – Resolution of Security Vulnerabilities	CSL5	<p>Extreme Risk: 95% of Security Vulnerabilities are Resolved within 24 hours after the Start Time</p> <p>High Risk: 95% of Security Vulnerabilities are Resolved within 5 business days after the Start Time</p> <p>Medium Risk/Low Risk: 90% of Security Vulnerabilities are Resolved within 1 month after the Start Time</p>	3%	(Number of Security Vulnerabilities of the relevant risk level that are Resolved within the corresponding time frame specified opposite and during the Period of Calculation / total number of Security Vulnerabilities of that risk level for which the end of the corresponding time frame specified opposite falls within the Period of Calculation) * 100	Monthly

Service/ Responsibility	Classification	Service Level	Service Credit Percentage	Measurement	Period of Calculation
<b>Table 2 Service Level Matrix</b>					

6.5 The Managed Services to which the Service Levels apply, and their respective Tiers (for the purposes of the Service Levels set out in the Service Level Matrix) are set out in Exhibit 1 to this SLA.

## 7. Service Credits

### CONTRACTOR ACKNOWLEDGEMENT

7.1 The Contractor acknowledges and agrees that:

- (a) the Service Credits set out in this SLA are a genuine pre-estimate of loss and do not constitute a penalty; and
- (b) the Contractor's obligation to provide the Customer with Service Credits does not in any way limit any other remedies available to the Customer.

7.2 Service Credits will apply (and the Contractor must pay the Customer Service Credits) where, subject to clause 7.3 below, the Contractor has failed in any month, or, if applicable, other Period of Calculation (**Failure Period**) to meet a CSL. Service Credits will be calculated in accordance with clause 7.4 below.

7.3 Notwithstanding any other provision in this SLA, the Contractor is not required to pay the Customer Service Credits in excess of 15% of the Total Billing Period Charges (as defined in clause 7.4 of this SLA) referable to the relevant Failure Period (and, for clarity, 15% of the Total Billing Period Charges is the maximum Service Credit payable in a Failure Period, but such cap on Service Credits is without prejudice to any other rights or remedies available to the Customer for such Service Level breaches).

7.4 If the Contractor fails to meet a CSL, then a Service Credit will be calculated as follows:

$$\text{Service Credit} = \text{Service Credit Percentage} \times \text{Total Billing Period Charges}$$

where:

“**Service Credit Percentage**” is the percentage amount for the CSL for the relevant Period of Calculation; and

“**Total Billing Period Charges**” are all charges under the Customer Contract referable to the relevant Failure Period.

7.5 If a Service Credit accrues under this clause 6.5, the Service Credit shall be calculated and applied by the Contractor, as a discount to the following monthly invoice (immediately after the month in which the Service Credits accrued), prior to generating and issuing that invoice to the

Customer.

- 7.6** If any Service Credit amount is outstanding following the last invoice under the Customer Contract, the Contractor must pay that outstanding amount to the Customer within 30 days of demand.
- 7.7** Service Levels apply on an end-to-end basis. Subject to clause 4.1 of this SLA, the Contractor is responsible for all Subcontractors and managed third party activities that may impact on the Service Levels and is not entitled to any relief from a Service Level failure caused or contributed to by a Subcontractor or managed third party.

#### **CONTRACTUAL REMEDIES**

- 7.8** Where the Contractor fails to meet the same Service Level(s) in each month of any consecutive three month period, or in any three months of any consecutive six month period, such failure is a Substantial Breach for the purposes of clause 25.2 of the Agreement, as per clause 7.1(d) of Item 43 (Additional Conditions) of the General Order Form.

### Exhibit 1: Service Request Tiers

The Parties agree that during the Transition-In Period, they will work together to determine appropriate categorisation of Service Request Tiers and to populate the table below. Once the Parties have agreed the foregoing, this Schedule 3 shall be updated accordingly.

Service Request Tier	Services
A	
B	
C	<ul style="list-style-type: none"> <li>All service requests not included in the above tiers.</li> </ul>
<b>Table 3 Service Request Tiers</b>	

## Exhibit 2 – Performance Management Framework

### 1.1 Service Management Service Levels

#### (a) All Processes

SMSL1 – Process Forum Attendance	
Category	Service Management Service Level
Measure Definition	Measures Contractor attendance to process forum workshops
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	85% attendance
Expected Performance Level	90% attendance
Measurement Methodology	
Measurement Points	<p>A Contractor is considered to be 'in attendance' to a process forum workshop if they:</p> <ol style="list-style-type: none"> <li>Receive an invitation to process forum workshop; and</li> <li>Attend the workshop at the scheduled time and sign the attendance sheet with all required identifying details; or alternatively</li> <li>Provide an acceptable reason (as judged by Customer) for</li> </ol>

<b>SMSL1 – Process Forum Attendance</b>	
	inability to attend workshop prior to scheduled commencement time for workshop
Calculation	(Number of Contractor representatives in attendance at process forum workshop) ÷ (Total number of Contractor representatives that were invited to attend process forum workshop) expressed as a whole number
Period of Calculation	Each process forum workshop
Frequency of Measurement	As per frequency of process forum workshop
Data Source	Process forum workshop attendance sheet
Measurement Responsibility	Service Integrator
Reporting Frequency	As per frequency of process forum workshop
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

(b) Event Management

<b>SMSL2 – Unknown Events</b>	
Category	Service Management Service Level
Measure Definition	Measures the number of Events that were escalated to Service Integrator where an Event template/record was not found
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	Maximum 15% of Events escalated by Contractor without Event template/record
Expected Performance Level	Maximum 10% of Events escalated by Contractor without Event template/record
<b>Measurement Methodology</b>	
Measurement Points	Events escalated to Service Integrator where Event template/record was either incomplete or completed with insufficient and/or unsatisfactory detail.
Calculation	(Number of Events where Event template/record was not found during Period of Calculation/Number of Events escalated by Contractor during Period of Calculation) x 100
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month

<b>SMSL2 – Unknown Events</b>	
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

(c) Incident Management

<b>SMSL3 – Incident Response Time</b>	
Category	Service Management Service Level
Measure Definition	Measures the amount of time taken for the Contractor to acknowledge they have received the Incident ticket, by Incident priority.
Service Coverage Hours	Twenty four (24) hours, seven (7) days a week for Major Incidents and P1 and P2 Incidents. Service Hours for P3 and P4 Incidents.
Measurement Hours	Twenty four (24) hours, seven (7) days a week for Major Incidents and P1 and P2 Incidents. Service Hours for P3 and P4 Incidents.
Minimum Performance Level (Service Hours Support)	Major Incidents – 95% within 15 minutes during Service Hours P1 – 95% within 15 minutes during Service Hours P2 – 90% within 30 minutes during Service Hours P3 – 85% within 90 minutes during Service Hours P4 – 85% within 2 Service Hours Timeframes are end to end across all Services.
Expected Performance Level (Service Hours Support)	Major Incidents – 100% within 15 minutes during Service Hours P1 – 100% within 15 minutes during Service Hours P2 – 95% within 30 minutes during Service Hours P3 – 90% within 90 minutes during Service Hours P4 – 90% within 2 Service Hours Timeframes are end to end across all Services.
Minimum Performance Level (Non-Service Hours Support)	Major Incidents – 95% within 60 minutes outside Service Hours P1 – 95% within 60 minutes outside Service Hours P2 – 90% within 90 minutes outside Service Hours Timeframes are end to end across all Services.
Expected Performance Level (Non-Service Hours)	Major Incidents – 100% within 60 minutes outside Service Hours

<b>SMSL3 – Incident Response Time</b>	
Support)	P1 – 100% within 60 minutes outside Service Hours P2 – 95% within 90 minutes outside Service Hours Timeframes are end to end across all Services.
<b>Measurement Methodology</b>	
Measurement Points	Incident response time is measured as the time between: <ul style="list-style-type: none"> <li>a. the time the Incident is recorded in ServiceNow, or should have been recorded by the Contractor; and</li> <li>b. the time at which the Contractor responds (e.g. via email, updating of ServiceNow ticket or over phone call to Service Integrator or the Customer's Service Desk) to acknowledge the allocation of this ticket.</li> </ul>
Calculation	The Service Level is calculated separately for each Priority Level in accordance with the following:  $\% \text{ variation} = \left( \frac{\text{number of Incidents with an Incident response time within the required Incident response time during the Period of Calculation}}{\text{total number of Incidents recorded during the Period of Calculation}} \right) \times 100$ <p>In order to achieve the Service Level, the Expected Performance Level must be met for all priority levels.</p>
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL4 – Service Recovery Action Time</b>	
Category	Service Management Service Level
Measure Definition	Measures the amount of time taken for the Contractor to provide a Service Recovery Action, by Incident priority.
Service Coverage Hours	Twenty four (24) hours, seven (7) days a week for P1 and P2 Incidents. Service Hours for P3 and P4 Incidents.
Measurement Hours	Twenty four (24) hours, seven (7) days a week for P1 and P2 Incidents. Service Hours for P3 and P4 Incidents.

<b>SMSL4 – Service Recovery Action Time</b>	
Minimum Performance Level (Service Hours Support)	P1 – 95% within 2 Service Hours P2 – 90% within 4 Service Hours P3 – 85% within 8 Service Hours P4 – 85% within 16 Service Hours Timeframes are end to end across all Services.
Expected Performance Level (Service Hours Support)	P1 – 100% within 2 Service Hours P2 – 95% within 4 Service Hours P3 – 90% within 8 Service Hours P4 – 90% within 16 Service Hours Timeframes are end to end across all Services.
Minimum Performance Level (Non-Service Hours Support)	P1 – 95% within 3 Hours P2 – 90% within 6 Hours Timeframes are end to end across all Services.
Expected Performance Level (Non-Service Hours Support)	P1 – 100% within 3 Hours P2 – 95% within 6 Hours Timeframes are end to end across all Services.
<b>Measurement Methodology</b>	
Measurement Points	Service Recovery Action time is measured as the time between: <ul style="list-style-type: none"> <li>a. the time the Incident is recorded in ServiceNow, or should have been recorded by the Contractor; and</li> <li>b. the time at which the Contractor provides a Service Recovery Action.</li> </ul>
Calculation	The Service Level is calculated separately for each priority level in accordance with the following:  $\% \text{ variation} = (\text{number of Incidents with a Service Recovery Action within the required Service Recovery Action time during the Period of Calculation} / \text{total number of Incidents recorded during the Period of Calculation}) \times 100$ <p>In order to achieve the Service Level, the Expected Performance Level must be met for all priority levels.</p>
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly



### SMSL4 – Service Recovery Action Time

Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.
--------------------------------	--

### SMSL5 – Incident Acceptance Time

Category	Service Management Service Level
Measure Definition	Measures the amount of time taken for the Contractor to either: <ol style="list-style-type: none"> <li>accept ownership of Incident; or</li> <li>reassign Incident back to Service Desk by Incident priority.</li> </ol>
Service Coverage Hours	Twenty four (24) hours, seven (7) days a week
Measurement Hours	Twenty four (24) hours, seven (7) days a week
Minimum Performance Level (Service Hours Support)	P1 – 90% within 30 minutes P2 – 90% within 60 minutes Timeframes are end to end across all Services.
Expected Performance Level (Service Hours Support)	P1 – 95% within 30 minutes P2 – 95% within 60 minutes Timeframes are end to end across all Services.
Minimum Performance Level (Non-Service Hours Support)	P1 – 90% within 120 minutes P2 – 90% within 150 minutes Timeframes are end to end across all Services.
Expected Performance Level (Non-Service Hours Support)	P1 – 95% within 120 minutes P2 – 95% within 150 minutes Timeframes are end to end across all Services.

### Measurement Methodology

Measurement Points	Incident acceptance time is measured as the time between: <ol style="list-style-type: none"> <li>the time the Incident is recorded in ServiceNow, or should have been recorded by the Contractor; and</li> <li>the time at which the Contractor responds to either accept ownership of Incident or reassign Incident back to Service Desk.</li> </ol>
Calculation	The Service Level is calculated separately for each priority level in accordance with the following:  $\% \text{ variation} = (\text{number of Incidents with an Incident acceptance time within the required time during the Period of Calculation} / \text{total number})$

<b>SMSL5 – Incident Acceptance Time</b>	
	of P1 & P2 Incidents recorded during the Period of Calculation) x 100 In order to achieve the Service Level, the Expected Performance Level must be met for all priority levels.
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL6 – Incident Process Data Record Update</b>	
Category	Service Management Service Level
Measure Definition	Measures the percentage of Incidents correctly updated in the Incident process data record by Contractor
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	90% of Incidents correctly updated
Expected Performance Level	95% of Incidents correctly updated
<b>Measurement Methodology</b>	
Measurement Points	Measured any time the Contractor is required to register an Incident within the Incident process data record.  If any element of information provided is incomplete or inaccurate, the Contractor is considered to have failed to correctly update the Incident process data record.
Calculation	$\% = (\text{number of correctly updated Incidents in the Incident process data record during the Period of Calculation} / \text{total number of Incidents recorded during the Period of Calculation}) \times 100$
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	Incident process data record

<b>SMSL6 – Incident Process Data Record Update</b>	
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL7 – Major Incident Technical Bridge Attendance</b>	
Category	Service Management Service Level
Measure Definition	Measures Contractor attendance to Major Incident technical bridge
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% attendance
Expected Performance Level	100% attendance
<b>Measurement Methodology</b>	
Measurement Points	<p>A Contractor is considered to be 'in attendance' to a Major Incident technical bridge if they:</p> <ol style="list-style-type: none"> <li>Receive an invitation to Major Incident technical bridge; and</li> <li>Attend the technical bridge at the scheduled time and sign the attendance sheet with all required identifying details; or alternatively</li> <li>Provide an acceptable reason (as judged by Customer) for inability to attend the technical bridge prior to scheduled commencement time for the technical bridge</li> </ol>
Calculation	(Number of Contractor representatives in attendance at Major Incident technical bridge) ÷ (Total number of Contractor representatives that were invited to attend Major Incident technical bridge) expressed as a whole number
Period of Calculation	Each Major Incident technical bridge
Frequency of Measurement	As per frequency of Major Incident technical bridge
Data Source	Major Incident technical bridge attendance sheet
Measurement Responsibility	Service Integrator
Reporting Frequency	As per frequency of Major Incident technical bridge

### SMSL7 – Major Incident Technical Bridge Attendance

Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.
--------------------------------	--

### SMSL8 – Complex Incident Technical Bridge Attendance

Category	Service Management Service Level
Measure Definition	Measures Contractor attendance to complex Incident technical bridge
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% attendance
Expected Performance Level	100% attendance

#### Measurement Methodology

Measurement Points	A Contractor is considered to be 'in attendance' to a complex Incident technical bridge if they: <ul style="list-style-type: none"> <li>a. Receive an invitation to complex Incident technical bridge; and</li> <li>b. Attend the technical bridge at the scheduled time and sign the attendance sheet with all required identifying details; or alternatively</li> <li>c. Provide an acceptable reason (as judged by Customer) for inability to attend the technical bridge prior to scheduled commencement time for the technical bridge</li> </ul>
Calculation	$(\text{Number of Contractor representatives in attendance at complex Incident technical bridge}) \div (\text{Total number of Contractor representatives that were invited to attend complex Incident technical bridge})$ expressed as a whole number
Period of Calculation	Each complex Incident technical bridge
Frequency of Measurement	As per frequency of complex Incident technical bridge
Data Source	complex Incident technical bridge attendance sheet
Measurement Responsibility	Service Integrator
Reporting Frequency	As per frequency of complex Incident technical bridge
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

(d) Request Management

<b>SMSL9 – Service Request Process Data Record Update</b>	
Category	Service Management Service Level
Measure Definition	Measures the percentage of Service Requests correctly updated in the Service Request process data record by Contractor
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% of Service Requests correctly updated
Expected Performance Level	100% of Service Requests correctly updated
<b>Measurement Methodology</b>	
Measurement Points	Measured any time the Contractor is required to register a Service Request within the Service Request process data record.  If any element of information provided is incomplete or inaccurate, the Contractor is considered to have failed to correctly update the Service Request process data record.
Calculation	$\% = (\text{number of correctly updated Service Requests in the Service Request process data record during the Period of Calculation} / \text{total number of Service Requests recorded during the Period of Calculation}) \times 100$
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	Service Request process data record
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

(e) Problem Management

<b>SMSL10 – Problem Resolution Time</b>	
Category	Service Management Service Level
Measure Definition	Measures the amount of time taken for the Contractor to provide a Problem resolution for a Problem Record, by Problem priority.

