ICT service continuity management

Department of Health Standard
QH-IMP-457:2018

1. Statement

Information is a critical enabler for providing and improving health care as well as enabling the effectiveness of Queensland Health staff. Growing dependence on information and communications technology (ICT) and increasing integration between biomedical, imaging, management information and clinical systems supported by departmental and Hospital and Health Services (HHS) ICT service providers demands higher system resilience, shorter recovery times and improved ICT continuity readiness to minimise impact on patient safety and clinical efficiency in the event of unplanned outages.

The ICT service continuity management (ICT SCM) standard identifies requirements for management of the departmental ICT service continuity management framework. The primary objectives are to:

- Guide continuous improvement of departmental ICT service continuity practice; and
- Improve alignment with HHS and departmental business continuity planning and disaster management arrangements.

2. Scope

This standard identifies the minimum ICT service continuity management requirements for applications, infrastructure and services provided by Department of Health ICT service providers that support critical Queensland Health clinical and non-clinical functions.

This standard applies to:

- all employees, contractors and consultants within departmental divisions and commercialised business units that are responsible for application and/or data custodianship and delivery of critical ICT services; and
- HHS and external ICT service providers who provide critical ICT applications, infrastructure and services to the Department of Health divisions and commercialised business units.

3. Requirements

3.1 Overview

The Departmental Leadership Team (DLT) shall maintain an appropriate departmental governance structure to ensure that ICT service continuity activities meet business requirements.

3.2 Governance

ICT service continuity management shall be aligned with the department's business continuity management framework and disaster management arrangements.

eHealth Queensland shall lead the ongoing management of the department's ICT service continuity framework and drive the strategy for provisioning and ongoing management of ICT service continuity performance for critical systems.

Departmental ICT service provider representation shall be provided through a working group formed under the direction of the Business Resilience Committee to inform development and ongoing management of the ICT service continuity framework.

The following committees will inform departmental ICT service continuity and disaster management requirements:

- Architecture and Standards Committee (ASC) - Governance of the Identification and Reporting of ICT Critical and At-Risk Systems;

- Business Resilience Committee (BRC) - alignment of departmental ICT service continuity with department-wide business continuity and crisis management;
- State Health Emergency Management Committee (SHEMC) – alignment of departmental ICT service continuity with SHECC/ HHS emergency and business continuity management arrangements; and
- The Information Management Strategic Governance Committee (IMSGC) - identification and appointment of application and data custodians.

3.3 ICT service continuity strategy

eHealth Queensland shall maintain the departmental ICT service continuity strategy. The ICT service continuity strategy shall be reviewed annually and endorsed by the BRC to ensure alignment with department-wide business continuity and crisis management objectives.

The departmental ICT Service Continuity Strategy shall articulate ICT service continuity objectives and goals and provide guidance for investment in service continuity capacity and capability to ensure alignment with the department's direction, business expectations and risk appetite. The strategy shall include:

- Departmental ICT service continuity objectives and goals;
- Future state of ICT service continuity preparedness including a roadmap of activities to achieve the desired levels of maturity;
- A development plan to address critical gaps in ICT service continuity capability and capacity across all departmental ICT service provider capabilities;
- Departmental ICT service continuity readiness performance indicators;
- Activities to improve alignment of ICT service continuity with business continuity planning and disaster management arrangements; and
- A list of all departmental ICT service providers.

3.4 ICT system criticality assessment

The departmental standard "ICT Critical and At-Risk Systems: Identification and Reporting" outlines the minimum requirements for identifying, managing and reporting on Critical ICT Systems and At-Risk Systems. ICT application criticality assessments shall be managed and reported in line with this standard.

3.5 ICT system custodianship

All critical clinical and non-clinical ICT applications shall have appointed Application and Data Custodians and Managers. Data and application custodianship includes the appropriate assignment of roles and responsibilities to delegated positions to ensure that Queensland Health data sets and applications are appropriately managed throughout their lifecycle.

The Application Custodian shall appoint an Application Manager who has primary responsibility for the day-to-day management of an application including the planning, development, installation, configuration, maintenance and support of the application. This role shall coordinate ICT service providers responsible for the technologies required to support the application including software technologies, hardware and network support. A single application may depend on multiple ICT service providers spread across departmental divisions and commercial business units as well as external vendors.

3.6 ICT service continuity framework

3.6.1 Business continuity requirements

Business continuity requirements shall be managed by the Application Custodian. The Application Custodian shall engage with agreed HHS and/or departmental application stakeholders to determine the level of dependence of critical business functions, services and processes on the enterprise application. The importance of this review is to check if the level

of business criticality has changed and should be performed on an annual basis for critical systems.

