

FINANCIAL AUDIT REPORT 19 November 2026

Information systems 2026

Report 4: 2026–27

Queensland Audit Office

Better public services

As the independent auditor of the Queensland public sector, including local governments, the Queensland Audit Office:

- provides professional audit services, which include our audit opinions on the accuracy and reliability of entities' financial statements
- provides insights on entities' financial performance, risk, and internal controls; and on the efficiency, effectiveness, and economy of public service delivery
- produces reports to parliament on the results of our audit work, insights, and advice, and provides recommendations for improvement
- connects our reports to regions and communities with graphics, tables, and other visualisations
- conducts investigations into claims of financial waste and mismanagement raised by elected members, state and local government employees, and the public
- shares wider learnings and best practice from our work with entities, our professional networks, industry, and peers.

We conduct all our audits and reports to parliament under the *Auditor-General Act 2009*.

Learn more about our publications on our website at www.qao.qld.gov.au/reports-resources/fact-sheets.

The Honourable P Weir MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

19 November 2026

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*.

Rachel Vagg
Auditor-General

© The State of Queensland (Queensland Audit Office) 2026.

The Queensland Government supports and encourages the dissemination of its information. The copyright in this publication is licensed under a Creative Commons Attribution-Non-Commercial-No Derivatives (CC BY-NC-ND) 4.0 International licence.

To view this licence visit https://creativecommons.org/licenses/by-nc-nd/4.0/

Under this licence you are free, without having to seek permission from QAO, to use this publication in accordance with the licence terms. For permissions beyond the scope of this licence contact copyright@qao.qld.gov.au

Content from this work should be attributed as: The State of Queensland (Queensland Audit Office) *Information systems 2026* (Report 4: 2026–27), available under CC BY-NC-ND 4.0 International.

Cover image is a stock image purchased by QAO.

ISSN 1834-1128

Contents

Report on a page 1

1. Information technology controls at state entities 2

2. Maturity assessment of general IT controls 12

3. Financial system implementations 21

4. Legacy systems 26

Appendices 32

A. Entity responses 33
B. How we prepared this report 36
C. Status of recommendations made in prior reports 38
D. Focus areas for remediating IT control deficiencies 39
E. Using third-party assurance reports 40
F. IT controls maturity assessment methodology 42

Acknowledgement

The Queensland Audit Office acknowledges the Traditional Owners and Cultural Custodians of the lands, waters, and seas across Queensland. We pay our respects to Elders past and present.

Reference to comments

In accordance with s. 64 of the *Auditor-General Act 2009*, we provided a copy of this report to relevant entities. In reaching our conclusions, we considered their views and represented them to the extent we deemed relevant and warranted. Any formal responses from the entities are at Appendix A.

Report on a page

This report summarises issues identified in our information systems audits for state entities in Queensland's public sector. We discuss information technology (IT) control weaknesses, control maturity, major financial system implementations, and challenges associated with ageing legacy systems.

Queensland public sector entities include the 21 core government departments (referred to as 'departments' in this report), statutory bodies, and government owned corporations.

IT control weaknesses are increasing security risks

While entities generally have effective IT controls for finance systems, the IT control environment is under pressure due to recurring weaknesses. Addressing these weaknesses can be complex and time-consuming and is affected by dependencies on major projects and third parties, legacy technology constraints, and the governance and behavioural changes required to embed new controls. As a result, entities often need to rely on interim measures or accept residual risks while working towards a sustainable long-term solution.

Challenges for timely remediation			
DEPENDENCIES Major projects Vendors / third parties	**SOLUTION CERTAINTY** Feasibility Legacy constraints	**CHANGE BURDEN** Governance Policy / behaviour	**RESIDUAL RISK** Manual controls Exceptions / acceptance
Impact: remediation pathways are harder to define, delivery is less controllable, and sustainable resolution may take longer			
Overall assessment: increased complexity of remediation activities where multiple drivers overlap			

Access controls continue to require improvement

Entities have improved some identity and access controls. However, they are not embedding strong processes to ensure that changes are not being treated as a one-off remediation activity.

Large system implementation for departments is underway

Many entities are undergoing major projects for digital transformation. Queensland Shared Services is leading a large and complex implementation of a finance system that many departments will use. It will result in transformed processes for Queensland Shared Services and the user departments. We have highlighted common areas of risk relating to system implementations, including decision making during design and testing.

Legacy system funding of $288 million allocated

The Queensland Government has allocated $414 million of its $1 billion digital fund (40 per cent), with $288 million allocated to projects aimed at addressing legacy systems. Gaps remain in data collection and reporting on IT projects, and departments do not consistently manage legacy risks.

1. Information technology controls at state entities

This chapter presents an overview of our 2026 audits of information technology (IT) controls at state entities. We report on the effectiveness of key IT controls relevant to financial reporting, including entities' progress in addressing control deficiencies identified in prior years.

Effective IT controls are critical because government entities rely on IT systems to process, store, and report financial information. These systems support the recording of financial transactions and account balances that underpin entities' financial statements. As entities increasingly adopt third-party and cloud-based technologies, robust governance and security controls remain essential to protect information assets and maintain the integrity of financial reporting.

While entities generally have effective IT controls supporting financial reporting, many continue to have unresolved and recurring control deficiencies. Although remediation is progressing, addressing IT weaknesses can be complex due to project dependencies, third-party providers, legacy systems, and the governance and behavioural changes needed to embed new controls. As a result, entities may rely on interim controls or accept residual risks while implementing longer-term solutions.

Chapter snapshot

IT controls for finance systems are generally effective

Finance systems are reliable for financial reporting purposes

Entities are addressing severe risks but not reducing total deficiencies identified

The backlog of issues has increased by 86% since 2024 and 49% of findings were raised in prior years

Greater attention is needed to strengthen defences in areas where we raise most issues

55% of deficiencies relate to access management and 29% to application controls

Maintaining effective IT controls needs to remain a priority

Government services need secure and reliable technology. While entities generally have effective IT controls for finance systems, IT threats change and become more sophisticated. Effective controls protect their systems, data, and critical services from threats such as cyber-attacks and data loss.

Strong governance, effective controls, and timely action help organisations build IT resilience and aid the recovery of systems and data when cyber-attacks, data loss, or other disruptions occur.

The overall IT control environment remains under pressure

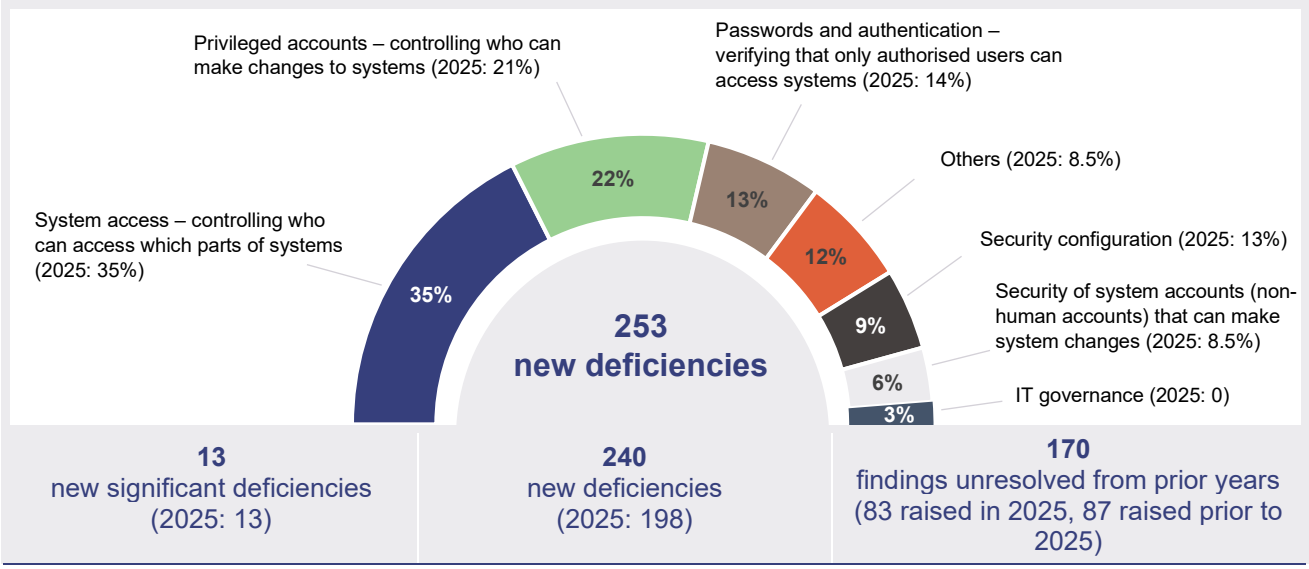
Entities have made good progress in addressing findings relating to significant deficiencies and their potential impact on security and financial reporting. However, the total number of unresolved deficiencies requires attention. The cumulative impact of unresolved deficiencies could increase overall risk if they are not addressed over a longer period.

Entities should focus on strengthening their overall control environment by:

- resolving findings more quickly and preventing long-standing issues from increasing operational and compliance risks
- strengthening security controls and improving accountability for remediation activities and issue management processes
- addressing the root causes of findings, particularly those caused by gaps in processes
- ensuring effective security controls are in place across all systems, not just those reviewed through our audit program.

Figure 1A details the deficiencies commonly found in the internal controls of IT systems.

Figure 1A
Types of deficiencies in internal controls identified in 2026



Source: Queensland Audit Office from our 2025 and 2026 audits.

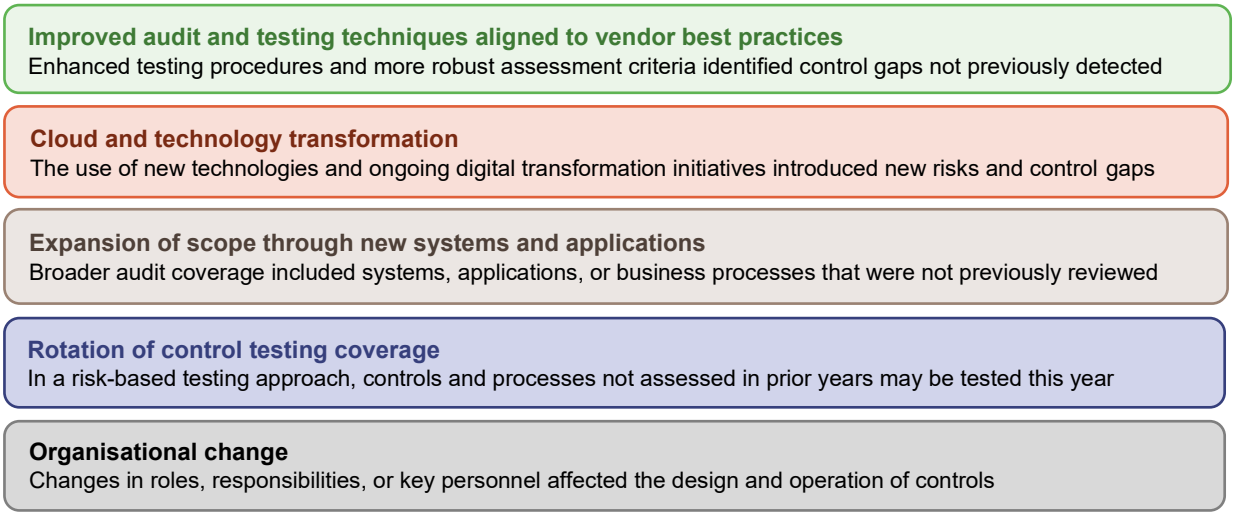
In 2026, we identified 13 new significant deficiencies and 240 new deficiencies in IT system controls. Significant deficiencies are serious control weaknesses that require immediate attention and corrective action. Deficiencies exist when controls are missing or not working properly.

The number of new significant deficiencies remains unchanged from last year, while the number of deficiencies increased by 21 per cent.

As in previous years, most findings relate to managing system access, privileged accounts, passwords and authentication, and security configuration.

Figure 1B shows the key factors contributing to the new deficiencies we identified in IT systems.

Figure 1B
Key factors contributing to new findings



Source: Queensland Audit Office from our 2026 audits.

