Queensland Health

ICT Critical and At-Risk Systems: Identification and Reporting

Department of Health Standard

QH-IMP-402-14:2018

1. Statement

Queensland Health has a responsibility to ensure that Information and Communication Technology (ICT) systems deemed critical to the delivery of Queensland Health services are appropriately managed, and that any risks to service delivery arising from ICT systems are appropriately mitigated.

This standard outlines the minimum requirements for identifying, managing and reporting on Critical ICT Systems and At-Risk Systems. In the context of this standard, managing refers to activities associated with managing the risk to Queensland Health services.

2. Scope

This standard applies to all employees, contractors and consultants within the Department of Health divisions and business units.

This standard applies to all ICT systems for which the financial or administrative accountability falls within the Department of Health.

Although Hospital and Health Services (HHSs) are required by the *Enterprise Architecture Health Service Directive* to report the same ICT systems, this standard does not apply. This standard can be used as a base for a HHH specific standard.

3. Requirements

3.1. Identification of Critical ICT Systems

3.1.1. All ICT systems must be identified and assessed for criticality where at least one of the following is considered true:

- Would present a significant impact to Queensland Health operations and therefore the needs of our patients should the system become unusable.
- Represent an investment larger than $500k.
- Is used by multiple divisions or HHSs.

3.1.2. A system may also be classified as a Critical ICT System where a system supports information assets and one or more of the information assets has a Business Impact Level (BIL) of High as per the Queensland Health Enterprise Information Asset Register located in the Queensland Health Information Knowledgebase (QHIK).

3.1.3. A person or group familiar with how the ICT system is utilised must perform an assessment as to whether an ICT System is critical using the Department of Health Risk Analysis Matrix consequence table. The

assessment should account for how impact may vary between business units using the same system in different manners. Potential assessors are service owners, subject matter experts, and program or project boards.

3.1.4. If the inherent risk of the system becoming unusable is “Major or “Extreme” in any category, then it is considered a Critical ICT System.

3.2. Management and Reporting of Critical ICT Systems

Service owner responsibilities

3.2.1. Critical ICT systems that are considered an “application” must be documented in the Queensland Health Enterprise Architecture Application Repository (ServiceNow) by submitting an application profile to Digital Architecture, eHealth Queensland using the Application Profile template available on QHEPS. Critical ICT systems that are considered “technology” must be documented in the eHealth Queensland Configuration Management Database (ServiceNow.)

3.2.2. Critical ICT Systems must be reviewed on at least an annual basis to confirm that all documented attributes are still current and correct.

3.2.3. Critical ICT systems that are considered applications must have an Application Custodian and a Data Custodian assigned and approved by the Information Management Strategic Governance Committee (IMSGC) as described in the *Queensland Health Data and Application Custodianship Standard.*

3.2.4. All critical ICT Systems must apply the requirements defined in the Queensland Health Information Security Policy and any supporting artefacts.

3.2.5. In accordance with the ICT Service Continuity Management Standard, any business unit relying upon a critical ICT system must have should have prescribed and tested system downtime protocols incorporated in their local business continuity plans that ensure critical business functions can continue with minimum impact when the ICT system is unusable.

3.2.6. Critical ICT systems must have will have endorsed and tested ICT service continuity plans in accordance with the ICT Service Continuity Management Standard.

3.2.7. In accordance with the ICT Service Continuity Management Standard, critical ICT systems and any underpinning technology must have documented service management objectives (uptime, maximum allowable outage, recovery point objective, etc) that are reflective of business requirements and must be delivered to those agreed service levels.

Digital Architecture responsibilities

3.2.8. Digital Architecture, eHealth Queensland must maintain and publish a register of critical ICT systems on QHEPS along with a description and the Division/HHS that owns the ICT system.

3.2.9. Digital Architecture, eHealth Queensland must be notified within one month of any critical ICT Systems being commissioned, decommissioned or if any details on the Critical Systems Register need to be amended. must

3.2.10. Digital Architecture, eHealth Queensland must coordinate a review of all critical ICT systems on at least an annual basis as part of preparing the ICT Resources report defined in the *Queensland Government Enterprise Architecture ICT Profiling Standard*.

3.3. Reporting of At-Risk ICT systems

An At-Risk ICT System is an ICT system with an associated High or Very high risk

Service owner responsibilities

3.3.1. Risks associated with ICT Systems must be identified, recorded and managed as per the Department of Health Risk Management Policy, Implementation standard and associated documents.

3.3.2. Notify Digital Architecture, eHealth Queensland within one month when a change to the At-Risk ICT systems register is required. This includes:

- When a new High or Very High risk associated with an ICT system has been identified.
- A change in risk status, or progress in a risk treatment activity has occurred.
- An associated risk has been accepted or mitigated below “High”.

3.3.3. All ICT systems designated as At-Risk ICT systems are to be reviewed by the service owner (or delegate) on at least a biannual basis as per the schedule for the “At-Risk ICT systems report” outlined in the *Queensland Government Enterprise Architecture ICT Profiling Standard*.

3.3.4. Managers of business areas providing technical support services must provide information as required to eHealth Queensland on the use of unsupported technologies determined to be at-risk. Unsupported technologies must be documented in the eHealth Queensland Configuration Management Database (ServiceNow.)

Digital Architecture responsibilities

3.3.5. Digital Architecture, eHealth Queensland will create, maintain, update and provided extracts of a register of all ICT systems with associated High or Very High risks. The “At-Risk ICT systems” register must contain supporting information required to meet reporting obligations as

defined in the *Queensland Government Enterprise Architecture ICT Profiling Standard*.

3.3.6. Digital Architecture, eHealth Queensland is responsible for the biannual coordination and submission of the At-Risk ICT Systems report to the Queensland Government Customer and Digital Group (QGCDG).