<b>SMSL10 – Problem Resolution Time</b>	
	<p>Problem resolution time is the end-to-end elapsed time required to resolve a Problem, commencing from the time a Problem Record is created and concluding when the Problem Record is resolved by the Contractor. A Problem Record can also be resolved where the Service Integrator agrees that continued investigation and/or resolution of the Problem is not in the best interest of the Customer, and the Problem will remain open with an agreed workaround.</p> <p>For the purpose of this Performance Measure, a Problem Record is resolved when:</p> <ol style="list-style-type: none"> <li>the Service Integrator or the Customer agrees that the Problem resolution has been successful; or</li> <li>the Service Integrator or Customer agrees that the Problem can be resolved and accepts the risk to not continue with the Problem resolution activity.</li> </ol>
Service Coverage Hours	Twenty four (24) hours, seven (7) days a week
Measurement Hours	Twenty four (24) hours, seven (7) days a week
Minimum Performance Level	P1 – 95% within an average of 25 Business Days P2 – 90% within an average of 50 Business Days Timeframes are end to end across all Services.
Expected Performance Level	P1 – 100% within an average of 25 Business Days P2 – 95% within an average of 50 Business Days Timeframes are end to end across all Services.
<b>Measurement Methodology</b>	
Measurement Points	<p>Problem resolution time is measured as the time between:</p> <ol style="list-style-type: none"> <li>the time the Problem is recorded in ServiceNow, or should have been recorded by the Contractor; and</li> <li>the time at which the Problem Record is resolved.</li> </ol>
Calculation	<p>The Service Level is calculated separately for each priority level in accordance with the following:</p> <p>Problem resolution time = (number of P1 or P2 Problems initiated during the Period of Calculation and resolved within the required time /total number of P1 or P2 Problems initiated during that Period of Calculation) x 100</p> <p>In order to achieve the Service Level, the Expected Performance Level must be met for all priority levels.</p>
Period of Calculation	Quarterly
Frequency of Measurement	Continuously each quarter
Data Source	ServiceNow

<b>SMSL10 – Problem Resolution Time</b>	
Measurement Responsibility	Service Integrator
Reporting Frequency	Quarterly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL11 – Root Cause Analysis</b>	
Category	Service Management Service Level
Measure Definition	Measures the percentage of all Problems where a root cause analysis was undertaken and a root cause successfully identified.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	65% of root causes found
Expected Performance Level	75% of root causes found
<b>Measurement Methodology</b>	
Measurement Points	Measures the percentage of all Problems where a root cause analysis was undertaken and the root cause was successfully identified by the Contractor during the Period of Calculation.
Calculation	$\% = (\text{number of all Problems for which a root cause analysis was undertaken and the root cause was successfully identified during Period of Calculation} / \text{total number of Problems recorded during Period of Calculation})$
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

**SMSL12 – Problem Process Data Record Update**

Category	Service Management Service Level
Measure Definition	Measures the percentage of Problems correctly updated in the Problem process data record by Contractor
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	90% of Problems correctly updated
Expected Performance Level	95% of Problems correctly updated
<b>Measurement Methodology</b>	
Measurement Points	Measured any time the Contractor is required to register a Problem within the Problem process data record.  If any element of information provided is incomplete or inaccurate, the Contractor is considered to have failed to correctly update the Problem process data record.
Calculation	$\% = (\text{number of correctly updated Problems in the Problem process data record during the Period of Calculation} / \text{total number of Problems recorded during the Period of Calculation}) \times 100$
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	Problem process data record
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

**SMSL13 – Problem Resolution Workshop Attendance**

Category	Service Management Service Level
Measure Definition	Measures Contractor attendance to Problem resolution workshop
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% attendance



<b>SMSL13 – Problem Resolution Workshop Attendance</b>	
Expected Performance Level	100% attendance
<b>Measurement Methodology</b>	
Measurement Points	A Contractor is considered to be 'in attendance' to a Problem resolution workshop if they: <ul style="list-style-type: none"> <li>a. Receive an invitation to Problem resolution workshop; and</li> <li>b. Attend the workshop at the scheduled time and sign the attendance sheet with all required identifying details; or alternatively</li> <li>c. Provide an acceptable reason (as judged by Customer) for inability to attend the Problem resolution workshop prior to scheduled commencement time for the workshop</li> </ul>
Calculation	$(\text{Number of Contractor representatives in attendance at Problem resolution workshop}) \div (\text{Total number of Contractor representatives that were invited to attend Problem resolution workshop})$ expressed as a whole number
Period of Calculation	Each Problem resolution workshop
Frequency of Measurement	As per frequency of Problem resolution workshop
Data Source	Problem resolution workshop attendance sheet
Measurement Responsibility	Service Integrator
Reporting Frequency	As per frequency of Problem resolution workshop
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL14 – Problem Analysis Workshop Attendance</b>	
Category	Service Management Service Level
Measure Definition	Measures Contractor attendance to Problem analysis workshop
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% attendance
Expected Performance Level	100% attendance

### SMSL14 – Problem Analysis Workshop Attendance

#### Measurement Methodology

Measurement Points	A Contractor is considered to be 'in attendance' to a Problem analysis workshop if they: <ul style="list-style-type: none"> <li>a. Receive an invitation to Problem analysis workshop; and</li> <li>b. Attend the workshop at the scheduled time and sign the attendance sheet with all required identifying details; or alternatively</li> <li>c. Provide an acceptable reason (as judged by Customer) for inability to attend the Problem analysis workshop prior to scheduled commencement time for the workshop</li> </ul>
Calculation	$(\text{Number of Contractor representatives in attendance at Problem analysis workshop}) \div (\text{Total number of Contractor representatives that were invited to attend Problem analysis workshop})$ expressed as a whole number
Period of Calculation	Each Problem analysis workshop
Frequency of Measurement	As per frequency of Problem analysis workshop
Data Source	Problem analysis workshop attendance sheet
Measurement Responsibility	Service Integrator
Reporting Frequency	As per frequency of Problem analysis workshop
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

(f) Change Management

### SMSL15 – Incidents from Change Requests

Category	Service Management Service Level
Measure Definition	Measures the number of Incidents caused by Contractor-created Change Requests during the Period of Calculation.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	Maximum 4 Incidents caused by Contractor
Expected Performance Level	Maximum 2 Incidents caused by Contractor

#### Measurement Methodology

<b>SMSL15 – Incidents from Change Requests</b>	
Measurement Points	The number of Incidents recorded in ServiceNow, or the number that should have been recorded by the Contractor
Calculation	Count of number of Incidents caused by Contractor-created Change Requests during the Period of Calculation.
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	<p>Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.</p> <p>Contractor must also, on request by Customer, provide detailed reporting on performance in relation to this SMSL, subject to availability of this data in ServiceNow.</p>

<b>SMSL16 – Change Process (Unauthorised Changes)</b>	
Category	Service Management Service Level
Measure Definition	<p>Measures that all Changes to the Customer's environment are managed in accordance with the Change Management Policies.</p> <p>An unauthorised Change is defined as a Change made to any IT infrastructure that violates or bypasses the Change Management Policies.</p> <p>This Service Level measures occurrences where the Change Management Policies have not been followed or have been followed incompletely by Contractor.</p>
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	Maximum 1 unauthorised Change detected
Expected Performance Level	Maximum 0 unauthorised Changes detected
<b>Measurement Methodology</b>	

<b>SMSL16 – Change Process (Unauthorised Changes)</b>	
Measurement Points	Retrospective Change raised to detail unauthorised work conducted and closed with a status of “unauthorised”.
Calculation	Count of Changes classified as “unauthorised”
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL17 – Change Request Process Data Record Update</b>	
Category	Service Management Service Level
Measure Definition	Measures the percentage of Change Requests correctly updated in the Change Request process data record by Contractor
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% of Change Requests correctly updated
Expected Performance Level	100% of Change Requests correctly updated
<b>Measurement Methodology</b>	
Measurement Points	Measured any time the Contractor is required to register a Change Request within the Change Request process data record. If any element of information provided is incomplete or inaccurate, the Contractor is considered to have failed to correctly update the Change Request process data record.
Calculation	$\% = (\text{number of correctly updated Change Requests in the Change Request process data record during the Period of Calculation} / \text{total number of Change Requests recorded during the Period of Calculation}) \times 100$
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month

<b>SMSL17 – Change Request Process Data Record Update</b>	
Data Source	Change Request process data record
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>SMSL18 – Change Analysis</b>	
Category	Service Management Service Level
Measure Definition	Measures the percentage of risk assessments of Contractor raised Change Requests correctly performed
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	90% of risk assessments correctly performed
Expected Performance Level	95% of risk assessments correctly performed
<b>Measurement Methodology</b>	
Measurement Points	<p>The Contractor is required upon submitting a Change Request to complete a risk assessment which highlights and classifies the likelihood and potential consequences of risks associated with the requested Change.</p> <p>A Change Request is considered correctly performed if:</p> <ol style="list-style-type: none"> <li>a. All relevant risks have been considered and classified according to the relevant policies, standards and laws (including the Customer's Risk and Resilience Framework (Exhibit 3 to the General Order Form));</li> <li>b. All elements of the risk assessment are completed and have been provided to both the Customer and the Service Integrator; and</li> <li>c. The Customer and the Service Integrator do not fundamentally disagree with any of the probability or consequence ratings of any of the highlighted risks.</li> </ol>
Calculation	$\% = (\text{number of risk assessments for Change Requests correctly performed during Period of Calculation} / \text{total number of risk assessments for Change Requests performed during Period of Calculation})$

<b>SMSL18 – Change Analysis</b>	
Period of Calculation	Monthly
Frequency of Measurement	Continuously each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	<p>Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.</p> <p>Contractor must also, on request by Customer, provide detailed reporting on performance in relation to this SMSL, subject to availability of this data in ServiceNow.</p>

<b>SMSL19 – CMDB Accuracy</b>	
Category	Service Management Service Level
Measure Definition	Measures the percentage of Configuration Items stored in Configuration Management Database (CMDB) that correctly reflect the related elements of infrastructure within the underlying environment.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	95% of infrastructure management records sampled are accurate
Expected Performance Level	98% of infrastructure management records sampled are accurate
<b>Measurement Methodology</b>	
Measurement Points	<p>Once every quarter, the Customer will develop a terms of reference used to define the scope of the audit. The Contractor must then undertake an audit of infrastructure management records in the CMDB to the extent applicable to the contracted scope of the Services, in accordance with the terms of reference to demonstrate achievement of this SMSL. The sample will be drawn from both:</p> <ol style="list-style-type: none"> <li>a. the CMDB record against the actual infrastructure, and</li> <li>b. the actual infrastructure against the CMDB record.</li> </ol> <p>The terms of reference may indicate that the audit be physical or logical, that it focus on a specific set of records (based on type or location) or that it is a random sample of the population of infrastructure. The information recorded in the CMDB for each of the</p>

<b>SMSL19 – CMDB Accuracy</b>	
	sampled infrastructure will be compared against the physical infrastructure. Any discrepancy in the information recorded in the CMDB will be counted as incorrectly recorded infrastructure.
Calculation	CMDB accuracy = (the number of items of infrastructure sampled during the Period of Calculation in accordance with the terms of reference for which the information is correctly recorded) / (the total number of items of infrastructure sampled during the Period of Calculation) x 100%.
Period of Calculation	Each quarter
Frequency of Measurement	Quarterly audit
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Quarterly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

(g) Release Management

<b>SMSL20 – Aborted Releases</b>	
Category	Service Management Service Level
Measure Definition	Measures the number of Contractor Releases aborted or other instances where Contractor fails to deploy Release within Release window.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Minimum Performance Level	Maximum of 1 aborted Release or Release the Contractor has failed to deploy
Expected Performance Level	0 aborted Release or Release the Contractor has failed to deploy
<b>Measurement Methodology</b>	
Measurement Points	<p>A Contractor is considered to have aborted a Release when any individual aspect of a deployed Change to any software, hardware, application or system within the environment are reversed and the impacted element is returned to its prior state.</p> <p>A Contractor has failed to deploy Release within Release window if;</p>

<b>SMSL20 – Aborted Releases</b>	
	<ul style="list-style-type: none"> <li>a. the Release is not deployed successfully and as originally intended with no unanticipated adverse consequence within the Release window; or</li> <li>b. the Release has been aborted.</li> </ul>
Calculation	Count of Releases aborted or other instances where Contractor fails to deploy Release within Release window.
Period of Calculation	Each Month
Frequency of Measurement	Monthly
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Expected Performance Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

**1.2 Critical Service Levels**

<b>CSL1 – Availability of Services</b>	
Category	Critical Service Level
Measure Definition	Measures the availability of Services.
Service Coverage Hours	Twenty four (24) hours, seven (7) days a week.
Measurement Hours	Twenty four (24) hours, seven (7) days a week.
Target Service Level	99.9% availability (approximately 44 minutes of downtime/month)
<b>Measurement Methodology</b>	
Measurement Points	<p>"AST" or "Agreed Service Time" means the period in each month during which the Customer requires the full functionality of a service to be available for use in accordance with its specifications, being 24 hours a day, 7 days a week, excluding any part of that period that is Excusable Downtime.</p> <p>"DT" or "Downtime" means the period in a month during which the full functionality of a service is not available for use in accordance with its specifications, excluding any part of that period that is Excusable</p>



