Queensland Government Enterprise Architecture

ICT as-a-service security assurance guideline

Final

June 2016

V1.0.0

PUBLIC

Document details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Security classification** | 1. PUBLIC | | | | | |
| 1. **Date of review of security classification** | 1. June 2016 | | | | | |
| 1. **Authority** | 1. Queensland Government Chief Information Officer | | | | | |
| 1. **Author** | 1. Department of Science, Information Technology and Innovation, ICT Modernisation | | | | | |
| 1. **Documentation status** |  | 1. Working draft |  | 1. Consultation release | 1. 🗹 | 1. Final version |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Department of Science, Information Technology and Innovation, ICT Modernisation  
[ICTModernisation@dsiti.qld.gov.au](mailto:ICTModernisation@dsiti.qld.gov.au)

Acknowledgements

This version of the *ICT as-a-service security assurance guideline* was developed and updated by Department of Science, Information Technology and Innovation, ICT Modernisation.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

*ICT as-a-service security assurance guideline*

Copyright © The State of Queensland (Department of Science, Information Technology and Innovation) 2016

Licence

[](http://creativecommons.org/licenses/by/4.0/)

This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au).

To attribute this material, cite the Department of Science, Information Technology and Innovation.

The licence does not apply to any branding or images.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Introduction 5](#_Toc453923065)

[1.1 Purpose 5](#_Toc453923066)

[1.2 What is this guideline for? 5](#_Toc453923067)

[1.3 Why does the Queensland Government need this guideline? 5](#_Toc453923068)

[1.4 Who should use this guideline? 5](#_Toc453923069)

[1.5 How does this guideline fit within the ICT as-a-service decision framework? 6](#_Toc453923070)

[1.6 When should I use this guideline? 7](#_Toc453923071)

[1.7 References 7](#_Toc453923072)

[2 Security assurance model 8](#_Toc453923073)

[3 Identify information and service attributes 9](#_Toc453923074)

[3.1 Business workload and planned service delivery profile 9](#_Toc453923075)

[3.2 Security and governance considerations 9](#_Toc453923076)

[3.3 Risk profile 10](#_Toc453923077)

[4 Shortcuts 11](#_Toc453923078)

[4.1 Compliance 11](#_Toc453923079)

[4.2 Industry accreditations 11](#_Toc453923080)

[4.3 Profiling available service offerings 12](#_Toc453923081)

[4.4 Other shortcuts 12](#_Toc453923082)

[5 Checklist and business security considerations 13](#_Toc453923083)

[5.1 Questions for use during sourcing and procurement 13](#_Toc453923084)

[6 Evaluation assurance 24](#_Toc453923085)

[6.1 Queensland Government Cloud computing implementation model 24](#_Toc453923086)

[6.2 Independent evaluation of security and audit reports 24](#_Toc453923087)

[6.3 Trial access and ICT security tests 24](#_Toc453923088)

[6.4 Technical evaluation of claims 24](#_Toc453923089)

[6.5 Embedded assurance claims in the contract 25](#_Toc453923090)

[7 Information sharing 25](#_Toc453923091)

[7.1 Contract clauses 25](#_Toc453923092)

[7.2 Risk treatment 26](#_Toc453923093)

[7.3 Security requirements 26](#_Toc453923094)

[8 Security assurance guideline roadmap 27](#_Toc453923095)

[Appendix A Demarcation of security roles and responsibilities 28](#_Toc453923096)

[Appendix B Evaluation – selection criteria 31](#_Toc453923097)

Figures

[Figure 1. ICT as-a-service decision framework 6](#_Toc453923117)

[Figure 2. ICT as-a-service security assurance model 8](#_Toc453923118)

[Figure 3. Customer managed to cloud service provider managed: The Continuum of Cloud Services 28](#_Toc453923119)

# Introduction

## Purpose

A Queensland Government Enterprise Architecture (QGEA) guideline provides information for Queensland Government agencies on the recommended practices for a given topic area. Guidelines are generally for information only and agencies are not required to comply. They are intended to help agencies understand the appropriate approach to addressing a particular issue or doing a particular task.

This document provides information and advice to support Queensland Government agencies in gaining adequate assurance of planned cloud and ICT as-a-service offerings through the evaluation, service integration design, contract and procurement activities.

While this document identifies some common mandatory obligations, such as privacy legislation, additional obligations may exist such as contract obligations (e.g. PCI-DSS or grants conditions), or domain specific legislation (e.g. health, law enforcement or child safety). Given this, agencies are strongly recommended to further investigate potential obligations that may exist in their own business domain.

## What is this guideline for?

This guideline is designed to assist agencies in developing a quality assessment process when considering the use of ICT as-a-service. It outlines the key security considerations, questions and possible answers with associated risk rankings that agencies should address as part of their existing quality and security management processes.

The guideline is a set of assurance criteria designed to:

* assess the risk of adopting cloud services
* compare different cloud provider offers
* obtain assurance from the selected or potential cloud providers.

## Why does the Queensland Government need this guideline?

The objective of this guideline is to ensure a common and consistent vetting of supplier security assurance levels across Queensland Government agencies.

## Who should use this guideline?

The intended audience for the ICT as-a-service quality and security assurance guideline is:

* a requestor of a service
* a buyer of a service
* architects
* an implementer of a service
* service management staff.

It is recommended that the reader be familiar with the [Queensland Government Information Security Classification Framework](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2417-queensland-government-information-security-classification-framework) (QGISCF) and essential that information that forms part of the ICT as-a-service has been through the classification process to understand its sensitivity.

## How does this guideline fit within the ICT as-a-service decision framework?



Figure 1. ICT as-a-service decision framework

Figure 1 above details the key steps in the decision-making process within the ICT as-a-service Decision Framework and also provides additional guidance to support each step.

| Key steps | Policy/framework |
| --- | --- |
| Understand the decision framework | [*ICT as-a-service Decision Framework* - Overview](https://www.qgcio.qld.gov.au/products/qgea-documents/3244-ict-as-a-service-decision-framework-overview) (see Figure 1) |
| Understand the policy – ICT as-a-service | [*ICT as-a-service policy*](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/3236-ict-as-a-service-policy) |
| Know your asset/s | [*Queensland Government Information Security Classification Framework*](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2417-queensland-government-information-security-classification-framework) *and*  [*Information asset custodianship – IS44*](https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2632-information-asset-custodianship-policy-is44) |
| Which service model (IaaS, PaaS, IaaS, BPaaS, hybrid)? | ICT as-a-service – Service Model Selection (under development) |
| Which deployment model? | [*ICT as-a-service deployment model selection*](https://www.qgcio.qld.gov.au/products/qgea-documents/3243-ict-as-a-service-deployment-model-selection) |
| Asset value and risk assessment (Phase 1 - pre–procurement) | [*ICT as-a-service risk assessment guideline*](https://www.qgcio.qld.gov.au/products/qgea-documents/3241-ict-as-a-service-risk-assessment-guideline) and [*ICT as-a-service risk assessment annexe*](https://www.qgcio.qld.gov.au/products/qgea-documents/3242-ict-as-a-service-risk-assessment-annexe) |
| Authority to use ICT as-a-service | [*ICT as-a-service offshore data storage and processing policy*](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/3237-ict-as-a-service-offshore-data-storage-and-processing-policy)and [*ICT as-a-service policy*](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/3236-ict-as-a-service-policy)and[*Information Security-IS18*](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy) |
| Cloud procurement (Phase 2 – Procurement) | [*Cloud solution buying guideline*](https://www.qgcio.qld.gov.au/products/qgea-documents/570-workflow/3463-cloud-solution-buying-guideline) and *ICT as-a-service security assurance guideline* (this document) |
| Solution decision | Internal procurement processes and policy to be followed |
| Deployment management and ongoing assurance | Internal project management processes and policy to be followed |

## When should I use this guideline?

This document assumes the decision to move an ICT workload to an as-a-service model has already been made, and the vendor selection process as part of phase 2 of the procurement cycle has started. Figure 1 illustrates where this guideline forms part of the ICT as-a-service decision framework.