Entities continue to carry a large backlog of findings. This backlog includes new findings raised during 2026 that the entities are still addressing and older findings that were not resolved by their agreed due dates. While some newer findings are still within their agreed remediation period, all open findings require attention and contribute to the overall backlog of work that entities need to complete.

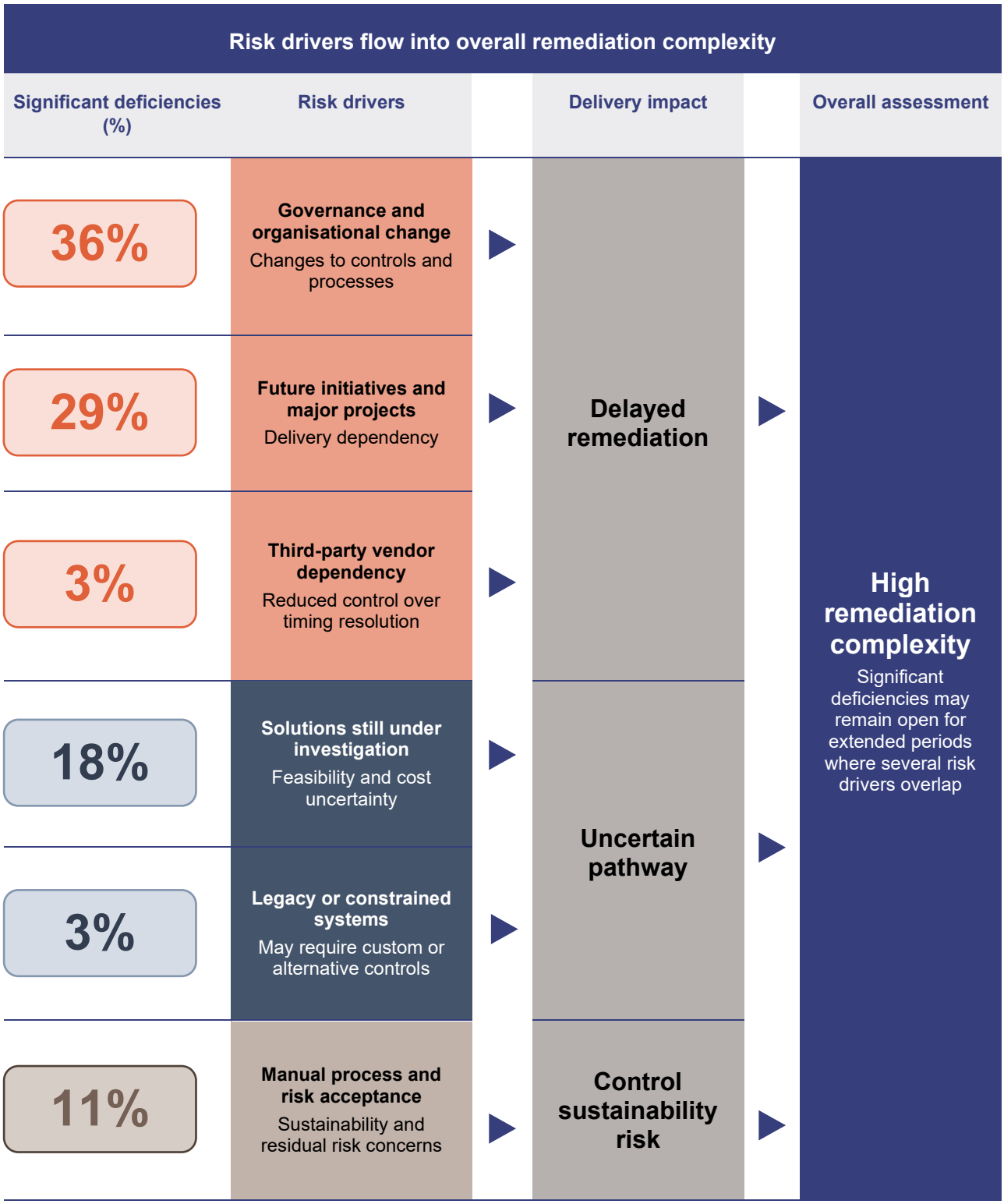
Entities continue to experience remediation delays

Entities remediated 63 per cent of information systems findings raised in 2025. Many issues, particularly significant deficiencies, have remained open for longer than intended, increasing the risk that information systems are not protected and operating as intended.

Figure 1C shows the factors contributing to the complexity of remediating significant deficiencies identified during our audits.

Different remediation drivers can affect an entity's ability to implement and sustain corrective actions. For example, deficiencies that require broader organisational change or depend on future projects were more likely to experience delayed remediation. Deficiencies that involve solution design uncertainty were more likely to have an unclear remediation pathway, while those managed through manual controls or risk acceptance may face ongoing sustainability challenges.

Figure 1C
Indicators that remediation may be difficult to deliver sustainably



Source: Queensland Audit Office from management responses on outstanding significant deficiencies as of 2026.

To help entities and audit committees better understand risks and assess whether remediation plans are realistic and likely to deliver the intended outcomes, we have included some key questions in Appendix D to monitor the progress and effectiveness of remediation activities.

Figure 1D outlines the key risks associated with each identified risk driver. Understanding these risks helps explain why some remediation activities may be delayed, less effective, or difficult to sustain.

Figure 1D
Risk drivers and associated risks that affect remediation

Remediation risk drivers	Associated risk
Governance and organisational change	• Multiple stakeholders are involved and require consultation • Entities require policy, process, and technology changes • Entities need to invest significant change management effort • Business resistance may occur • Controls are still maturing • Adoption and effectiveness may take time
Future major projects	• Entities cannot fully remediate risks until they deliver the project • Delays, funding constraints, scope changes, or implementation issues may defer remediation • Entities do not implement interim remediation to address existing risks • Exposure may continue for extended periods • Risks remain dependent on future project delivery • Entities accept interim risk rather than performing adequate risk assessment and mitigating gaps with compensating controls
Third-party dependency	• Management has limited direct control over implementation • Vendor capability constraints may prevent remediation • Timelines depend on external parties • Entities may require contractual negotiations
Solution still under investigation	• Entities have not fully defined remediation plans • Technical feasibility remains uncertain • Investigation activities may extend timelines • Proposed solutions may prove impractical or costly
Legacy or constrained systems	• Existing technology may not support the required controls • Systems may require custom development • Implementation costs and effort may increase
Manual process and risk acceptance	• Manual controls are difficult to sustain consistently • Human error may continue even after procedural updates • Ongoing monitoring is required • Security improvements may conflict with operational requirements • Exceptions may persist over the long term

Source: *Queensland Audit Office from management responses on outstanding significant deficiencies as of 2026.*

The opportunities below highlight key areas that all entities should consider to improve remediation outcomes, reduce the number of long-standing findings, and strengthen their control environment over time.



Opportunities to improve remediation effectiveness and reduce outstanding findings

Entities should:

- address control requirements early when planning system changes and transformation projects
- identify recurring findings and conduct a root-cause analysis
- assign clear ownership and timelines for remediation activities and monitor progress until issues are resolved
- consider short- to medium-term compensating controls
- ensure remediation actions address the root cause of findings, not just the immediate issue
- use lessons from previous findings to strengthen controls across other systems and business areas
- monitor outstanding findings and focus resources on areas with a high number of recurring issues.

Strengthening identity, access, and application controls should be a key focus

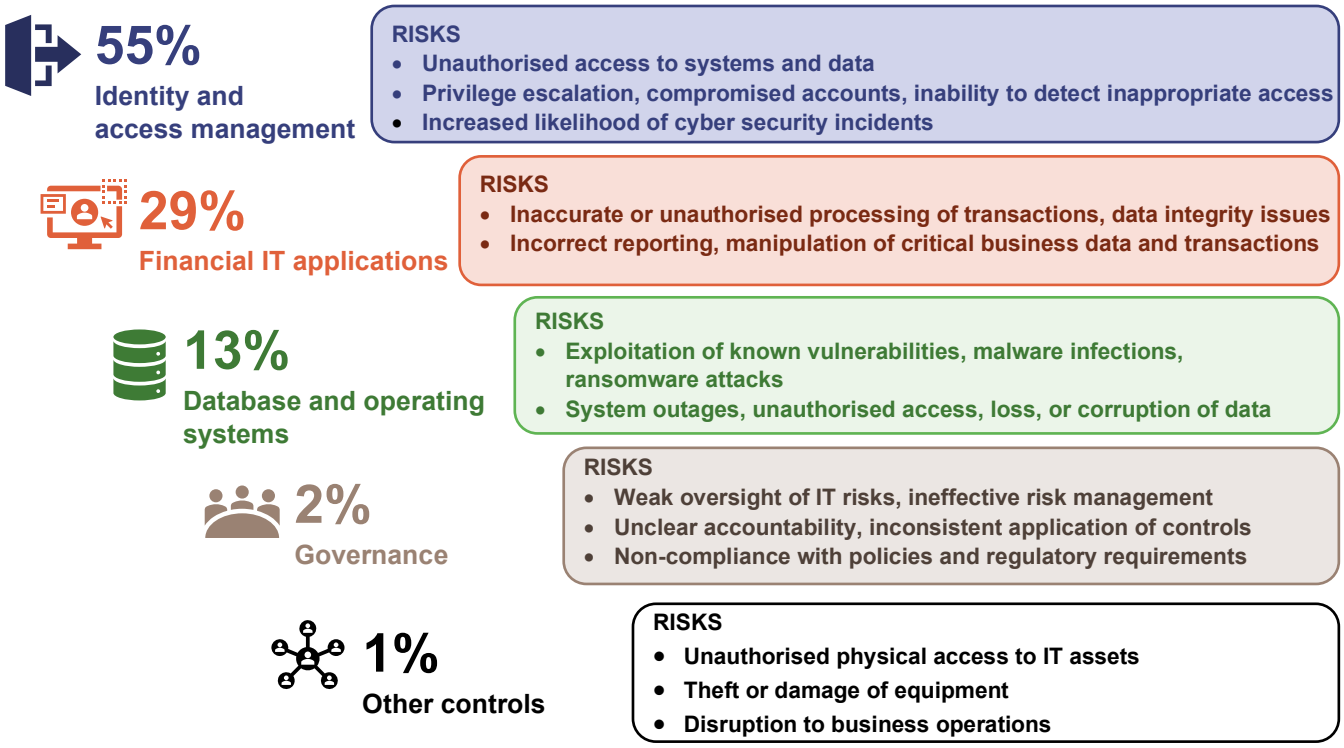
We identified 367 deficiencies (55 per cent of overall deficiencies) relating to identity and access management and 191 deficiencies (29 per cent of overall deficiencies) relating to application controls.

Identity and access management controls form the first line of defence against cyber threats. When these controls do not operate effectively, organisations may not be able to restrict access to systems and information to unauthorised users, increasing the risk of cyber incidents, data breaches, fraud, and disruption to business operations. The Australian Signals Directorate reported that, in 2024–25, 42 per cent of cyber incidents involved compromised accounts or credentials.

We identified 86 deficiencies relating to security controls over IT infrastructure, for example, databases and operating systems. These weaknesses may expose entities to security vulnerabilities, malware, service disruptions, and unauthorised access to information.

Figure 1E shows the common IT controls and associated risks identified through our audits.

Figure 1E
Common IT control deficiencies and associated risks



Source: Queensland Audit Office from our 2026 audits.