<b>CSL1 – Availability of Services</b>	
	Downtime.
Calculation	Total availability % = ((AST – DT)/AST) x 100
Period of Calculation	Monthly
Frequency of Measurement	Continuous during each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>CSL2 – Service Request Resolution Time</b>	
Category	Critical Service Level
Measure Definition	Measures the percentage of Service Requests delivered within the timeframe specified
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	95% of: Tier A Service Requests completed within 1 hour Tier B Service Requests completed within 1 Business Day Tier C Service Requests completed within 3 Business Days
<b>Measurement Methodology</b>	
Measurement Points	Delivery time is measured as the time between: a. the time at which the approved Service Request is recorded in ServiceNow, or should have been recorded by the Contractor; and b. the time at which the Service Request is fulfilled.
Calculation	The Service Level is calculated separately for each priority level in accordance with the following:  % variation = (number of Service Requests with a delivery time within the required Service Request deliver time during Period of Calculation/total number of Service Requests recorded during

<b>CSL2 – Service Request Resolution Time</b>	
	Period of Calculation) x 100 In order to achieve the Service Level, the Target Service Level must be met for all Tiers.
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>CSL3 – Change Process (Unauthorised Changes)</b>	
Category	Critical Service Level
Measure Definition	<p>Measures that all Changes to the Customer's environment are managed in accordance with the Change Management Policies.</p> <p>An unauthorised Change is defined as a Change made to any IT infrastructure that violates or bypasses the Change Management Policies.</p> <p>This Service Level measures occurrences where the Change Management Policies have not been followed or have been followed incompletely by Contractor.</p>
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	0 unauthorised changes detected
<b>Measurement Methodology</b>	
Measurement Points	Retrospective Change raised to detail unauthorised work conducted and closed with a status of “unauthorised”.
Calculation	Count of Changes classified as “unauthorised”
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month

<b>CSL3 – Change Process (Unauthorised Changes)</b>	
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>CSL4 – Optimisation and Efficiency</b>	
Category	Critical Service Level
Measure Definition	Measures the level of optimisation and efficiency provided by Contractor through the provision of Services.
Service Coverage Hours	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Measurement Hours	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Target Service Level	<b>[To be agreed by the Parties during the Transition-In Period]</b>
<b>Measurement Methodology</b>	
Measurement Points	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Calculation	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Period of Calculation	Monthly
Frequency of Measurement	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Data Source	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Measurement Responsibility	<b>[To be agreed by the Parties during the Transition-In Period]</b>
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>CSL5 – Threat Protection – Resolution of Security Vulnerabilities</b>	
Category	Critical Service Level

CSL5 – Threat Protection – Resolution of Security Vulnerabilities	
Measure Definition	Measures the number of Security Vulnerabilities Resolved within corresponding time frame.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	<p>Extreme Risk: 95% of Security Vulnerabilities are Resolved within 24 hours after the Start Time</p> <p>High Risk: 95% of Security Vulnerabilities are Resolved within 5 business days after the Start Time</p> <p>Medium Risk/Low Risk: 90% of Security Vulnerabilities are Resolved within 1 month after the Start Time</p> <p>In order to achieve the Service Level, the Target Service Level must be met for all risk levels.</p>
Measurement Methodology	
Measurement Points	<p>Measures the amount of time taken for the Contractor to Resolve a Security Vulnerability, by relevant risk level.</p> <p>Security Vulnerability Resolution time is the end-to-end elapsed time required to resolve a Security Vulnerability, commencing from the Start Time and concluding when the Security Vulnerability is Resolved by the Contractor.</p> <p>For the purpose of this Performance Measure, a Security Vulnerability is Resolved when:</p> <ol style="list-style-type: none"> <li>the Service Integrator or the Customer agrees that the Security Vulnerability Resolution has been successful; or</li> <li>the Service Integrator or Customer agrees that the Security Vulnerability can be Resolved and accepts the risk to not continue with the Security Vulnerability Resolution activity.</li> </ol>
Calculation	(Number of Security Vulnerabilities of the relevant risk level that are Resolved within the corresponding time frame specified above and during the Period of Calculation / total number of Security Vulnerabilities of that risk level for which the end of the corresponding time frame specified above falls within the Period of Calculation) * 100
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow or alternative Security Vulnerability log if appropriate
Measurement Responsibility	Contractor
Reporting Frequency	Monthly

### CSL5 – Threat Protection – Resolution of Security Vulnerabilities

Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.
--------------------------------	--

### 1.3 Key Performance Indicators

#### KPI1 – Reliability of Services

Category	Key Performance Indicator
Measure Definition	Measures the number of Incidents by Incident priority per month.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	<p>≤ 1 P1 Incidents</p> <p>≤ 2 P2 Incidents</p>
<b>Measurement Methodology</b>	
Measurement Points	The P1 and P2 Incidents recorded in ServiceNow, or should have been recorded by the Contractor.
Calculation	Number of P1 and P2 Incidents
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow
Measurement Responsibility	Contractor
Reporting Frequency	Monthly
Special Reporting Requirements	<p>Where Contractor does not meet the Target Service Level it must provide details of the Incident, cause of the Incident and preventative and remedial action to mitigate the recurrence of such Incident.</p> <p>Contractor must also, on request by Customer, provide detailed reporting on performance in relation to this SMSL, subject to availability of this data in ServiceNow.</p>

<b>KPI2 – Incident Resolution Time</b>	
Category	Key Performance Indicator
Measure Definition	Measures the percentage of Incidents resolved within the specified time by priority level. Contractor is responsible for resolving all Incidents relating to the Services within the timeframes below.
Service Coverage Hours	Twenty four (24) hours, seven (7) days a week for P1 and P2.
Measurement Hours	Twenty four (24) hours, seven (7) days a week for P1 and P2.
Target Service Level	P1: 90% within 4 Service Hours P2: 90% within 8 Service Hours Timeframes are end to end across all services.
<b>Measurement Methodology</b>	
Measurement Points	<p>Incident resolution time is measured as the time between:</p> <ol style="list-style-type: none"> <li>the time the Incident is recorded in ServiceNow, or should have been recorded by the Contractor; and</li> <li>the time at which the Incident is resolved.</li> </ol> <p>For the purpose of this KPI, an Incident record is 'resolved' when:</p> <ol style="list-style-type: none"> <li>all activities are confirmed as completed;</li> <li>the permanent solution has been applied (or workaround applied where Customer has approved that a workaround is sufficient);</li> <li>affected end users have been consulted to confirm that the permanent solution (or otherwise approved workaround) has rectified the Incident; and</li> <li>ServiceNow is updated</li> </ol>
Calculation	<p>The KPI is calculated separately for each priority level in accordance with the following:</p> <p><math>\% \text{ variation} = (\text{number of Incidents with an Incident resolution time within the required time during Period of Calculation} / \text{total number of Incidents recorded during the Period of Calculation}) * 100</math></p> <p>In order to achieve the Service Level, the Target Service Level must be met for all priority levels.</p>
Period of Calculation	Monthly
Frequency of Measurement	Incident resolution time is measured for each Incident. Service Level performance measured on a monthly basis.
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly

**KPI2 – Incident Resolution Time**

Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.
--------------------------------	--

**KPI3 – Reporting Management**

Category	Key Performance Indicator
Measure Definition	Measures the timely delivery of reports in accordance with Customer's requirements.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	1 ≤ Late report per month

**Measurement Methodology**

Measurement Points	A report is only considered to be 'complete' if it contains accurate information and is undertaken in accordance with Customer's requirements as set out in Item 40 of the General Order Form, Exhibit 1 to the General Order Form and any other specific requirements set out in this agreement.
Calculation	Number of late reports = (Total number of reports delivered on time during Period of Calculation/total number of reports that were required to be delivered during Period of Calculation) expressed as a whole number
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	Contractor shall act as the data source however Customer reserves the right to access its internal records (e.g. e-mail logs, etc.) to validate and reconcile against Contractor's information.
Measurement Responsibility	Contractor
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>KPI4 – Compliance with Security and ICT Policies</b>	
Category	Key Performance Indicator
Measure Definition	Measures the level of non-compliance with applicable Customer ICT and Security policies
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	Information resulting from periodic audit activities and random compliance checks conducted by both Customer and Customer independent third parties, results in $\leq 1$ non-compliance
<b>Measurement Methodology</b>	
Measurement Points	Ongoing audit of non-compliance captured by adverse findings or failure to address adverse findings resulting from periodic ICT and security audits conducted by both the Customer and independent third parties.
Calculation	Count of audit non-compliances after each audit report or other Customer or third party compliance check report in regards to compliance with Customer IT Policies and Procedures (including security policies)
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	Periodic ICT and security audits conducted by Customer or independent third parties, as well as any other activity which may lead to adverse findings
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>KPI5 – Back-up as A Service</b>	
Category	Key Performance Indicator
Measure Definition	Measures the percentage of data back-ups completed on time.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours



<b>KPI5 – Back-up as A Service</b>	
Target Service Level	98% of scheduled data back-ups for recovery completed on time.
<b>Measurement Methodology</b>	
Measurement Points	<p>Back-up schedule to be agreed between Contractor and Customer during Transition-In.</p> <p>A Contractor is considered to have failed to complete a data back-up on time if;</p> <ol style="list-style-type: none"> <li>the back-up is not completed successfully and as originally intended with no unanticipated adverse consequence or gaps in backed up data; or</li> <li>the back-up is not completed on time as per the mutually agreed back-up scheduled.</li> </ol>
Calculation	Total of all data back-ups completed on time during the Period of Calculation / total of all data back-ups scheduled in the Period of Calculation * 100
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow or other agreed back-up logging tool
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

<b>KPI6 – Change Management Quality</b>	
Category	Key Performance Indicator
Measure Definition	Measures the number of Incidents caused by the introduction of Changes by the Contractor.
Service Coverage Hours	Service Hours
Measurement Hours	Service Hours
Target Service Level	<p>≤ 1 P1 Incidents</p> <p>≤ 2 P2 Incidents</p> <p>0 Incidents (P1, P2, P3 or P4) not covered by an Effective Rollback Plan.</p>

KPI6 – Change Management Quality	
Measurement Methodology	
Measurement Points	<p>The number of Incidents recorded in ServiceNow, or that should have been recorded by the Contractor, which occurred as a result of a Change introduced by the Contractor.</p> <p>An Incident is considered to be covered by an Effective Rollback Plan if all aspects of the Incident-causing Change, including any adverse impact to any software, hardware, application or system within the environment, can be reversed and the impacted elements can subsequently be returned to their prior state.</p>
Calculation	Count of the number of Incidents caused by the introduction of Changes by the Contractor during the Period of Calculation, and the number of these not covered by an Effective Rollback Plan.
Period of Calculation	Monthly
Frequency of Measurement	Continuously during each month
Data Source	ServiceNow
Measurement Responsibility	Service Integrator
Reporting Frequency	Monthly
Special Reporting Requirements	Where Contractor does not meet the Target Service Level it must provide details of the cause, and preventative and remedial action to mitigate the recurrence of such failure.

### Exhibit 3 – Priority Levels

Priority Level	Description
<b>P1 Critical</b>	<p><b>Mission-critical business function or entity down</b></p> <p>Impact to one or more critical services other than during scheduled maintenance</p>
<b>P2 Major Impact</b>	<p><b>Critical application Incident/s</b></p> <p>Impact means degradation to one or more critical services or the loss of service to a development Environment other than during scheduled maintenance</p>

<p><b>P3 Minor Impact</b></p>	<p><b>Non-critical Application Incident/s</b></p> <p>Impact means degradation to one or more critical services or the loss of service not referred to in P1 or P2 above that affects users, other than during scheduled maintenance</p>
<p><b>P4 Minimal Impact</b></p>	<p><b>Non-critical, non-business impacting issue</b></p> <p>Impact means degradation to a service not referred to in P1, P2 or P3 above for which a workaround is available and/or impact is minimal and transparent to users</p>

## Schedule 4: Variation Procedures

### 1. Procedures

- 1.1 Each request or recommendation for a change to the PIPP or any part of the Customer Contract must be submitted in a form substantially similar to the Change Request form attached to this Schedule.
- 1.2 For each draft Change Request submitted:
- (a) the Customer must allocate it with a sequential number; and
  - (b) the draft Change Request must be logged and its progress documented by recording its status from time to time by the Contractor as follows:
    - requested;
    - under evaluation;
    - awaiting authorisation;
    - cancelled;
    - pending
    - approved/authorised;
    - expired;
    - in progress;
    - applied;
    - delivered;
    - accepted.
- 1.3 The Party receiving the draft Change Request must within 5 Business Days of receipt (or such longer period set out in the Change Request):
- (a) request further information; or
  - (b) provide written notification to the other Party of its approval or rejection of the Change Request.
- 1.4 If the Customer submits a draft Change Request to the Contractor, and the Contractor believes that there is more than 1 Business Day's work involved in the evaluation of the Change Request, then prior to commencing work on evaluating the draft Change Request the Contractor may request that the Customer pays for the work involved to evaluate the draft Change Request. The Customer may then either revise the draft Change Request to require less than 1 Business Day's work to evaluate it, or agree to pay for the Contractor's work to evaluate the Change Request in an amount agreed by the Parties, or in absence of agreement, at the Contractor's then current commercial rates.
- 1.5 If the Customer Contract has been entered into under a Head Agreement, and the Change Request seeks to vary any terms or conditions of the Customer Contract, including a Protected Clause and the Customer approves of the Change Request, the Customer must submit the Change Request to the Contract Authority and the Secretary of the New South Wales Department of Customer Service, for approval immediately after it has notified the Contractor that it approves the Change Request.

### 2. Status

- 2.1 A Change Request is binding on the Parties only when both Parties have signed it. Once signed by both parties the Change Request updates the Customer Contract in accordance with the terms of the Change Request. The Contractor must not implement any draft Change Request until the Customer has signed the Change Request form.

### 3. Change Request Form

#### CHANGE REQUEST BRIEF DETAILS

<b>Change Request Number</b>		<i>Insert Change Request Number (supplied by the Customer)</i>
<b>Date of Change Request</b>		<i>Insert date of draft Change Request</i>
<b>Originator of need for Change Request</b>		<i>Customer or Contractor</i>
<b>Proposed Implementation Date of Change</b>		<i>Insert proposed date of implementation</i>
<b>Date of expiry of validity of Change Request</b>		<i>Insert validity expiry date. The Change Request is invalid after this date.</i>
<b>Contractor's estimated time and cost of evaluation</b>		<i>Insert estimated time and cost of evaluation</i>
<b>Amount agreed to be paid to the Contractor for evaluating the draft Change Request, if any (This applies only if the Customer is the Party that originated the need for a Change Request; and the Contractor estimates the cost of evaluating and drafting the Change Request exceeds 2 Business Days)</b>		<i>Insert amount to be paid to the Contractor for evaluating the draft Change Request</i>

#### CHANGE REQUEST HISTORY LOG

Change Request Version History			
Date	Issue Version	Status/Reason for New Issue	Author
<i>Insert date</i>	<i>Insert version</i>	<i>Insert status/reason</i>	<i>Insert author</i>

#### DETAILS OF CHANGE REQUEST

##### Summary

[Insert a summary of the changes, if required]

##### SCOPE

[Insert changes to the scope of Products to be provided and/or any Services, including any extensions to the Contract Period.]