While this guideline is targeted at evaluating an as-a-service offering for procurement purposes, it also provides guidance for the solution design, development, implementation and service management phases.

## References

The following documents and guidelines were used in the development of this paper:

| Name | Version | Originator |
| --- | --- | --- |
| ICT as-a-service Decision Framework - Overview | 1.0.0 | Queensland Government Enterprise Architecture (QGEA) |
| ICT as-a-service policy | 1.0.0 | QGEA |
| Cloud first strategy-released | - | Queensland Government Chief Information Office (QGCIO) |
| Cloud solution buying guideline | 1.0.0 | QGEA |
| ICT as-a-service offshore data storage and processing policy | 1.0.0 | QGEA |
| IRAP cloud considerations | 0.2 | The Frame Group |
| CSA\_CSM \_V3.01-09-16-2014 | 3.01 | Cloud Security Alliance |
| Cloud computing security considerations | - | Australian Signals Directorate |
| Security for cloud computing – 10 steps to ensure success | 0.2 | Cloud Standards Customer Council |
| Queensland Government information security classification framework | 3.1.0 | QGEA |
| Cloud computing risk assessment guideline | 1.0.2 | QGEA |
| Cloud computing risk assessment guideline annexe - risk considerations | 1.0.2 | QGEA |
| Information Security Classification Framework | 1.3 | QGEA |
| Queensland Government Network Transmission Security Assurance Framework | 1.0.1 | QGEA |
| IS18 – Information security implementation guideline | 1.0.2 | QGEA |
| Managing the record keeping risks associated with cloud computing | - | Queensland State Archives |
| Cloud Computing Information Assurance Framework | - | European Network and Information Security Agency |

# Security assurance model

Figure 2 below depicts the ICT as-a-service security assurance process for the vetting of cloud and as-a-service offerings in alignment with the Queensland Government’s ICT as-a-service Decision Framework.



Figure 2. ICT as-a-service security assurance model

The assurance model, on the left of figure 2, is representative of the advice detailed in this guide. Each section flows directly into the yellow outcomes from that section. Typically, these would usually represent a range of project artefacts to support a procurement process and guide any implementation project. Various business, procurement and ICT stakeholders are responsible for development of these artefacts.

The nature of the service (ICT as-a-service) and its risk profile, would dictate the number and detail of artefacts required to achieve an acceptable level of service assurance against an agreed risk position. For example, if the ICT as-a-service pertained to non-critical, low risk public information contained on a website, very little security assurance may be required, therefore few artefacts outside the business case and related procurement documents and final contract may be required. Contrasting that with an ICT as-a-service that contains private financial information, a far more rigorous set of security assurance documentation would be required.

# Identify information and service attributes

## Business workload and planned service delivery profile

From a business assurance perspective, the following should be addressed as part of the evaluation and pre-implementation of any ICT as-a-service.

Business workload profile:

What is the business driver for this ICT as-a-service?

* Is the workload largely standalone or part of a broader tightly integrated and/or complex business process?
* Does the workload have demanding network data flow requirements to other systems separate from the service provider?
* Is the workload business critical, does it have high resiliency, recovery point/time or long data retention requirements?
* Does the workload have high audit or integrity requirements, if so, how will appropriate visibility be achieved and assured?

Planned service delivery profile:

* Will it be totally outsourced and administered under contract?
* Will the solution elements be managed by both the agency and the as-a-service provider? If so, are the boundaries and touch points well described.
* Are any other third party contracts/providers likely to be a part of the delivery of this as-a-service?

## Security and governance considerations

From a security and governance perspective, the following process and controls should be evaluated to ensure the integrity of an agency’s ICT security posture, and to meet good practice for the governance of ICT.

* Compliance: does the ICT as-a-service offering meet all internal and externally applicable laws, regulations and policies, standards? What relevant independent assurance can they offer and/or can be obtained through planned evaluation e.g. ISO27000 and other standards based certification, security reviews, and audits.
* Conformance: does the ICT as-a-service offering meet all privacy laws, commercial confidentiality constraints, acceptable intellectual property contract clauses and other government security standards?
* Have all operational rules/constraints and resiliency provisions for the ICT as-a-service offering been fully described? This would include, but not be limited to: archiving, backups, audit logs, business continuity practices and service level agreement (SLA) reporting.
* Will the introduction of this ICT as-a-service necessitate a change to the agency structure? If so, has this change been documented and agreed to by the business owner/s?
* What is the mix of users and organisations involved in meeting the business driver for this service? How is it envisaged they will interact with and move data in/out of the service?
* Have both the technical and contractual aspects of transitioning in and out of the service been adequately resolved? Specifically, exit criteria, lock in prevention and continued provider support arrangements during the transition out phase should be established at the beginning of the engagement.
* Will the agency require new skills and competences with the introduction of this ICT as-a-service? If so, have these skills and competences been documented, funded and agreed to by the business owner/s?
* Will the introduction of this ICT as-a-service change any business processes (internally or externally) or workflows? If so, have any impacts been documented and agreed to by the business owner/s? What documentation will need to be updated?

## Risk profile

Certain services and information have an inherently higher risk profile than others.

The profile can vary in part due to potential for malicious actors to make money either directly or indirectly, for example: stealing identity information, corrupting approvals and licenses, early access to business information, redirecting refunds and medical script fraud. Additionally, due to the nature of the service being provided some services will have broader exposure to attacks, for example: lots of untrusted users, the need to handle a variety of untrusted data, and exposure to the internet when high availability is important.

Where a service has a particularly low risk profile, less rigour is likely to be required to meet an agency’s risk appetite. An example might be limited use cloud service, to support an optional business activity such as generating graphs that are copied into presentations using near public information.

Where a service has a high risk profile, involvement of technical and process expertise is important from early on in the process through to the validation of a final production environment.

Legal risk should be considered as part of establishing the risk profile. Specific information or agency attributes may prescribe limitations on how and where data can legally be transmitted or stored. These include but are not limited to personally identifiable information (PII), financial information, heath information, legal/police and child safety information. These types of data need to be individually assessed against the ICT as-a-service offering and relevant domain specific legal drivers.

# Shortcuts

The Queensland Government is committed to leveraging assurances where possible and appropriate to reduce the impact on vendors through streamlining the assessment process.

## Compliance

While as-a-service providers may comply with industry standards and gain common industry accreditations, it is important to verify what specific systems or processes were assessed in gaining the certification, and whether those systems or processes are the ones being procured as the agency’s intended as-a-service implementation.

