

Information security external party governance guideline

Final

November 2010

v1.0.0

PUBLIC

Queensland Government Enterprise Architecture

ICT Policy and Coordination Office
Department of Public Works

Queensland Government

Document details

Security classification	PUBLIC		
Date of review of security classification	November 2010		
Authority	Queensland Government Chief Information Officer		
Author	Queensland Government ICT Policy and Coordination Office		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

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

Director, Policy Development
ICT Policy and Coordination Office
ICTPolicy@qld.gov.au

Acknowledgements

This version of the *Information security external party governance guideline* was developed and updated by the ICT Policy and Coordination Office.

Feedback was also received from a number of agencies, including members of the Information Security Reference Group, which was greatly appreciated.

Copyright

Licence

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

1.1 Purpose

This guideline has been developed to assist Queensland Government agencies to ensure that external party governance arrangements align with the requirements of Information Standard 18: Information security (IS18).

Adherence to this document is not mandatory.

1.2 Audience

This document is primarily intended for:

- Chief Information Security Officers
- Information asset custodians
- ICT asset custodians
- Information technology managers
- Information security governance bodies
- Information security policy officers responsible for developing external governance policies and procedures
- Agency staff that manage arrangements with external parties including Government Information Technology and Communications (GITC) contracts, memorandums of understanding (MOUs), operating level agreements (OLAs) and service level agreements (SLAs).

1.3 Scope

This guideline relates to the external party governance domain within the information security policy framework of the Queensland Government Enterprise Architecture (QGEA).

This document does not address:

- how to identify whether there is a business need to work with an external party
- other information management issues that may need to be addressed in external governance arrangements including recordkeeping, right to information, intellectual property, copyright – for advice on recordkeeping in this context, please refer to the Queensland State Archives' Custody and ownership guideline: Managing public records during outsourcing or privatisation
- general ICT procurement policy requirements or contractual terms in detail (refer to Information Standard 13: Procurement and disposal of ICT products and services (IS13) and the GITC contracting framework)
- controls to be applied when an external party shares its information with an agency, see the Queensland Government Information Security Controls Standard (QGISCS).

1.4 Background

The Information Security Policy Framework defines external party governance as 'all activities related to the governance, authorisation and auditing of information security arrangements for external parties that handle organisational information'.

Agencies should implement controls that maintain the security of information and ICT assets that are accessed, processed, communicated to, or managed by external parties.

External parties may include service providers, customers, outsourcing suppliers, consultants, auditors, cleaners.

It should be noted that it is not possible to outsource compliance. Although an agency may outsource or externally host information or ICT assets, the agency retains accountability for the security of the information involved. Therefore, it is important to document information security requirements of external parties in an agreement, and to monitor adherence to that agreement throughout the life of the arrangement with the external party.

2 External users of agency information and ICT assets

2.1 Identifying the risks

Prior to granting external users access to agency information and ICT assets, the agency should:

- conduct a risk assessment
- document the risk assessment.

Where it is evident that the requirements of IS18 are not or are highly likely to not be met, the agency needs to decide whether it is willing to accept the risk or not. If it is willing to accept the risk, it needs to formally sign off on these risks.

External parties granted access to agency systems must be made aware of their responsibilities and relevant agency information security and other policies (eg. Recordkeeping).

General risk management guidance is available within AS/NZS ISO 31000:2009 Risk management – Principles and guidelines.

2.2 Common risks and issues to be addressed

Risks associated with external user access to agency information and ICT assets can arise from a number of factors including:

- software vulnerabilities
- external user self-selection
- external user's direct, unsupervised access to the agency's information and ICT assets
- opportunity for the external user to load and manipulate information on those systems[1].

Common issues to be addressed commensurate with risk include:

- how assets will be protected
- how breaches will be identified
- how access will be controlled, including authentication requirements
- how incidents relating to customer access will be dealt with
- how and when access may be revoked
- legalities eg. information privacy[2].

[1] A. Calder & S. Watkins, 2006. *International IT governance: An executive guide to ISO 17799 / ISO 27001,* Kogan Page, London, p. 103.

[2] Ibid; AS/NZS ISO/IEC 27002:20006 Information technology – Security techniques – Code of practice for information security management.'

3 External ICT service providers

3.1 Identifying the risks

The same principles that applied in section 2.1 apply to arrangements with external ICT service providers. The considerations in section 3.4 below may assist in the risk identification process for those ICT services proposed to be delivered by an external party.