##### EFFECT OF CHANGE ON CONTRACT SPECIFICATION

[Insert any changes to the Contract Specification]

##### EFFECT OF CHANGE ON PROJECT TIMETABLE

[Insert changes to the project timetable]

**New PIPP (annexed)**

[Annex new PIPP if required]

**EFFECT OF CHANGE ON CHARGES AND TIMING OF PAYMENT**

[Insert new charges and the timing of payment into the new PIPP]

**CHANGES TO CSI**

[Insert any changes to the CSI]

**CHANGES TO CUSTOMER PERSONNEL**

[Insert any changes to the Customer's Personnel]

**CHANGES TO CUSTOMER ASSISTANCE**

[Insert any changes to the Customer's Assistance]

**PLAN FOR IMPLEMENTING THE CHANGE**

[insert the plan for implementing the change – if any.]

**THE RESPONSIBILITIES OF THE PARTIES FOR IMPLEMENTING THE CHANGE**

[Insert the responsibilities of the respective Parties for implementing the change – if any.]

**Responsibilities of the Contractor**

[Insert the responsibilities of the Contractor for implementing the change – if any.]

**Responsibilities of the Customer**

[insert the responsibilities of the Customer for implementing the change – if any.]

**EFFECT ON ACCEPTANCE TESTING OF ANY DELIVERABLE**

[Insert if there will be any effect on the Acceptance Testing of any Deliverable – or alternatively insert None.]

**EFFECT OF CHANGE ON PERFORMANCE OF ANY DELIVERABLE**

[Insert if there will be any effect on performance of any Deliverable – or alternatively insert None.]

**EFFECT ON USERS OF THE SYSTEM/SOLUTION**

[Insert if there will be any effect on users of the system/solution – or alternatively insert None.]

**EFFECT OF CHANGE ON DOCUMENTATION DELIVERABLES**

Changes will be required to the following documents:

[Add any other documents which may be affected.]

**EFFECT ON TRAINING**

Insert if there will an effect on training or alternatively insert None.]

**ANY OTHER MATTERS WHICH THE PARTIES CONSIDER IMPORTANT**

[insert if there are any other matters.]

**ASSUMPTIONS**

The plan for implementing the changes outlined in this Change Request is based on the assumptions listed below:

[Insert any assumptions. If none then this section will be deleted].

If the assumptions are or become untrue, the Parties will address the effect of this through a subsequent Change Request.

### **LIST OF DOCUMENTS THAT FORM PART OF THIS CHANGE REQUEST**

[Insert a list of the documents that form part of this Change Request]

### **CUSTOMER CONTRACT CLAUSES, SCHEDULES AFFECTED BY THE PROPOSAL ARE AS FOLLOWS:**

[Insert amendments to clauses in the Customer Contract, relevant Schedules including Service Level Agreement]

Note that variations to any of the terms and conditions of the Procure IT Framework including the Protected Clauses require the Customer to obtain the prior written approval of the Contract Authority and the Secretary, New South Wales Department of Customer Service approval in accordance with directions and policies issued by the Board from time to time. (clause 26.2))

### **AUTHORISATION**

The Contractor must not commence work on the Change Request until is signed by both Parties. Once signed by both Parties, the Customer Contract is updated by this Change Request and any provisions of the Customer Contract that conflict with this Change Request are superseded.

# SIGNED AS AN AGREEMENT

Signed for and on behalf of *[insert name of Customer]*

[Redacted signature area]

By *[insert name of Customer's Representative]* but not so as to incur personal liability

[Redacted signature area]

[Redacted signature area]

Signature of Customer Representative

[Redacted signature area]

Print name

[Redacted signature area]

Date

Signed for and on behalf of *[insert Contractor's name and ACN/ABN]*

[Redacted signature area]

[Redacted signature area]

Signature of Authorised Signatory

[Redacted signature area]

Print name

[Redacted signature area]

Date





**Schedule 5: Not used**



**Schedule 6: Not used**



**Schedule 7: Not used**



**Schedule 8: Not used**



**Schedule 9: Not used**



**Schedule 10: Not used**



## Schedule 11: Dispute Resolution Procedures

### 1. Expert Determination

- 1.1 If a Referral Notice is submitted under clause 24.7 of the Customer Contract, the expert is to be agreed between the Parties. If they cannot agree within 28 days of the Referral Notice, the expert is to be nominated on the application of either Party by the Chief Executive Officer, Australian Disputes Centre of NSW.
- 1.2 The expert nominated must be a person who is an experienced Australian legal practitioner or a person with practical experience in the technology that is the subject matter of the dispute, unless otherwise agreed. The expert must not be:
- (a) an employee of the Parties;
  - (b) a person who has been connected with this Customer Contract or has a conflict of interest, as the case maybe; or
  - (c) a person who the Parties have not been able to agree on.
- 1.3 The expert may appoint any person that the expert believes will be able to provide the specialists skills that are necessary to make a determination, including an Australian legal practitioner. The expert must consult with both Parties prior to appointing such person.
- 1.4 When the person to be the expert has been agreed or nominated, the Customer, on behalf of both Parties, must engage the expert by letter of engagement (and provide a copy to the Contractor) setting out:
- (a) the issue referred to the expert for determination;
  - (b) the expert's fees;
  - (c) the procedure for the determination set out in this Schedule; and
  - (d) any other matter which is relevant to the engagement.

### 2. Submissions

- 2.1 The procedure for submissions to the expert is as follows:
- (a) The Party that has referred the issue to expert determination must make a submission in respect of the issue, within 30 Business Days after the date of the letter of engagement referred to in clause 1.4.
  - (b) The other Party must respond within 30 Business Days after receiving a copy of that submission. That response may include cross-claims.
  - (c) The Party referred to in clause 2.1(a) may reply to the response, but must do so within 20 Business Days after receiving the response, and must not raise new matters.
  - (d) The other Party may comment on the reply, but must do so within 20 Business Days after receiving the reply, and must not raise new matters.
  - (e) The expert must ignore any submission, response, reply, or comment not made within the time given in this clause 2.1, unless the Customer and the Contractor agree otherwise.
  - (f) The expert may request further information from either Party. The request must be in writing, with a time limit for the response. The expert must send a copy of the request and response to the other Party, and give the other Party a reasonable opportunity to comment on the response.
  - (g) All submissions, responses, replies, requests and comments must be in writing. If a Party gives information to the expert, it must at the same time give a copy to the other Party.

### **3. Conference**

- 3.1** The expert must arrange at least one conference with both Parties. The request must be in writing, setting out the matters to be discussed.
- 3.2** Each Party is entitled to be represented at any preliminary conference before the expert by its legal representatives and other authorised representatives, with information and knowledge of the issues.
- 3.3** The expert is not bound by the rules of evidence and may receive information in any manner the expert sees fit, but must observe the requirements of procedural fairness. Consultation between the expert and a Party must only take place in the presence of the other Party, unless a Party fails to attend a conference or meeting which has been convened by the expert and of which prior notice has been given. Any Party providing information to the expert must provide that information to the other Party.
- 3.4** The Parties agree that such a conference is considered not to be a hearing that would give anything under this Schedule the character of arbitration.
- 3.5** In answer to any issue referred to the expert by a Party, the other Party can raise any defence, set-off or counter-claim.

### **4. Questions to be determined by the Expert**

- 4.1** The expert must determine for each issue the following questions (to the extent that they are applicable to the issue):
- (a) is there an event, act or omission that gives the claimant a right to compensation under the Customer Contract:  
for damages for breach of the Customer Contract, or  
otherwise in law?
  - (b) if so:  
what is the event, act or omission?  
on what date did the event, act or omission occur?  
what is the legal right which gives rise to the liability to compensation?  
is that right extinguished, barred or reduced by any provision of the Customer Contract, estoppel, waiver, accord and satisfaction, set-off, cross-claim, or other legal right?
  - (c) in the light of the answers to clause 1.4:  
What compensation, if any, is due from one Party to the other and when did it fall due?  
What interest, if any, is due when the expert determines that compensation?
- 4.2** The expert must determine for each issue any other questions required by the Parties, having regard to the nature of the issue.
- 4.3** The Parties must share equally the fees of the expert, any other costs associated with the process, including room hire expenses, transcript expenses and the like and the fees of any person appointed by the expert under clause 1.3 for the determination, and bear their own expenses.
- 4.4** If the expert determines that one Party must pay the other an amount exceeding the amount specified in General Order Form (calculating the amount without including interest on it and after allowing for set-offs), then either Party may commence litigation, but only within 56 days after receiving the determination.
- 4.5** Unless a Party has a right to commence litigation or otherwise resolve the dispute under the Customer Contract:
- (a) in the absence of a manifest error the Parties must treat each determination of the expert as final and binding and give effect to it; and



- (b) if the expert determines that one Party owes the other money, that Party must pay the money within 20 Business Days.

## **5. Role of Expert**

**5.1** The expert must:

- (a) act as an expert and not as an arbitrator, adjudicator or as expert witness;
- (b) make its determination on the basis of the submissions of the Parties, including documents and witness statements, and the expert's own expertise;
- (c) act impartially, free of bias and with no vested interest in the outcome of the dispute;
- (d) adopt procedures for the Expert Determination suitable to the circumstances of the dispute so as to provide for an expeditious cost effective and fair means for the determination of the dispute; and
- (e) issue a certificate in a form the expert considers appropriate, stating the expert's determination and giving reasons, within 45 Business Days after the receipt of the information in clause 2.1(d).

**5.2** If a certificate issued by the expert contains a clerical mistake, an error arising from an accidental slip or omission, a material miscalculation of figures, a mistake in the description of any person, matter or thing, or a defect of form, then the expert must correct the certificate and give notice to the Parties of such correction.

## **6. Confidentiality**

**6.1** Each Party involved in the expert determination process, including the expert, the Parties, their advisors and representatives shall maintain the confidentiality of the expert determination process and may not use or disclose to anyone outside of the expert determination process, the expert's determination, or any information received or obtained, in the course of the expert determination process, including the existence of that information, except to the extent:

- (a) the Parties have otherwise agreed in writing;
- (b) the information is already in the public domain;
- (c) disclosure is required to a Party's insurers, auditors, accountants or other professional advisers;
- (d) disclosure is required for the purposes of any legal proceedings relating to the dispute or the expert's determination; or
- (e) disclosure is otherwise required by law.

# Schedule 12: Project Implementation and Payment Plan (PIPP)

## 1. Introduction

### DOCUMENT SCOPE

This Project Implementation and Payment Plan (**PIPP**) outlines the various Services and activities to be undertaken by the Contractor (also referred to as '**AC3**' in this PIPP) to enable it to effectively transition-in and assume responsibility for the provision of managed computing integration services (**CI Services**, being the Managed Services performed under Module 12) under the Customer Contract (**Transition-In**). It is the intention of the Customer (also referred to as '**DCS**' in this PIPP) that on completion of Transition-In, Go Live will occur.

**Go Live** means when:

- (a) the Customer and the Contractor have agreed in writing that the Transition-In Services (as defined in Module 12) have been successfully performed and Transition-In is complete; and
- (b) the Contractor commences the performance of the CI Services as per the specifications in Exhibit 1 (Services), Exhibit 2A (General Requirements) and Exhibit 2B (Functional Requirements) to the General Order Form.

To avoid doubt, notwithstanding the occurrence of Go Live, the Contractor remains obliged to produce any Deliverables described in this PIPP which are due to be provided after the Go Live date.

This PIPP forms part the Customer Contract and defines the scope of the Services, the Deliverables, the project resources, the implementation methodology, the project schedule and the pricing details for the Transition-In project.

## 2. Project Overview

The objective of the Transition-In project is for the Contractor to Transition-In for the purpose of assuming responsibility for the provision of managed CI Services under this Customer Contract.

In order for the Transition-In project to achieve this objective, the Contractor must achieve the following:

1. the delivery of the CI Services with high and professional standards of efficiency, value and quality;
2. maintenance of the provision of the CI Services with current industry and technological innovation and developments;
3. engagement in knowledge transfer and shadowing sessions conducted or arranged by the Customer, its third party cloud and other service providers or any other relevant parties for the purpose of increasing the Contractor's capability and understanding of the Customer's core cloud and on-premise environments and pre-existing knowledge artefacts;
4. the establishment of necessary governance frameworks, committees and forums;

5. recruitment of capable resources so as to ensure optimal and consistent delivery of the CI Services in accordance with the Contract Specifications;
6. engagement in significant training activities conducted by the Customer, its third party cloud and other service providers or any other relevant parties so as to provide sufficient understanding of the Customer's cloud and on-premise environments and empower the Contractor's subject matter experts to ensure delivery of the CI Services in accordance with the Customer Contract;
7. documentation of all designed and required processes so as to ensure consistent delivery of the CI Services and minimal onboarding delay for new resources;
8. organisational change management activities including the engagement of internal and external stakeholders and establishment of a robust change management strategy;
9. engagement in meetings, activities and early life support so as to plan and execute a seamless cut-over and integration of the currently siloed cloud management services and management of legacy physical environments from their respective cloud and other service providers;
10. the establishment of reporting capability including to produce key reports in the format and frequency as detailed in Item 40 of the General Order Form; and
11. thorough post-implementation review activities designed to assess the success of the Transition-In project against defined objectives and the potential need for any remedial activities.

### 3. Scope of Work

#### PRODUCTS AND SERVICES

The Contractor must perform the Services and deliver the Deliverables in accordance with this PIPP and Exhibit 1 (Services), Exhibit 2A (General Requirements) and Exhibit 2B (Functional Requirements) to the General Order Form.

#### OVERVIEW OF DELIVERABLES

The Contractor must deliver each of the following Deliverables in the format listed below.