## Industry accreditations

The following industry accepted security standards, regulations, and control frameworks may be useful in shortlisting ICT as-a-service providers. The evaluation may be streamlined by requesting the full prior assessment material and reports associated with certifications/accreditations when these are directly relevant to the planned service implementation.

| Standard/Framework | Description |
| --- | --- |
| ISO/IEC 27001:2013 | Information technology – Security techniques - Information security management systems - Requirements |
| ISO/IEC 27002 | Information technology – Security techniques – Code of practice for information security management |
| CCM 3.01 | Cloud Controls Matrix – Cloud Security Alliance |
| SSAE16 SOC-1 Type II, SSAE16 SOC-2 Type II | Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization |
| ISO/IEC 38500 | ICT Governance – International Standards Organisation (ISO) |
| COBIT5 | Framework for IT Governance and Management – Information Systems Audit and Control Association (ISACA) |
| IT Audit and Assurance Program for Cloud Computing | Cloud Computing Assurance Program – Information Systems Audit and Control Association (ISACA) |
| Cloud Computing Information Assurance Framework | [European Union Agency for Network and Information Security](https://www.enisa.europa.eu/) (ENISA) |
| Cloud Computing Risk Assessment | [European Union Agency for Network and Information Security](https://www.enisa.europa.eu/) (ENISA) |
| AS/NZS ISO 31000:2009 | Risk Management – Principles and guidelines |
| NIST SP 800 and 1800 series | NIST computer security and cyber security practice guides. |

Depending on the specific application of the as-a-service, agencies may require suppliers to comply with the following policies:

| **Policy Compliance Requirements** | **Source** |
| --- | --- |
| ICT as-a-service offshore data storage and processing policy | Queensland Government Chief Information Office |
| Queensland Government Information Security Classification Framework (QGISCF) | Queensland Government Chief Information Office |
| Queensland Government Network Transmission Security Assurance Framework | Queensland Government Chief Information Office |
| Information Security - IS18 | Queensland Government Chief Information Office |
| AISEP Policy Manual  AISEP Certifier Policy  AISEP Evaluator Policy | Australasian Information Security Evaluation Program (AISEP) - Australian Signals Directorate |
| ASD Certified Cloud Services List | Information Security Registered Assessors Program - Australian Signals Directorate |
| Cloud Computing Security Considerations | Cyber Security Operations Centre - Australian Signals Directorate |

## Profiling available service offerings

Agencies may wish to procure cloud access security brokerage (CASB) services to assist in vetting cloud service providers. For instance, services are available that process all published terms, conditions and provide security commitments to provide vendor/service report cards. These report cards could be used to quickly rule out selected services and/or arrive at a list of services with suitable conditions.

Where a service is low risk (information is not sensitive, low business impact) with alternative data recovery options, little additional assurance may be required beyond a report card. Changes to the use of a service, threat environment or service provider’s practices and hosting may necessitate future reassessment.

Additional CASB services (e.g. policy enforcement, monitoring, integration) can be used to enable an organisation to gain visibility into cloud usage, access cloud services, review risk profiles, enforce security policies, and detect/respond to potential threats.

## Other shortcuts

Other shortcuts may arise from the sharing of information between agencies ([Section 7 Information Sharing](#_Information_sharing)).

# Checklist and business security considerations

## Questions for use during sourcing and procurement

The questions below are to provide criteria and guidance for Queensland Government agencies to consider during sourcing and procurement of services from an as-a-service provider.

The questions have a security focus and the list is meant to be indicative rather than comprehensive i.e. there are many more considerations, both technical and business related, when making a decision to transition an ICT workload to an as-a-service model or selecting a service provider. There are many documents published to assist agencies in this process, some of which can be found on the [Queensland Government Information Office website](https://www.qgcio.qld.gov.au/products/qgea-documents).

The responses from service providers will provide input to the final risk assessment for the service being considered. Risk treatment controls can be applied to the final assessment which will guide the solution decision. The Cloud Controls Matrix from the Cloud Security Alliance provides a controls framework which is cross referenced to industry accepted security standards and regulations which will assist agencies in developing internal controls that align with industry standards.

The column title ‘Sample responses and risk’ is to assist agencies in selecting the appropriate questions for the solution in question. It is not prescriptive. By example, if a solution is of low risk and low dollar value and deals with only unclassified or public information it may not be important as to the location of the service provider’s data centres or the country where the data is resident.

Use the following questions to assess the security posture of potential service offerings whether sought through tender or via a direct purchase in the case of low dollar value offerings.

Public information will typically have no confidentiality risk. While risk profile will generally increase in line with information security classification due to the associated impact (PROTECTED implies higher impact than IN-CONFIDENCE), this is not always the case. Attacker motivation and other factors can impact likelihood e.g. platform, solution design, denial of service susceptibility, political/protest motivators, service profile and the potential for malicious actors to achieve financial gain.

The following checklist is designed to guide the user through a range of threshold questions to allow for the overall evaluation of various ICT services. It is not a complete or authoritative set of questions, however it is based on a variety of Australian and international standards and industry best practice at the time of writing. It allows the user to understand when an activity may require access to a subject matter expert for further input and to continue with evaluation ensuring a high degree in confidence in the execution and due diligence for each activity. Note that the checklist in this section is to be used as a guideline and not all questions/considerations will be applicable under all circumstances. Where the guidance isn’t relevant it should be ignored. Where it is applied and the risk is seen as moderate or above, additional guidance may be required to supplement and extend the list.

The following guidance provides typical questions and anticipated answers/responses with colour coded consideration guidance.

**Red**. This usually indicates a ‘showstopper’ when the answer is poor, omitted or substantiation is omitted for an apparent strong response. Cease all activity and seek out subject matter expert input or informed executive sign off to proceed.

**Amber**. Generally, this would indicate that detailed expertise is probably required. Proceed with caution and consider input from subject matter expert.

**Green**. Proceed after providing business level documentation around the context of the decision. This relates to any non-security/ICT technical specialised attributes that are being considered.