Entities need to actively manage security risks in cloud environments

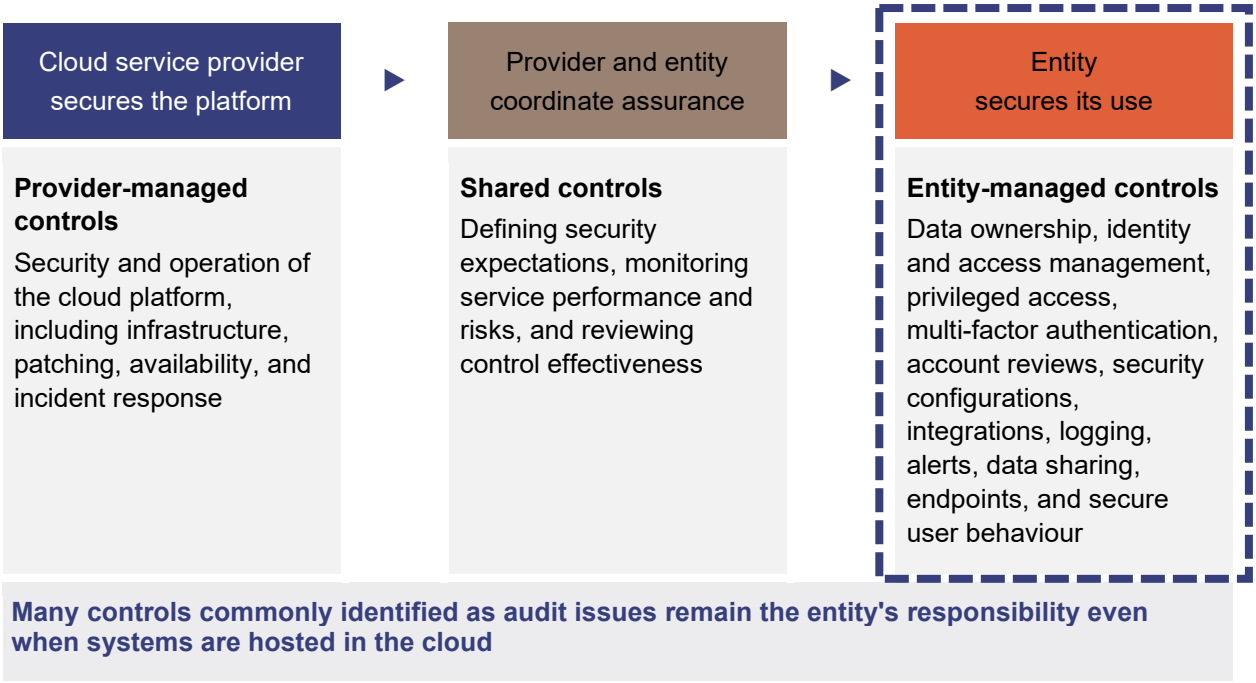
Many entities use cloud services to support critical business functions and store sensitive information. While there are benefits for cloud services, they also introduce security risks that entities must actively manage.

Our 2026 audits identified that 85 per cent of deficiencies relate to identity and access management, security monitoring, and user privilege management. These risks can be amplified in cloud environments where entities operate under a shared-responsibility model. While cloud service providers are responsible for securing the underlying cloud platform, entities remain responsible for managing user access, protecting information, monitoring security events, and complying with legislative and policy requirements.

In our report *Information Systems 2025* (Report 6: 2025–26), we highlighted the importance of managing cyber security risks associated with third-party service providers. As more critical systems and information move to the cloud, effective management of these risks becomes increasingly important to maintain secure and resilient information systems.

Figure 1F illustrates how security responsibilities are commonly shared between cloud service providers and entities.

Figure 1F
Common shared security responsibilities for cloud services



Source: Queensland Audit Office from Microsoft guidance on shared responsibility in the cloud and Cloud Security Alliance guidance on shared responsibility in cloud.

The Australian and Queensland governments provide a range of frameworks, policies, standards, and guidance to help entities manage cyber security and third-party cyber security risks.

Our report *Managing third-party cyber security risks* (Report 13: 2025–26) highlights better practice approaches for identifying, assessing, monitoring, and managing third-party risks. These approaches include understanding supply chain risks, conducting risk assessments, implementing appropriate controls, and regularly monitoring third-party arrangements.

By following these practices, entities can better manage cyber security risks and ensure risks remain within acceptable levels.

The case study in Figure 1G shows that establishing a framework is only the first step in managing third-party cyber security risks. Entities must also consistently undertake risk assessments and assurance activities. Without them, entities may not have enough visibility over third-party risks or confidence that controls are effectively protecting against unauthorised access, data breaches, security incidents, and weaknesses in system administration.

Figure 1G
Case study 1

Third-party risk assessment framework established but not operationalised
In response to an audit observation in 2024, a Queensland Government department introduced a third-party risk management framework to strengthen how it identifies, assesses, and manages cyber security risks from third-party vendors. The entity planned to use the framework to assess both existing vendors and new third-party engagements. However, by 2026, the entity had not completed assessments for existing or new vendors. In 2026, the entity implemented a new public-facing system that relies on a cloud service managed by an external vendor. Although the contract required the vendor to maintain recognised security standards and provide assurance over its security practices, the department did not obtain an independent controls assurance report and did not implement other measures to verify the vendor's controls were operating effectively. The entity did not complete a formal assessment of the vendor's security controls, despite previously identifying this as one of the actions for managing third-party risk. As a result, the entity does not know whether there are adequate controls in place to secure the system and data.

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits.

Independent assurance reports are one of the main ways entities can gain confidence that controls are in place and operating as expected. These reports are independently prepared and assess the design and the effectiveness of a service providers' controls. These reports provide valuable insight into how vendors manage key risks, including access management, privileged accounts, change management, incident response, data protection, and service availability.

Assurance reports are particularly important when entities use cloud-based or outsourced technology services because they provide independent evidence that vendor controls are operating effectively and reduce the need for entities to perform their own detailed assessments.



To better assist entities that are using cloud applications, we have listed the different types of assurance reports and the purposes they serve in Appendix E.

The guide in Figure 1H helps entities to assess third-party assurance reports and determine whether they provide sufficient assurance over vendor controls.

Figure 1H
Guide to using third-party assurance reports

Area	Questions for entities
Selecting the right report	• Does the report cover the specific service, system, location, and provider components the entity uses? • Do control assurance reports and other security certifications provide information about the operating effectiveness of controls? • Would the selected type of assurance report provide useful cyber security assurance, but not replace evidence needed for financial reporting controls?
Contract requirements	• Has the entity specified the assurance reports the provider must supply before entering or renewing the contract? • Do contract terms cover report scope, reporting period, delivery timing, bridge letters, subservice providers, and incident notification obligations? • Can the entity obtain updated reports or other evidence if the provider's report is delayed, qualified, or does not cover the period needed?
Annual review and monitoring	• Has the entity received the report in time to review it as part of third-party risk management? • Has the entity reviewed the auditor's opinion, scope, control objectives, testing period, exceptions, and complementary user entity controls? • For financial reporting systems, has the entity reviewed the report early enough to support audit work before it signs financial statements?

Source: Queensland Audit Office.

Opportunities for entities to strengthen governance of cloud environments

Entities should:

- understand and document security responsibilities under cloud shared-responsibility models
- perform risk assessments commensurate with how critical the service is and obtain independent assurance before adopting new cloud solutions
- establish contractual arrangements that include security obligations, incident notification requirements, and audit rights where appropriate
- implement ongoing monitoring processes to verify that shared-responsibility controls remain effective.

2. Maturity assessment of general IT controls

This chapter details the results of our general information technology controls (GITC) assessment for 5 selected departments. This is the first time we have performed a GITC maturity assessment.

A GITC maturity assessment, based on a GITC audit, focuses narrowly on selected information technology (IT) systems, access management, applications, databases, and change procedures to ensure the security and integrity of systems and data. It is a subset of the broader information security management system (ISMS) used to systematically manage organisation-wide information security risks, including human resources, physical security, legal compliance, governance, and business policies.

GITC audits form the basis of the information system audits we perform each year to support our annual audits of state entities' financial systems.

Our maturity assessment uses audit evidence spanning the 2024, 2025, and 2026 audits of 5 departments. It illustrates the entities' control maturity improvements year on year and highlights control areas that need further improvement.

Chapter snapshot



Noted improvements in the maturity of Microsoft Active Directory controls

7 of 11 (64%) Microsoft Active Directory control categories meet or exceed the target maturity level

Greater attention is needed for maturity of Microsoft Entra controls

Only 3 of 10 (30%) Microsoft Entra control categories meet or exceed the target maturity level



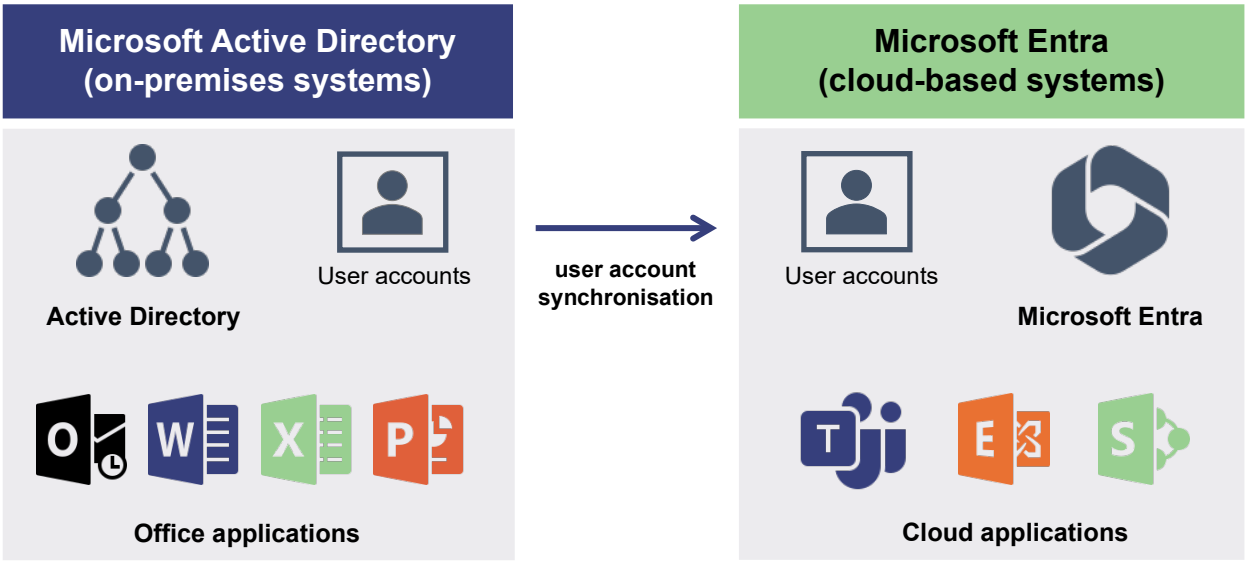
Our GITC maturity assessment scope

We assessed the control maturity for Microsoft Active Directory and Microsoft Entra computing systems for 5 selected departments.

Microsoft Active Directory is responsible for the authentication of staff to their local physical office computers and information. Microsoft Entra provides similar authentication for staff to cloud-based systems and information. Both services act as digital gatekeepers to ensure only authorised personnel can access government systems.

Figure 2A illustrates the Microsoft Active Directory and Microsoft Entra computing environments and a selection of common applications used by the departments.

Figure 2A
Microsoft Active Directory and Microsoft Entra systems



Source: Queensland Audit Office based on Microsoft information.

Figure 2B details the specific control categories covered by our information system audits and included in our GITC maturity assessment.

Figure 2B
Assessed IT control categories

Microsoft Active Directory control categories	Microsoft Entra control categories
• IT governance (policies/standards) • Security of default accounts • Passwords and authentication • Highly privileged account management • Service account management • Dormant user accounts • Terminated users and accounts • Third-party account management • Patching • Secure administration • Audit logging and security monitoring	• Cloud governance • Baseline security configuration • Passwords and authentication • Privileged role management • User account synchronisation • Dormant cloud native accounts • Terminated users and accounts • Guest account management • Secure administration • Audit logging and security monitoring

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits.

We used a 0–5 rating scale to perform the maturity assessment, based on Carnegie Mellon's Capability Maturity Model (CMM) framework. The CMM framework and its categories are discussed in Appendix F.

We defined a target Level 2 (repeatable) maturity level, meaning that IT control processes exist with an appropriate level of documentation and tasks are repeatable. However, process and control gaps, weaknesses, or errors may exist. Level 2 (repeatable) represents a baseline target or expected minimum.

Level 3 (defined) represents a higher level of organisational maturity, where processes are standardised, defined, and documented, with minimal gaps or errors existing. Additionally, some level of automation may exist.

