AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

August 2024

Australian Framework for National Clinical Quality Registries 2024

Attachment 2: Australian CQR security compliance guideline

Published by the Australian Commission on Safety and Quality in Health Care

Level 5, 255 Elizabeth Street, Sydney NSW 2000
Phone: (02) 9126 3600
Email: mail@safetyandquality.gov.au
Website: www.safetyandquality.gov.au

ISBN: 978-1-922880-89-5

The Commission's preference is that you attribute this publication (and any material sourced from it) using the following citation:

Australian Commission on Safety and Quality in Health Care. Australian Framework for National Clinical Quality Registries 2024. Attachment 2 Australian CQR security compliance guideline. Sydney; ACSQHC, 2024.

Disclaimer

The content of this document is published in good faith by the Australian Commission on Safety and Quality in Health Care for information purposes. The document is not intended to provide guidance on particular healthcare choices. You should contact your healthcare provider on particular healthcare choices.

The Commission does not accept any legal liability for any injury, loss or damage incurred by the use of, or reliance on, this document.

Contents

1. Introduction

Purpose

The purpose of the *Australian CQR security compliance guideline* (the Guideline) is to provide guidelines that aid CQR operators in meeting security requirements. It is designed as a resource to guide practices and strategies that align with established security standards for Australian national clinical quality registries (CQRs). The guidelines are formulated to enhance the understanding and implementation of security measures, ensuring effective compliance with necessary security criteria.

This Guideline is intended to support CQR operators (and third-party hosting organisations on behalf of the CQR operator) to evaluate their adherence to security standards and techniques current in February 2024. It is intended to serve as a resource for internal review and drive maturity enhancement of CQRs over time.

About the Guideline

The Guideline builds on the work of the Australian Digital Health Agency's *National eHealth Security and Access Framework – v4.0*. (NESAF)[1] which provides guidance for the Australian healthcare sector and businesses to build and implement secure systems that protect patient data and e-health related assets, while providing the provenance needed to ensure patient safety and privacy.[1]

The Guideline has been developed in consultation with an Advisory Group, including CQR experts and representatives from all states and territories, as well as CQR experts in health data systems.

Section 2: Considerations in securing Clinical Quality Registries defines the key elements of information security and outlines some of the common threats to CQRs.

Section 3: System and infrastructure risk profiles outlines risk profiles for CQRs.

Section 4: Security assessment approach describes a high-level approach to the assessment of CQR security compliance, including the measures to be taken to address any identified security gaps.

Section 5: Security compliance checklists for CQR 'recommended practice' help CQRs assess their security practices across a number of key security domains for minimum 'recommended practice' requirements.

Section 6: Data breaches provides guidance from the Office of the Australian Information Commissioner (OAIC) on how to respond to data breaches.

2. Considerations in securing Clinical Quality Registries

> **This section defines the key elements of information security and sets out the context for information security for CQRs including confidentiality, integrity and availability. It discusses possible threats to a CQR, requirements to be managed, and relevant influences from legislation.**

Definitions of key elements of information security

The information held by CQRs is a core health data asset. Protecting the confidentiality, integrity and availability of this asset is the focus of information security. These three key elements of information security are defined below[2]:

Element	Description
Confidentiality	Refers to ensuring that information is accessible and available only to those authorised to have access.
Integrity	Refers to being able to store, use, transfer and retrieve information with confidence that the information has not been tampered with or altered other than through authorised transactions. Information integrity contributes to confidentiality by protecting access control data, audit trails and other system data that enable the identification of breaches in confidentiality.
Availability	Ensures that information can be accessed by authorised individuals when and where it is required.

Common threats to information

Threats to information security exploit not only vulnerabilities in information systems, but also vulnerabilities in the processes and people that support and use those systems. Threats may come from internal or external sources. They may be accidental or deliberate, malicious, or well intentioned. Threats may have an impact on elements of information security individually or on all the elements at the same time.

The process of identifying, categorising and assessing threats to CQRs is an important part of this Guideline. In essence, it is a threat 'catalogue' that lists the potential ways the information and functions of a CQR may be compromised. The following are the most common cybersecurity threats and associated vulnerabilities that may exist within the CQR environment:

- **Phishing**
  This attack is designed to steal sensitive information, such as usernames and passwords. Phishing attacks come in the form of phishing emails or messages that are designed to look legitimate. They may impersonate reputable websites and personal contacts. Once the user clicks the URL or replies to the message, they are prompted to enter their credentials,

unwittingly sharing this information with the malicious source. The user may use those same credentials to access the CQR system.

- **Virus, malware or spyware attacks**
  Cyber attackers use various means to get malware onto a user's device, such as sending an SMS or email and asking the user to click a link, download a file or launch an application. Once the malware is installed, it can monitor user activities, send confidential data to the attacker, and assist the attacker in penetrating other targets within a healthcare provider's IT network.

- **Password attacks**
  A hacker can gain access to an individual's password information by guessing (in either a random or systematic way), monitoring network traffic aka 'sniffing', or gaining access to the CQR system.

- **SQL injection attacks**
  SQL injection is a web security vulnerability that allows an attacker to interfere with the queries an application makes to its database. In general, it allows an attacker to view data that normally they should not be able to retrieve. This may include data belonging to other users, or any other data the application itself can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

Section 5 of this Guideline (*Security compliance checklists for CQR 'recommended practice'*) provides detailed guidance and explanation on each security control, categorised by security domain details that will facilitate secure operation in an environment characterised by such threats.