| **Question** | **Guidance** |  | **Sample responses and risk** | **Level of risk** | **CSA\_CSM Control ID** |
| --- | --- | --- | --- | --- | --- |
| **Section1: Data sovereignty and hosting services** | | | | | |
| Are all data centres in Australia? | Data classification, domain specific legislation or other sensitives may limit or render unsuitable offshore data transfer, storage and analysis services.  The [ICT as-a-service offshore data storage and processing policy](https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/3237-ict-as-a-service-offshore-data-storage-and-processing-policy) includes the following policy requirements: • PR1: Offshoring data must be subject to an information security classification assessment  - data classified above PROTECTED must not be stored offshore • PR2: A risk assessment must be conducted prior to offshoring information  - a range of specific issues that must be included in the risk assessment are identified • PR3: Offshored data must be adequately protected through contractual arrangements  - a range of key areas that must be addressed and contract templates are identified • PR4: Decisions to use offshore ICT as-a-service must be approved by the appropriate authority  - PROTECTED requires Departmental CEO and Whole of government approval  - below PROTECTED requires Departmental CEO or nominated delegate |  | Yes. All data centres and service operators are located within Australian sovereign territories | Low | DSI-02 |
|  | No. Our data centres are located outside of Australia.  *[Agency has reason to believe they can meet obligations of ICT as-a-service offshore data storage and processing policy, at an acceptable level of risk and service assurance]* | Medium |  |
|  | In addition to the above, be sure to understand the following:   * primary and backup locations * any cross border service administration arrangements which may allow uncontrolled access to the data from unexpected jurisdictions. |  | No. Our data centres are located outside of Australia.  [*Agency has not completed all obligations of ICT as-a-service offshore data storage and processing policy, or there is concern about the information in the service, inability to gain assurance and/or vendor willingness to provide contractual assurances such as compliance with privacy legislation]* | High |  |
| What is the nature of the data to be stored on this service | Services that contain personal information are subject to national privacy obligations and the *Information Privacy Act 2009 (QLD)* (the IP Act). Additional legislation may also need to be considered. For example the following areas have additional legislation to be considered: child protection, law enforcement and the health sector. |  | *[Agency has completed a data and privacy assessment. No PII or information otherwise sensitive to location will be part of the data retained within or exposed to risk via the service.]* | Low | GRM-01 |
| The IP Act only permits personal information to be sent out of Australia in the circumstances set out in section 33. Agencies should check where a cloud provider operates from, even when dealing with an Australian company. If the provider, or the hardware used by that provider, is not located in Australia, agencies will need to ensure they comply with section 33 for any personal information sent to the cloud. |  | Our solution is designed to hold your transaction data within our system. Independent assurance of and contractual commitment to meeting Australian and Queensland Privacy legislation obligations will be provided.  *[Agency to satisfy itself of the adequacy and applicability of assurances available and to ensure privacy provisions are adequately reflected in the contractual arrangements]* | Medium |  |
| When moving to cloud services, agencies may be able to comply with the obligations in section 33, at least in part, by entering into a contract with the cloud services vendor which provides for the same level of privacy protections as are in the IP Act. See: [https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/cloud-computing-and-the-privacy-principles](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/cloud-computing-and-the-privacy-principles%20) |  | *[While the vendor offers a range of technical controls such as statements of encryption, these do not come with independent assurance. The vendor will not commit to contractual obligations to meet section 33 or concerns remain about overall solution protection of data.]* | High |  |
| How and where will the live, standby and recovery instances/data be hosted? | Cloud and ICT as-a-service often have high availability of service and data mobility. Additionally, high availability is not equivalent to having separate media copies of service data available in the event of service failure, compromise or service disputes. Agencies must have a clear understanding of the arrangements and business risk should service data become unavailable or withheld. This is of elevated importance when the underpinning data is held offshore. |  | Our service hosting resilience and backup data are managed in a consistent manner as per the live service instance. Customer has equal visibility and control of service, data and administration access for all data/service instances including: backups (under the service), administrative access, service instances (live and high availability). | Low |  |
| Technical issues of backup and service resiliency are covered later in this table. |  | Our cloud servers are located in various world regional data centres to ensure maximum availability of your data.  *[Agency must understand if the data and service movement have adequate assurance that all service related data is managed within agency geographic, control and contract expectations]* | Low |  |
|  | *[Services with the only backups offshore and available solely through the main service provider should only be considered for low value information.]* | Medium |  |
| **Section 2. Hosting support services** | | | | | |
| What backup and service log retention options are available along with recovery and analysis support? | If backups and service logs are continually provided and captured within the control of the department or agency, then the risk level is as low as any other internal data source. Check that data ownership and custodianship has been correctly identified. |  | Under the proposed service all backups are controlled by the department/agency and are dealt with in accordance with Queensland government guidelines. Recovery points and times to move data under recovery situation have been demonstrated to be within acceptable recovery time objectives. Data transition-out of the service and/or into another service is covered under the contract and technical provisions to support it are understood. | Low | IAM-04, IAM-05, IAM-07 |
|  | Failure to retain access to independent, common mode fail safe recovery copies of data may be acceptable for low value data, however access to trustworthy recovery snapshots from a range of time periods is generally required for disaster recovery (including security incidents), service disputes and transition out support. An additional challenge with remotely hosted services can be data transfer times to or between service sites and from backup data copies. |  | Service application programming interfaces (APIs) are available to enable backup and log access.  *[Agencies should understand the opportunity and risks. Agencies should understand the cost and practicality of using the API.]*  Backup options are available within the service as are log access functions.  *[Agencies should understand exactly what is offered and assess against business objectives]* | Medium |  |
|  | Agencies should understand the nature of any data backup and recovery mechanisms, its degree of separation from the main service, along with times to utilise the backups in a recovery situation. Additionally, traditional considerations such as recovery time objective, recovery point objective and recovery retention objectives should be well understood. Similarly, any business expectation around service log retention and analysis capability should be understood, along with the proposed service's ability to meet the expectations. |  | The service is highly available.  *[Agency has not been able to confirm backup and recovery options, protection from common failures of both the service and backup environment or the ability to recover the service]*  *[Even though the supplier makes the statement ‘the service is highly available’, there is no assurance for the statement’s veracity.]* | High |  |
| When providing support, what controls and visibility of access are available to assure the customer that the access is appropriate and limited? | If the data is likely to be accessed by the ‘as-a-service’ provider’s staff, then those staff will need to be located in Australia (or as otherwise agreed as per section 1 of this checklist). |  | Any data that is to be accessed by vendor staff is only done so after prior notification and approval. Vendor identifies a range of specific technical, logging and customer visibility controls that provide customer confidence of at least the ability to detect and respond to service provider data access. The service as provided has been assured by XYZ [e.g. ASD certified cloud service] for ABC information. All staff with access to data have had XYZ background check processes  *[Agency is satisfied with the staff background/vetting process appropriateness given the data involved and/or with the assurance of the technical control environment]* | Low | DSI-02, DSI-03, DCS-01 |
|  | A description of the security model, service staff access and logging options are attached. XYZ independent reviews are available after a non-disclosure agreement (NDA) | Medium |
|  | We use best practices but will not disclose information about our internal process for security reasons.  *[Unless the service is of a truly trivial nature with no sensitivity, some degree of assurance should be achieved]* | High |
| **Section 3. Security measures** | | | | | |
| Please provide details of data protection controls for data in transit (to end users and between service components over shared networks) and for data at rest within the service | Adequate assessment of security controls even for lower risk use will require some level of subject matter expert (SME) advice. |  | No  *[Service providers that do not provide details of security controls should be avoided even for low impact uses]* | High |  |
|  | *[Details are provided. SME to assess]* | Medium |
| Describe the mechanisms for protection of the user accounts/profiles in transit and at rest. | User authentication and the underpinning user profile data (including credentials) requires protection in transit and at rest.  For example failure to encrypt passwords in solutions is a fundamental vulnerability and a warning indicator of other poor security practices. Another indicator of poor security practice is a failure to protect authentication information in transit e.g. a login screen without https://. |  | We take security seriously and use our encryption methods to protect your credentials.  *[Limited information or proprietary encryption used would be cause for concern]* | High |  |
|  | Full details are provided in XYZ along with independent assurance by ABC Information Security Registered Assessors Program (IRAP) assessment.  *[SME can advise on applicability and credibility of the supporting assessment]* | Medium |
| Does your solution include access controls to ensure only authorised staff have access to the data? | It is expected that all systems will have audit logs against all system activity relevant to a customer. These would be detailed within the final contract. |  | No | High |  |
|  |  | Yes, we fully audit all access controls and can make your logs available to you as a part of an agreed SLA | Low |
|  |  | Yes we fully audit all activity however we provide these logs only when a valid 'need to know' can be claimed. | Medium |
| Is data segregated from other customers’ data? | Investigate with SME and evaluate against the response. |  | No  *[this is typically not suitable unless it is a trivial service with no sensitivity]* | High |  |
|  |  | Yes, virtual data and network segmentation | Medium |
|  |  | Yes, physical data and network segmentation | Low |
| If your solution requires the customer to provide existing data, does your solution provide a secure method for uploading the data? | . |  | Yes, data is loaded directly by the customer into the secure solution | Low |  |
|  |  | Yes, data is transferred via an encrypted USB | Low |
| Seek SME input and assistance to confirm suitability |  | No, data is sent via email or file transfer protocol (FTP)  *[for public and low sensitivity information weakly protected information transfer may be acceptable]* | Medium |
|  |  | Not applicable, no data is transferred | Low |
|  |  | Yes via secure FTP, SSH or other secure protocol. | Low |
| Do you conduct criminal history checks on your employees and sub-contractors? | Each agency and potentially business area will have differing requirements for police checks. |  | No  *[Assess relative sensitivity of use, potential to be leveraged for access and standard agency requirements]* | High |  |
|  | Yes, additionally all staff have Australian security clearances | Low |
|  | Yes | Low |
| What physical access controls are in place at the locations from which data may be stored or accessed? | Prior validation of datacentres may be leveraged to reach adequate confidence in the relevant datacentre and/or virtual hosting environments. This validation will typically indicate the classification levels that are able to handled.  Physical security consideration will also extend to remote access locations used by the service provider.  In some instances alternative controls can compensate for limited physical access controls e.g. hardware encryption. |  | We use best practice physical security but will not disclose information about our internal process for security reasons.  *[Unless the service is of a truly trivial nature with no sensitivity, some degree of assurance should be achieved]* | High |  |