3.2 Agreements

If after conducting a risk assessment the agency decides to proceed with the arrangement, it should document the arrangement and its conditions. The security classification of the information assets and the business impact of the ICT assets involved will dictate the level of formality required to meet IS18 obligations. For example, an operationally critical system or information source usually requires formal contracts and agreements covering maximum outage times, dispute resolution and breach penalties. A research and development system will often have simpler, more informal arrangements.

The agency's information security policy and plan should form the basis of any such agreement.

3.2.1 Standard agreements and information security

Depending on the security classification of the information assets involved, it may not be sufficient to rely on the pre-existing information security related clauses within the GITC. Generally, agencies need to document their information security requirements within the offer, contract documents, specifications and schedule of particulars.

This applies equally to agency standard templates for MOUs, OLAs and SLAs.

3.3 QGEA mandated external ICT providers

Agencies should conduct a risk assessment prior to entering an arrangement with any QGEA mandated external ICT provider. The same principles apply in this scenario as outlined above. That is, where it is evident that the requirements of IS18 are not, or are highly likely to not be met, the agency needs to decide whether it is willing to accept the risk or not. If it is willing to accept the risk, it needs to formally sign off on these risks. If the agency is not willing to accept the risk, it may apply for a QGEA exception from adoption of the mandated external ICT provider.

It is strongly recommended that agencies enter a documented contract/OLA/SLA with QGEA mandated external ICT providers.

3.4 Considerations for external party agreements

This section provides a checklist of information security relevant items to be considered prior to documenting and entering an external party agreement. It is based on and organised according to the mandatory principles within IS18.

3.4.1 Policy, planning and governance

Have agency expectations (eg. the direction, scope and approach to information security issues and risks) been communicated to the external party?

- Have information security requirements and risks been specified in sufficient detail to be included in communications and agreements with the external party?
- Are they consistent with the mandatory clauses outlined in the Information Security Compliance Checklist?
- Has the external party outlined sufficient risk mitigation strategies for identified risks?

Have changes in business and information security risks been reflected in existing and future external party arrangements?

- How are information security requirements and risks communicated to the external party?
- Does the agreement allow information security requirements and risks to be changed?
- How does the agency ensure that current information security requirements and risks are addressed by the agreement?
- Are external party agreements regularly reviewed and monitored?

Is the external party arrangement consistent with the agency's general security plan, information security plan and security risks?

- Have information security requirements from the general security plan and information security plan been considered during the development of agreements?
- How will changes to the general security plan and information security plan be incorporated into new and existing agreements?

Have the expected information security governance, functions, roles and responsibilities been documented in external party agreements?

- Are agreements with external parties consistent with the agency's documented information security functions, roles and responsibilities?
- Are any new functions, roles and responsibilities required to manage/execute the agreement?
- How are new functions, roles and responsibilities documented and addressed?

Have agency requirements for information security been documented in outsourcing contracts and arrangement with contractors and consultants?

3.4.2 Asset management

Have information security classification controls been put in place or defined in appropriate agreements or contracts with the external party?

- Does the agreement describe the information involved, and its information security classification?
- For all information that is to be handled by the external party, has the external party been given a copy of the controls as per the QGISCF? Can they meet these controls? What is the highest level of information security classified information that the external party is equipped to handle?
- Are all ICT assets that store security classified information assigned appropriate controls in accordance with the QGISCF?
- Will security classified information be returned or securely disposed of at the expiration or termination of the arrangement?
- Does the agreement stipulate that confidentiality/non-disclosure survives the expiration or termination of the arrangement?

Has an owner for the outsourcing arrangement been identified and documented?

- Have ownership responsibilities been documented and given to the arrangement owner?

3.4.3 Human resources management

Does the external party have appropriately qualified and experienced information security employees or representatives?

Does the agreement with the external party require the external party to notify the agency if any of their employees or representatives is charged criminally?

Are all agency staff with external party governance responsibility aware that information security expectations must be included in external party agreements?

- Have external party responsibilities been documented?
- Are the relevant staff aware of external party responsibilities?

Have information security expectations been included in external party arrangement documentation (eg. offers, contracts)?

Do separation agreements with the external party consider information security arrangements (eg. at the end of a contract or breaking of a contract)?