The maturity assessment should be interpreted and used as a tool for identifying practical and achievable improvement opportunities, not as an expectation that all organisations will attain the highest maturity level.

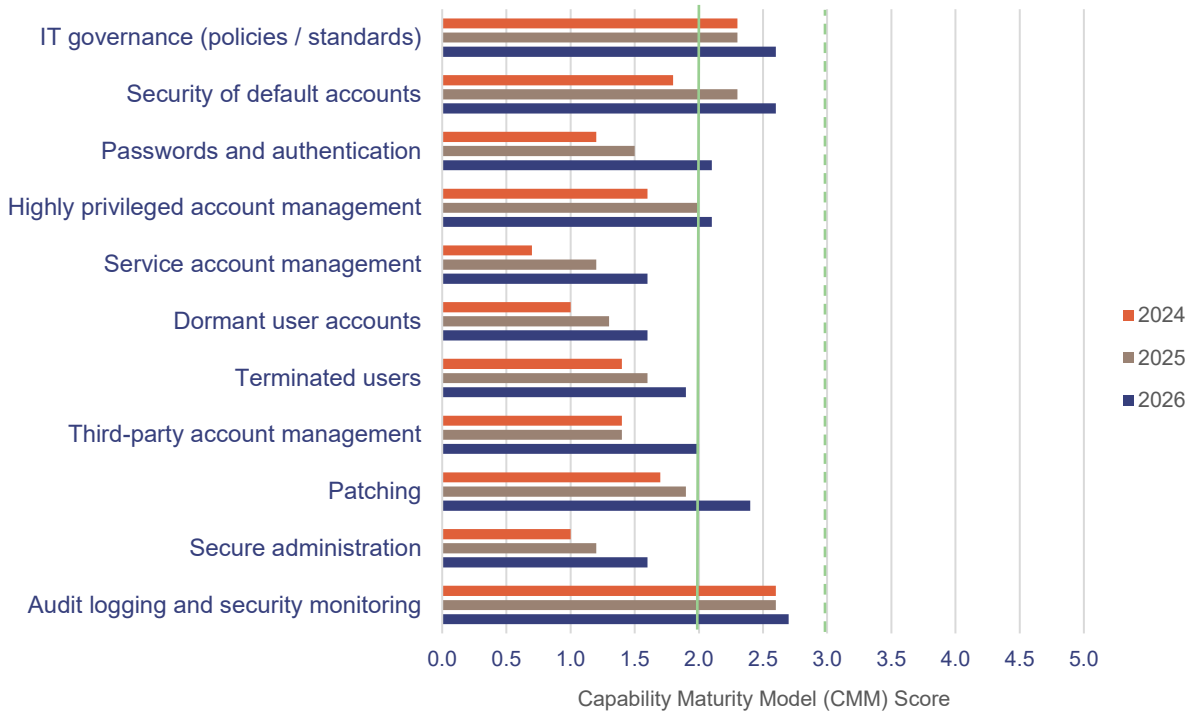
Entities have improved the maturity of their Microsoft Active Directory IT controls

Over the 3-year period from 2024 to 2026, the 5 departments we assessed achieved an established, Level 2 (repeatable) maturity level or higher across most of their on-premises Microsoft Active Directory control categories. We found that 7 of 11 assessed Microsoft Active Directory control categories met or exceeded Level 2 maturity. This is an improvement from only 2 of 11 control categories meeting or exceeding Level 2 maturity in 2024.

While our maturity assessment considered only 5 departments, the themes and areas requiring attention are consistent with our audit results across other departments.

Figure 2C shows the average maturity assessment scores for the 5 departments for each of the 11 Microsoft Active Directory control categories.

Figure 2C
Microsoft Active Directory control maturity improvement, 2024–2026

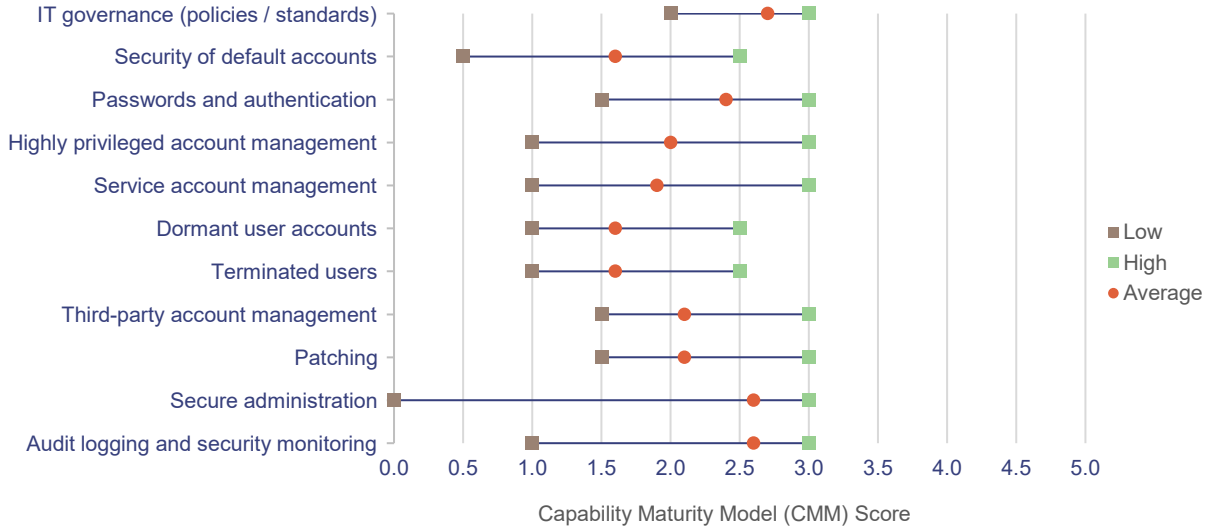


Note: The solid green line indicates the target Level 2 (repeatable) maturity while the dashed green line indicates the higher Level 3 maturity.

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits of 5 departments.

Figure 2D presents the 5 departments' average maturity score for 2026 with the low and high score for each control. It highlights areas of potential weakness in maturity that may be unintentionally concealed by presenting only the average score.

Figure 2D
Microsoft Active Directory maturity assessment, 2026



Source: Queensland Audit Office from our 2024, 2025, and 2026 audits of 5 departments.

Action is needed to address control categories not yet at the target maturity level

All entities should focus on improving their management of terminated and dormant user accounts and their management of service accounts. Figure 2E provides details of these areas for improvement.

Figure 2E
Microsoft Active Directory control categories to focus on for maturity improvement

Control category	Entities should
Service accounts Some entities have inventories of service accounts (machine or non-human accounts). However, there is inconsistent application of necessary security controls to secure these accounts.	• Implement all industry-recommended security controls • Inventory, track, and implement regular compliance reporting of all service accounts
Dormant accounts Entities have processes for identifying unused accounts, but effectiveness and monitoring of processes is not consistent.	• Improve effectiveness of dormant user account identification to minimise the number of unknown or unmanaged dormant accounts • Implement user-access review to supplement dormancy testing • Implement regular compliance reporting
Terminated accounts Entities have processes for terminated user accounts, but removing access for terminated users is often not timely.	• Remove system access promptly when users are offboarded • Implement compliance monitoring and reporting of terminated user accounts
Secure administration Entities use dedicated administration user accounts, separate from day-to-day user accounts. However, they do not use a secure administration system (controlled access system) to perform tasks.	• Implement and enforce use of a secure administration system to protect the administration user account when performing system administration tasks • Require multi-factor authentication (MFA) to perform system administration tasks • Prevent use of standard day-to-day client devices to perform system administration tasks

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits of 5 departments.

Figure 2F provides a case study to illustrate the importance of using a secure administration system for performing system administration tasks.

Figure 2F
Case study 2

Impact of not using a secure environment for performing system administration tasks

Control maturity weakness: mixing daily work with system administration tasks

When IT staff manage department computing environments, they use privileged user accounts. Cyber criminals target these specific user accounts. If:

- a cyber-criminal obtains the user account credentials, they could potentially gain full access to the entire computing environment and obtain sensitive information or disrupt vital public services
- an IT staff member accidentally clicks a malicious link in a phishing email, their computer could become infected. Since that same computer is used to access sensitive systems, the cyber-criminal could obtain the privileged user account credentials or monitor an existing privileged user session.

Either scenario could allow the cyber-criminal unauthorised access to potentially sensitive information.

Our maturity assessment found that many departments share a common, insecure practice: IT administrators often use their day-to-day computer, used for everyday tasks, to perform privileged system administration tasks. The day-to-day computer, used to browse the internet and read external emails, is at increased risk of compromise.

Control maturity improvement: deploy and use a dedicated and secure management environment

The Australian Cyber Security Centre (ACSC) notes that failing to isolate privileged user activities from internet-facing devices allows cyber criminals an opportunity to obtain privileged user credentials.

To improve the control maturity and mitigate this vulnerability, entities must deploy and enforce the use of separate, dedicated administrative devices. Guidance for this is detailed in ACSC's webpage on secure administration.

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits.



Opportunities for entities to improve Microsoft Active Directory control maturity

Entities should:

- improve timely identification and removal of user accounts belonging to terminated users
- improve the effectiveness of dormant user account identification and actioning processes
- implement industry-recommended security controls for use and management of service accounts
- deploy and enforce use of dedicated secure administration systems to perform system administration tasks
- implement compliance monitoring and reporting of all control management activities.

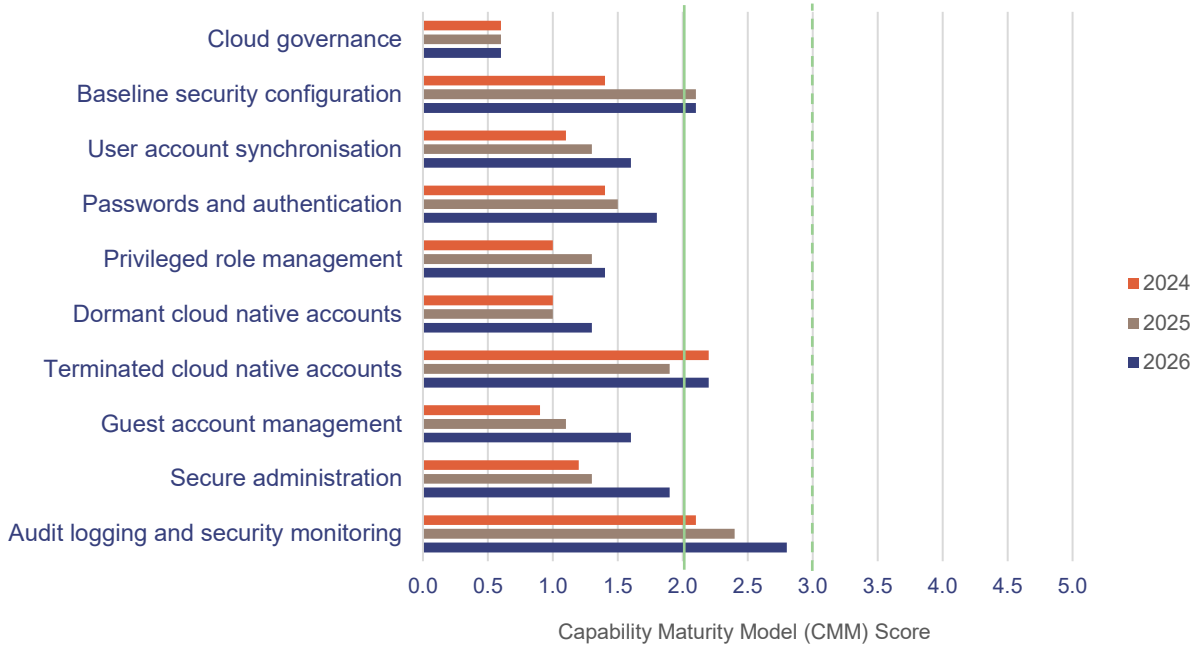
Entities need to improve the maturity of their Microsoft Entra IT controls

The maturity of Microsoft Entra controls has not kept pace with the maturity of Microsoft Active Directory controls.