|  | We use secure swipe card access, biometrics, coded access, physical escort, CCTV monitoring, and Tier 3 certification.  *[While the above may sound impressive, the specific application to all access areas is complex. SME or independent assurance of applicability will generally be required for use of services for sensitive information]* | Medium |
| What remote access controls are used? | The level of access granted will be tied to the classification of the data. |  | We use best practice remote access controls but will not disclose information about our internal process for security reasons.  *[Unless the service is of a truly trivial nature with no sensitivity, some degree of assurance should be achieved]* | High |  |
|  | Multifactor authentication through a company owned device | Low |
|  | Multifactor authentication | Low |
|  | Not applicable, no remote access rights are granted | Low |
| How frequently do you conduct vulnerability testing? | These will need to be described and tracked in the SLA. As a minimum a right test and vulnerability scan of the service should be included. Failing this, visibility of some equivalent independent assurance mechanism should be established. |  | Every release and every X month(s). All issues addressed with results made available to customers after X weeks. Details of past patching performance is available through the XX report once you have signed the non-disclosure agreement. We also run a bug bounty program and have a proactive monitoring of vendor patch releases. | Low |  |
|  | Every 4-12 months | Medium |
|  | Every 13 months or longer | High |
| How frequently do you conduct penetration testing? | These will need to be described and tracked in the SLA. As a minimum a right test and commission penetration testing of the service should be included. Failing this, visibility of some equivalent independent assurance mechanism should be established e.g. copy of Australian Signals Directorate Certified Cloud security assessment, other credible independent assessments and certifications, independent audit results, and penetration testing details, and that the contract requires that these are maintained. |  | No | High |  |
|  | Yes, critical vulnerabilities resolved within 3 days | Low |
|  | Yes, critical vulnerabilities resolved within 4-14 days | Medium |
|  | Yes, critical vulnerabilities resolved in greater than 14 days | High |
| Do you implement remediation strategies within a reasonable amount of time? | These will need to be described and tracked in the SLA and considered in conjunction with maintenance windows. |  | No | High |  |
|  | Yes, critical vulnerabilities resolved within 3 days | Low |
|  | Yes, critical vulnerabilities resolved within 4-14 days | Medium |
|  | Yes, critical vulnerabilities resolved in greater than 14 days | High |
| Do you conduct investigations into security breaches and implement remediation strategies? | The data centre may conduct such investigations, however, they may choose not to share their insights. This should be agreed and understood prior to signing contracts. |  | No | High |  |
|  | Only upon request | Medium |  |
|  | Yes | Low |  |
| Do you conduct regular security training for all staff to prevent inadvertent disclosures? | Best practice and international standards would see all staff put through at least annual security training. |  | No | High |  |
|  | Yes, every 12 months | Low |
| How is the service, data and/or service provider independently assured and/or certified? | Reputable ICT as-a-service providers including cloud service providers will have had a range of service reviews and security assessments performed. They should be willing to make these available to customers along with detailed scope information to validate their relevance to the actual service being acquired. |  | We take security very seriously and use industry best practices*….[implied ‘trust us’]*  *[Motherhood statements without supporting specifics and independent assurance can be a warning sign]* | High |  |
|  | Yes, we can make available XYZ security review, details of ABC certifications.  *[Agencies should engage internal expertise to assess the relevance and adequacy of assessments/certifications relative to the business risk of the service. Only for low value, low risk services used by a small number of staff should skipping expert involvement be considered.]* | Medium |
| Do you immediately notify your customers of any security breaches? | An agreed process should be written into any contract or SLA. Generally for any information with sensitivity an obligation to notify you as a customer in a timely manner should be included in the service conditions. |  | No | High |  |
|  | Yes in our monthly SLA report | Medium |
|  | Yes | Low |
| What data breaches has the service experienced in the last 12 months?  What monitoring and controls are in place to detect and support response to security events? | Recent detection of a security issue is not necessarily an indication of poor security, it may be an indication of effective monitoring. However a track record of repeated security incidents experienced by a service or its underpinning platform and environment could be an indicator of poor security architecture.  Similarly, failure to detect any compromises does not necessarily mean a service is secure.  Agencies need to understand the security environment including detection and response capabilities, along with any available assurance of vendor claims. |  | Breach data is not shared | High |  |
|  | Section XYZ of our response describes nature of security incident detections and mechanisms in place.  *[Agency requires expert assistance in assessing vendor responses]* | Medium |
| Please provide a description of service audit log review and monitoring.  Please provide details of customer options to review and export audit logs related to our use of the service. This should include details of what logs are available. | Limited audit log visibility may be acceptable if the data to be stored is public in nature with limited integrity concerns. |  | No | High |  |
|  | Only upon request | Medium |
|  | Yes | Low |
| Do you regularly conduct reviews of user access levels? | ‘No’ may be acceptable if the data to be stored is public in nature. |  | No  *[Unless data stored is public in nature]* | High |  |
|  | Yes, frequency of reviews and approach is described in section XYZ of our response. | Low |
| Do you store printed copies of data securely? | ‘No’ may be acceptable if the data to be stored is public in nature. |  | No  *[Unless data stored is public in nature]* | High |  |
|  | Not applicable, no printed copies created | Low |
|  | Yes, detailed storage policies are described below … | Medium |
| **Section 4. User access controls** | | | | | |
| Does the solution uniquely identify users e.g. through unique usernames and passwords for end users and all administrative functions? | The solution will not track an individual’s changes for an audit trail if users are not assigned a unique userid |  | No | Medium |  |
|  |  | Yes | Low |
| Provide details of credential and access management options supported, including details of storage protection for passwords and other credentials? | Passwords are generally stored using a security hash within a key server |  | No, passwords are stored in clear text | High |  |
|  |  |  | Yes, reputable independent security reviews and testing with visibility of credential management has been conducted. Full details of the findings are attached.  *[Agency should still apply internal expertise to validate the applicability of the assessments]* | Low |  |
| What are the account authentication reset protocols? | Depending on the classification, reset protocols may need to be straight forward or comprehensive for renewed access to an account. Seek SME advice to strike the appropriate level of response. |  | These can be determined by each client or we have a fully -self-service password reset facility. | Medium |  |
|  | We conduct a full identity check | Low |  |
| Please describe security architecture and access controls for all levels of users | SME is required to make this assessment for all but trivial services with low sensitivity. |  | No access controls | Medium |  |
| Does the Solution support multi-factor authentication (MFA)? | Subject to a risk assessment, understanding access granted, application context and other detective controls, basic passwords are often acceptable. As per the Queensland Government Authentication Framework (QGAF) remote access to PROTECTED information requires multi factor authentication. |  | No | Medium |  |
|  | Increasingly MFA has become common practice and is available in many consumer grade services. Given the issues with simple passwords, the demand for MFA is to the point where many users expect it to at least be an option. Additionally, for bulk sensitive data or where compromise can result in making money, MFA is recommended.  Multifactor authentication is typically suitable for all types of data, however be mindful of the imposition on your users. |  | Yes  *[Subject to agency validation of the MFA and how it is deployed and managed. Appropriateness of registration process must also be understood.]* | Low |  |
| **Section 5. Quality controls** | | | | | |
| Have you implemented change control processes to minimise disruption during business hours? | If your business would be impacted by the solution being “offline”, explore these items further. |  | No  *[Generally not acceptable unless the service is of little to no business impact, such as an optional limited use cloud service]* | High |  |
|  |  | Yes  *[Subject to the agency understanding, accepting and being offered assurance about the processes]* | Low |
| Do you have a Business Continuity Plan in the event of a disaster, a cyber incident or physical attack on the service environment? |  |  | No  *[Generally not acceptable unless the service is of little to no business impact, such as an optional limited use cloud service]* | High |
|  | Yes, and it can be read at our web site. Business continuity of the solution has been certified against ISO 22301 and we can make the full assessment available to you, including details of testing.  *[Subject to agency assessment of applicability to the planned deployment and assurance commensurate with business criticality]* | Low |
| What is the availability of the Solution, underpinning platform(s) and connectivity? | Availability of business service often extends beyond the availability of individual technical service components and often depends on service integration decisions. Aside from simple standalone services, wherever availability of a service is business critical an SME who understands the interdependencies of the likely deployment design should be consulted.  Availability needs to match business needs. Contractually obligated true high availability (HA) will often increase costs. |  | *[Consult SME]* | Low |
| Do you notify your customers of all security incidents, including all cases where their data or service may be impacted? Impacts may include corruption of data, unauthorised access and availability impacts or loss | If data integrity is critical, explore these items in further detail with the system provider. |  | Yes | Low |  |
|  | No  [*Generally not acceptable unless the service is of little to no business impact, such as an optional limited use cloud service]* | High |
| Does your solution use data loss prevention (DLP) technologies? | If data integrity is critical, explore these items in further detail with the system provider. |  | No | Medium |  |
|  | Yes. We use a range of proprietary tools to ensure your data is safe …  *[Where DLP is a considered a key mitigating control, an SME should be engaged to confirm the effectiveness of the solution.]* | Low |  |
| What is the recovery time objective (RTO)? | The RTO represents how long the vendor will take to recover your data, therefore the vendor’s response should align, or exceed, how long your business would be able to survive without the solution. |  | Yes. Choose the RTO that applies to your service 99.99% = 5 min 99.95% =10 min 99.8% = 30 min 99.5% = 2 hours 98% = 4 hours not stated = best effort  *[Agency must understand their own business requirement compared to as-a-service provider commitment, and include contract compensation for failure to meet service level]* | Low |  |
|  | *[None specified]* | High |  |
| What is the Recovery Point Objective (RPO)? | The RPO represents how much data could be lost in the recovery, therefore the vendor’s response should align, or exceed, how much data you could accept losing. |  | Yes. Choose the RPO that applies to your service 99.99% = 0 min 99.95% =5 min 99.8% = 15 min 99.5% = 12 hours 98% = 1 day | Low |  |
|  | *[None specified]* | High |  |
| Do you make the data available to the customer in an agreed format upon request? | If you are required to retain copies of the data for record keeping purposes, then you may wish to explore these items further. |  | No | Medium |  |
|  | Yes, as specified in our contract. | Low |
|  | Yes, but in predefined format | Low |
|  | Yes, our data retention policy aligns with the *Queensland Government* Public Records Act 2002Public Records Act 2002 | Low |  |
|  | Yes, we will retain data as long as you require it.  *[Format may not be readable]* | Medium |  |
| How long do you retain data for? | Differing data types have varying retention obligations. Please check with the national archives act or state government archive act to determine retention times. |  | Once deleted, your data is effectively gone unless you have purchased a backup service. | High |  |
| Do you delete the data upon the customer’s request and certify that deletion? | The ASD Information Security Manual describes the various types of secure data deletion and when they should be employed. |  | No | High |  |
|  | Yes | Low |
|  | Yes but certificate not provided | Medium |