The Application Custodian shall represent the agreed stakeholder requirements to the Application Manager for negotiation and agreement. The Application Custodian shall advise the Application Manager of key business continuity parameters such as hours of usage, application criticality, maximum allowable outage (MAO) and the level of tolerance for data loss due to a disruptive ICT event. This input informs service level requirements and negotiations with the Application Manager and ICT service providers in terms of application recovery priority, recovery time objective (RTO) and recovery point objective (RPO).

The Application Custodian shall maintain a business continuity plan (BCP) describing temporary arrangements and workarounds required to continue business processes and operations during disruptive events causing the application to be fully or partly unavailable.

As a minimum, the business continuity plan shall include:

- BCP owner
- scope and description of application
- critical business functions, services and processes
- business recovery priorities
- system criticality, business and service continuity objectives including MAO, RTO and RPO
- system overview
- criteria for activation and deactivation of the BCP
- response and recovery strategies including manual processes/workarounds to mitigate the effects of disruptions and return to business as usual including acceptance testing
- resource requirements
- contact details for relevant personnel and stakeholders
- communication strategies to keep staff, supplies and stakeholders informed
- internal and external interdependencies including critical information systems
- support model including agreed and supported actions by upstream providers and downstream customers where relevant;
- BCP testing plan.

3.6.2 System recovery plans

ICT service continuity readiness shall be managed by the Application Manager. The Application Manager shall engage with the Application Custodian to inform and establish the ICT service continuity requirements to meet the business continuity requirements.

The Application Manager shall maintain an application specific system recovery plan (SRP) detailing failover and recovery actions to be taken where there is an impact to critical ICT components. The application SRP response and recovery resilience design, timeframes (RTO and RPO) and recovery priorities are informed by application criticality and MAO. As a minimum the application SRP shall include:

- SRP owner
- scope and description of application
- system criticality, business and service continuity objectives including MAO, RTO and RPO
- system overview, resilience architecture and dependencies
- information security requirements
- time critical business functions and recovery priorities
- criteria for activation and deactivation of the SRP

- response and recovery strategies
- resource requirements
- support model
- failover/ failback processes and work instructions including user acceptance testing
- ICT service continuity testing plan.

The Application Manager shall engage the internal and external ICT service providers supporting the application to ensure that component ICT system recovery objectives comply with the relevant application business continuity objectives. Where ICT component RTO and/or RPO parameters do not meet the committed application performance, the Application Manager shall undertake the necessary steps to address the gap with the ICT service providers.

Where the gap cannot be resolved within existing ICT service capabilities, the Application Manager shall perform a risk assessment to determine risk rating and recommend the required treatments for Application Custodian consideration and endorsement. Any consequent risks for which the Application Manager is accountable including ICT service provider gaps shall be recorded in the Application Manager's risk management system and managed in accordance with the endorsed treatments.

ICT service providers shall ensure that component ICT systems for which they are responsible meet the required RTO and RPO criteria. They shall participate in planning, documentation, validation and testing of the performance of their services as agreed with the Application Manager.

3.6.3 ICT infrastructure service continuity plans

eHealth Queensland shall maintain an overarching ICT Service Continuity Plan (ICT SCP) that outlines the overall process for the recovery of critical underpinning departmental ICT infrastructure and systems by asset (e.g. data centre, enterprise network, identity management).

The ICT SCP shall align with strategic QH disaster and departmental crisis response plans to enable a coordinated response to widespread disruptions or threats to critical ICT services.

The ICT SCP shall include as a minimum:

- ICT SCP owner
- scope and related plans
- ICT environment
- critical service dependencies and recovery priorities
- criteria for and activation/deactivation of the ICT SCP
- potential scenarios and recovery strategies
- roles and responsibilities
- key contacts
- communication protocols
- related BCP, SCP, incident management, crisis and disaster response plans
- ICT SCP resource requirements (staff, equipment, facilities)
- management response checklists and incident log templates
- exercise and testing of IT SCP and technology components
- related documents and locations
- post recovery processes
- document control and distribution.

3.6.4 Alignment with HHS ICT service continuity plans

Hospital and Health Service are responsible for ensuring all ICT service providers meet their respective service level requirements relating to ICT service continuity and disaster recovery planning (DRP).

Where departmental ICT service providers deliver critical applications, underpinning infrastructure or services under formal service and support agreements directly to HHS, they shall engage the accountable HHS ICT representative (CIO or similar position) to agree the approach for aligning departmental ICT service continuity response with HHS ICT service continuity plans.