#### List of Deliverables

Deliverable ID	Name of Deliverable	Format
D1001	Programme Management Plan (PMP)	Word
D1002	Baseline Schedule	Word/Excel/Project
D1003	Programme Governance Terms of Reference	Word
D1004	Risk and Issues Register	Word/Excel
D1005	Service Transition Workbook	Word/Excel
D1006	Service Transition Plan	Word
D1007	CSA Report - Network Connectivity	Word
D1008	CSA Report – GovConnect	Word
D1009	CSA Report - GovConnect Compute & Storage Platforms	Word
D1010	CSA Report - BRD & SIRA	Word

<b>Deliverable ID</b>	<b>Name of Deliverable</b>	<b>Format</b>
D1011	CSA Report – Revenue NSW	Word
D1012	CSA Report – Service NSW	Word
D1013	CSA Report - Spatial	Word
D1015	CSA Report – NTT Private Cloud	Word
D1016	CSA Report – OutcomeX Private Cloud	Word
D1018	CSA Report - VMC GovConnect	Word
D1020	CSA Report - Citrix GovConnect	Word
D1022	CSA Report - BUAAS Veeam & Commvault	Word
D1024	CSA Report - Storage-aaS	Word
D1026	As-Built Documentation - GovConnect-Unisys	Word
D1027	As-Built Documentation - GovConnect-NTT	Word
D1028	As-Built Documentation - Unisys	Word
D1029	As-Built Documentation - BRD	Word
D1030	As-Built Documentation - Service NSW (Platform)	Word
D1031	As-Built Documentation - Spatial	Word
D1032	As-Built Documentation - Service NSW	Word
D1033	As-Built Documentation - Revenue	Word
D1034	As-Built Documentation - Unassigned	Word
D1035	As-Built Documentation - NDIS	Word
D1036	As-Built Documentation - IPFX	Word
D1037	Management Stack Low Level Design	Word
D1038	Completed System Access Management & Validation Plan	Word
D1039	Completed Monitoring Management & Alerting Integration Test Results	Word/Excel
D1014	ServiceNow Integration Technical Design	Word
D1040	ServiceNow Completed Test Summary Report	Excel/Word
D1041	ServiceNow Integration - As Built Documentation	Word
D1042	Governance Framework	Word
D1043	Service Delivery Playbook	Word
D1045	Service Delivery Reporting	Word
D1046	Transition Out / Exit Plan	Word
D1047	Go Live Criteria - GovConnect	Word/Excel
D1048	Post Implementation Review Report - GovConnect	Word
D1049	Preliminary Service Delivery Report - GovConnect	Word
D1050	Transition Project Closure Report - GovConnect	Word
D1051	Go Live Criteria - BRD	Word/Excel

<b>Deliverable ID</b>	<b>Name of Deliverable</b>	<b>Format</b>
D1052	Post Implementation Review Report - BRD	Word
D1053	Preliminary Service Delivery Report - BRD	Word
D1054	Transition Project Closure Report - BRD	Word
D1055	Go Live Criteria - Revenue NSW	Word/Excel
D1056	Post Implementation Review Report - Revenue NSW	Word
D1057	Preliminary Service Delivery Report - Revenue NSW	Word
D1058	Transition Project Closure Report - Revenue NSW	Word
D1059	Go Live Criteria - SIRA	Word/Excel
D1060	Post Implementation Review Report - SIRA	Word
D1061	Preliminary Service Delivery Report - SIRA	Word
D1062	Transition Project Closure Report - SIRA	Word
D1063	Go Live Criteria - Spatial	Word/Excel
D1064	Post Implementation Review Report - Spatial	Word
D1065	Preliminary Service Delivery Report - Spatial	Word
D1066	Transition Project Closure Report - Spatial	Word
D1067	Go Live Criteria - Service NSW	Word/Excel
D1068	Post Implementation Review Report - Service NSW	Word
D1069	Preliminary Service Delivery Report - Service NSW	Word
D1070	Transition Project Closure Report - Service NSW	Word

Where the Contractor wishes to provide a Deliverable in a format other than that designated above, it must first obtain written approval to do so from the Customer.

Timing for delivery of the above is as per the Project Plan detailed in Section 10 of this PIPP.

### **ACCEPTANCE TESTING OF DELIVERABLES**

Acceptance Testing must be conducted on all of the Deliverables included in the table above in accordance with clause 10 of Part 2 (Customer Contract), as amended by clause 3 of Item 43 (Additional Conditions) of the General Order Form.

The Contractor shall conduct reasonable testing and quality assurance for the Deliverables prior to their submission to the Customer for review.

The Customer will review each Deliverable provided by the Contractor and either accept or reject the Deliverable. The Customer may communicate its rejection by way of providing comments on areas for improvement in relation to the Deliverable. A Deliverable will only be accepted upon express written communication of acceptance by the Customer to the Contractor.

### **CONTRACT PERIOD**

Refer to Item 10 of the General Order Form.

The period for the Transition-In project is as per the Project Plan detailed in Section 10 of this PIPP.

## CONTRACT SPECIFICATIONS

As per Item 13 of the General Order Form (which includes Exhibit 1 (Services) and Exhibit 2A (General Requirements) and Exhibit 2B (Functional Requirements) to the General Order Form.)

## 4. Implementation

### ROLES AND RESPONSIBILITIES

The Contractor is to provide Services related to the Transition-In and ongoing managed CI Services as detailed within this PIPP and Part 2 (Customer Contract). The roles and responsibilities of the Parties and, for completeness, of any third party cloud service provider of the Customer in relation to Transition-In are as follows:

R – Responsible – Party who performs the activity / function.

A – Accountable – Party who has the decision making authority for the activity / function and has capacity to veto / make key 'Go / No' decisions.

C – Consulted – Party who provides feedback and contributes to the activity / function.

I – Informed – Party who is informed of the key decisions related to the activity / function.

Activity	Third Party Cloud Service Provider(s)	Customer	Contractor
Recruitment	-	I	R/A
Stakeholder Engagement and Communication	I	R/A	C
Knowledge Acquisition	C	A	R
Risk and Issue Management	C	A	R
Shadowing	C	A	R
Training	-	C	R/A
Go Live Criteria Development	I	R/A	C
Go/No Go Meeting	I	R/A	C
Go Live Delivery	C	A	R
Early Life Support	C	I	R/A
Post Implementation Review	-	A	R

Activity	Third Party Cloud Service Provider(s)	Customer	Contractor
Reporting	-	C	R/A
Invoicing	-	C	R/A

## 5. Project Management

### ISSUES LOG

The Contractor will maintain and update the Issues Register on a monthly basis as per the reporting requirements contained under Item 40 of the General Order Form.

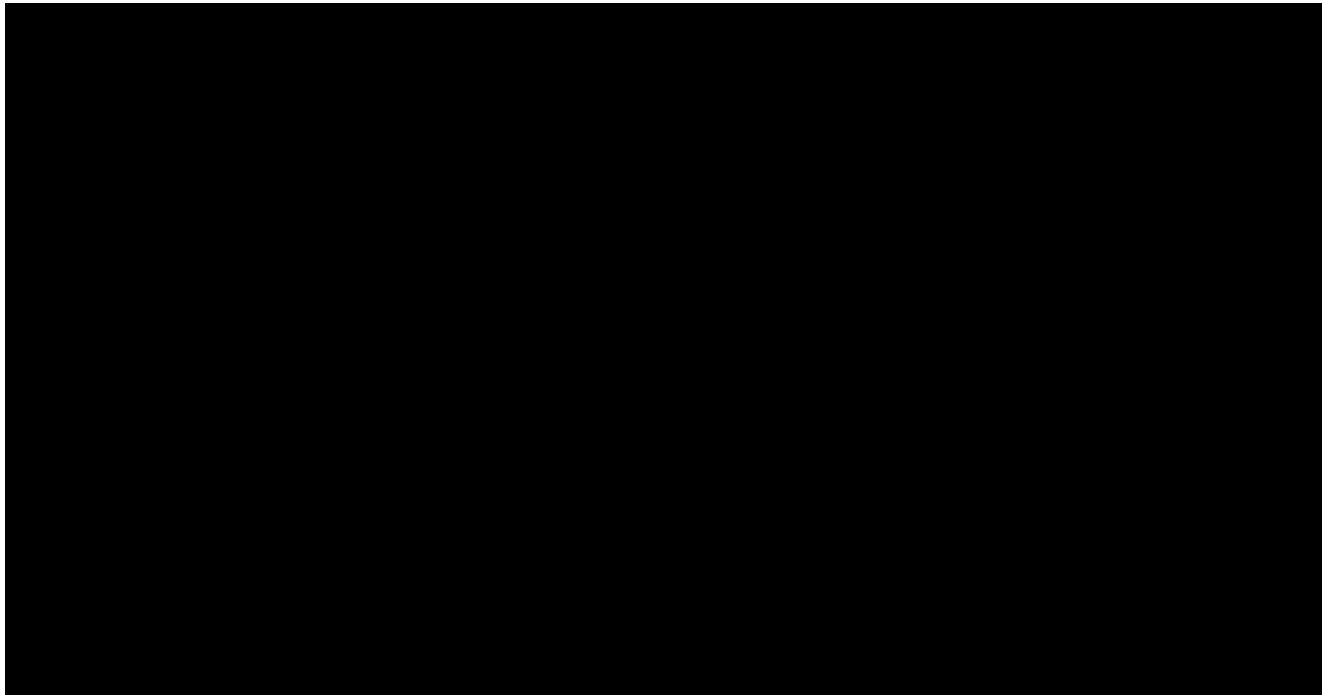
### RISK MANAGEMENT PLAN

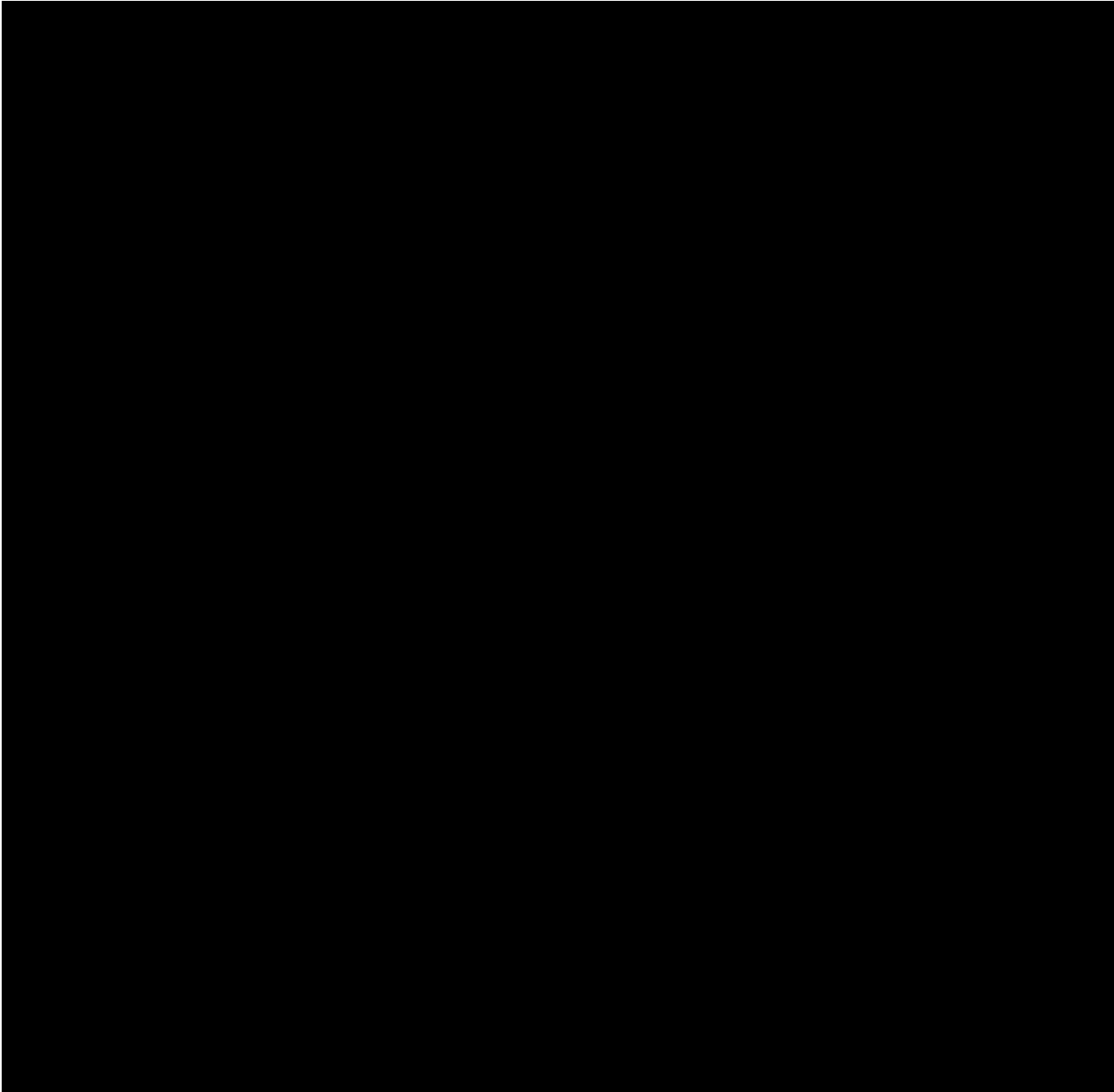
The Contractor will maintain and update the Risk Register on a monthly basis as per the reporting requirements under Item 40 of the General Order Form.

The Risk Log is considered a key Deliverable (D1004).

Risk reporting and management should be conducted in accordance with Exhibit 4 to the General Order Form (Risk and Resilience Framework v6.0).

## 6. Customer Supplied Items (CSI)

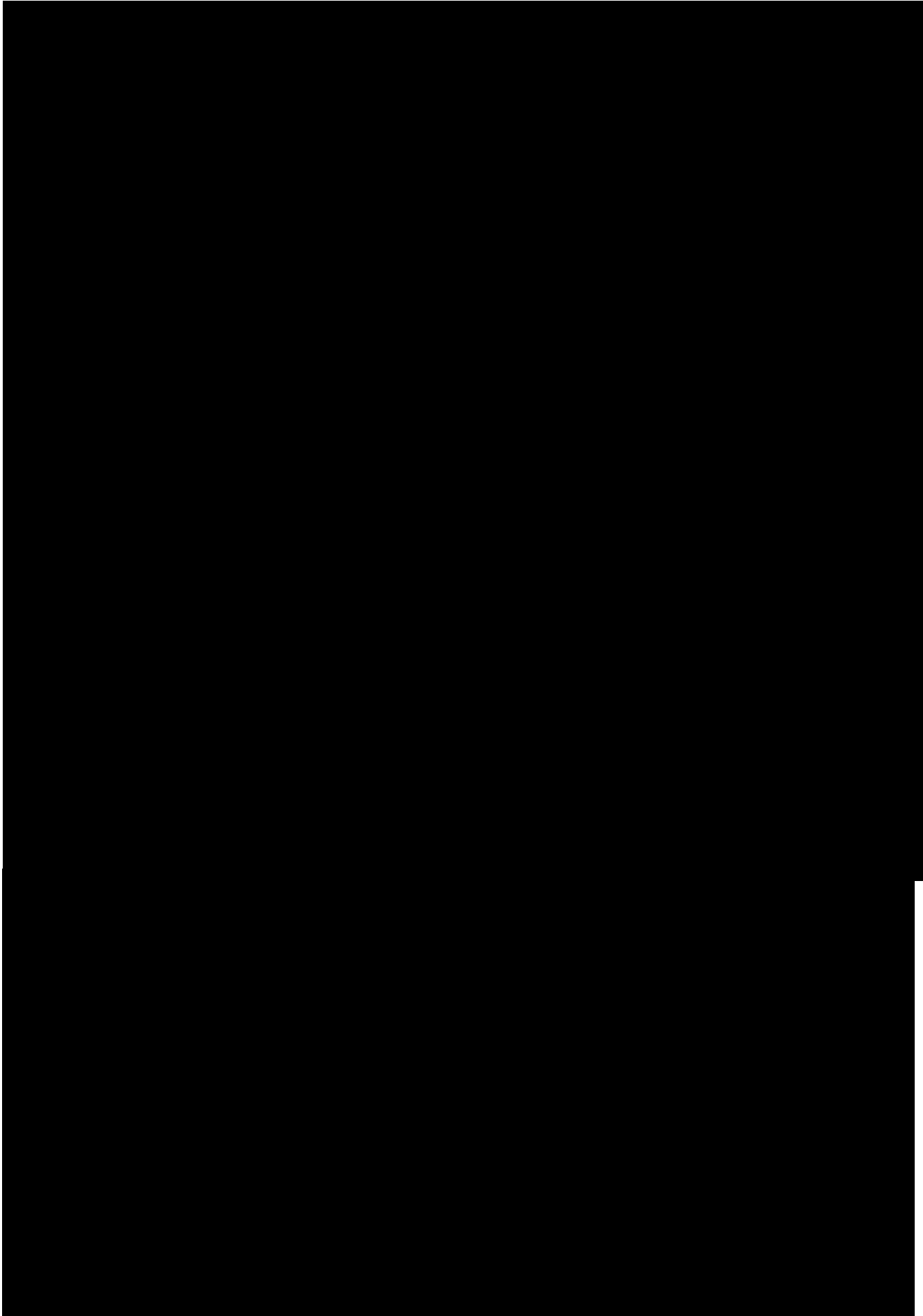




[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

[REDACTED]







## **7. Specified Personnel**

Refer to Item 27 of the General Order Form.