# Evaluation assurance

## Queensland Government Cloud computing implementation model

The QGCIO maintains the [Cloud computing implementation model](https://www.qgcio.qld.gov.au/products/qgea-documents/570-workflow/3269-cloud-computing-implementation-model) which provides a strong set of guidelines to assist the business owner who may be considering purchasing an as-a-service offering. It guides the reader through all the base-level decisions and covers off in some detail ‘cloud readiness’ of the organisation as well as key implementation considerations for the business user.

## Independent evaluation of security and audit reports

When a business impact is considered moderate or above, or the information security classification is PROTECTED or higher, then due diligence would require a full evaluation assurance assessment as outlined in this guideline. If the overall risk profile is low (for all business risk impact levels) and the solution is not dealing with sensitive data, then the requirement for assurance is reduced appropriately.

Once a business decision has been made to purchase a cloud service, agencies should seek any available independent analysis of the service and associated provider’s operating environment. Security reviews, penetration tests and audit reports may demonstrate compliance with information security and confidentiality, access control, service definitions, and service level agreement commitments in contracts. Many of these base requirements are outlined in the [decision support checklist in section 5](#_Checklist_and_business). More detailed specifications can be found in other Queensland Government standards and those published by the Australian Signals Directorate (ASD), as outlined in the reference list in this guide.

## Trial access and ICT security tests

Once a service provider has been selected, an agency should consider establishing a proof of concept (PoC) environment. A PoC will allow the agency to validate technical claims made by the service provider as well as provide a low risk environment for the agency to conduct those ICT security tests that have been deemed necessary. These tests may range from no-security tests for low risk, low value services to complex and extensive security tests by accredited providers for high value, high risk implementations.

There should be a clear PoC period or trigger for completion of the PoC. At its completion, a review of the effectiveness of the solution concept should be conducted to inform the decision whether to roll forward into production. PoCs are often conducted and established in a manner that may not be suitable for production. The review should identify further treatments required to be addressed prior to using in the final production environment. These may include: configuration hardening, data flow understanding, network filtering and monitoring, logging, proper backups and other security considerations.

## Technical evaluation of claims

Agencies should seek a level of assurance over the validity and relevance of service provider claims.

A common mistake is to trust in a certification or independent assessment that is not relevant to the planned solution.

With non-trivial services that are integrated into other business flows, often only staff with specific technical and architectural knowledge of the planned solution can assess the applicability of claims and advise on further assurance steps. In these cases claims made by service providers should be referred to technical staff and architects for assessment of credibility and verification of relevance to the planned solution as it will be deployed.

## Embedded assurance claims in the contract

Service provider assurances provided as part of assessing suitability should be reflected in the contract with contractual remedies for breach or failure to adhere to those assurances.

# Information sharing

The cloud and as-a-service landscape is evolving rapidly with new services emerging daily and thus new security threats and vectors are evolving rapidly. (A vector is a path or means by which a malicious user can gain access to exploit system vulnerabilities.)

A common set of security assurance questions across Queensland Government agencies would help alleviate the compliance and auditing burden on service providers as well as assist those service providers in understanding the security requirements that agencies require.