- Have separation expectations and processes been documented (eg. return of equipment, access passes, deactivation of access credentials/accounts)?
- Will the agency be notified in the event of the external party's insolvency? Can the agency terminate the contract?
- Have escrow agreements been established to ensure that rights to data, systems, and codes will be transferred to the agency in the case of the external party's collapse?
- What formal disciplinary processes and or legal actions will be applied if a deliberate violation or breach occurs due to the external party's action or inaction?

3.4.4 Physical and environmental management

Are appropriate building and entry controls in place for areas the external party uses to process or store security classified information?

- Are requirements relating to building and entry control included in agreements?
- Do the external party's building controls meet the requirements of the QGISCF and QGISCS?

Does the external party have adequate security protection for premises where agency assets will be handled?

- Are requirements relating to protection of premises included in agreements?
- Do the external party's premise protection controls meet information security classification requirements?

Are the communications and computer equipment used to host agency assets appropriately secure, via either physical or other control methods?

- Are communication and computer equipment information security requirements included in agreements?

Does the external party have the capability to appropriately dispose of or reuse equipment, storage devices and media that have been used with agency assets?

- Have disposal and reuse expectations been included in agreements?
- Are disposal and reuse processes commensurate with the highest security classification level of the information assets therein?

Can the external party support general control policies such as clear desk and clear screen if they are dealing with security classified information?

3.4.5 Communications and operations management

Will the external party's controls to prevent, detect, remove and report attacks on systems and networks meet agency expectations?

- Can the external party ensure that inbound system information is scanned for malware, viruses and suspect information quarantined?
- How often will the external party review system risks and vulnerabilities?
- How will the agency be notified of new risks or vulnerabilities?
- How will virus prevention be assured?
- How often will the external party patch systems or networks? Does this meet agency expectations?

Does the external party have appropriate controls for protecting its internet gateways (including firewall and intrusion detection/prevention systems)?

Does the external party have appropriate network security controls? Are network transmissions secured in accordance with the NTSAF, including for wireless and mobile network access?

Do system maintenance processes and procedures (operator and audit/fault logs, information backup) meet agency requirements?

- What information is captured in system logs (eg. successful/unsuccessful log-on and log-off attempts; identification and authentication failures; failed attempts to access information)? Is this information available under the terms of the agreement?
- Can the external party track system events and associated information (eg. user ID, date and time, information/system accessed, associated terminal/port/network address)?
- Can the external party monitor system activity for the duration of the user session?
- How long are logs kept for? Does this meet agency and legislative requirements (including archiving)?
- How are the logs protected from unauthorised access?
- How often does the external party review system logs? How are findings (positive/negative) reported to the agency?

Will all legislative and regulatory requirements, including the QGISCF, be met when information is exchanged?

- Will the external party meet QGAF requirements if online transactions and services are enabled?

For outsourcing online transactions and services:

- Has QGAF been used to identify requirements for online transactions and services?
- Is the security of the transactional part of the site equal to or better than the security of the other agency websites?
- Have measures to protect servers and systems from unauthorised entry or use been undertaken, and are they regularly reviewed?
- How does the service manage the transmission of security classified information?
- Does external arrangement involve an ICT asset that stores, transmits or processes credit card information? If so, has the requirement to comply with the Payment Card Industry Data Security standard (PCI-DSS) been communicated to the external party?

Is the external party's service consistent with the agency's policies and procedures for managing and operating system security?

Have all ICT assets provided by the external party been risk assessed by the agency prior to their adoption?

- Are risk assessments routinely performed on new ICT assets?
- Have the external party's products/services been integrated into regular risk assessment processes?
- Does the external party perform its own risk assessments on its offerings and do these meet agency requirements?

Have requirements for the stability and speed of network connections been specified?

3.4.6 Access management

Can agency access requirements that reflect QGAF be provided by the external party?

- What authentication mechanisms are used?
- What encryption mechanisms are used? Do they match agency policy?
- Are credentials for authentication to external systems encrypted?
- Do the registration processes for the service match the risk profile of the service?

Can the external party provide unique individual authentication to agency information systems?

- Are user IDs unique?
- What factor authentication can the service support? Does this match QGAF requirements?
- Do password management practices meet agency expectations (eg. forced change on first use of system; requirements for password length/composition)?
- How is user access revoked? Is this appropriate?
- How are credentials other than passwords managed? Does their use match or exceed password requirements?

Can the external party's service display restricted access and authorised use only warnings? (This is a mandatory clause with the Information Security Compliance Checklist.)