## **8. Customer Assistance**

Refer to Item 22 of the General Order Form.

## **9. Subcontractors**

Not Applicable.

# 10. Project Plan

## HIGH LEVEL PROJECT PLAN

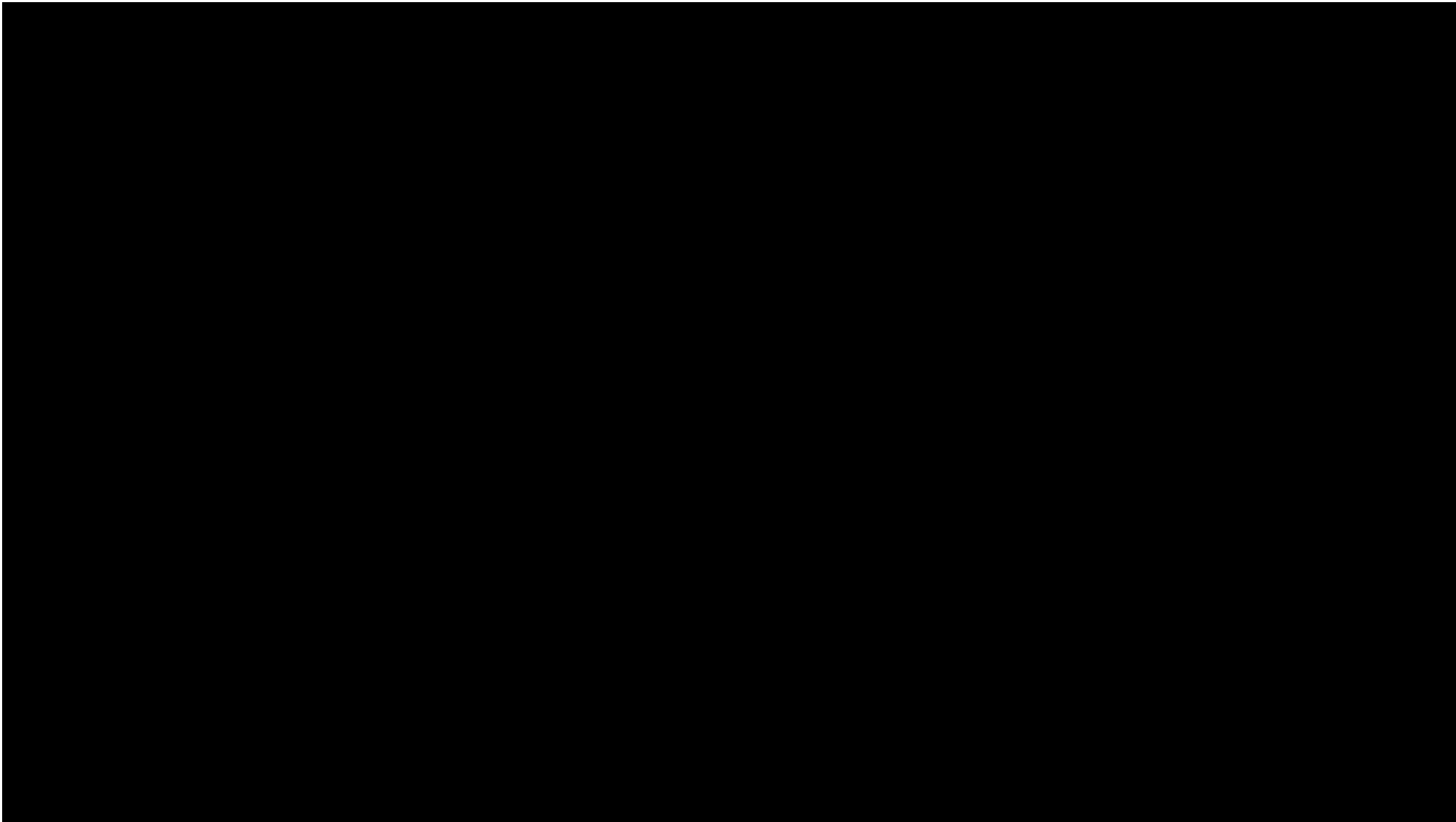
The delivery of the Transition-In project can be split into several Milestones, each comprising a collection of Deliverables and key activities. The Contractor must deliver the Deliverables and conduct the activities by the due dates for those Deliverables indicated in the following high-level Project Plan.

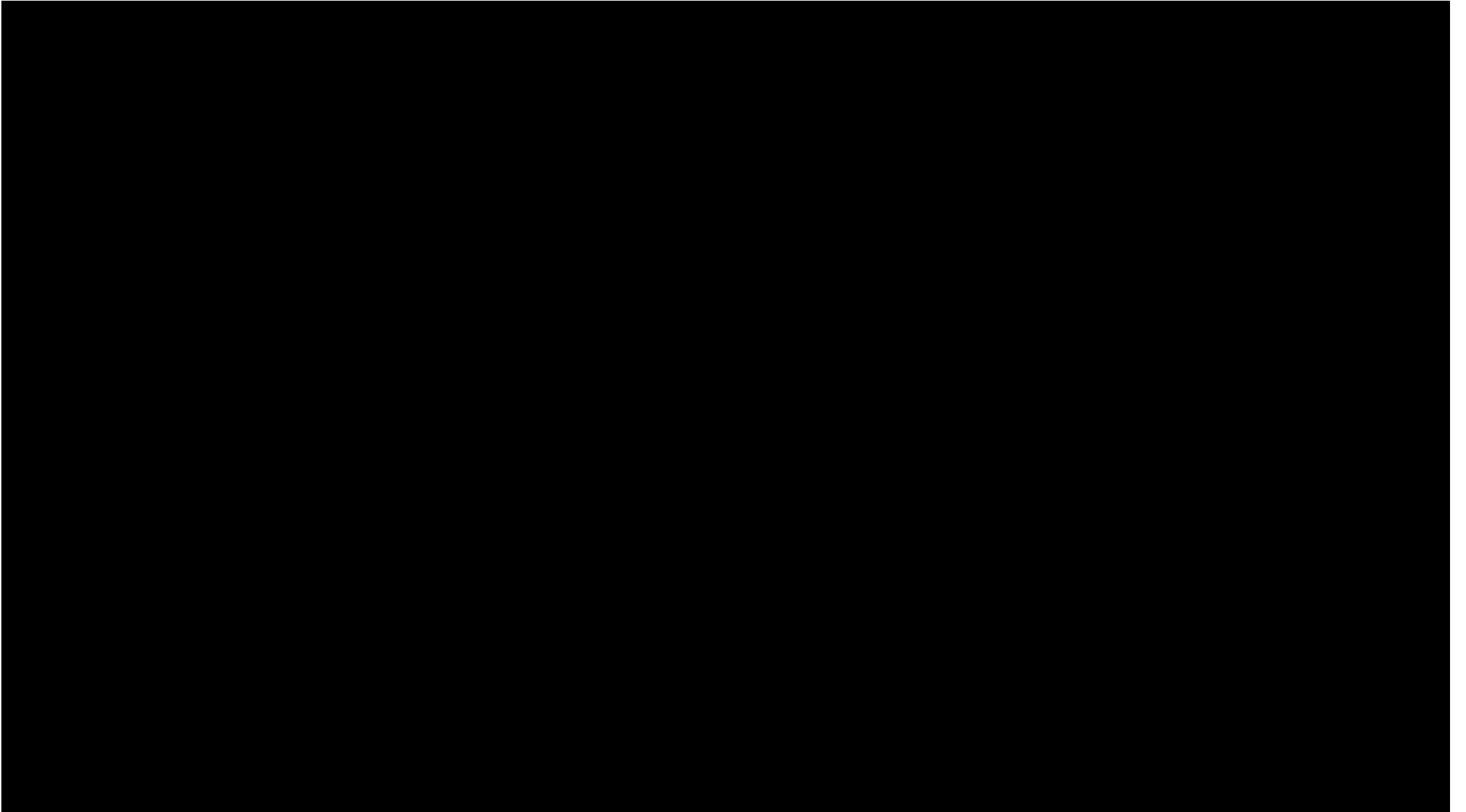
### DELIVERABLES

A Deliverable in the table below will not be considered to have achieved AAD until:

- (a) all activities for that Deliverable and appearing earlier in the table below have been conducted and have been accepted by the Customer; and
- (b) all Deliverables required to be provided prior to the relevant Deliverable in the table below have achieved AAD.

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] <sup>2</sup>









## MILESTONES

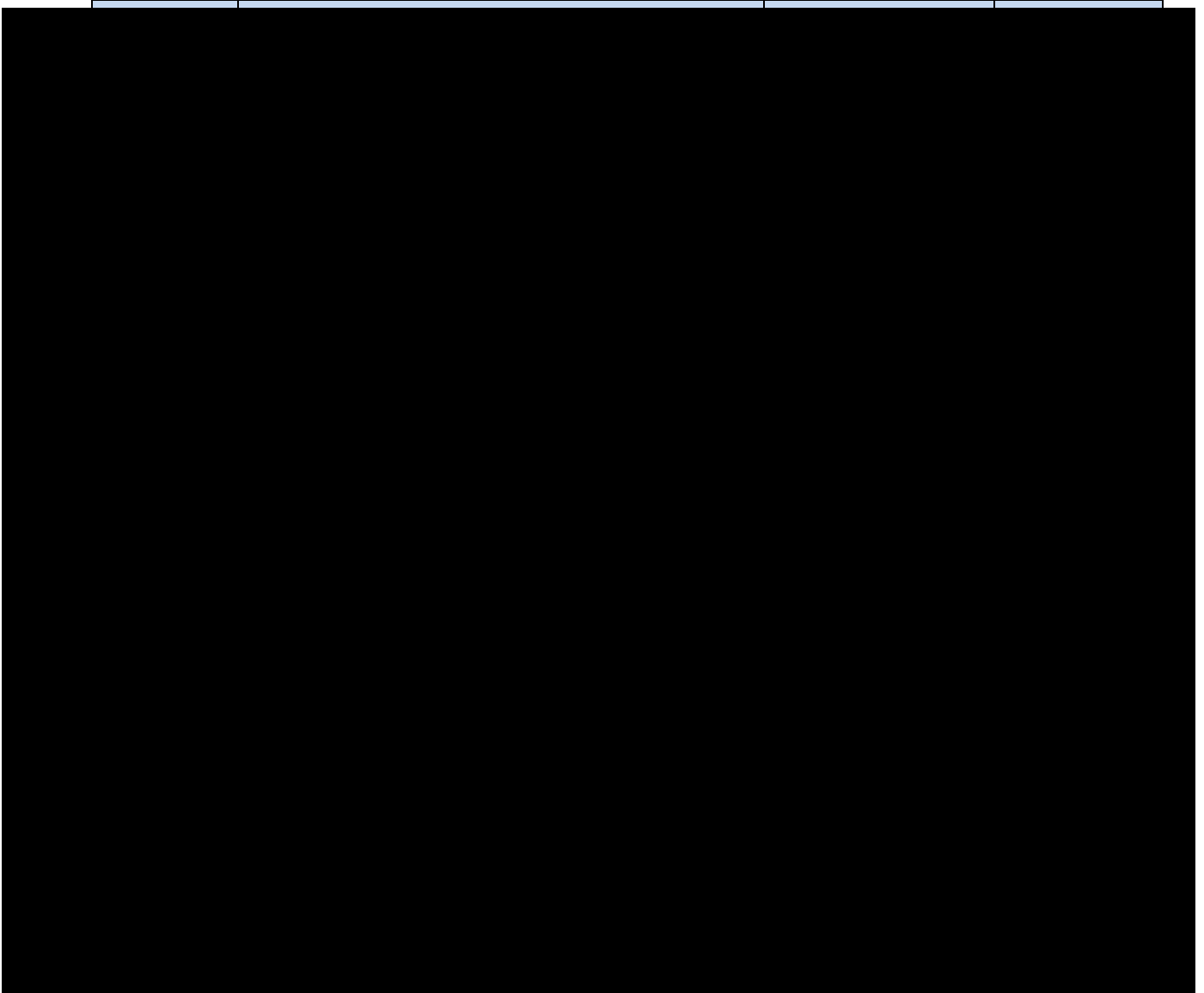
Completion of a Milestone occurs when:

- (a) all previous Milestones have been Completed, unless otherwise agreed in writing by the Customer's authorised representative;
- (b) all activities for all Deliverables for the Milestone have been completed and those Deliverables have been delivered to and accepted by the Customer; and
- (c) all Deliverables for the Milestone have achieved AAD,