For detailed information on cyber security and protective measures, healthcare providers should consult the Australian Digital Health Agency's resources at ADHA Cyber Security.[3]

To help fully identify threats that CQRs may encounter, refer to Section 4.4 of NESAF v4 – Business Blueprint v1.0, available to download as part of the National eHealth Security and Access Framework v4.0.[4]

Legislation and regulation

The privacy of personal health information in Australia is determined by Australian, state and territory government legislation and regulation, as well as private health sector principles and policies.

Australian Government agencies and all private sector health service providers are covered under the *Privacy Act 1988*[5] and are subject to *Section 95* of the Act, which governs health data for medical research. Australian Privacy Principle 11[6] is also concerned with the security of personal information.

Guidelines under Section 95 of the Privacy Act 1988[7], issued by the National Health and Medical Research Council (NHMRC), state that "security standards [are] to be applied to the personal information… in a form that is at least as secure as it was in the sources from which the personal information was obtained."

Organisations in the private health sector must also comply with the *Privacy Act 1988* and are subject to *Section 95A* and the Australian Privacy Principles.

The states and the Northern Territory are subject to varying legislative Acts, regulations, privacy principles and policies.

For up-to-date information on privacy law in the states and the Northern Territory, refer to the 'State and territory privacy legislation' webpage on the Office of the Australian Information Commissioner (OAIC) website.[8]

A summary of legislation and health data custodial arrangements relating to CQRs is also available on the website of the Australian Commission on Safety and Quality in Health Care.[9]

In addition to taking measures to adequately secure information held in CQRs, it is recommended that operators of CQRs seek advice about the privacy issues that may affect the information that they hold.

Approaches to managing risk

The management of security risks can take a range of forms, and it may not be practical for an organisation to address all identified risks. Priority should be given to those threats and associated vulnerabilities that have the highest likelihood of compromising the confidentiality, integrity, and availability of healthcare information, and those that would have the greatest impact on the CQR and its information should the threat be realised.

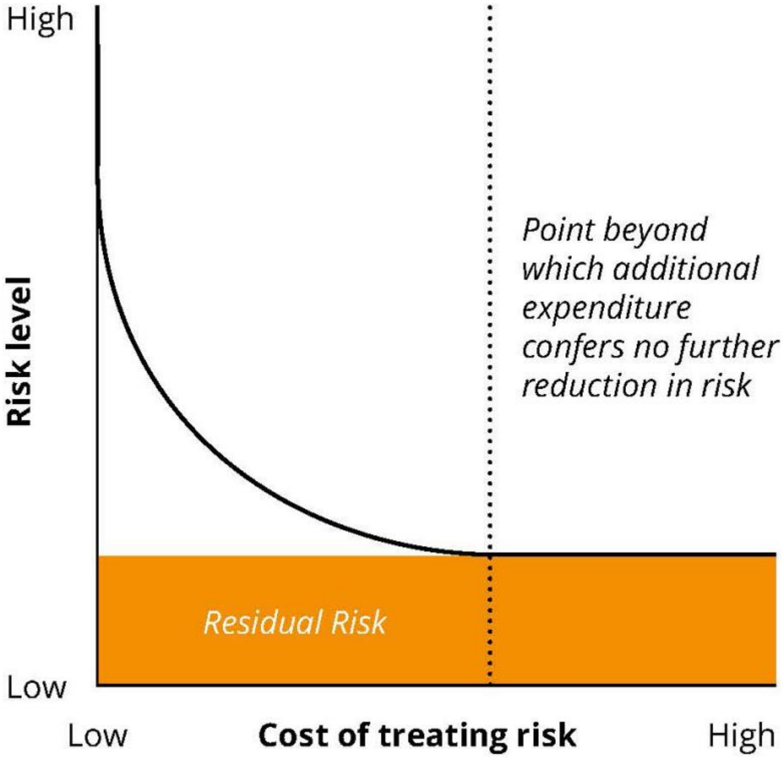
Risk management options[10] can include:

- Risk avoidance – risk is avoided by deciding not to start or continue with the activity that would cause the risk.
- Risk acceptance – accept the potential risk but put in place plans to manage the consequences of the risk should it occur.
- Changing the likelihood – through implementation of controls and preventative actions, for example, audit and compliance programs, contract conditions, policies and procedures, testing.
- Changing the consequences – through implementation of controls such as business continuity management, disaster recovery, back-up, emergency procedures, to reduce the consequences of the risk occurring.
- Risk transfer – sharing the risk with another party or parties, for example, through the use of contracts, insurance, outsourcing arrangements.

When selecting an approach and controls to manage risk, a balance must be struck between mitigating the risk, and the time, effort and resources required to protect against it. Figure 1 illustrates the cost-benefit trade-off that organisations should consider when selecting and implementing appropriate controls.

The costs of implementing controls must be justified by the reduction in the level of risk or assessed against the risks associated with not implementing the control. Almost no information system is risk free and not all implemented controls can reduce the risk level to zero. The risk remaining after implementing new controls is the residual risk.

Figure 1: Cost-benefit trade-off – risk treatment options



This Guideline uses a checklist approach for managing CQR risks (*Section 4: Security assessment approach*). This approach stipulates specific measures to treat, to a particular level, the identified risks.

As highlighted in Figure 1, residual risk cannot be completely removed. However, the application of the recommended controls can provide an appropriate level of risk treatment to the key areas for a CQR.

Table 1 provides an example of the nature and extent of information security risks associated with running the CQR infrastructure.