4. Legislation

- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Public Records Act 2002*
- *Public Service Act 2008*
- *Right to Information Act 2009*

5. Supporting documents

Queensland Health and Department of Health documents can be located on QHEPS. Queensland Government Enterprise Architecture documents can be located at www.qgcio.qld.gov.au.

Policies and Directives

- Queensland Government Enterprise Architecture ICT Resources Strategic Planning Policy (IS2)
- Queensland Government Enterprise Architecture Hardware Currency Policy
- Queensland Government Enterprise Architecture Software Currency Policy
- Department of Health Enterprise Architecture Policy (QH-POL-402:2014)
- Department of Health ICT Service Continuity Management Policy (QH-POL-457:2018)
- Department of Health Risk Management Policy (QH-POL-070:2015)
- Queensland Health Data and Application Custodianship Policy (QH-POL-469:2019)
- Queensland Health Information Security Policy (QH-POL-468:2019)

Standards

- Queensland Health Business Continuity Management Standard (QH-IMP-070-2:2017)
- Queensland Health Data and Application Custodianship Standard (QH-IMP-469-3:2019)
- Department of Health Risk Management Standard (QH-IMP-070-1:2015)

- Department of Health ICT Service Continuity Management Standard (QH-IMP-457:2018)
- Department of Health Information Security Standard (QH-IMP-066-1:2015)
- Queensland Government Enterprise Architecture ICT Profiling Standard

Other Documents/Repositories

- Department of Health Risk Analysis Matrix
- Queensland Health Application Profile template
- Queensland Health Critical Systems Register
- Queensland Health Data and Application Custodianship Roles and Responsibilities
- Queensland Health Information Knowledgebase (QHIK)
- BCI Good Practice Guidelines 2018 (thebci.org)

6. Definitions

Term	Definition
Agency	Agency refers to Queensland Health in its entirety, inclusive of the Department of Health and Hospital and Health Services.
Application	A software system deployed by the agency which has part of an agency's business process embedded within it. This excludes infrastructure software which is broad-based or commodity in nature. An Application relates to particular business processes (for example, SAP which would typically be provided only for finance, asset or procurement staff); whereas a Technology is involved with either essential infrastructure or general productivity (such as systems management software or standard issue tools like Microsoft Office which would typically be provided to all staff.
Application Custodian	A position designated with overall accountability and responsibility for decision making in relation to the ongoing development, management, compliance, care and maintenance of an application to support business needs (Data and Application Custodianship Roles and Responsibilities).
Application Repository	A register of information about the applications in the agency's Application Portfolio. For each application used, the register could hold details of the functions it performs as well as its scope of use, supporting technologies, level of support, anticipated end-of-life and cost. Also referred to as an Application Register.

Term	Definition
At-Risk ICT System	An at-risk ICT system refers to an ICT system assessed from a whole-of-department perspective as posing a "High" or "Very High" risk to the business. This does not include the inherent business risk of a critical ICT System or any risk that has been accepted with no further treatments to occur.
Business Continuity Plan	A document describing temporary arrangements and workarounds required to continue business processes and operations during disruptive events (e.g. the critical ICT System is fully or partly unusable.)
Business Impact Level	The result of an Information Security CIA assessment that determines the impact to the business resulting from the loss, compromise, and misuse of information for the agency in terms of the impact to confidentiality (C), integrity (I) and availability (A).
Configuration Management Database	A database that contains all relevant details of each configuration item and details of the important relationships between configuration items. In the context of this standard, this refers to technologies and applications.
Critical ICT System	An ICT System that has an availability Business Impact Level (BIL) of High. A High BIL is defined as an inherent consequence of "Major" or "Extreme" in any category according to the Department of Health risk analysis matrix should the system be unusable. Referred to as "significant" in the ICT Profiling Standard.
Information Asset	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions thereby satisfying a recognised agency requirement.
ICT System	An information (ICT) system is an organised collection of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information. For example, this may include a human resource (HR) system used to process payroll, a radio network used to transmit public safety information, etc.
Legacy System	ICT Systems that continue to be used but are past their nominal end-of-life, possibly retained for data retention and retrieval purposes. A legacy system is not automatically unsupported or at-risk; risk should be identified and managed as per any other ICT system.
Service Owner	A person with financial and/or administrative accountability for an ICT System, and therefore is responsible for ensuring the system is delivered within the agreed service levels. For an Application, this would be the Application Custodian.

Term	Definition
System Recovery Plan	An ICT Service Provider technical artefact detailing failover and recovery actions to be taken where there is an impact to critical ICT components. May sometimes be referred to previously as an ICT Disaster Recovery Plan.
Technology	The products required to support the application portfolio of the business, including software, hardware, and network support. This includes infrastructure software which is broad based or commodity in nature. Technologies are involved with either essential infrastructure or general productivity software and hardware (horizontal focus); an application relates to particular business processes (vertical focus).
Unsupported Technology	A technology that has left mainstream support and represents a risk from a whole-of-system perspective. It requires action to be taken such as decommissioning, upgrading or replacing the unsupported technologies with supported versions, products or services.

Version Control

Version	Date	Comments
1.0	27/03/2018	New document. Approved by Architecture Standards Committee.
2.0	18/08/2021	Formal review: The following changes were made to the standard: • Streamlined content and aligned with related artefacts and processes where possible. • Updated statement and scope to better describe what this standard applies to and how this standard relates to HHS reporting. • Content reworded to better support the inclusion of ICT systems other than applications. • Reporting timelines clarified • Expanded definitions table and aligned with related artefacts where applicable • Definition of *Legacy System* added • Updated list of supporting documents Approved by Architecture and Standards Committee