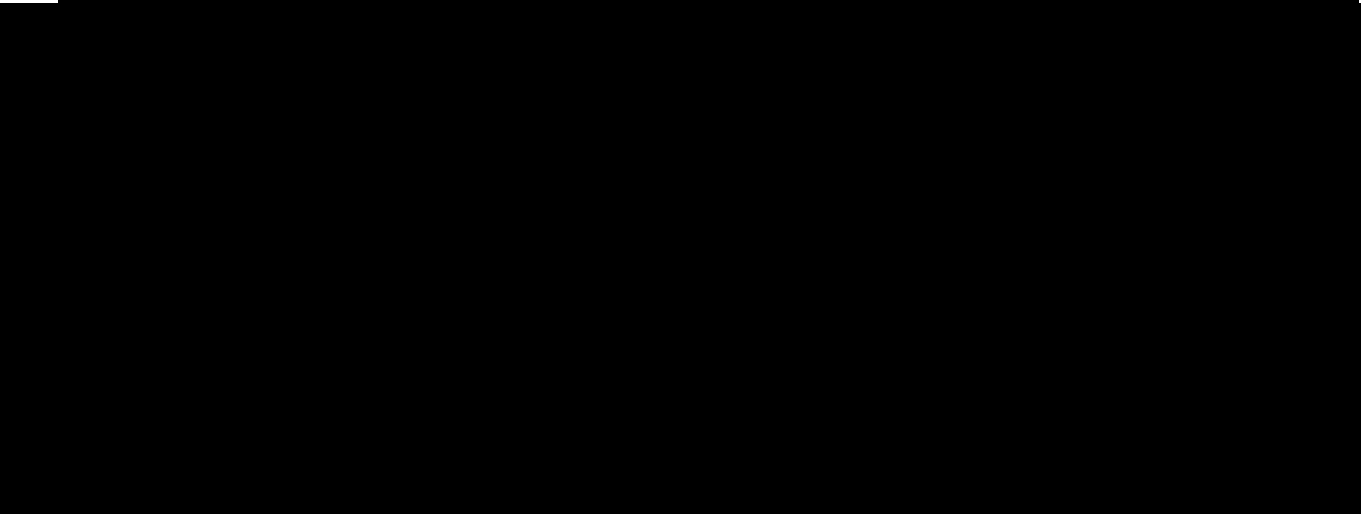
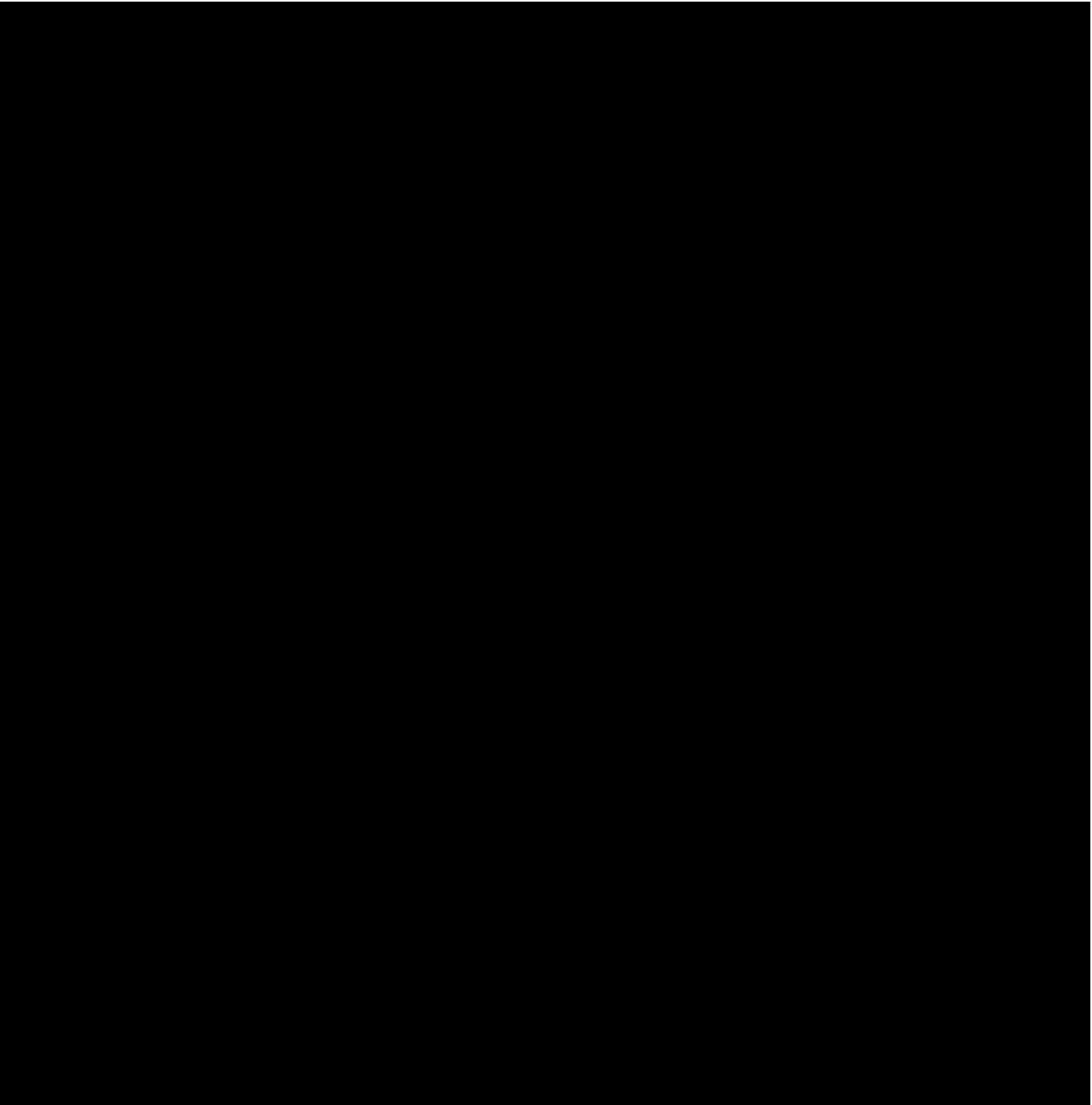
in accordance with clause 10 of Part 2 (Customer Contract), as amended by clause 3 of Item 43 (Additional Conditions) of the General Order Form.

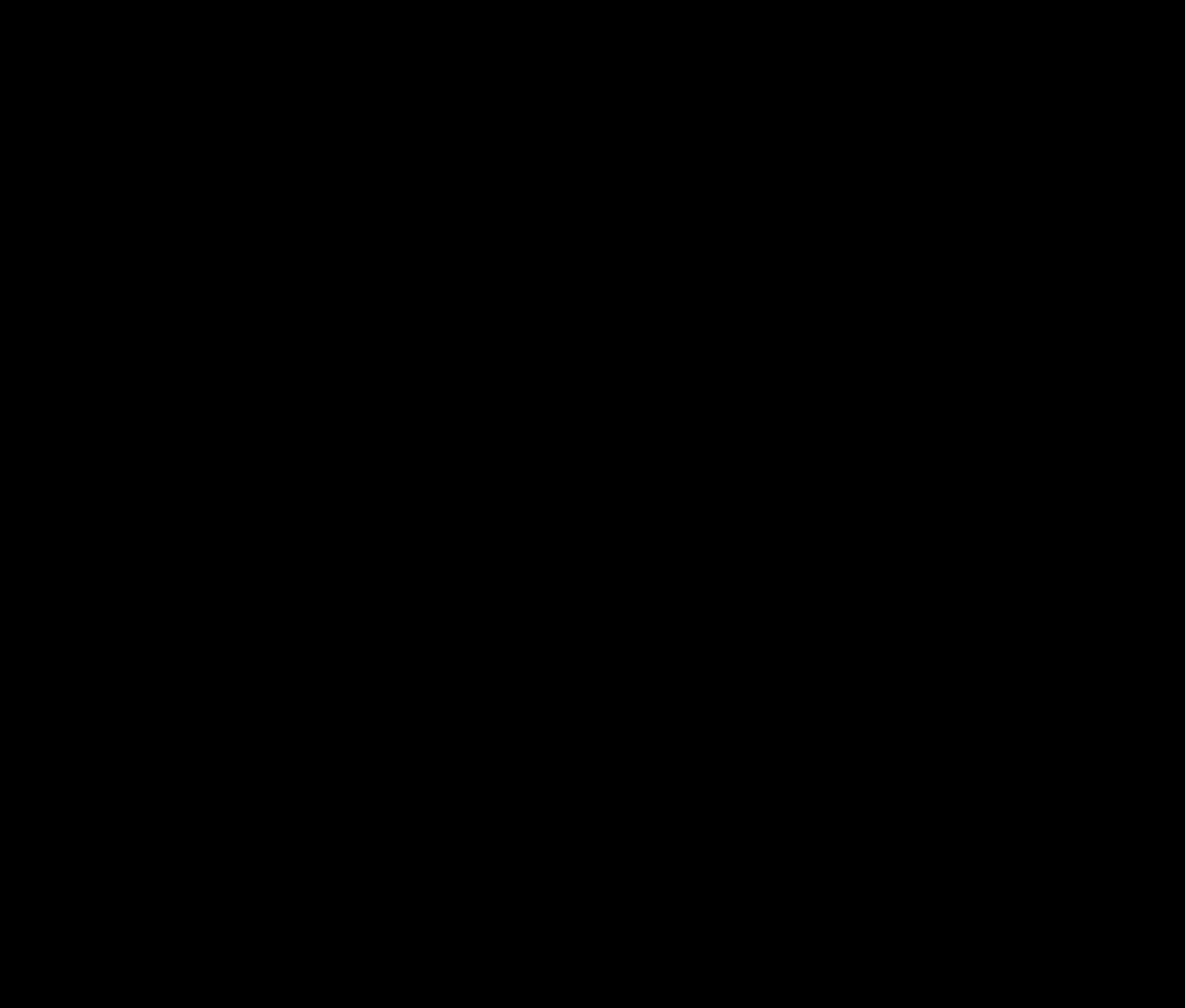
The Contractor must Complete the Milestones by the following Agreed Dates:

--	--	--	--









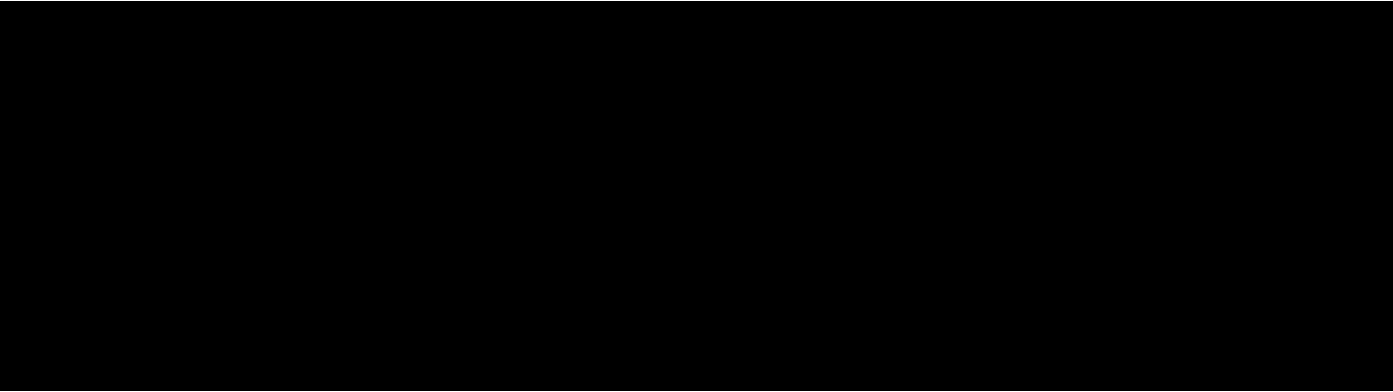
\*Note: For the avoidance of doubt, the above Agreed Dates should take into account the timeframe for the Deliverables to undergo the required Acceptance Testing and achieve the Customer's acceptance, as a Deliverable will not be treated as delivered, complete and accepted until the Customer provides the Contractor with its written acceptance of the Deliverable.

#### **LIQUIDATED DAMAGES**

The above table sets out which Milestones are LD Obligations.

Liquidated Damages are calculated in accordance with the table below, with the maximum amount payable for each LD Obligation being capped at an amount equal to the:

Liquidated Damages payable per day in respect of that LD Obligation multiplied by the maximum number of days for Liquidated Damages to be paid in respect of that LD Obligation in each case as set out in the table below.



Formal Go Live acceptance criteria is considered a key Deliverable (**D1047, D1051, D1055, D1059, D1063, D1067**) within the requirements of this Transition-In project and is to be developed jointly between the Customer and the Contractor.

Any development of Go Live acceptance criteria must include a consideration of the following:

1. Delivery and performance of the Services in accordance with the Contract Specifications which are required for the Contractor to achieve Go Live.
2. Completion of sufficient resourcing activities so as to ensure continuous delivery of Services in accordance with the Service Levels.
3. Satisfactory completion of all required training activities, with all staff resources having reviewed the prepared training materials.
4. Achievement of AAD of all Deliverables outlined earlier in the Project Plan and documentation of all processes.
5. Completion of all activities outlined earlier in the Project Plan that are required to be completed prior to Go Live.

## 11. Payment Plan

### ADDITIONAL PRODUCTS / SERVICES

The Contractor agrees that if the Customer requests the Contractor to provide any additional products or services in writing, it will comply with such requests.

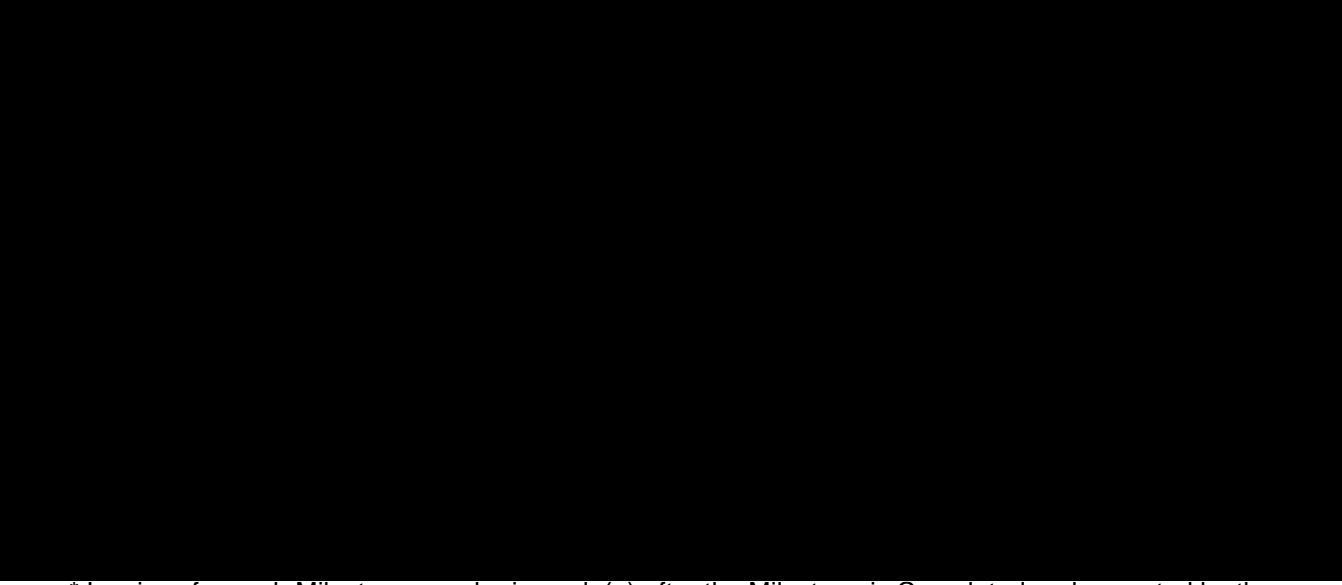
### PRICE FOR MANAGED SERVICES

The Price for ongoing Managed Services (as set out in Item 11 of the General Order Form) will be payable on and from completion of Transition-In and is to be paid monthly in arrears as per the General Order Form.

### PRICE FOR TRANSITION-IN SERVICES

Price for the Transition-In (including the Transition-In Services (as defined in the Module 12 Order Form) performed under Module 12) is as per Item 11 of the General Order Form (**Transition-In Price**).