The ‘elements’ listed in Table 1 are the three key elements of information security as defined in *Section 2*. The ‘security domains’ indicated in **Error! Reference source not found.**are reflected in the security compliance checklists in *Section 5*.

3. System and infrastructure risk profiles

This Guideline may be used to assess the risk profile of Australian CQRs, while acknowledging the many levels of organisational maturity and deployment models of CQRs. This section will provide details of the types of risks that may be encountered.

Risk profile for running CQR infrastructure

Table 1 provides an example of the nature and extent of information security risks associated with running the CQR infrastructure.

The 'elements' listed in Table 1 are the three key elements of information security as defined in *Section 2*. The 'security domains' indicated in **Error! Reference source not found.** are reflected in the security compliance checklists in *Section 5*.

Table 1: CQR infrastructure risk

No.	Element	Risk	Likelihood	Impact	Risk rating	Security domain
1	Confidentiality	Loss of confidentiality of multiple records due to staff accidentally disclosing information leads to loss of privacy, embarrassment for the CQR and/or financial penalties.	Unlikely	Major	High	Information security policy; HR security
2	Confidentiality	Accidental breach of legislation (by central administration staff) due to central administration staff managing multiple jurisdictions.	Unlikely	Major	High	Access control; Compliance
3	Confidentiality	Loss of confidentiality of information due to staff or contractors purposely disclosing health information (likelihood is increased in central administration).	Unlikely	Major	High	Information security policy; HR security; Organising information security
4	Confidentiality	Changing to new central administration environment may put information at additional risk due to the difficulties in identifying users.	Possible	Moderate	High	Information security policy; Organising information security

No.	Element	Risk	Likelihood	Impact	Risk rating	Security domain
5	Confidentiality	Loss of confidentiality of information while in transit externally (e.g. from data suppliers).	Possible	Moderate	High	Communications and operations management
6	Confidentiality	Portable devices may store confidential information and could be left in public areas or stolen, leading to breach of confidentiality of multiple records.	Unlikely	Major	High	HR security; Communications and operations management
7	Confidentiality	Breach of legislation due to information being used in a way that is not the purpose for which it was collected (e.g. violation of consent).	Unlikely	Moderate	Medium	Compliance; HR security
8	Confidentiality	Theft of (non-portable) information systems containing multiple records of confidential information.	Unlikely	Major	High	Physical and environmental security
9	Confidentiality	Authorised user inadvertently gives information to unauthorised user.	Possible	Moderate	High	HR security
10	Integrity	Data integrity errors in bulk upload or external file transfers.	Unlikely	Major	High	Information systems acquisition, development and maintenance
11	Integrity	Individual record data quality errors through data entry (transposition).	Possible	Minor	Medium	Information systems acquisition, development and maintenance; HR security
12	Integrity	Malicious staff purposely change multiple records.	Unlikely	Major	High	HR security; Communications and operations management; Access control
13	Integrity	Untrained/unskilled staff accidentally change multiple records.	Unlikely	Moderate	Medium	HR security; Access control

No.	Element	Risk	Likelihood	Impact	Risk rating	Security domain
14	Integrity	Database errors due to environmental factors (e.g. loss of power causes system failure which corrupts database).	Unlikely	Moderate	Medium	Information security aspects of business continuity management; Physical and environmental security
15	Integrity	Message received or sent from unauthorised party.	Unlikely	Moderate	Medium	Access control; Communications and operations management
16	Integrity/Availability	Malware/viruses resulting in loss of integrity/availability of multiple records.	Unlikely	Major	High	Communications and operations management; Information security incident management
17	Integrity	Incompatibility between data and metadata/reference tables – they get out of sync over time – and backwards incompatibility causes loss of integrity of many records.	Unlikely	Moderate	Medium	Information systems acquisition, development and maintenance
18	Integrity	Application errors – e.g. dates stored in US format lead to multiple records becoming corrupt.	Unlikely	Moderate	Medium	Information systems acquisition, development and maintenance
19	Availability	Power loss or other environmental issues lead to CQR becoming unavailable for more than a day.	Unlikely	Moderate	Medium	Business Continuity Management; Physical and environmental security
20	Availability	Denial of service attacks through external services (malicious or accidental).	Unlikely	Moderate	Medium	Communications and operations management; Information security incident management
21	Availability	Infrastructure capacity issues – e.g. low server RAM/HDD, etc.	Unlikely	Moderate	Medium	Communications and Operations Management

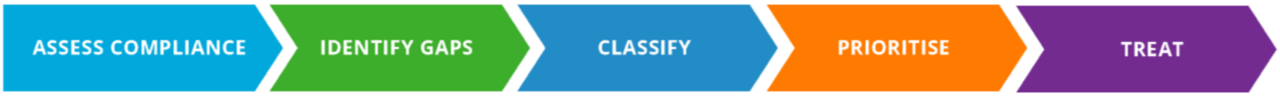
No.	Element	Risk	Likelihood	Impact	Risk rating	Security domain
22	Availability	Unauthorised software/hardware changes cause outages beyond acceptable period.	Unlikely	Moderate	Medium	Communications and operations management
23	Availability	User accidentally causes environmental issues – e.g. turns off server, spills liquid, etc.	Unlikely	Moderate	Medium	HR security; Physical and environmental security
24	Availability	Vendor fails to meet service level agreement (SLA) for availability.	Unlikely	Moderate	Medium	Organising information security
25	Availability	Loss of small number of records due to reluctance by contributors to re-enter or re-provide data following loss of availability or other factors.	Unlikely	Moderate	Medium	HR security
26	Confidentiality/ Integrity/ Availability	Loss of confidential information due to cyber-attacks such as phishing, SQL injection attacks, password attacks, virus attacks, malware attacks and spyware attacks.	Possible	Major	High	Access control; Information security incident management

4. Security assessment approach

> **This section describes a high-level approach to assessing CQR security compliance, including measures to be taken to address any identified security gaps. To assess security compliance, assessors should first identify the security compliance checklists (provided in *Section 5*) applicable to the CQR organisation being assessed.**

Methodology

A checklist approach is used to assess the security compliance of CQRs. Each area of the checklist is tested against the local CQR environment to assess compliance. Gaps in compliance are identified, classified in importance, prioritised for action, and treated. The chart below shows these steps in the methodology.