Does the agreement specify whether the external party should notify the agency if there is a request for the agency's information from any other person or organisation (eg. a court)?

Can the external party control access to system files to ensure the integrity of business systems, applications and data?

- Have access control requirements been included in the agreement?
- Can agency access controls be maintained by the external party's service?

At the end of an arrangement, is there provision for external party building access permits to be returned and access cease?

3.4.7 System acquisition, development and management

Have security requirements been included in specifications provided to the external party?

If the outsourcing arrangement involves financial or critical business information and/or ICT assets, have internal or external audit bodies been consulted? (In the case of financial information and/or ICT assets, this is a specific requirement of the *Financial and Performance Management Standard 2009*).

Are the external party's authentication requirements consistent with agency needs and QGAF?

If the arrangement requires the external party to develop custom-built applications, does the external party adhere to secure software development practices?

Does the external party have appropriate change control, acceptance and system testing, planning and migration controls for upgrading or installing software?

- Have change control, testing and migration expectations been documented and communicated to the external party?
- Have change control, testing and migration requirements been included in external party agreements?
- Do software licence terms allow for the operation of software on the external party's systems?
- Is sufficient notice given to the agency in the event of upgrades to the external party's software or infrastructure?
- Are interoperability requirements included in the external party agreement?

3.4.8 Information security incident management

Do the external party's applications include data validity checks, audit trails and activity logging?

- When and how will exceptions identified by data validity checks, audits or activity logging be communicated to the agency?

Do agreements include notifying the agency when and if security breaches, threats or weakness occur or are discovered?

- Does the agreement include how information security incidents and risks will be tracked, treated and communicated back to the agency?
- How are information security incidents investigated? How will the agency and external party work together?
- Do they include employee disciplinary actions and/or legal actions where the incident is a result of a deliberate information security breach by the external party's employee?

Can the external party monitor and review information security events and incidents to the satisfaction of the agency?

- What information security incident policies does the external party have?
- Can the information security incident response efforts isolate systems if required?
- Can the information security incident response efforts remove malicious software from systems if required?
- Can the information security incident response efforts fully restore systems after an attack (including re-instating security controls, restoring data)?

Do the external party's information security incident management procedures and mechanisms match the agency's expectations?

- What information security incident management procedures does the external party have?
- What are the agency's expectations regarding information security incident management?

3.4.9 Business continuity management

Have information and ICT asset disaster recovery processes been established that include the external party's services?

Do agreements with the external party include methods to reduce known business continuity risks?

- What are the processes and business impacts to the agency during loss of critical services or information?
- Are contractual provisions in place to cover business continuity obligations such as indemnities or service credits?
- What backup arrangements are in place? Does their frequency reflect acceptable losses of information?
- What testing and backup arrangements are in place for installing new systems/software? Do these meet agency expectations?
- Is backup material stored at a different secure location to the main site? Is the backup site appropriate?
- Is sufficient information (eg. software, instructions) and the means to support restoring backups also stored away from the main site?
- How frequently is the integrity of the backups tested? Does this meet agency needs?
- Does the agency or service provider have insurance coverage? What are the terms and conditions of the insurance?

Have information and ICT asset disaster recovery and business continuity plans for the outsourced service been maintained and tested to ensure they meet agency expectations?

- Do information and ICT asset disaster recovery and business continuity plans include the arrangement with the external party?
- What information and ICT asset disaster recovery and business continuity plans does the external party have for the service?
- Do the agency and external party information and ICT asset disaster recovery and business continuity plans include arrangements to recover from a range of incidents (minor to major)?
- How frequently are the plans reviewed and tested?

3.4.10 Compliance management

Does the agreement with the external party ensure that the agency can continue to meet all relevant legislative requirements?

- Have legislative obligations been identified, to ensure that the agreement does not violate any requirements?
- For proposed external governance arrangements that involve personal information, will the arrangement meet the requirements of the *Information Privacy Act 2009*?
- Is the external party contractually obliged to implement controls to ensure compliance with the *Information Privacy Act 2009*, *Public Records Act 2002*, *Right to Information Act 2009*?
- How will the agency minimise the risk of litigation from other parties affected by a breach of legislation by the external party?

Is the Information Security Compliance Checklist used to check the external party's compliance?

Does the agreement require the external party to assist the agency within a particular timeframe to conduct audits or information security reviews of the external party and its environment? Have routine audits and checks been included in the agreement.