Payment of the Transition-In Price is on a milestone basis as defined below.



\* Invoices for each Milestone may be issued: (a) after the Milestone is Completed and accepted by the Customer; and (b) in accordance with Item 11 of the General Order Form.

## 12. Governance

Governance frameworks and procedures as defined below are to be established during the Transition-In and maintained throughout the duration of the Contract Period.

### **AUTHORISED REPRESENTATIVE**

#### **Customer's Authorised Representative**

Refer to Item 3 of the General Order Form.

#### **Contractor's Authorised Representative**

Refer to Item 6 of the General Order Form.

### **MANAGEMENT COMMITTEE**





The management committee must, at a minimum:

- (a) review and monitor progress under the Customer Contract; and
- (b) carry out any other functions stated in Item 16 of the General Order Form or clause 6 of Part 2 (Customer Contract).

#### **Management committee meetings**

The management committee must meet weekly for the duration of the Transition-In Period at the Customer's address as per Item 2 of the General Order Form or as otherwise specified by the Customer.

After the completion of Transition-In, management committee meetings will be conducted at the direction of the Customer, at the Customer's address as per Item 2 of the General Order Form or as otherwise specified by the Customer.

#### **Management committee progress report**

The Contractor's project manager is to produce a management committee progress report prior to each meeting of the management committee, which must, at a minimum, include:

- (a) details (including dates) of Deliverables and Milestones commenced, completed or accepted;
- (b) any Delays or issues arising from the Transition-In project, including any known reasons for the Delay or issue arising, and plans for the management of such Delays and issues;
- (c) a review of:
  - (i) any minutes and actions from the last meeting;
  - (ii) issues logs;
  - (iii) the risk management plan, which must be prepared and maintained by the Contractor in accordance with AS/NZS ISO 31000 Risk Management Standard or equivalent as well as Exhibit 1 (Risk and Resilience Framework v6.0) annexed to this PIPP, unless agreed in writing;
  - (iv) details of any outstanding invoices and any payments that are about to become due;
- (d) draft updates of relevant parts of the Contract Specifications;
- (e) any new Change Requests or Contract Variations (if applicable); and
- (f) reviewing progress of any draft Change Requests or Contract Variations (if applicable).

# PROCURE IT VERSION 3.2

## MODULE ORDER FORM

### MODULE 12 – MANAGED SERVICES

#### Box 1 Managed Services

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
<b>Service Description (clause 1.11)</b>	
<p>Specify the Managed Services to be provided, such as management of:</p> <ol style="list-style-type: none"> <li>a. Hardware, desktop Environments, server Environments or mainframes;</li> <li>b. telephony services;</li> <li>c. software, databases or applications (excluding SaaS, IaaS and PaaS);</li> <li>d. help desk or support services;</li> <li>e. printers, copiers or print related services;</li> <li>f. any combination of the above; or</li> <li>g. any other technology or Environment that is agreed by the Parties.</li> </ol>	<p>The Managed Services to be provided by the Contractor are as follows:</p> <ol style="list-style-type: none"> <li>(a) all Services outlined in Exhibit 1 (Services) to the General Order Form, including:               <ol style="list-style-type: none"> <li>(i) multi-cloud management services, including but not limited to:                   <ol style="list-style-type: none"> <li>1. leveraging the Customer's existing cloud management platform to enable the delivery of computing integration services;</li> <li>2. proactive and reactive system operations services; and</li> <li>3. development operations services for engineering support of automated software delivery pipelines in public cloud environments;</li> </ol> </li> <li>(ii) computing integration services, including but not limited to:                   <ol style="list-style-type: none"> <li>1. management of infrastructure as a service across public cloud, private cloud and on-premises environments;</li> <li>2. management of backup as a service including management of multiple backup platforms;</li> <li>3. management of storage as a service;</li> <li>4. delivery of cloud optimisation solutions to reduce current and future costs;</li> <li>5. delivery of data engineering Services;</li> <li>6. configuration of specific security postures as required by the Customer and participation in the</li> </ol> </li> </ol> </li> </ol>

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
	<p>Customer's overarching security environment; and</p> <p>7. management and operation of system integrity activities; and</p> <p>(iii) on request from the Customer, Citrix cloud transformation project delivery services, subject to the Parties agreeing and entering into a Change Request in respect of those Services .</p> <p>(b) any other services described in the Contract Specifications including, to avoid doubt, Exhibit 2A (General Requirements) and Exhibit 2B (Functional Requirements) to the General Order Form; and</p> <p>(c) any services, functions and responsibilities not specifically identified above but are inherently required for the proper performance and provision of the services to be provided by the Contractor under the Customer Contract as set out in (a) and (b) above,</p> <p>in respect of the Customer's various public cloud, private cloud and physical on-premises hosted environments.</p> <p>In the event of any conflict or inconsistency between:</p> <p>(i) Exhibit 1 (Services) to the General Order Form;</p> <p>(ii) Exhibit 2B (Functional Requirements) to the General Order Form; and</p> <p>(iii) Exhibit 2A (General Requirements) to the General Order Form</p> <p>the document higher up in the above list shall prevail to the extent of the conflict or inconsistency.</p>
<b>Contract Period (clause 2.1)</b>	
Specify the Commencement Date	The Managed Services will commence on the date that the Contractor achieves 'Go Live' (as defined in the PIPP) in accordance with the PIPP ( <b>Services Commencement Date</b> ).
Specify the Contract Period (if different from default period) <i>Note: default period under Module 12 is three years</i>	The Contract Period for the Managed Services will commence on the Services Commencement Date (as specified above) and end on the end date of the Contract Period of the Customer Contract as specified in Item 10 (Contract Period) of the General Order Form. Such end date is the date that is 3 years from the Commencement Date of the Customer

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
	Contract as specified in Item 10 (Contract Period) of the General Order Form, subject to a one-year extension option, followed by a second one-year extension option, both at the Customer's option as outlined in Item 10 (Contract Period) of the General Order Form.
Specify the Consolidation Period <i>Note: the default Consolidation Period is the first month of the Managed Services</i>	The default Consolidation Period will apply.
<b>Performance and Pricing Assumptions (clause 1.4)</b>	
Assumptions as agreed between the Parties regarding performance of the Managed Services and Price	There are no Assumptions to be incorporated into the Customer Contract.
<b>Supplementary Processes (clause 4.13)</b>	
Specify any supplementary processes and terms that apply to the Managed Services	As per Contract Specifications
<b>System (clause 1.16)</b>	
Specify the Contractor's information technology facilities dedicated to the provision of the Managed Services (unless set out in the PIPP)	Not applicable



## Box 2 Transition In Plan

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
<p><b>Completion Date (clause 3.31)</b></p>	
<p>Specify the completion date for Transition In Services</p> <p><i>Note: the Transition In Plan is to be annexed to this Order Form. The completion date may be set out in the PIPP</i></p>	<p>The date which is 199 days from the Commencement Date of the Customer Contract (as specified in Item 10 (Contract Period) of the General Order Form).</p> <p>The Parties acknowledge and agree that for the purposes of this Module 12:</p> <p>(a) the Transition In Plan is the PIPP, which is attached to the General Order Form; and</p> <p>(b) all references in the Customer Contract to the Transition In Plan are references to the PIPP.</p>
<p><b>Specification of Transition In Services (clause 3.3)</b></p>	
<p>Specify whether the Contractor is required to perform due diligence</p> <p><i>Note: 'due diligence' may include assessment and definition of the:</i></p> <ol style="list-style-type: none"> <li><i>Customer's goals, requirements and expectations in respect of the Managed Services;</i></li> <li><i>Contractor's understanding of the Customer's and/or user's experience and requirements in relation to the Managed Services;</i></li> <li><i>objectives to be met by the Contractor;</i></li> <li><i>nature and scope of the Managed Services, including Environment, the Assets, Client Contracts and Third Party Contracts (and any requirement to novate or assign any of them);</i></li> <li><i>end users who will be supported by the Managed Services;</i></li> <li><i>necessary Assets and Additional Items and how they may need to be procured;</i></li> <li><i>migration of Customer Managed Services Data;</i></li> <li><i>Transition In Plan;</i></li> <li><i>required Deliverables;</i></li> <li><i>resources required (including any Customer Supplied Items or Customer assistance);</i></li> <li><i>complexity of the project; and</i></li> <li><i>any Transition Out Plan.</i></li> </ol>	<p>Yes <input type="checkbox"/></p> <p>No <input checked="" type="checkbox"/></p> <p>If Yes, specify the period in which due diligence must be completed (if different from default period of 30 days).</p> <p>For the avoidance of doubt, clauses 3.3 to 3.10 of Module 12 (Managed Services) will not apply.</p>
<p>Additional Assets or Additional Items to be acquired by the Contractor? (Clause 3.11)</p>	<p>Yes <input type="checkbox"/></p> <p>No <input checked="" type="checkbox"/></p>

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
	If Yes, what are the Additional Items/Assets?
<b>Valuation of Assets and Additional Items (clause 3.12)</b>	
Specify the method of valuation for the Assets and Additional Items (unless set out in the PIPP)	Not applicable
<b>Title and Risk to Assets and Additional Items (clause 3.14)</b>	
Specify when Title to the Assets and Additional Items passes to the Contractor <i>Note: the default position is that Title passes on the Services Commencement Date</i>	Not applicable
Specify when Risk to the Assets and Additional Items passes to the Contractor <i>Note: the default position is that Risk passes on the date the Contractor takes possession of the Assets and Additional Items</i>	Not applicable
<b>Client and Third Party Contracts (clause 3.15)</b>	
Client Contracts or Third Party Contracts transferred to the Contractor?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>  If Yes, list the Client Contracts/Third Party Contracts
Party who bears the costs associated with novation of a Client Contract/Third Party Contract, procurement of management rights or the performing of obligations under clauses 3.16 and 3.17 <i>Note: the default position is Customer bears the associated costs</i>	Not applicable
<b>Data migration (clause 3.23)</b>	
Specify if the Managed Services require migration of the Customer Managed Services Data	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>  If Yes, list the Parties' obligations in relation to the migration of Customer Managed Services Data
<b>Payment (clause 8.1)</b>	

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
Specify the payment details for the Transition In Services	The Price of \$2,151,174.08 ex-GST for the Transition In Services is payable in seven instalments in accordance with the PIPP and Items 11 (Common Details) and 14 (Payment) of the General Order Form.

### Box 3 Transition Out

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
<b>Specification of Transition Out Plan (clause 7.1)</b>	
<p>Specify if the Contractor must develop a Transition Out Plan</p> <p><i>Note: the Transition Out Plan must include</i></p> <ol style="list-style-type: none"> <li><i>Price payable for Transition Out Services;</i></li> <li><i>costs associated with selling, transferring, assigning or relocating assets exclusively used in the provision of the Managed Services;</i></li> <li><i>costs associated with winding down or stranded assets; and</i></li> <li><i>how and when the Price and any other sums are due and payable.</i></li> </ol>	<p>Yes <input checked="" type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>The Contractor must provide a Transition Out Plan that (at a minimum) meets the requirements of:</p> <ol style="list-style-type: none"> <li>clause 13.1 and 13.4 of Item 43 (Additional Conditions) of the General Order Form; and</li> <li>clauses 7.1 and 7.2 of Module 12 (Managed Services).</li> </ol>
<p>Specify the Transition Out Services provided by the Contractor</p> <p><i>Note: Transition Out Services may include:</i></p> <ol style="list-style-type: none"> <li><i>selling, transferring, assigning or relocating assets exclusively used in the provision of the Managed Services and the amount payable to the Contractor for such items;</i></li> <li><i>providing reasonable assistance in procuring novations or assignments of the Client Contracts/Third Party Contracts to a new services provider or to the Customer;</i></li> <li><i>returning or destroying documents or materials containing the Customer's Confidential Information together with any reproduction of those documents or materials;</i></li> <li><i>transitioning the Managed Services to a new service provider or to the Customer; and</i></li> <li><i>granting or assisting the Customer (or new service provider) to procure a licence to continue using any generally commercially available software in the Australian market which is the same as that being used in the System and any software owned by the Contractor which is</i></li> </ol>	<p>The Transition Out Services required to be provided by the Contractor must:</p> <ol style="list-style-type: none"> <li>address the matters set out in clause 7.2 of Module 12 (Managed Services) and clause 13.4 of Item 43 (Additional Conditions) of the General Order Form; and</li> <li>comply with all other requirements as agreed in the Transition Out Plan(s).</li> </ol> <p>The applicable resource rates are as set out in Appendix A (Rate Card) of the PIPP.</p> <p>The method that is used to calculate the Price for the Transition Out Services will be set out in the Transition Out Plan, subject to the requirements of clauses 13.7 to 13.10 of Part A of Item 43 (Additional Conditions) and the requirements of Item 42 (Termination for Convenience) of the General Order Form.</p>

<i>integral to the ongoing provision of the Managed Services, subject to payment of licence fees by the Customer (or new service provider).</i>	
Specify the Transition Out Period (if different from the default period of 3 months)	The Transition Out Period is as specified in clause 1.1 of Part B of Item 43 (Additional Conditions) of the General Order Form (subject to paragraph (b)(ii) of Item 42 (Termination for Convenience) of the General Order Form).

#### Box 4 Services

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
<b>Security measures (clause 4.6)</b>	
Specify the level of security and encryption required for the Customer Managed Services Data <i>Note: Contractor should provide security measures that are in line with best practice industry standards. Any access to the Customer Managed Services Data is subject to these measures</i>	As set out in Item 25 (Secrecy and Security) of the General Order Form.
<b>Additional Services (clause 6.2)</b>	
Specify the rates at which any Additional Services will be charged <i>Note: if there is no rate specified, Additional Services will be charged as the Contractor's then current rates for government</i>	Additional Services will be charged using the applicable time and materials rates as set out in Appendix A (Rate Card) of <b>the PIPP</b> . The Contractor may only charge for Additional Services to the extent agreed in writing by the Customer in advance.

#### Box 5 Service Levels

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
<b>Personnel (clause 5.3)</b>	
Specify any person/s who is/are organised by, or under the direction of the Customer	There are no persons being organised by or under the direction of the Customer who are relevant to the Contractor's ability to meet or exceed the Service Levels (if any).

#### Box 6 Payment

Details to be included from Module 12	Order Details agreed by the Contractor and the Customer
<b>Payment for Services (clause 8.2)</b>	
Specify how the Customer will pay the Contractor <i>Note: default position is Customer pays monthly in arrears</i>	As set out in Item 11 (Common Details) and Item 14 (Payment) of the General Order Form.
<b>Payment for Assets and Additional Items (clause 8.4)</b>	

Specify the period in which the Contractor must pay the Customer the purchase price for the Assets and Additional Items <i>Note: default position is within 30 days of receipt of a tax invoice, such invoice to be provided on or after the Services Commencement Date</i>	Not applicable.
<b>Licence fees for Contractor Services Data (clause 9.8)</b>	
Specify any licence fees that must be paid by the Customer to the Contractor for the Contractor's Services Data	No such licence fees are payable.