Assessing compliance

Compliance

ISO 27001 compliance implies that a CQR has conducted a self-assessment against the ISO standards and deems itself in alignment with these standards. This involves internally evaluating their processes and security measures to make sure they meet the criteria set out in the ISO 27001 standards.

Certification

ISO 27001 certification indicates that a CQR's adherence to these standards has been externally validated by a certified auditing or certifying organisation. This certification process involves a thorough, independent examination of the CQR's security infrastructure and processes, confirming their conformity to the rigorous standards of ISO 27001.

Assessment checklists

This Guideline identifies two separate checklists (provided at *Section 5*):

1. CQR Business Operations Checklist

The CQR Business Operations Checklist is used to identify the current status of security controls concerning the business operations of a CQR. This includes, but is not limited to, employment screening controls, authorisation of users and business continuity practices. Regardless of the underlying data hosting infrastructure of each CQR, these business operation security controls should be similar across all CQRs and the same level of security is required.

2. CQR System Hosting Checklist

The CQR System Hosting Checklist is used to identify the current status of security controls concerning a CQR's hosting infrastructure. These security controls apply for both on-premise and cloud-hosting environments.

The CQR System Hosting Checklist is used where ISO 27001 certification or Australian Signals Directorate (ASD)[11] guidelines are not applied.

Formally accredited by authorised certifiers, ISO 27001 is the international standard for information security management and, where satisfied, provides a high level of confidence in an organisation's security control measures. Similarly, ASD evaluates ICT security products used by Australian governments to protect official information. These evaluations provide confidence that ICT security products perform as claimed by the vendor.

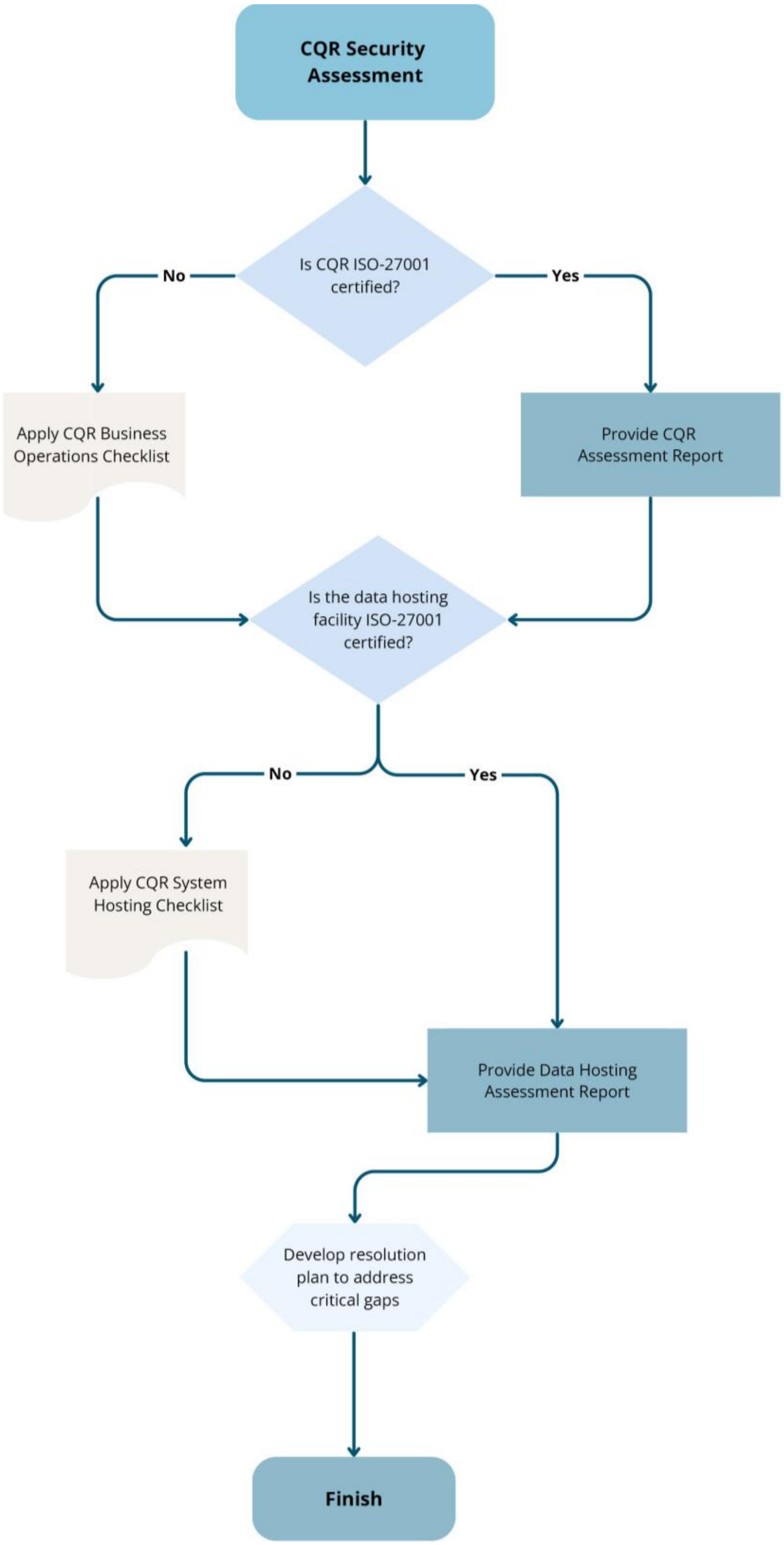
It is expected that few CQR organisations within Australia will have ISO 27001 or ASD evaluation, in which case the checklist should be used. The CQR System Hosting Checklist involves best practice controls for securing CQR information within the system hosting environment and is recommended to review annually.