Departmental ICT service providers shall:

- publish service level details for the relevant critical applications, underpinning infrastructure or services, including key contacts and escalation arrangements, support hours of coverage, service availability targets, RTO and RPO targets;
- participate in HHS ICT service continuity planning and testing as required to ensure alignment of critical applications, underpinning infrastructure or services response and restoration activities with HHS business continuity and ICT service continuity arrangements;
- maintain system recovery plans for the restoration of the relevant critical applications and underpinning infrastructure and services in accordance with agreed performance criteria; and
- perform routine testing and validation of system recovery plans and report readiness to HHS in accordance with the service and support agreement.

To assist effective departmental ICT service continuity readiness, it is desirable that HHSs will:

- plan for and manage HHS business continuity response in the event of a major incident that impacts access to critical applications, underpinning infrastructure or services used by the HHS;
- conduct business impact assessments on critical HHS functions to inform ICT service criticality and continuity requirements to develop business continuity objectives including MAO and downtime procedures;
- engage with Application Custodians and ICT service providers to align departmental ICT service continuity plans with HHS business continuity and disaster management procedures;
- maintain an overarching HHS ICT service continuity (disaster recovery) plan incorporating critical HHS and departmental applications and underpinning infrastructure and services to minimise the business impact and provide timely recovery of ICT services in accordance with HHS business requirements; and
- coordinate testing and validation of HHS ICT service continuity (disaster recovery) plans with departmental ICT Service Providers as required.

3.6.5 ICT service continuity testing

Critical applications, infrastructure and services must undergo scheduled ICT service continuity tests to:

- ensure that resilience design and recovery strategies meet business objectives;
- demonstrate the ability of ICT providers to respond and recover services within agreed service levels and recovery objectives;
- ensure familiarity of business and ICT staff with downtime and recovery practices.

The Application Custodian shall determine the risk and appetite for testing ICT service continuity and associated business continuity procedures across all critical applications in collaboration with HHS and/or departmental application stakeholders.

Where critical ICT applications are to be excluded from ICT service continuity testing, the Application Manager will prepare a risk assessment for Application Custodian review and endorsement. The Application Manager will update the ICT Service Continuity Register and escalate the risk in accordance with the departmental risk management process.

Application Managers shall develop and execute ICT service continuity test strategies and plans which identify the frequency, methodology, resourcing needs, accountabilities, objectives and reporting requirements. ICT service continuity testing schedules for critical systems shall be recorded in the ICT Service Continuity Register. ICT service continuity testing will be managed and scheduled in accordance with the ICT Change process and calendar.

eHealth Queensland shall develop and execute the ICT service continuity test schedule for critical underpinning ICT infrastructure and services including data centres, networks, power, data storage and backup systems, telephony, and hosting infrastructure.

3.6.6 ICT service continuity readiness reporting

eHealth Queensland shall maintain a register of departmental applications, infrastructure and services that provides a single view of ICT service continuity readiness across the department. As a minimum the ICT Service Continuity Register shall record:

- Application/infrastructure/service name and description;
- Responsible customer and ICT service provider contacts including Application Custodian, Data Custodian, Application Manager;
- Criticality rating, MAO, support hours of coverage, service availability targets, RTO and RPO targets;
- ICT service continuity plan revision status and schedule, storage location;
- Testing schedule and results;
- BCP revision status and storage location (where applicable).

All Application Managers shall update the ICT Service Continuity Register to reflect the following changes to departmental applications, underpinning infrastructure and systems:

- Changes to the ICT service continuity plan;
- Changes to service levels including key contacts and escalation arrangements, support hours of coverage, service availability targets, RTO and RPO targets and business MAO;
- Outcomes of validation process to confirm alignment of redundancy, resiliency and recovery capability of critical systems with business requirements; and
- ICT service continuity testing results including exceptions to ICT service continuity testing for critical systems.

eHealth Queensland shall report on the coverage and currency of departmental ICT service continuity readiness to the DLT.

3.7 Responsibilities

3.7.1 Director-General

The Director-General establishes and maintains appropriate systems of internal control and risk management in accordance with the *Public Sector Ethics Act 1994, Financial Accountability Act 2009* and *Financial and Performance Management Standard 2009*.

3.7.2 Deputy Director-Generals/Chief Executives responsible for ICT Service Providers shall:

- ensure capability to conduct ICT service continuity is maintained for their accountability area;
- communicate the importance of effective ICT service continuity management and ensure ICT service provider staff are aware of their roles and responsibilities to ensure effective response to disruptive events; and

- confirm responsibility and point(s) of contact for coordinating ICT Service Continuity arrangements within their divisions/commercialised business units.