A Cloud Community of Practice (CoP) has been established across Queensland Government. The aim of the CoP is to increase maturity and capability in cloud computing practices across whole-of-government. To find out how to connect with the Cloud CoP email: [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au).

Additionally, the knowledge base (a place for agencies to share tools and guides) continues to be available through the QGCIO portal for agencies to share their own useful guidelines and resource material (Queensland Government employees only).

## Contract clauses

Contract clauses used by agencies to mitigate as-a-service risk may have broader applicability, so sharing them will assist improvement in practices across the sector.

The [Government Information Technology Contracting Framework documents page](https://publications.qld.gov.au/dataset/gitc-framework) provides contract resources. Included on this page is “Module 10 - Additional Provision for Cloud Services”.

Many cloud services are offered on standard service contracts with little or no scope for negotiated variations or use of a standard government contract template. It is important that agencies be aware of and address the potential risks when accepting vendor terms and conditions. Key issues and considerations include:

* data security
* back-up processes
* that data sensitivity is catered for in level of security provided
* dealing with security breaches
* data privacy
* compliance with Australian Privacy Principles, 2104: (APP8 – cross border disclosures, APP11 - protecting personal information from interference, misuse, loss and unauthorised access, modification and disclosure)
* location of data

onshore considerations

offshore considerations – legal jurisdiction, data access and recovery, legal restrictions on storage location, access by foreign governments.

* confidentiality

signed confidentiality deeds for provider employees

notification requirements if data is accessed by foreign agencies.

* liability

provider’s caps on liability

determining each party’s liabilities and relevant indemnities.

* intellectual property

the Queensland Government default position is ‘non-consultative co-ownership of intellectual property’ (arising from action 2.05 of the Queensland Government ICT Strategy 2013-2017 Action Plan).

* warranties

providers’ desired limits on warranties, e.g. to ‘fit for purpose’

need for customer due diligence on warranties

arrangements for control of ‘functional changes’ by provider during the warranty period.

* service levels

number of simultaneous users

service desk response times

change management controls

times service is available

performance metrics and measures.

* termination

termination for convenience or non-performance provisions

transition out support including technical mechanisms and business process considerations to allow a successful service migration at the end of the agreement.

## Risk treatment

Risk assessments of services already completed by other agencies may assist an agency in risk profiling of as-a-service offerings.

Policies and/or procedures adopted by agencies to mitigate risk where it is not possible to vary service provider terms and conditions may also be relevant to other agencies.

Agencies should follow the ISO/IEC 31000 (and/or ISO 27005) Risk Management standard approach for the risk assessment using the 5 x 5 Impact and Likelihood risk assessment matrix. This approach enables appropriate responses and risk treatments to be developed based upon a clear understanding of the risk environment. It also provides a common language to facilitate the sharing of risk analyses and management plans between agencies.

## Security requirements

Agency specifications of security requirements for go-to-market documents may be appropriate for re-use for similar applications.

# Security assurance guideline roadmap

This document will be revised throughout 2016 as part of the wider ICT as-a-service review. It will incorporate lessons and material from the Cloud Computing Community of Practice.

1. Demarcation of security roles and responsibilities

Prior to embarking on the security assurance process there needs to be a clear definition and understanding between the agency and the provider of security-relevant roles and responsibilities. The lines of such a demarcation will vary greatly between software as-a-service (SaaS) offerings and infrastructure as-a-service (IaaS) offerings, with the latter delegating more responsibility to the agency. A typical and rational allocation of responsibility is shown in the following tables. In any case, for each type of service, the agency and provider should clearly define which of them is responsible for all the items in the list below. In the case of standard terms of service (i.e. no negotiation possible), as-a-service agencies should verify what lies within their responsibility.

ICT as-a-service criteria

The security assurance guideline approach and principles are applicable to any as-a-service procurement initiative.

The most common forms of ICT service procurement are software as-a-service, platform as-a-service, and infrastructure as-a-service. Therefore, below are the key considerations that are specifically applicable to each of the service type packages.

Figure 3 below (source: Business Cloud News - November 16, 2015) delineates the responsibility between in-house service management and cloud service providers. From a security assurance perspective, the need for due diligence is proportional to the service type that is procured and the extent of control that the agency has i.e. for SaaS, the end-to-end control for the service is with the cloud provider.

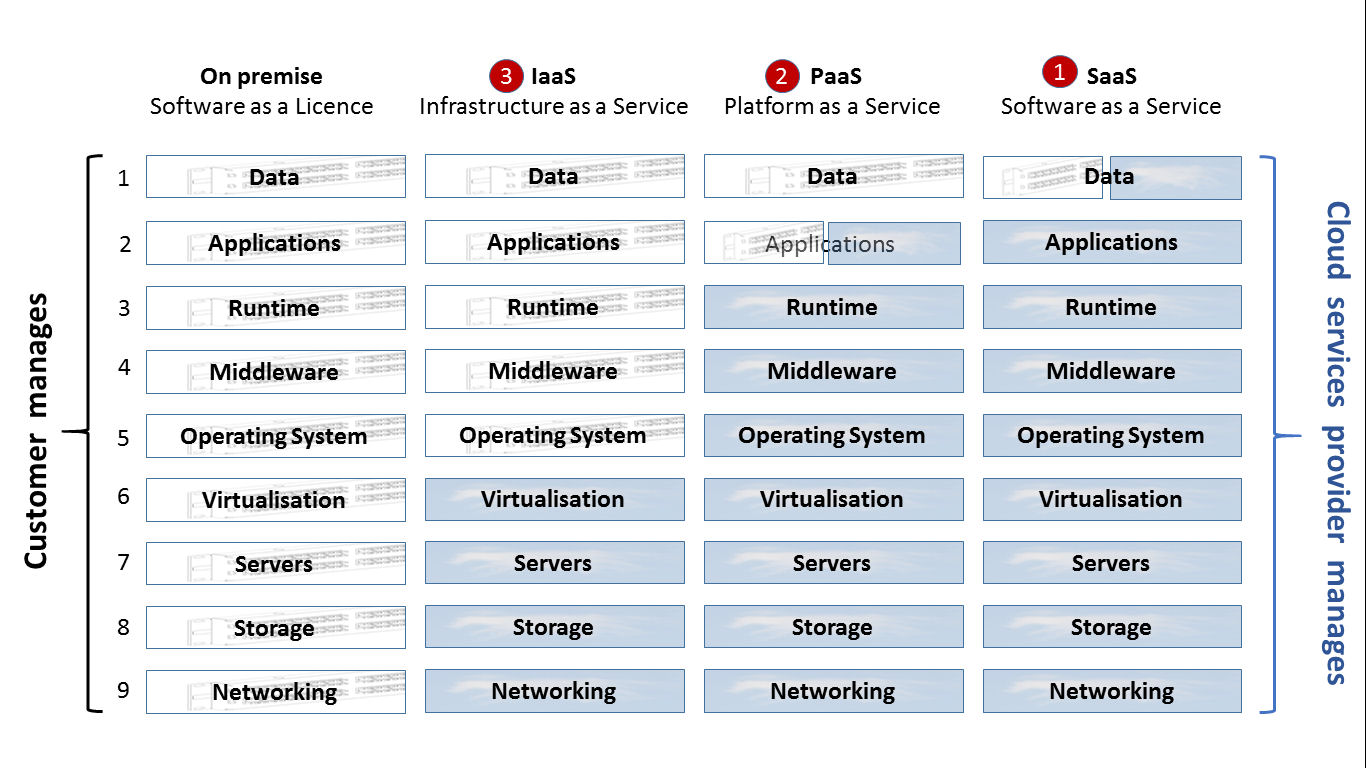


Figure 3. Customer managed to cloud service provider managed: The Continuum of Cloud Services