Determining the appropriate checklists

The flowchart (**Error! Reference source not found.**) and matrix (Table) should be used to determine the appropriate checklists for assessing an organisation's security control measures.

Please see following pages for Figure 2 and Table 2.

Figure 2: Flowchart for determining the appropriate assessment checklists


CQR Security Assessment
Is CQR ISO-27001 certified?
No
Yes
Apply CQR Business Operations Checklist
Provide CQR Assessment Report
Is the data hosting facility ISO-27001 certified?
No
Yes
Apply CQR System Hosting Checklist
Provide Data Hosting Assessment Report
Develop resolution plan to address critical gaps
Finish

CQR: Clinical Quality Registry

ISO 27001: Information Security Management System standard

Table 2: Matrix for determining the appropriate assessment checklists

The matrix complements the **Error! Reference source not found.**.

The organisation being assessed is a…	**The certification checklist(s) that the organisation needs to complete is (are)…**		
	CQR Business Operations Checklist	CQR System Hosting Checklist	Other
Existing CQR with an internal data hosting platform (all data and applications are hosted and maintained by CQR staff).	✓	✓	
New CQR infrastructure with internal data hosting platform that hosts information for multiple CQRs.	✓ (per CQR)	✓	
New CQR infrastructure that hosts information for multiple CQRs using an external data hosting provider (e.g. Cloud provider) that DOES have ISO 27001 certification.	✓ (per CQR)		✓ Proof of certification to be sighted by CQR
New CQR infrastructure that hosts information for multiple CQRs using an external data hosting provider (e.g. Cloud provider) that DOES NOT have ISO 27001 certification.	✓ (per CQR)	✓ CQR is responsible for ensuring the external provider complies.	
New and existing CQR Infrastructure using an external data hosting provider (e.g. Cloud provider) that DOES NOT have ISO 27001 certification.	✓	✓ CQR is responsible for ensuring the external provider complies.	
Existing or new CQR infrastructure that uses an external data hosting provider that DOES have ISO 27001 certification.	✓		✓ Proof of certification
CQR infrastructure that hosts information for multiple CQRs that has previously attained certification and another CQR wishes to join the existing central jurisdictional infrastructure services).	✓ (per CQR)	Not required – already accredited once.	

Identify gaps

Following the compliance assessment, any security control gaps should be identified and recorded. Security control gaps are any areas that are noted as not meeting recommended practice.

Classifying and prioritising gaps

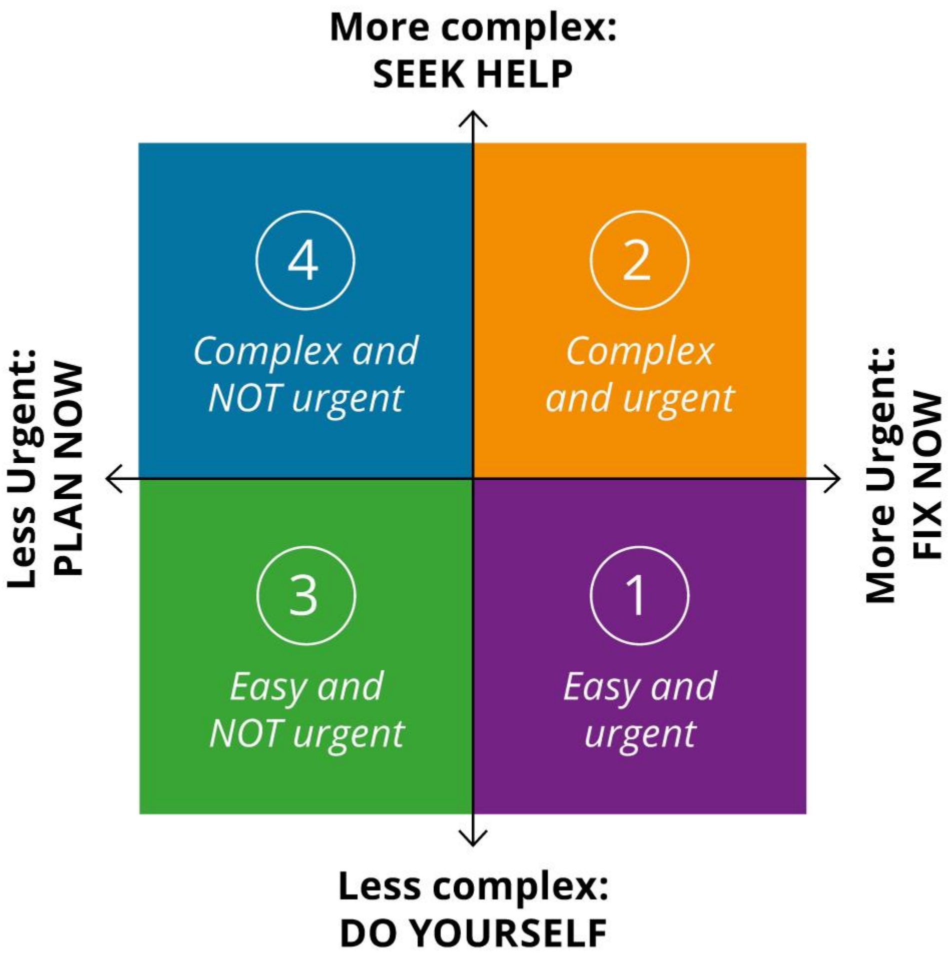
Once a security control gap has been identified, the next stage is to classify the gap's importance in terms of urgency and complexity. Classifying security gaps in this way helps build a logical priority list for gap remediation work.