Over the 3-year period from 2024, 2025, and 2026, only 3 of 10 Microsoft Entra control categories met or exceeded the target maturity level. This leaves 7 control categories at an initial or ad-hoc maturity level.

Figure 2G shows the average maturity assessment scores for each of the 10 Microsoft Entra control categories.

Figure 2G
Microsoft Entra control maturity improvement, 2024–26

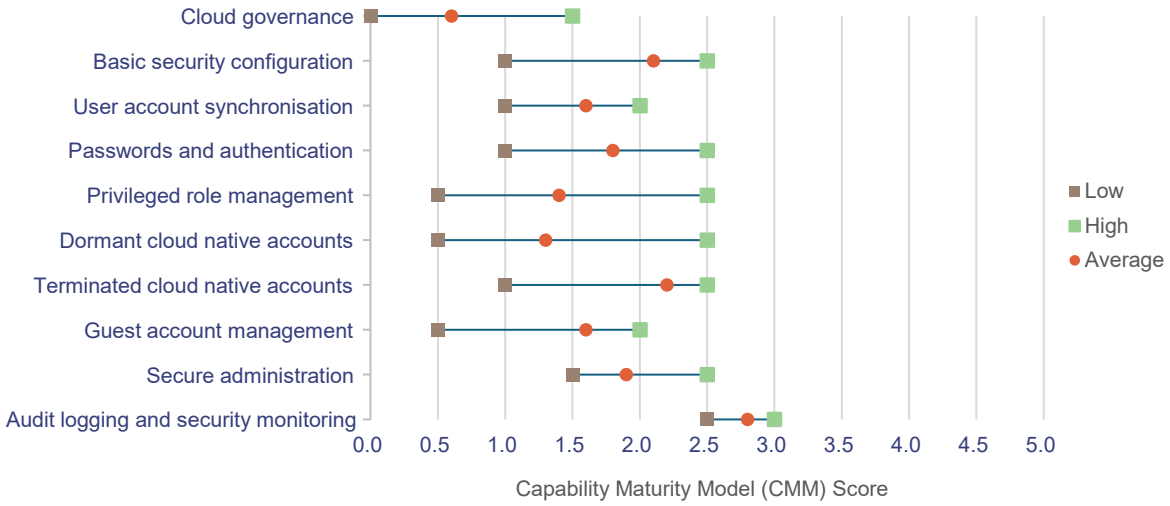


Note: The solid green line indicates the target Level 2 (repeatable) maturity while the dashed green line indicates the higher Level 3 maturity.

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits of 5 departments.

Figure 2H presents the average maturity score for 2026 with the low and high score for each control. It highlights areas of potential weakness in maturity that may be unintentionally concealed by presenting only the average score.

Figure 2H
Microsoft Entra maturity assessment, 2026



Source: Queensland Audit Office from our 2024, 2025 and 2026 audits of 5 departments.

Greater focus is required to address weaknesses in overall control maturity

Common control areas that all entities should focus on to improve their Microsoft Entra control maturity are summarised in Figure 2I.

Figure 2I
Microsoft Entra control categories to focus on for maturity improvement

Control category	Entities should
Cloud governance requirements Entities leverage their existing legacy IT control requirements and governance responsibilities. However, entities have not done the same for the newer cloud-based environments.	• Document security control and governance requirements for of all cloud-based services
User account synchronisation Entities synchronise user accounts between on-premises Microsoft Active Directory and cloud-based Microsoft Entra. Entities have basic processes in place to enforce compliance. However, periodic reviews are not consistently performed.	• Document requirements and scope of user account synchronisation • Implement monitoring and alerting of all synchronisation activities
Passwords and authentication Password configuration is aligned to documented requirements, and MFA is used to perform system administration tasks.	• Implement and enforce MFA for all user accounts, not just for system administration tasks • Perform monitoring and alerting of authentication anomalies
Privileged role management Privileged user access requires MFA. However, significant numbers of users possess highly privileged access; use of access is not strongly validated; and manual, not automated, privileged user-access reviews occur.	• Reduce the number of users with access to highly privileged roles • Assign eligible, not permanent, access to privileged roles • Implement and enforce time-bound access restrictions for all privileged roles • Implement monitoring and alerting for anomalous activities
Dormant cloud native accounts Entities have processes for identifying unused accounts, but effectiveness and monitoring of processes is not consistent.	• Improve effectiveness of dormant user account identification processes to minimise the number of unknown or unmanaged dormant accounts • Implement user-access review to supplement dormancy testing • Implement regular compliance reporting
Guest account management Security settings align with industry recommendations and guest user accounts are manually, but often inconsistently, reviewed for dormancy.	• Formalise and document applicable requirements for guest user access • Implement compliance reporting for guest user accounts
Secure administration Enforced use of MFA for administration is in place, but there is a lack of secure administration environment.	• Implement and enforce use of secure administration systems to perform system administration tasks • Prevent use of uncontrolled devices to perform system administration tasks • Implement monitoring and alerting of anomalous activities

Source: Queensland Audit Office from our 2024, 2025, and 2026 audits of 5 departments.

Of these common control areas that require greater focus, 2 require specific attention: multi-factor authentication (MFA) and privileged role management.

Elevated risk of unauthorised access due to gaps in MFA enforcement

Most Queensland Government staff use cloud-based services every day to send emails, write documents, and access other departmental information. These cloud systems can hold large amounts of sensitive information, including personally identifiable data, internal policy plans, and confidential documents.

To access services and information, staff typically enter a username and a password. Passwords alone are no longer enough to keep this information safe. If a staff member's password is somehow compromised, a cyber-criminal could use the credentials to gain unauthorised access to information.

Our maturity assessment found that some departments do not strongly enforce MFA for all users. MFA is an extra identity check, for example when someone receives an SMS message on their mobile phone when authenticating to their personal bank account.

To protect sensitive information, all departments should use MFA for every user account accessing its cloud-based services.

The ACSC states that compromised user credentials remain one of the most frequent vectors used by malicious actors to target government and enterprise systems. It highlights that using passwords alone leaves systems vulnerable to unauthorised access and it strongly urges entities to enforce MFA across all user accounts as a primary baseline control to block intruders from exploiting compromised credentials. For more information, see: www.cyber.gov.au/publication/personal-cyber-security-handbook/set-up-multi-factor-authentication.

Privileged role access is larger than required

In cloud-based computing environments, user accounts can be granted access to roles that give the user account various levels of privilege. Depending on the specifics of the role, a user can manage resources, modify credentials, configure security policies, or access restricted data.

Our maturity assessment found that many departments do not properly manage access and use of these privileged roles. Departments often assign staff permanent and active access rather than limiting access to the role for when a specific administrative task arises. This means the privileged user account maintains access permanently, even when the privileged account is not being used.

Departments frequently do not use just-in-time access, which temporarily grants privileged access only when requested and approved, and only for a specific period. In some instances, staff can switch on or request privileged access without even being authorised to use the privileges.

The ACSC warns that permanent or uncontrolled privileged access significantly increases an organisation's exposure to system compromises. Failing to enforce role-governance controls allows malicious actors who obtain privileged account credentials to have potentially unfettered access to cloud-based resources. Examples of role-governance controls include requiring justification, approval workflows, and strict MFA before role activation.

The ACSC's advice to restrict administrative privileges highlights that traditional approaches, such as permanently assigning high-level access rights to staff members, fails to safely protect systems. For more information, see: www.cyber.gov.au/publication/restricting-administrative-privileges.



Opportunities for entities to improve Microsoft Entra control maturity

Entities should:

- document security control and governance requirements for use of all cloud services
- document requirements and scope of user account synchronisation
- implement and enforce multi-factor authentication (MFA) for all user accounts
- reduce the number of users with access to highly privileged roles
- utilise eligible, not permanent, access to all privileged roles
- implement time-bound access for all privileged roles
- improve effectiveness of dormant user account identification processes
- implement and enforce the use of a secure administration system while preventing use of unmanaged devices
- implement user-access review and compliance reporting for dormant user and guest user accounts
- implement compliance reporting for guest user accounts
- implement monitoring and alerting for anomalous authentication and other activities.

Maturity improvements require leadership support

Sustaining improvements and control maturity requires leadership support through the establishment of culture of improvement, risk reporting, and allocation of resources to the risk identified.

3. Financial system implementations

This chapter considers the financial management systems and the system upgrades for departments that are currently underway.

Departments use the SAP finance system. Queensland Shared Services (QSS) manages the SAP system on behalf of 16 departments. It is currently upgrading the system as the system and IT infrastructure will be out of support.

Chapter snapshot

State entities are upgrading or replacing key finance systems

QSS is planning to upgrade its SAP system during 2027, another department is beginning the upgrade, and the other departments have all upgraded

QSS is moving its finance system from on premises to public cloud

A complex public cloud implementation for government

QSS's system upgrade will change QSS and departments' processes

QSS and departments will need to work closely to manage the change and to ensure all key controls are effectively designed and understood

State entities are upgrading or replacing their key finance systems

Many state entities use the SAP system to run their day-to-day businesses. SAP is an integrated system that can manage finance, purchasing, payroll, and asset management.

The older SAP ECC6 system is reaching its end of life. Mainstream support for SAP ECC6 will end in December 2027, with a negotiable option to extend support until December 2030 at an increased cost.

State entities are upgrading or have upgraded to the newer SAP S/4HANA to replace their SAP ECC6 finance system:

- QSS manages the finance system for 16 departments. QSS is in the process of upgrading to S/4HANA, which is currently expected during 2027. The upgrade will result in changed processes within the departments and QSS.
- Five departments manage their own finance systems. Of these, 4 have upgraded to S/4HANA and one is in the process of upgrading.
- State entities in the energy and water sector have upgraded to S/4HANA.
- One entity in the infrastructure sector is currently upgrading to S/4HANA.

QSS will upgrade to S/4HANA during 2027

QSS manages the finance system for 16 departments. It also uses its system to process transactions for other state entities through a shared service model. The transactions include accounts payable, accounts receivable, vendor and customer master data, assets, taxation, general ledger, and reporting.

QSS has used the SAP system since its formation in 2000. It has used SAP ECC6 since 2017.

QSS's initial plan was to implement the upgrade to S/4HANA by 2026 in 2 releases, based on risk assessment and consultation with departments. In response to emerging risks and delivery challenges, the plan has been revised and is now expected to be completed in 2027.

QSS is moving its on-premises finance system to the public cloud

Currently, QSS uses an on-premises finance system, maintained through CITEC, which manages the IT infrastructure. QSS is implementing S/4HANA as a public cloud system.

The QSS implementation of S/4HANA will be the first time a Queensland Government department has used an SAP public cloud system to this extent.

In 2022, one department implemented a public cloud solution with SAP. This system provides a specialised procurement and supplier management component, not the full core functionalities of a finance system.

Figure 3A describes the features, benefits, and challenges of on-premises, private, and public cloud solutions.

Figure 3A
Features of on-premises, private, and public cloud systems

Delivery model	Description	Analogy	Benefit	Challenge
 **On-premises system**	• Entity owns, maintains, secures, and upgrades the system	• Entity owns an office building and is responsible for maintenance, repairs, and upgrades	• Greater control over the system • Can be highly customised to the entity's requirements	• Operating costs can be higher • More technologies to maintain • Upgrades can take longer • Infrastructure can become outdated
 **Private cloud**	• Technology provider hosts the system in a cloud environment that is dedicated to a single entity • Technology provider manages much of the underlying technology; the entity retains greater control over the system (e.g. customisation and security)	• Entity rents a secure building with its own dedicated floor • Entity does not own the building but has its own controlled space	• Reduced infrastructure management • Supports more complex business requirements and customisations	• More expensive than public cloud • Less standardised and more customised, which can increase complexity
 **Public cloud**	• Many entities share the same technology platform • The technology provider manages the IT infrastructure and delivers regular upgrades • The entity focuses on using the system rather than managing it	• Entity rents space in a building with other tenants • The system owner takes care of maintenance, security, and upgrades	• Lower infrastructure costs and reduced management effort • Faster implementation (due to limited customisation) • Regular updates and new features	• Limited flexibility to customise • Entities may need to change their business processes to align with the system

Source: Queensland Audit Office.