* 1. Software as-a-service

| **Agency** | **As-a-service provider** |
| --- | --- |
| * Compliance with data protection law in respect of agency data collected and processed * Maintenance of the agency identity management systems * Management of the agency identity management systems * Management of authentication platforms, active directory integration and or federation (including enforcing password policy). | * physical support infrastructure such as facilities, rack space, power, cooling and structured cabling * physical infrastructure security and availability for infrastructure including servers, storage and network bandwidth * Operating systems patch management and hardening procedures * security platform configuration including firewall rules, access control lists and IDS/IPS tuning * systems management and monitoring * security platform maintenance including firewall, bastion routers, host intrusion detection service (IDS)/ intrusion prevention service (IPS), antivirus, packet filtering * log collection and security monitoring * management, patching and maintenance of the application software. |
| 1. Relative risk: Low to medium |  |

Platform as-a-service

|  |  |
| --- | --- |
| **Agency** | **As-a-service provider** |
| * maintenance of agency identity management systems * management of agency identity management system * management of authentication platforms, active directory integration and or federation (including enforcing password policy). | * physical support infrastructure such as facilities, rack space, power, cooling and structured cabling * physical infrastructure security and availability for infrastructure including servers, storage and network bandwidth * OS patch management and hardening procedures * security platform configuration including firewall rules, access control lists and IDS/IPS tuning * systems monitoring * security platform maintenance including firewall, bastion routers, host IDS/IPS, antivirus, packet filtering * log collection and security monitoring. |
| 1. Relative risk: Medium to high |  |

Infrastructure as-a-service

| **Agency** | **As-a-service provider** |
| --- | --- |
| * maintenance of agency identity management systems * management of agency identity management system * management of authentication platforms, active directory integration and or federation (including enforcing password policy) * management of guest OS patch and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) * configuration of guest security platform including firewall rules, access control lists and IDS/IPS tuning * guest systems monitoring * security platform maintenance including firewall, bastion routers, host IDS/IPS, antivirus, packet filtering * log collection and security monitoring Maintenance of identity management system. | * physical support infrastructure such as facilities, rack space, power, cooling and structured cabling * physical infrastructure security and availability for infrastructure including servers, storage and network bandwidth * host systems including hypervisors, virtual firewalls and other supporting infrastructure. |
| 1. Relative risk: High |  |

Evaluation – selection criteria

Application/service profile

The following general criteria should be considered as part of the evaluation of any application or system that is potentially being migrated or implemented as an ICT as-a-service offering:

* What is the risk profile with the preferred vendor?
* From a cost benefit perspective, what are the application’s costs in-house versus a service offering by a cloud vendor? (This would examine but not be limited to: licence costs, WAN data usage, maintenance costs, migration costs, integration costs, restructuring costs either related to in-house support e.g. service desk capability etc., network management upgrade costs, asset depreciation cost, support contract negotiation etc.)
* Can one environment be moved? For example, can a specific production test/development application be moved without moving the corresponding production environment?
* What are the data management requirements? This relates to backups and tiering.

SaaS criteria

The following criteria should be considered as part of evaluating SaaS packages:

* What is the application’s service availability requirement?
* What are the application’s performance requirements?
* What resilience is required by the application? Consider the following:

Recovery level objective (RLO) refers to the level of availability a service needs to be recovered to, following a disruption. An RLO will be time-specific, e.g. a service must be available during business hours of operation; and it may be location-specific, e.g. the service must be available to specific departments or building floors, but it is not essential at others.

Recovery point objective (RPO) is the point at which loss of data is tolerated as a result of disruption and recovery of a service. For example:

* + - zero RPO means that no data loss is tolerated
    - 1 day RPO means that up to one day loss of data is tolerated.

Recovery Time Objective (RTO) is the elapsed time needed for recovery of a service after a disruption.

* what application and/or data integration requirements are required?
* can the existing security environment/policy of the application or service be maintained by the provider or if not, can the application accept a new security risk profile?
* in moving an application to an as-a-service model, what is the financial impact of the data transmission and retrieval, that is what WAN data volume costs, will be incurred?
* has the application realised the cost benefit analysis as per its business case objectives?
* what administration controls are provided and can these be used to assign read and write privileges to other users?
* is the SaaS access control fine grained and can it be customised to your organisation’s policy?

PaaS criteria

Generally speaking, PaaS service providers are responsible for the security of the platform software stack; the following questions of the service provider should assist in evaluating their offerings:

* request information on how multi-tenanted applications are isolated from each other – a high level description of containment and isolation measures is required.
* what assurance can the PaaS provider give that access to your data is restricted to your enterprise users and to the applications you own?
* the platform architecture should be classic ‘sandbox’ – does the provider ensure that the PaaS platform sandbox is monitored for new bugs and vulnerabilities?
* PaaS providers should be able to offer a set of security features (re-useable amongst their clients) – do these include user authentication, single sign on, authorisation (privilege management), and SSL/TLS (made available via an API)?

IaaS criteria

IaaS service providers treat IaaS applications and services as a ‘black box’. Agencies are responsible for the operation and management of their applications and services. The following is a brief checklist/description relating to best practice for secure application design and management:

* Cloud deployed applications must be designed for the internet threat model (even if they are deployed as part of virtual private cloud (VPC). They must be designed/embedded with standard security countermeasures to guard against the common web vulnerabilities (see Open Web Application Security Project (OWASP) guides)
* Agencies are responsible for keeping their applications up to date – and must therefore ensure they have a patch strategy (to ensure their applications are screened from malware and hackers scanning for vulnerabilities to gain unauthorised access to their data within the cloud). Agencies should not be tempted to use custom implementations of authentication, authorisation and accounting (AAA) as these can become weak if not properly implemented.

As-a-service candidacy criteria

The following criteria should be used when assessing the viability of migrating applications or systems to an as-a-service model:

* systems which are not part of the active network
* applications that do not require tight integration with the active network
* applications that do not require guaranteed, consistent (high) performance and availability
* applications or systems which do not provide security functions or support security functionality
* applications that do not have low network latency requirements
* applications or data that do not require higher security levels than can be contracted by the cloud provider
* applications which do not require large amounts of data to be transferred in or out of the organisation’s network (e.g. data warehouse systems).

Implementation criteria

ICT as-a-service governance considerations

From a governance perspective, the following should be addressed as part of the implementation of any ICT as-a-service:

* risk management (increased complexity and reduced direct control)
* impact on change management
* compliance, internal and external to the organisation (as this relates to applicable government laws, regulations and policies, standards)
* conformance, internal and external to the organisation (as this relates to privacy laws, commercial confidentiality, intellectual property and security)
* operational rules (archiving, backups, audit copies)
* what new skills and competences are required? (this may entail re-engineering the current workforce through either training or hiring in skills)
* is there a change to the organisation structure?
* how will the organisation monitor and audit the new service?
* what processes and workflows will be impacted and need to be updated?
* is there a change to the configuration management process?

Security and risk governance considerations

From a security and risk perspective, the following process and controls should be evaluated on an ongoing basis to maintain the integrity of the agency’s ICT security posture.

* are initial and ongoing processes and controls in place to ensure that the security posture of the service provider’s ICT environment is maintained consistently throughout the operation of any cloud service.
* similarly, this includes processes and activities to ensure that the risks are periodically remedied in light of new policies, new threats or new business requirements.