3.7.3 The Chief Technology Officer, eHealth Queensland shall:

- develop and maintain the departmental ICT service continuity strategy for provisioning and ongoing management of ICT service continuity levels for critical systems;
- develop and maintain the departmental ICT Service Continuity Framework;
- ensure capability to manage the ICT service continuity function on behalf of the department;
- provide advice in relation to ICT service continuity management
- maintain, support and distribute the overarching ICT Service Continuity Plan and associated ICT crisis response facilities; and
- provide regular reporting to the DLT on the performance and overall effectiveness of ICT Service Continuity activities across the department.

3.7.4 Chief Digital Strategy Officer, eHealth Queensland shall:

- develop the criteria for classifying the level of ICT system criticality across Departmental ICT services;
- develop and implement a systematic and consistent approach for reviewing and assigning system criticality; and
- establish, maintain and update a system for recording the criticality level for ICT systems.

3.7.5 Application Custodians shall:

- ensure business continuity objectives are set (e.g. criticality, availability, support requirements, MAO);
- represent and approve business continuity objectives and requirements for applications on behalf of the data custodian(s) and consuming HHS and /or departmental stakeholders;
- maintain a business continuity plan describing temporary arrangements and workarounds required to continue business processes and operations on behalf of the HHS and/or departmental stakeholders; and
- determine the risk and appetite for testing ICT service continuity and associated business continuity procedures across all critical systems in collaboration with HHS and/or departmental application stakeholders.

3.7.6 Application Managers shall:

- provide information pertaining to business function continuity arrangements to function owners including system capability, ICT service continuity planning measures and recovery objectives;
- ensure application service continuity objectives are set (e.g. RTO, RPO, recovery priority);
- ensure ICT defined recovery times, priorities and activities are discussed, understood and agreed with business areas;
- prioritise ICT disaster recovery activities for all critical business functions and associated ICT assets;
- maintain system recovery plans for their applications to address system availability and functionality requirements including disaster recovery arrangements, planned and unplanned system outages and testing;
- engage all ICT Service Providers to ensure that component ICT services comply with the relevant application business continuity objectives;

- establish testing schedules in collaboration with application custodians and ICT Service Providers and exercise continuity arrangements at appropriate intervals with key stakeholders (internal and external).

3.7.7 ICT service providers or positions responsible for technologies required to support an application are required to:

- participate in testing and exercises for continuity arrangements related to ICT component systems for which they are responsible;
- contribute to business continuity arrangements and BCPs developed by Application Managers;
- ensure the redundancy, resilience and recovery performance of all component ICT component systems meet the agreed business criticality and continuity requirements; and
- maintain component ICT documentation and work instructions as part of the system recovery plans.

3.7.8 Contract managers, service managers and project managers when involved in work that affects or supports ICT service continuity readiness for critical business function are required to:

- comply with and participate in strategies for preparedness, prevention, response and recovery including ensuring appropriate monitoring and governance
- proactively communicate risks with relevance to critical business functions to their responsible executive and/or governing board
- consider any necessary provisions to support business continuity and/or ICT disaster recovery in contracts and third-party agreements.

3.7.9 All staff shall:

- Be aware of the Department of Health business continuity arrangements, where appropriate (through training, awareness and testing of plans).
- Comply with and participate in preparedness, prevention, response and recovery strategies to ensure business continuity of critical business functions.

4. Legislation

- *Public Sector Ethics Act 1994*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Information Privacy Act 2009*

5. Supporting documents

- Emergency Preparedness and Continuity Management Policy (QH-POL-28028)
- Risk Management Policy (QH-POL-070)
- Cyber Security Policy (QH-POL-066:2014)
- Information Security Standard (QH-IMP-066-1:2015)
- ICT Service Continuity Management Policy (QH-POL-457)
- WHS Risk Management Implementation Standard (QH-IMP-401-3)
- Business Continuity Management Standard (QH-IMP-070-2:2017)
- Department of Health Crisis and Continuity Plan
- AS/NZS 5050:2010 Business continuity – Managing disruption related risk
- ISO 22301 Societal security – Business continuity management systems