The QSS implementation requires effective planning and risk management

The QSS implementation of a public cloud solution is significant, due to its size, complexity, and the number of entities involved. This type of change requires understanding of existing business processes, custom configurations, data quality, and ways of working. There is a commensurate change required in the supported entities.

QSS's initial budget in 2024 for the implementation was $42 million. It was revised to $43 million in 2026. As of September 2026, it has spent $32 million.

Figure 3B details the areas of complexity that require planning and risk management.

Figure 3B
Area of complexity for the change

Current state (on premises)	Need	Future state (public cloud)
16 departments have different business processes and requirements	Effective 'fit-to-standard' exercises with all departments Effective coordination and communication with departments	Departments to use standard processes from the technology provider
4,500 custom configurations accumulated over 2 decades	Effective needs analysis of existing custom configurations	Minimal customisation
Data collected over years contains duplicates, obsolete records, and historical errors	Effective data strategy, cleansing, transformation, and migration	New data model and structure
QSS processes transactions on behalf of departments	Operating model redesign and business (department) readiness	Departments responsible for processing transactions, requiring a new target operating model
QSS and CITEC share responsibilities for system maintenance	Understanding of roles and responsibilities and effective governance	SAP responsible for system maintenance and patching

Source: Queensland Audit Office from information provided by QSS.

Areas of focus for successful implementations

Drawing on our experience in auditing system implementations, we have identified areas of focus that QSS can use when assessing the implementation. Key areas of focus include:

- business requirements and scope
- business change and readiness
- schedule and delivery
- system testing and resolution of defects
- design and solution
- resourcing.

QSS have advised us that they are addressing risks and undertaking management action.

Two of our reports provide lessons learnt from previous system implementations in Queensland Government: *Queensland Health's new finance and supply chain management system* (Report 4: 2020–21) and *Effectiveness of the State Penalties Enforcement Registry ICT reform* (Report 10: 2019–20). QSS can also benefit from other departments' SAP implementations.

Figure 3C provides key risk indicators and questions entities could use when implementing new systems.

Figure 3C
Key risk indicators and questions for system implementation

Key risk area	Key questions
Governance and leadership, including executive oversight	• Do senior leaders challenge project assumptions, status reports, and benefit claims? • Is there adequate and effective escalation of emerging risks? • Are assurance findings resolved in a timely manner? • Is there any leadership optimism bias despite weakened or deteriorating project indicators or confidence about readiness to go live? • Are adequate project management tools for effective planning, scheduling, and risk management in place?
Strategy and business case	• Is the solution fit for purpose for the departments using the system? • Are business case assumptions being revalidated regularly? • Are there adequate considerations on business impact that balance any perceived technology urgency?
Business requirements and scope	• Is there effective alignment of standard functionalities and business expectations? • Is there adequate understanding of end-to-end business processes and control requirements? • Has the target operating model been defined and the readiness of departments to accept the change been assessed objectively?
Resourcing	• Do QSS and departments have adequate resources available for the key phases of the implementation? • Is there high turnover of project staff? What is the process to manage knowledge transfer and quality of deliverables? • Are there adequate business-as-usual and project resources?
Business change and readiness	• Are stakeholders sufficiently and effectively engaged? • Are there effective communications across stakeholders? • Do departments have high confidence and user readiness, including sign off to go live?
Design and solution	• Is there effective gap analysis at the design phase? • Have all identified gaps been addressed throughout the implementation? • Have future state operating models been defined?
System testing and resolution of defects	• Is the integration testing performed on time, with adequate and effective resolution of defects? • Is there clear understanding of the volume, quality, and complexity of data for the target state? • Is there effective and timely management of defect backlogs? • Are high-severity defects resolved in a timely manner?
Schedule and delivery	• Is there a realistic implementation timeline and go-live commitments? • Are there adequate buffers for unplanned risks on technology deliverables, testing cycles, integration readiness, and data readiness?
Risk management and assurance	• Do project health checks identify no significant concerns with appropriate action in place? • Is there an effective escalation pathway for project health concern?
Technology and infrastructure	• Is the infrastructure ready, with a stable environment? • Have cyber security requirements been identified and implemented?

Source: Queensland Audit Office from our previous reports to parliament on system implementations.

4. Legacy systems

This chapter provides updated insights about legacy systems used by departments, extending the insights we provided last year.

The Queensland Government classifies a legacy system or technology as having one or more of these attributes:

- an age greater than the average age of all government systems
- past its end-of-use date
- classified as 'retire' or 'streamline' as part of the planning methodology for information and communication technology (ICT).

In 2025, the Queensland Government announced a $1 billion digital fund to drive a coordinated whole-of-government approach to digital investment and information technology (IT) systems. This includes legacy modernisation projects.

The Department of Customer Services, Open Data and Small and Family Business (CDSB) administers the digital fund.

Chapter snapshot

40% of the digital fund was allocated in the first funding round

$414 million approved in 2025–2026

$288 million for legacy modernisation projects

1/3 of systems we audited were legacy systems

This is a reduction from last year, when we reported that half the systems we audited were legacy

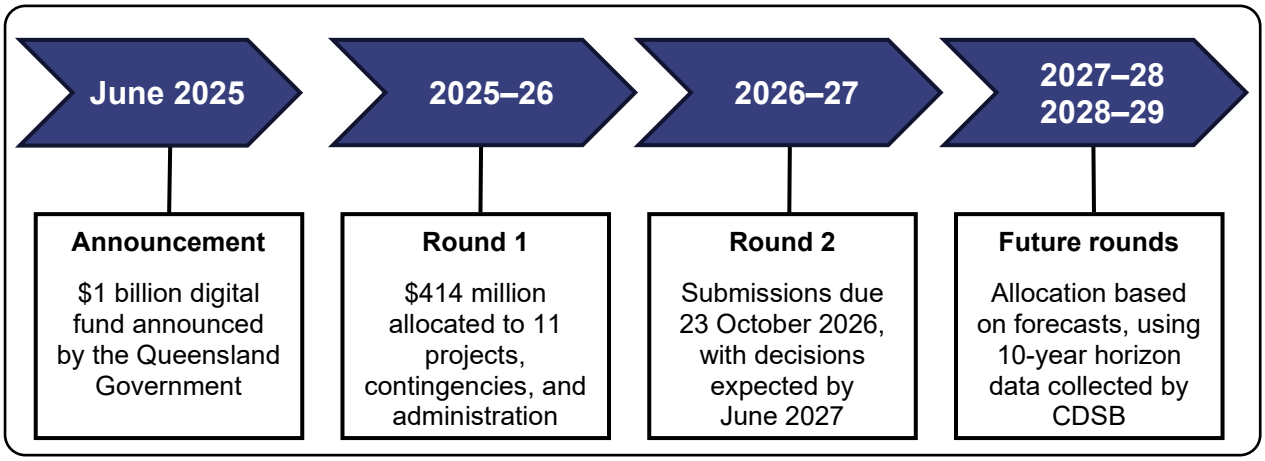
ICT profiling information continues to have gaps

In particular, the digital projects dashboard is incomplete and not updated as required

About 40 per cent of the $1 billion digital fund has been allocated

In the first funding round, the Queensland Government allocated $414 million to 11 projects, representing about 40 per cent of the total fund. A second funding round is underway. Figure 4A provides an overview of the digital fund's timeline.

Figure 4A
Digital fund timeline

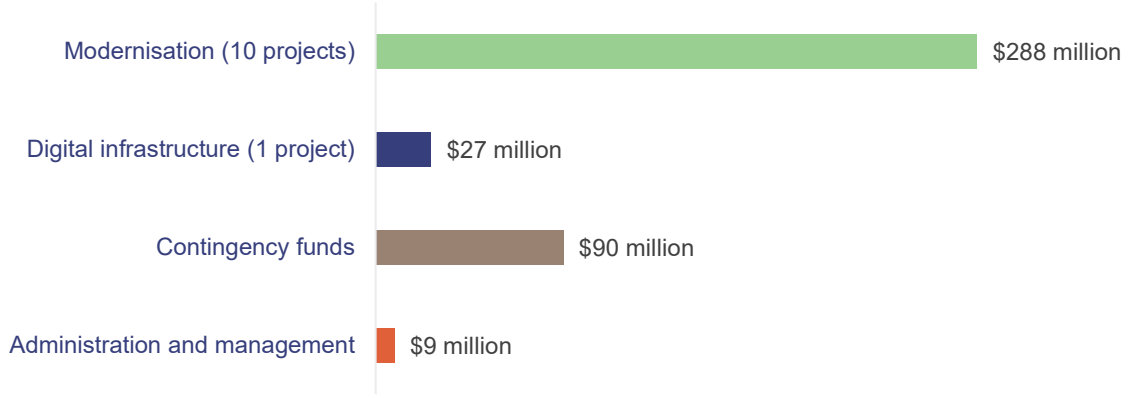


Source: Queensland Audit Office from information provided by CDSB.

Figure 4B provides an overview of the government's initial allocation of $414 million in 2025–26, including:

- $315 million in committed project funding to 8 entities for 11 projects – 10 of these are to replace legacy systems (modernisation)
- $90 million in contingency funding
- $9 million across 4 years for administrative and management activities.

Figure 4B
Digital fund allocations 2025–26



Source: Queensland Audit Office from 2026–27 Budget Measures (Budget Paper No. 4) and information provided by CDSB.

Budget Paper No. 4 includes high-level information about each project, including information about funding for 10 of the 11 projects.

TRAILS (Transport Registration and Integrated Licensing System), a Department of Transport and Main Roads system, is not included in the information as contracts have not yet been awarded. This project will be co-funded by the Department of Transport and Main Roads and the digital fund. Figure 4C lists the funded projects.

Fund governance was refreshed in 2026

CDSB administers the digital fund with oversight from the Digital Queensland Investment Committee (DQIC), which comprises the Under Treasurer, the Directors-General of CDSB, and Department of the Premier and Cabinet.

The DQIC recently released a new digital investment and assurance framework, which details its approach to evaluating and prioritising digital initiatives and establishes governance committees.

Information about funded projects was not recorded in the digital projects dashboard

The digital projects dashboard is a publicly accessible resource that contains information about digital projects across all Queensland Government departments. It aims to provide transparent information about investments.

Data should be entered into the digital dashboard within 8 weeks. The 11 funded projects were included in Budget Paper No. 4, released on 23 June 2026. However, the allocated funding had not appeared in the dashboard until 15 September 2026, 12 weeks later.

Figure 4C shows the projects, digital fund allocation, and the status of information on the dashboard. This information is the total cost of change, not just technology or procurement costs.

Figure 4C
Digital projects dashboard status for digital fund projects

Department	Project	Digital fund allocation ($ mil.)	Digital projects dashboard
Department of Housing and Public Works	Queensland Building and Construction Commission Digital Transformation Roadmap	$15.2	Not captured
	Build to Enable Program	$37.2	Captured, but budget not updated to reflect the digital fund allocation
Department of Justice	Queensland Worker Screening	$5.7	Not captured
Department of Local Government, Water and Volunteers	Digital Water Systems	$51.1	Not captured
Department of Primary Industries	Replacement of the Forest Sales Management Information System	$8.8	Captured, but budget not updated to reflect the digital fund allocation
Department of the Environment, Tourism, Science and Innovation	High-Performance Computing and Data Platforms	$26.7	Not captured
Department of Transport and Main Roads	Registration and Licensing Modernisation	Not stated	Not captured
Queensland Health	Clinical Imaging Informatics Systems Replacement and Establishment of Enterprise Vendor Neutral Archive – Stage 1	$63.5	Not captured
	Replacement of the Pathology Queensland Laboratory Information System	$30.5	Not captured
	Corporate Enterprise SAP Re-platforming	$28.1	Not captured
Queensland Police Service	Disaster Event Management System Replacement	$6.1	Not captured

Source: Queensland Audit Office from the digital dashboard (accessed 15 September 2026) and budget paper.