The level of urgency is based on the potential impact on a CQR if that security gap or weakness were exploited. In other words, *the level of urgency should be measured by the level of risk that is being mitigated by the control* (as referenced in the checklist provided in Section 5).

The level of complexity is measured by the expected effort and expertise required to implement a control.

The numbered quadrants in Figure 3 suggest a simple approach to prioritising any remediation work that may be needed. Any work that is urgent but simple should be top priority and may be possible to undertake in-house.

Figure 3: Classifying and prioritising gaps



Treat

Treatment of identified security gaps involves implementing the required controls identified in the appropriate checklist. CQR organisations and external data hosting service providers should plan for the remediation of any gap areas on a priority basis as determined through the classification process described previously.

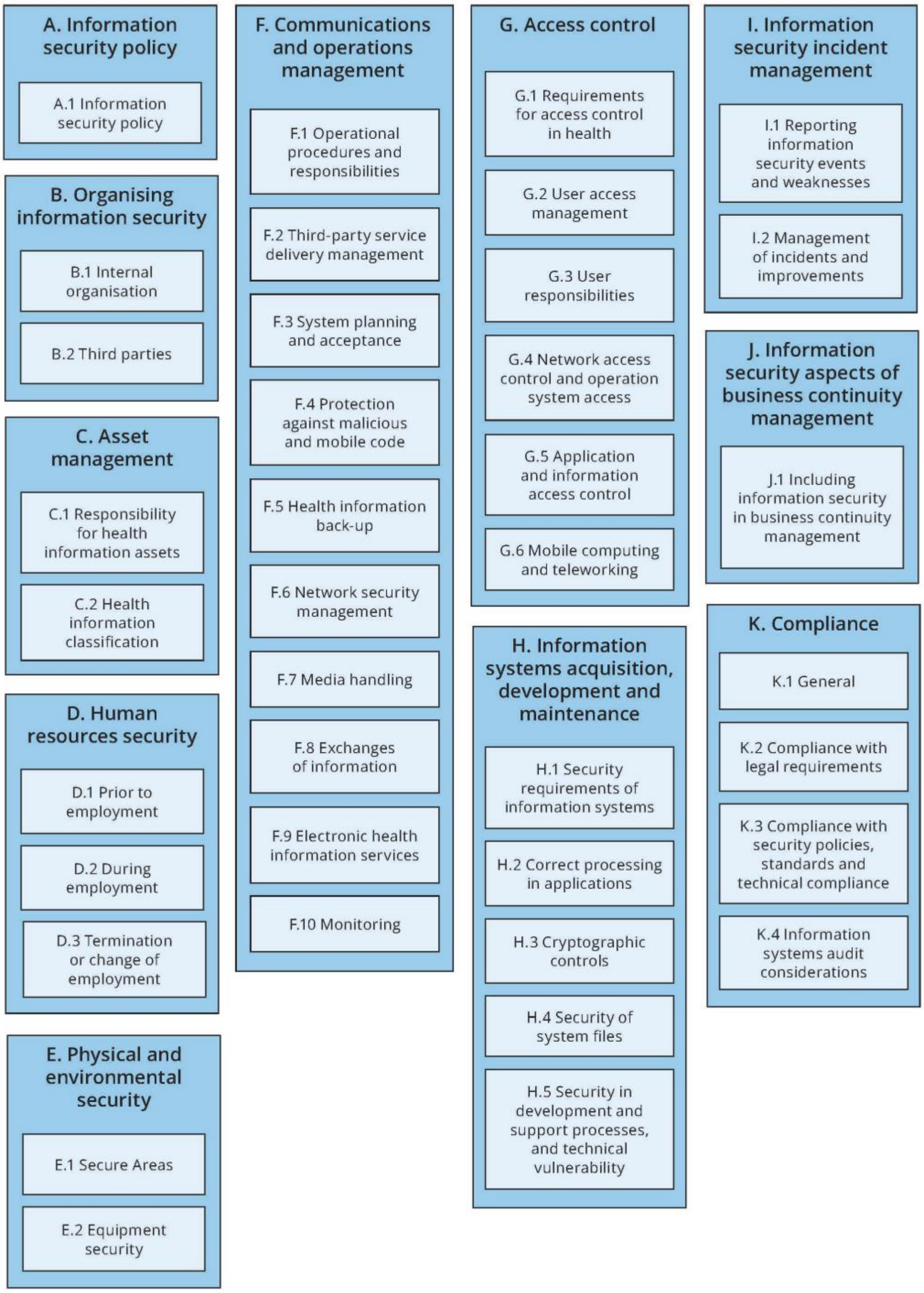
Other guidelines such as NESAF have a broader body of detailed information that can be used to inform the treatment of gap areas.