- AS ISO 22301:2017 Societal security – Business continuity management systems - Requirements
- AS ISO 22301:2017 Societal security – Business continuity management systems - Guidance
- ISO 27031:2011 Information technology – Security and techniques – Guidelines for information and communication technology readiness for business continuity
- AS ISO/IEC 27035.2:2017 Information technology – Security techniques – Information security incident management
- AS ISO/IEC 27035:2017 Information technology – Security techniques – Information security incident management Guidelines to plan and prepare for incident response
- Data and Application custodianship – Roles and responsibilities (November 2017)
- ICT Critical and At-Risk Systems: Identification and Reporting Standard (QH-IMP-402-14:2018)

6. Definitions

Term	Definition
Application / ICT System	A software system deployed by the agency which has part of an agency's business process embedded with it.
Application Custodian	A position designated with accountability for the development, management, care and maintenance of an Application.
Application Manager	A position designated with responsibility for the day-to-day management of an application including the planning, development, installation, configuration, maintenance and support of the application.
Business Continuity	The uninterrupted availability of essential business functions.
Business Continuity Management (BCM)	A holistic management process that allows an organisation to identify potential threats and impacts to business operations, if realised, might cause, and which provides a framework for building organisational resilience with the capability to effectively manage disruption related risks against critical business functions.
Business Continuity Plan (BCP)	Documented procedures that provide guidance on how to prepare, prevent, respond and recover from a disruptive event. This includes business activities associated with maintaining availability of people, assets and property vital for the continuity of critical business functions.
Business Impact Analysis (BIA)	The process of analysing business functions and the effect that a disruption may have upon them.
Crisis	A situation that is beyond the capacity of normal management structures, resources and processes to deal with effectively.
Critical business functions / Critical processes	A business function, or part of a function (process), identified as time critical or essential for achievement of the department's objectives.
Critical ICT Service	An ICT system that is relied upon to the extent that an outage would pose significant risk to the business and therefore required a higher level of maintenance to ensure availability and performance. This is reflected in the ICT system having a consequence of failure of High or Very High according to the Department of Health risk analysis matrix. This would usually reference the business operation, delivery of safe clinical services, health service delivery or financial criteria.
Data Custodian	A position designated with responsibility and overall accountability for the Data within the Data Set, Data Collection and/or Application allocated

Term	Definition
	and the capture, development, management, care and maintenance of the Data.
Disruptive event	An event that threatens to disrupt critical business functions.
Disaster	A disaster is defined in Section 13 of the Disaster Management Act 2003 as a serious disruption in a community, caused by the impact of an event that requires a significant coordinated response by the State and other entities to help the community recover from the disruption.
Function owner	The owner (should be a single owner) of a business function, or part of a function (process), identified as time critical or essential for achievement of the department's objectives.
ICT Service Continuity Management (ICTSCM)	The process, policies, and procedures related to prevention and preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organisation after a disaster or outage. ICT Service Continuity focuses on the information or technology systems that support business functions, as opposed to Business Continuity which involves planning for keeping all aspects of a business functioning during disruptive events. ICTSC readiness enables good business continuity practice. **Note:** The term "ICT Disaster Recovery (ICT DR)" is not used for the following reasons: • "Disaster" has a specific and important meaning in the context of Hospital and Health Service and broader state government crisis response. The use of the term disaster in relation to ICT services is not aligned with this meaning and potentially causes confusion; • The ICTSCM framework also encompasses preventative and risk reduction measures and the implication that the function only addresses "recovery" is misleading.
ICT Service Continuity Plan (ICTSCP)	Outlines how an organisation, application, service, or technical component is to manage and recover from an ICT emergency event. The ICTSCP supports the criticality of ICT systems with an aim to reduce extensive interruptions to service by using relevant policies, procedures, processes, instructions to enable effective and efficient recovery measures.
ICT Service Provider	A position designated with responsibility for the technologies required to support the application including software technologies, hardware and network support. Technologies are involved with either essential infrastructure or general productivity software and hardware; an application is related to business processes.
Maximum Allowable Outage (MAO)	Maximum time that an organisation can tolerate the disruption of a critical business function. Also known as Maximum Tolerable Period of Disruption (MTPD).
Recovery point objective (RPO)	The point in time to which systems and data must be recovered after an outage (e.g. end of previous day's processing). RPO(s) are often used as the basis for the development of backup strategies.
Recovery time objective (RTO)	The period of time in which minimum levels of services and /or products and the supporting systems, applications or functions must be recovered after a disruption has occurred.

Term	Definition
System Recovery Plan (SRP)	An ICT Service Provider technical artefact detailing failover and recovery actions to be taken where there is an impact to critical Information and Communications Technology (ICT) Components.

Version Control

Version	Date	Comments
Version 1.0	25 June 2018	New standard.