The new digital investment forecast aims to reduce legacy risk

Previously, departments submitted annual ICT work plans to CDSB to enable a whole-of-government view of ICT investments and planned initiatives. From this financial year, the new Digital Investments Forecast (the forecast) replaces those work plans.

The forecast will provide a 10-year outlook of current, planned, and prospective digital and ICT initiatives. One of its stated objectives is to reduce the risk of investing in outdated or soon-to-be-obsolete technologies.

Departments are required to submit forecast data to CDSB twice a year – in October and April. The first submission was due by 31 October 2026. CDSB expects this information to enhance whole-of-government ICT planning, coordination, and decision-making.

ICT profiling information continues to have gaps

ICT profiling is a regular program of data gathering and analysis conducted by CDSB to support whole-of-government objectives. The ICT profiling standard identifies information that departments should report centrally, including:

- at-risk data – collected in June and December about systems deemed strategically important and at a high or extreme risk to the business
- ICT resources – collected in June to list all systems used by departments
- digital projects dashboard – collected every 4–6 weeks, with an 8-week maximum reporting timeline, to provide a publicly accessible dataset about digital projects across departments.

Information about projects is not always recorded in the digital projects dashboard as required

In the digital projects dashboard, some projects are captured late, and some are not updated regularly. Examples include:

- the $15 million Forestry Systems Continuity Project (Stage 1) for the Department of Primary Industries, which started in April 2023 but was first reported in January 2026, after half the approved budget had been spent
- the $25 million Enterprise Data Platform Project for the Department of Education, which started in July 2023 but was first reported in June 2026, after 60 per cent of the approved budget had been spent
- the $194 million Build to Enable Project for the Department of Housing and Public Works has been in the dashboard since May 2024. However, as at 15 September 2026, the most recent update was provided on 30 May 2026 (15 weeks old). The project received $37.2 million from the digital fund in 2025–26.



Opportunities to improve the reporting process

CDSB should:

- assess the project reporting requirements and consider why they are not followed consistently
- determine whether the 8-week reporting period is optimal or could be changed to improve the quality of data.

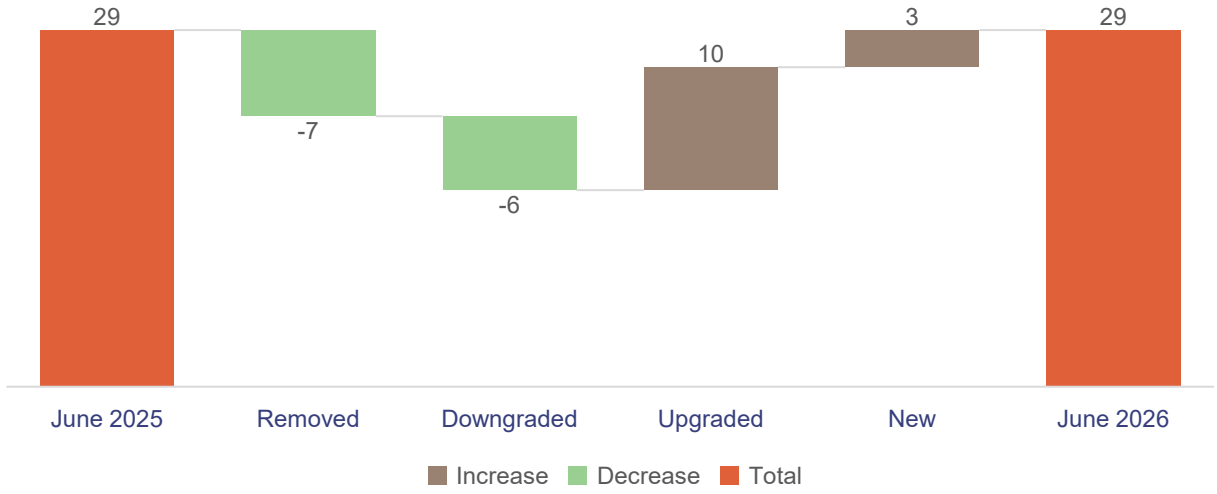
Departments should:

- follow the guidelines for reporting projects to the digital projects dashboard.

The number of systems at extreme risk has remained the same, with some systems dropping off the list and new ones added

Departments reported 29 systems at extreme risk in June 2026, the same number reported in June 2025. However, the makeup of the list changed, as detailed in Figure 4D.

Figure 4D
Systems at extreme risk



Source: Queensland Audit Office from the at-risk systems listing.

Some departments are closing legacy gaps, but departments do not manage risks consistently

In 2025, we reported that half of the systems we audited were legacy systems. In 2026, this has reduced to one third, mainly due to upgrades of applications or supporting infrastructure to newer, supported versions.

Departments do not manage legacy risks consistently

The case study in Figure 4E shows the different ways that 2 departments manage legacy deficiencies.

Figure 4E
Case study 3

Departments accepting the risk associated with legacy systems
Departments often have audit deficiencies that cannot be remediated because the relevant systems are old. One of the systems we audit has been at-risk since 2023, with a large program of work underway to modernise it. For some of the associated deficiencies, the department elected to accept the risk without implementing mitigating controls. The risk acceptance has not been formally documented. This is not optimal, as the department's risk acceptance is not properly supported and communicated. A different department has several legacy systems, with projects initiated to modernise them. This department formally documents the risk acceptance process for each deficiency. Management submits a paper to the department's audit and risk committee to provide its risk acceptance rationale. The risk is accepted if the committee agrees. This is a better practice.

Source: Queensland Audit Office from our 2025–26 audits.



Opportunities for departments to strengthen their risk-acceptance processes

Departments should:

- formalise the process for accepting risks associated with deficiencies or control weaknesses
- implement mitigating controls where feasible
- obtain approval from a relevant governance committee for each risk accepted.

Our performance audit *Managing the risks of aging technology* is underway. In this audit, we will assess how effectively selected entities manage the risks associated with legacy IT infrastructure and systems.

Appendices

A.	Entity responses	33
B.	How we prepared this report	36
C.	Status of recommendations made in prior reports	38
D.	Focus areas for remediating IT control deficiencies	39
E.	Using third-party assurance reports	40
F.	IT controls maturity assessment methodology	42

A. Entity responses

As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to:

- Minister for Customer Services and Open Data and Minister for Small and Family Business
- Director-General, Department of Customer Services and Open Data and Minister for Small and Family Business.

We also provided a copy of the report to the following and gave them the option of providing a response:

- Premier and Minister for Veterans
- Treasurer, Minister for Energy and Minister for Home Ownership
- Under Treasurer, Queensland Treasury
- Director-General, Department of the Premier and Cabinet
- Directors-General of the departments selected for maturity assessments.

This appendix contains the responses we received.

The heads of these entities are responsible for the accuracy, fairness, and balance of their comments.

Comments received from Acting Director-General, Department of Customer Services, Open Data and Small and Family Business

DELIVERING FOR QUEENSLAND | Queensland Government

Our Ref: MN09325-2026

Department of
Customer Services, Open Data and Small and Family Business

12 November 2026

Ms Rachel Vagg
Auditor-General
Queensland Audit Office
Email: qao@qao.qld.gov.au

Dear Ms Vagg,

Thank you for your email of 26 October 2026 regarding the proposed *Information Systems 2026* report. The Department of Customer Services, Open Data and Small and Family Business (CDSB) supports the report's findings and recognises its dual role in maintaining effective departmental IT controls and supporting whole-of-government digital investment, governance and cyber security.

CDSB acknowledges that recurring control weaknesses require sustained attention and continues to strengthen identity and access management controls across both on-premises and cloud-based environments. Alongside this work, we will continue providing whole-of-government cyber security policy, advice and services to support agencies, including in managing third-party supply-chain risks.

In relation to the Queensland Shared Services SAP S/4HANA upgrade, we acknowledge the areas identified in the report requiring further attention. We will consider the findings as implementation progresses and continue to manage the upgrade through established governance and risk management arrangements, in consultation with participating departments.

More broadly, we recognise the opportunities identified in the report to improve legacy-system risk management and digital project reporting. We will review dashboard reporting requirements with departments to better understand the reasons for inconsistent application and assess whether the current eight-week reporting period supports timely and accurate reporting.

Should require any further information, please contact Mr Mark Howard, Deputy Director-General, Data and Digital, Department of Customer Services, Open Data and Small and Family Business, at .

Yours sincerely

David Sinclair
Acting Director-General

Level 29, 1WS Street Brisbane
PO Box 15086 City East
Queensland 4002 Australia
Website www.cdsb.qld.gov.au
ABN 81 919 425 843

Comments received from Directors-general of departments selected for maturity assessments

Three of the 5 departments selected for maturity assessment provided comments. The responses have been summarised as:

- noting the value of maturity assessment and benchmarking of control environments across government
- welcoming the insights and improvement opportunities for consideration and action.

B. How we prepared this report

Queensland Audit Office reports to parliament

The Queensland Audit Office (QAO) is Queensland's independent auditor of public sector entities and local governments.

QAO's independent public reporting is an important part of our mandate. It brings transparency and accountability to public sector performance and forms a vital part of the overall integrity of the system of government.

QAO provides valued assurance, insights and advice, and recommendations for improvement via the reports it tables in the Legislative Assembly, as mandated by the *Auditor-General Act 2009*. These reports may be on the results of our financial audits, on the results of our performance audits, or on our insights. Our insights reports may provide key facts or a topic overview, the insights we have gleaned from across our audit work, the outcomes of an investigation we conducted following a request for audit, or an update on the status of Auditor-General recommendations.

We share our planned reports to parliament in our 3-year forward work plan, which we update annually: www.qao.qld.gov.au/audit-program.

A fact sheet about how we prepare, consult on, and table our reports to parliament is available on our website: www.qao.qld.gov.au/reports-resources/fact-sheets.

About this report

This report assesses information systems controls used by Queensland's state government entities. It is designed to recognise the collective need across government for more focus on the security of information.

What we cover

Through our information systems audit program, we form opinions about the security and reliability of information technology (IT) to ensure financial data is protected and trustworthy for financial reporting.

QAO completes these audits under the related Auditing and Assurance Standards Board standards. Each respective entity publishes our audit opinions in its annual report.

Our information systems audit reports to parliament provide the results of our audits and assess the quality and effectiveness of internal controls related to information systems. This report highlights key insights and information from across our work.

Our approach

Information systems control deficiencies

We used the following data to prepare this report:

- types of deficiencies we found in information systems controls at state entities this year (Figure 1A) – we sourced this data from the information systems audit reports we issued to state entities
- comparison of deficiencies at state entities between the current year and prior years (Figure 1C) – we sourced this data from the audit reports we issued to state entities this year and our report *State entities 2025* (Report 11: 2025–26)
- the Australian Signals Directorate's general guidance, which recommends strong identity governance, least-privilege access, privileged access management, and timely deprovisioning to mitigate risk.

Maturity assessment of general information technology controls

We used the following data to prepare this report:

- information and data collected from departments as part of the general information technology control (GITC) / information system audits performed from 2024 to 2026
- audit findings and remediation of audit findings sourced from information systems audit reports issued to departments from 2024 to 2026
- assessment of changes in the control environment based on year-on-year audit findings and remediation of findings from audit reports issued to departments from 2024 to 2026.

We used the following external references:

- Capability Maturity Model (CMM) framework devised at Carnegie Mellon University: www.sei.cmu.edu/library/a-systems-engineering-capability-maturity-model-version-11/.

Legacy systems

We used the following data to prepare this report:

- statement made by the Treasurer and the Minister for Customer Services and Open Data on 24 June 2025 about the $1 billion Queensland Government digital fund
- data collected by the Department of Customer Services, Open Data and Small and Family Business (CDSB) from most departments of at-risk systems (June 2025 and June 2026) and digital projects (from July 2013 to September 2026)
- our comparison of the at-risk systems reported with the list of systems used for our general IT controls testing for departments.

We have not audited the accuracy and completeness of the data we collected for at-risk systems and digital projects from CDSB.

C. Status of recommendations made in prior reports

The following table provides the current status of the issues raised in our prior reports.