Section 6: Data breaches provides guidance from the OAIC on how to respond to data breaches.

5. Security compliance checklists for CQR ‘recommended practice’

This section provides detailed security compliance checklists to be used by CQR organisations to assess their business operations and CQR system hosting. The security compliance checklists contain the key domains for minimum ‘recommended practice’ for information security. The domains of information security are represented in Figure 4.

Figure 4: Domains of information security



A. Information security policy
- A.1 Information security policy

B. Organising information security
- B.1 Internal organisation
- B.2 Third parties

C. Asset management
- C.1 Responsibility for health information assets
- C.2 Health information classification

D. Human resources security
- D.1 Prior to employment
- D.2 During employment
- D.3 Termination or change of employment

E. Physical and environmental security
- E.1 Secure Areas
- E.2 Equipment security

F. Communications and operations management
- F.1 Operational procedures and responsibilities
- F.2 Third-party service delivery management
- F.3 System planning and acceptance
- F.4 Protection against malicious and mobile code
- F.5 Health information back-up
- F.6 Network security management
- F.7 Media handling
- F.8 Exchanges of information
- F.9 Electronic health information services
- F.10 Monitoring

G. Access control
- G.1 Requirements for access control in health
- G.2 User access management
- G.3 User responsibilities
- G.4 Network access control and operation system access
- G.5 Application and information access control
- G.6 Mobile computing and teleworking

H. Information systems acquisition, development and maintenance
- H.1 Security requirements of information systems
- H.2 Correct processing in applications
- H.3 Cryptographic controls
- H.4 Security of system files
- H.5 Security in development and support processes, and technical vulnerability

I. Information security incident management
- I.1 Reporting information security events and weaknesses
- I.2 Management of incidents and improvements

J. Information security aspects of business continuity management
- J.1 Including information security in business continuity management

K. Compliance
- K.1 General
- K.2 Compliance with legal requirements
- K.3 Compliance with security policies, standards and technical compliance
- K.4 Information systems audit considerations

Compliance checklists – CQR Business Operations and System Hosting

These checklists identify the security control and outline the objective of the security control, the recommended practice and detailed guidance. The detailed guidance combines information from relevant security guidelines and specific details to suit CQR environments. The guidance borrows from the National eHealth Security and Access Framework and ISO/IEC 27002 Standard.[12]

The checklists should be used in line with the methodology, flowchart (Figure 2) and matrix (Table 2) provided in *Section 4*.

To be completed by each CQR organisation/system hosting organisation.

The checklists can be accessed in Excel on the Commission's website.[13]

6. Data breaches

Response to data breaches

The response to a data breach of the information being protected within the CQR should follow the steps outlined by the Office of the Australian Information Commissioner (OAIC). The OAIC is the regulatory authority in Australia responsible for overseeing privacy and information management practices. The response should be tailored to the specific incident and, in general, follow four steps:

1. *Contain* the breach
2. *Assess* the situation
3. *Notify* relevant parties
4. *Review* the incident to prevent future breaches.

Given the sensitive nature of data in CQRs, a breach could have significant implications. Adhering to these steps ensures effective management of any breach, minimises harm and maintains trust in the CQR's data handling processes. This approach also aligns with best practices in data security and privacy management, which are vital for a project handling sensitive health information.

For more detailed information please visit the ‘Responding to data breaches’ webpage on the OAIC website.[14]

Glossary

Term	Definition
Access control	A means of controlling access by users to computer systems or to data on a computer system.
The Commission	Australian Commission on Safety and Quality in Health Care.
Asset	Anything that has value to an organisation.[15]
Authentication	Means that one can verify whether the sender is who they say they are.[16]
Availability	Refers to the property of being accessing and usable on demand by an authorised entity.[17,18]
Centrally hosted	Centrally hosted jurisdictional (Australian, state and territory infrastructure model) national infrastructure
Confidentiality	The requirement that information is not made available or disclosed to unauthorised individuals, entities or processes.
CQR	Clinical Quality Registry.
Data hosting infrastructure	In this document, data hosting infrastructure refers to capacity and/or capability of ICT infrastructure such as data hosting services, hardware and software applications.
Denial of service	A cyber-attack that prevents authorised access to and availability of organisational information/services/resources.
External data hosting infrastructure provider	In the context of this document, an external data hosting infrastructure provider refers to organisations that provide technology infrastructure such as hosting services, hardware or applications to standalone CQRs through a third-party service provider arrangement.
Encryption	Data are electronically 'scrambled' so it cannot be read unless the information is decrypted.[19]
Firewall	Device(s) designed to prevent unauthorised transmission to or from a private network based on a set of rules. Used to protect networks from unauthorised access while permitting legitimate communications to pass through.
Health information system	Repository of information regarding the health of a patient in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users.[20]
Health care	Any type of service provided by professionals or paraprofessionals with an impact on health status[21]

Healthcare organisation	Generic term used to describe many types of organisations that provide healthcare services.[21]
Information security	Preservation of confidentiality, integrity and availability of information.
Integrity	The property of data that has not been altered or destroyed. Also the property of a system that can perform its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system.[21]
NESAF	National eHealth Security and Access Framework.
Malicious code	Programs such as viruses and worms designed to exploit weaknesses in computer software and replicate and/or attach themselves to other software programs on a computer or a network.
Personal health information	Information about an identifiable person which relates to the physical or mental health of the individual or to provision of health services to the individual.[20]
Register	The file of data concerning all cases of a particular disease or other health-relevant condition in a defined population such that the cases can be related to a population base. With this information, incidence rates can be calculated. If the cases are followed up, information on remission, exacerbation, prevalence and survival can also be obtained.
Registration	The system of ongoing registration for individuals entered into a register. For the purpose of this document, the functions performed by a CQR are defined in the *Australian Framework for National Clinical Quality Registries 2024*: *Overview of CQR Functions*. These include data custodianship, provider enrolment, data collection, data quality management and data analysis and outcome reporting.
Risk	The probability that a given threat will exploit a given vulnerability.[20]
Risk assessment	The process of identifying risks to a business and determining the probability of occurrence, the resulting impact, and identifying actions that would treat the risk.
Threat	An action or event that may result in a detrimental outcome to a system or information asset.[21]
Vulnerability	A weakness that can be exploited that may cause damage to a system or information assets.[21]

References

1. Australian Government Australian Digital Health Agency. National eHealth Security and Access Framework v4.0. Canberra: ADHA. https://developer.digitalhealth.gov.au/resources/national-ehealth-security-and-access-framework-v4-0 (accessed Feb 2024)
2. Australian Government Australian Digital Health Agency. National eHealth Security and Access Framework v4.0. Canberra: ADHA. https://developer.digitalhealth.gov.au/resources/national-ehealth-security-and-access-framework-v4-0 (accessed Feb 2024)
3. Australian Government Australian Digital Health Agency. For healthcare providers: Cyber security. Canberra: ADHA. https://www.digitalhealth.gov.au/healthcare-providers/cyber-security (accessed Feb 2024)
4. Australian Government Australian Digital Health Agency. National eHealth Security and Access Framework v4.0. Canberra: ADHA. https://developer.digitalhealth.gov.au/resources/national-ehealth-security-and-access-framework-v4-0 (accessed Feb 2024)
5. Australian Government Office of the Australian Information Commissioner. The Privacy Act. Canberra: OAIC. https://www.oaic.gov.au/privacy/the-privacy-act (accessed Feb 2024)
6. Australian Government Office of the Australian Information Commissioner. Read the Australian Privacy Principles. Canberra: OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles (accessed Feb 2024)
7. National Health and Medical Research Council. Guidelines under Section 95 of the Privacy Act 1988. Canberra: NHMRC; 2015. https://www.nhmrc.gov.au/about-us/publications/guidelines-under-section-95-privacy-act-1988 (accessed Feb 2024)
8. Australian Government Office of the Australian Information Commissioner. State and territory privacy legislation. Canberra: OAIC. https://www.oaic.gov.au/privacy/privacy-legislation/state-and-territory-privacy-legislation/state-and-territory-privacy-legislation (accessed Feb 2024)
9. MinterEllison for Australian Commission on Safety and Quality in Health Care. Legislation and regulation relating to clinical quality registries. Sydney: ACSQHC; May 2020. https://www.safetyandquality.gov.au/our-work/health-and-human-research/national-arrangements-clinical-quality-registries#legislation-and-regulation-relating-to-clinical-quality-registries (accessed Feb 2024)
10. Australian Government Australian Digital Health Agency. National eHealth Security and Access Framework v4.0. Canberra: ADHA. https://developer.digitalhealth.gov.au/resources/national-ehealth-security-and-access-framework-v4-0 (accessed Feb 2024)
11. ASD is now cyber.gov.au and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) leads the Australian Government’s efforts to improve cyber security.
12. Standards Australia. AS ISO 27799:2023 Health informatics — Information security management in health using ISO/IEC 27002. Sydney: Standards Australia; 2023. https://store.standards.org.au/product/as-iso-27799-2023 (accessed Feb 2024)
13. Compliance checklists – CQR Business Operations and System Hosting
14. Australian Government Office of the Australian Information Commissioner. Part 3: Responding to data breaches – four key steps. Canberra: OAIC. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps (accessed Feb 2024)
15. Standards Australia. AS ISO 27799:2023 Health informatics — Information security management in health using ISO/IEC 27002. Sydney: Standards Australia; 2023. https://store.standards.org.au/product/as-iso-27799-2023 (accessed Feb 2024)

16. Royal Australian College of General Practitioners. Information security in general health practice. Melbourne: RACGP; 2022. https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice (accessed Feb 2024)
17. Australian Government Australian Digital Health Agency. National eHealth Security and Access Framework v4.0. Canberra: ADHA. https://developer.digitalhealth.gov.au/resources/national-ehealth-security-and-access-framework-v4-0 (accessed Feb 2024)
18. Standards Australia. AS ISO 27799:2023 Health informatics — Information security management in health using ISO/IEC 27002. Sydney: Standards Australia; 2023. https://store.standards.org.au/product/as-iso-27799-2023 (accessed Feb 2024)
19. Royal Australian College of General Practitioners. Information security in general health practice. Melbourne: RACGP; 2022. https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice (accessed Feb 2024)
20. Standards Australia. AS ISO 27799:2023 Health informatics — Information security management in health using ISO/IEC 27002. Sydney: Standards Australia; 2023. https://store.standards.org.au/product/as-iso-27799-2023 (accessed Feb 2024)
21. *Ibid.*

AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

Level 5, 255 Elizabeth Street, Sydney NSW 2000
GPO Box 5480, Sydney NSW 2001

Phone: (02) 9126 3600

Email: mail@safetyandquality.gov.au
Website: www.safetyandquality.gov.au