Figure C1
Status of recommendations from *State entities 2023* (Report 11: 2023–24)

Manage the cyber security risks associated with services provided by third parties (all entities)		Status
REC 1	We recommend that all entities implement a process to manage the security risks relating to third-party services for information systems and technologies, and introduce procedures that will: • identify how they use third-party services, the extent to which they use them, and the associated security risks • establish due diligence (vetting and continuous monitoring) processes when engaging new third parties or continuing with third-party services • define security standards and the appropriate contractual agreements to manage security risks • establish a process to continually assess how well each third party manages its security risks and responds to and recovers from security incidents.	We consider the recommendations as closed as: • we have reported our observations to state entities that we audited • our report *Managing third-party cyber security risks* (Report 13: 2025–26) has also highlighted better practice approaches for identifying, assessing, monitoring, and managing third-party risks.

Source: Queensland Audit Office.

D. Focus areas for remediating IT control deficiencies

We encourage public sector entities and those charged with governance oversight responsibilities to consider the following questions to assess whether remediation plans are realistic and likely to deliver the intended outcomes. These questions also help audit committees determine whether remediation activities are reducing risk and strengthening controls.

Figure D1
Agency and audit committee focus areas

Area	Questions and actions for entities and audit committees
 **Agency focus** ➢ **Execution** ➢ **Delivery** ➢ **Ownership** ➢ **Operational effectiveness**	• Are findings prioritised based on risk and dependencies? • Have root causes been adequately addressed? • Are remediation milestones achievable and realistic? • Are delivery obstacles identified and managed? • Are interim controls reducing current risk exposure? • Are vendor dependencies actively managed? • Are remediation metrics demonstrating sufficient progress? • Have alternative remediation options been assessed? • Do accepted risks remain justified? • Are resources sufficient to deliver remediation? • Are overdue findings receiving executive attention? • What is preventing timely remediation closure?
 **Audit committee focus** ➢ **Oversight** ➢ **Assurance** ➢ **Sustainability** ➢ **Risk exposure** ➢ **Accountability**	• Will remediation sustainably address underlying risks? • Is the entity confident in delivery time frames? • How dependent is remediation on external factors? • Are delays increasing residual risk exposure? • Are interim controls operating effectively? • Is risk reduction proportionate to investment? • Are risks within appetite and tolerance? • What assurance supports remediation effectiveness? • Are recurring themes driving ageing findings? • Is additional intervention required for delivery? • Will residual risks remain after remediation? • Are remediation outcomes sustainable long term?

Source: Queensland Audit Office.

E. Using third-party assurance reports

Assurance reports enable governance and reduce waste

Entities remain accountable for their financial statements and the security of their information, even when a third party hosts their system or holds their data. Without an assurance report, entities have no independent evidence that the provider's controls work. The third party is audited once, and distributes the report to many of its customers, therefore reducing effort and costs for government services.

External auditors also need evidence that controls at service providers operate effectively. Assurance reports are the main way to obtain this evidence. When reports are missing, incomplete, or late, audits take longer and the auditor often has to complete alternate procedures. This means the entity pays its auditor to do work it has already paid the service provider to cover often leading to delays and additional costs.

Reports and certificates do not all provide the same assurance

ASAE 3402 reports are the base standard for financial reporting

ASAE 3402 reports cover a service provider's controls relevant to its customers' financial reporting. The service provider describes its controls. An independent auditor tests them and gives and opinion on them.

The Auditing and Assurance Standards Board issues Standard on Assurance Engagements ASAE 3402 *(Assurance Reports on Controls at a Service Organisation).* ISAE 3402 is the international equivalent, and System and Organization Controls 1 (SOC 1) is the United States equivalent. They are nearly identical. In practice, they serve the same purpose, and external auditors rely on them equally.

A Type 1 report covers whether controls are properly designed at a point in time. A Type 2 report also covers whether the controls operated effectively over a period, typically 6 months or 12 months. Auditors generally need a Type 2 report.

These reports are not public. Providers give them to their customers and their customers' auditors, usually when a contract requires it. They also often exclude the provider's own service providers; this is called a carve-out. For example, a report may exclude the data centre that physically hosts a system, even though the contract with the third party includes hosting services. The data centre controls are then not covered by the auditor's opinion.

SOC 2 reports cover security, not financial reporting

System and Organization Controls 2 (SOC 2) reports cover a provider's controls over security, availability, processing integrity, confidentiality, and privacy. They are useful for overseeing cyber security risks but are not designed for financial audit reliance. Many providers offer both SOC 1 and SOC 2 reports; they have some overlap but serve different purposes.

Certificates are not replacements for assurance reports

Certifications such as ISO 27001, which covers information security management systems, confirm that a provider's management system meets a standard at a point in time. A certificate does not describe the provider's individual controls, does not report the results of testing them, and does not give an opinion on whether they operated effectively over a period.

Certificates are a useful signal of a provider's security practices, but entities cannot rely on them in place of an assurance report. Auditors do not rely on these documents. Figure E1 provides an overview of the types of third-party reports used by entities.

Figure E1
Types of third-party reports

Report	What it covers	What it is useful for
ASAE3402 Type 2 (or ISAE 3402 / SOC1)	Controls relevant to customers' financial reporting, tested over a period	Third-party risk management Reliance by external auditors
SOC2	Controls over security, availability, processing, integrity, confidentiality, and privacy	Overseeing cyber security risks
Certificates (like ISO 27001)	Confirms a management system meets a standard's requirements at a point in time	A signal of the provider's practices at a point in time. Not a substitute for an assurance report.

Source: Queensland Audit Office.



Assurance reports and certifications are not interchangeable. Entities should match the report to the risk, system, control objective, and period it needs assurance over.

Entities need to obtain and review assurance reports

Entities can typically only obtain assurance reports if their contracts specify them.

Management should:

- when negotiating a contract – require the service provider to deliver an annual assurance report and specify the standard to be used (for example, ASAE 3402 Type 2), the scope, the period it must cover, and when the entity will receive it. Entities should obtain the assurance report, not just be given access to view it
- when renegotiating or renewing a contract – add an assurance report requirement if the current contract does not include it. Renewal is often the only practical opportunity to address this gap
- every year – obtain the assurance report and the check the period it covers aligns with the entity's financial year. Where there is a gap between the end of the report period and the end of the financial year, obtain a bridging letter from the provider or a Type I report at the period end date.

Management should review each report as part of good third-party risk management and governance. Management should check and document:

- whether the auditor is independent and reputable
- whether the scope covers the systems used by the entity
- scope exclusions (including carve-outs) and whether they need a separate report
- the auditor's opinion, including any qualifications
- exceptions found in testing, if any, and whether they affect the entity
- complementary user entity controls – these are controls the report assumes the entity performs itself, and the entity should confirm it performs them.

Entities should receive and review assurance reports in time for the auditor to review them, well ahead of when the financial statements are to be certified. Late reports delay the audit.

F. IT controls maturity assessment methodology

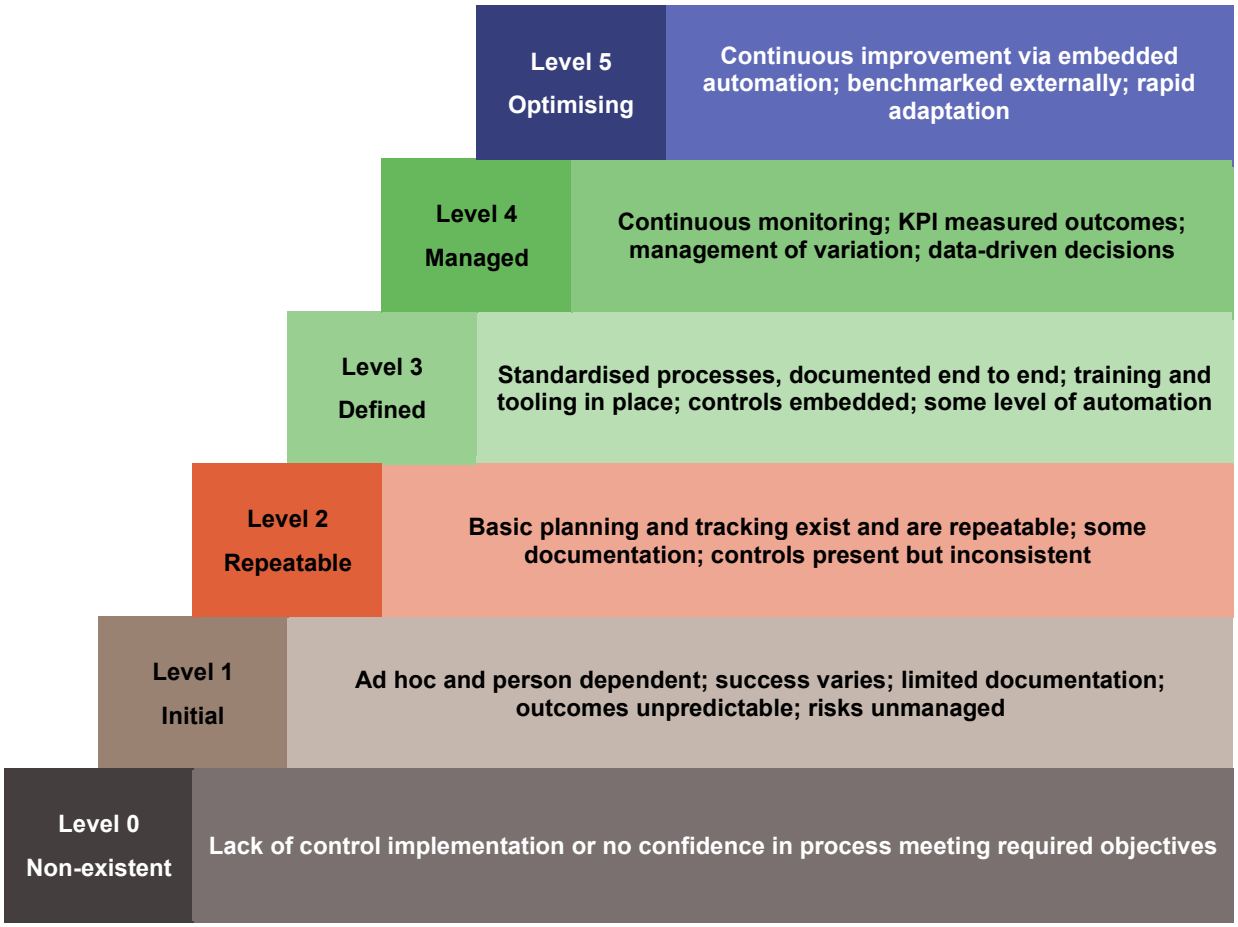
Our information technology (IT) controls maturity assessment methodology utilises the 5-level Capability Maturity Model (CMM) framework devised at Carnegie Mellon University in 1987.

The framework was originally designed to evaluate and improve software development processes used by Department of Defence contractors in the USA.

The CMM framework is now used by numerous organisations spanning different industries to assess and monitor maturity assessment of technical and non-technical processes.

Under the framework, control categories are assessed from being largely ad hoc and reactive (Level 1 – initial) to being continuously monitored, improved, and fully automated (Level 5 – optimising).

Figure F1
Capability Maturity Model (CMM) maturity levels



Source: Developed by Queensland Audit Office from the Carnegie Mellon University CMM framework.

The target maturity level for entities is Level 2 (repeatable), which represents a baseline or minimum expected level of maturity. At Level 2, IT control processes are established, and tasks are repeatable, however, process gaps, weaknesses, or errors may exist.

Level 3 (defined) represents a higher level of organisational maturity, in which processes are defined, documented, and standardised, with minimal gaps or errors existing.

Achieving Levels 4 (quantitatively managed) or 5 (optimising) represents leading practice, with extensive measurement, automation, predictive analytics, and continuous optimisation. Levels 4 and 5 generally require significant investment in technology, specialist capability, and organisational change. For most organisations, the costs and ongoing effort required to achieve and sustain these levels are unlikely to be proportionate to the associated reduction in risk.



qao.qld.gov.au/reports-resources/reports-parliament

qao.qld.gov.au/contact-us

T: (07) 3149 6000
E: qao@qao.qld.gov.au
W: www.qao.qld.gov.au
53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Queensland Audit Office
Better public services