New Zealand Government

# Assuring Digital Government Outcomes

## All-of-Government ICT Operations Assurance Framework

V3.1 October 2019

*Better information, better conversations, better decisions*

# Document History

| Version | Issue date | Description of changes |
|---|---|---|
| Version 1.0 | February 2014 | Initial version |
| Version 2.0 | May 2015 | Removed combined assurance plan template (Appendix E) and added Web link to updated template |
| Version 3.0 | July 2019 | Refresh of entire framework |
| Version 3.1 | October 2019 | Minor updates to reflect website updates to New Zealand's digital environment |

"a positive declaration intended to give confidence"

**Confidence**

Informative

Certainty

*"the goal of improving information or the context of information so that decision makers can make more informed, and presumably better, decisions"*

**Independence**

**"the comfort that can be derived from credible information"**

"an independent and objective oversight of the likely future performance of major investments for those responsible for sanctioning, financing or insuring such undertaking"

*Assurance* is the process of providing confidence to stakeholders that *an investment* will achieve their objectives, and realise their benefits.

AN OBJECTIVE EXAMINATION AND INDEPENDENT ASSESSMENT OF AN INVESTMENT INCLUDING RISKS, CONTROLS, PROCESSES, AND GOVERNANCE.

Credibility

# Table of Contents

# 1 Introduction

## 1.1 New Zealand's digital environment

We need to keep up with the current pace of digital evolution to maintain New Zealand's standing as a digital leader.

***"Digital government is about more than improving IT systems and processes. In the broadest sense, it means doing things differently in an increasingly connected world — using new mind-sets, skillsets, technologies and data to benefit people, government and the economy."***

The 2017 Digital Planet report[1], produced by The Fletcher School at Tufts University, places New Zealand among the world's digital elites – along with Singapore and the United Arab Emirates – with high levels of digital development and a fast rate of digital evolution.

The report ranked 60 countries on their digital competitiveness and market potential for further digital economic growth. It tracks the progress that countries have made since the first report in 2014 in developing their digital economies and providing integrated connectivity (the infrastructure that enables everyone to have an internet connection).

New Zealand is part of the Digital 9 (D9), a network of the world's most advanced digital nations with a track record for leading digital government transformation.

In subscribing to the charter developed by the D9, New Zealand is contributing to the shared goal of harnessing the potential global power of digital technology by helping each member to become an even better digital government through sharing and learning from each other.

Accelerating New Zealand's government digital transformation will help people:

- Access personalised services when, how and where they need them
- Engage in decisions about the issues they care about
- Trust in an open, transparent and inclusive government.

## 1.2 Role of the System Assurance team

The System Assurance team works collaboratively with government organisations to lift risk management and assurance capability.

"***We provide Ministers, the Government Chief Digital Officer (GCDO) and other key stakeholders with confidence that the system of assurance supporting digital government outcomes is effective."***

[1] https://www.digital.govt.nz/news/new-zealands-digital-economy-a-standout-among-standouts/

We do this by:

- Publishing government's formal assurance frameworks and guidance
- Providing independent assurance oversight over high risk digital investments
- Providing independent assurance oversight over how well government organisations are managing their ICT risks
- Managing a panel of third-party assurance providers giving government organisations access to highly qualified providers of assurance services
- Sharing lessons learned and good practice examples to help government organisations to work smarter
- Managing the government online Self-Assessment Tool which enables government organisations to assess their current level of risk maturity and identify ways they can improve
- Providing strategic advice on system-wide risks, capabilities and settings.

## 1.3 The system of assurance

The system of assurance comprises the frameworks, processes, monitoring, capability and culture that, when operating effectively, give stakeholders confidence (assurance) that digital government investments will deliver the right things in the right way to realise the expected benefits.


The system of assurance includes:

- Government organisations and their delivery partners
- Central agencies and functional leads, including the GCDO
- Third-party assurance providers.

Our vision is:

***"A valued system of assurance that delivers high levels of trust and confidence in digital public services in New Zealand."***

As part of a valued system of assurance, we contribute to the following outcomes:

- Improved governance and decision-making as a result of high quality assurance information provided at the right time
- Improved confidence that digital investments and ICT risks are well managed and will deliver the expected outcomes and benefits
- Improved business resilience and management of risk as a result of greater visibility of system-wide risks.

## 1.4 ICT assurance landscape

There have been several changes in the assurance landscape since the original ICT Operations Assurance Framework was published in 2014. There is now an established network of functional leads that look after specific areas of ICT risk. Working together, they operate as a multi-functional group, using their shared expertise to advise Ministers and government organisations on how to improve the management of ICT risk across the State services.

The following functional leads are the most relevant to ICT assurance and further detail on how to engage with them can be found using the links below:

- Investment Management and Asset Performance[2] (IMAP) team, The Treasury
- Protective Security Requirements[3] (PSR)
- Government Chief Information Security Officer[4] (GCISO)
- Government Chief Privacy Officer[5] (GCPO)
- New Zealand Government Procurement and Property team[6] (NZGPP), Ministry of Business, Innovation & Employment (MBIE).

[2] https://treasury.govt.nz/information-and-services/state-sector-leadership/investment-management/review-investment-reviews/about-imap-team
[3] https://protectivesecurity.govt.nz/
[4] https://www.gcsb.govt.nz/our-work/government-chief-information-security-officer-gciso/
[5] https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/
[6] https://www.procurement.govt.nz/

# 2 Digital Assurance Roadmap

Government organisations are increasingly dependent on technology to deliver public services. The traditional ICT function is also changing to support new ways of working, including a shift towards continuous delivery through Agile/DevOps approaches.

Now more than ever, managing ICT risk requires a well-coordinated, integrated approach that prioritises understanding the business impacts of ICT risk. Integrated ICT risk management means that government organisations are in a better position to achieve their strategic business outcomes as well as to create opportunities to exceed them.

Government organisations face several challenges to digital transformation:

- A lack of a strategic, portfolio level view of ICT investment, which makes it more difficult to know if the business is investing in the right things. This includes knowing where there might be opportunities to collaborate with other government organisations to deliver improved services.
- Legacy ICT assets that are operating beyond their intended use are now an organisational constraint in the transition to a digital operating model, not just from an investment perspective but also from an ongoing cost challenge. This is because legacy assets are costlier to support, maintain and provide operational assurance over.
- Understanding the risks and opportunities presented by new and emerging technologies, such as cloud computing, artificial intelligence (AI), blockchain and machine learning, as well as increasing reliance on complex data analytics.
- Developing digital skills and capabilities, including attracting digital talent, to support the transition to a digital operating model while at the same time continuing to manage legacy ICT operations.

These challenges require a strategic risk management focus. While government organisations need to continue to manage their day-to-day ICT operational risks, they must also identify, manage and govern the risks arising from digital transformation.

This strategic focus is reflected in the GCDO's shift from a 'pure' ICT operations assurance focus to a broader digital assurance focus that provides Ministers and other key stakeholders with confidence that government organisations have the right skills and capabilities to manage the transition to a digital operating model. Achieving an appropriate level of digital maturity is a key enabler of the Digital Government Strategy.

Lifting digital capability to enable government organisations to successfully undertake digital transformation is the foundation of our Digital Assurance Roadmap. The roadmap sets out how the GCDO's independent assurance oversight role is changing. It supports moving to a more informed evidence-based assurance approach. This will provide greater value to government organisations and the system of assurance that supports digital government outcomes. For example, it will inform investment decisions and provide system insights to improve business resilience and the management of ICT risks.

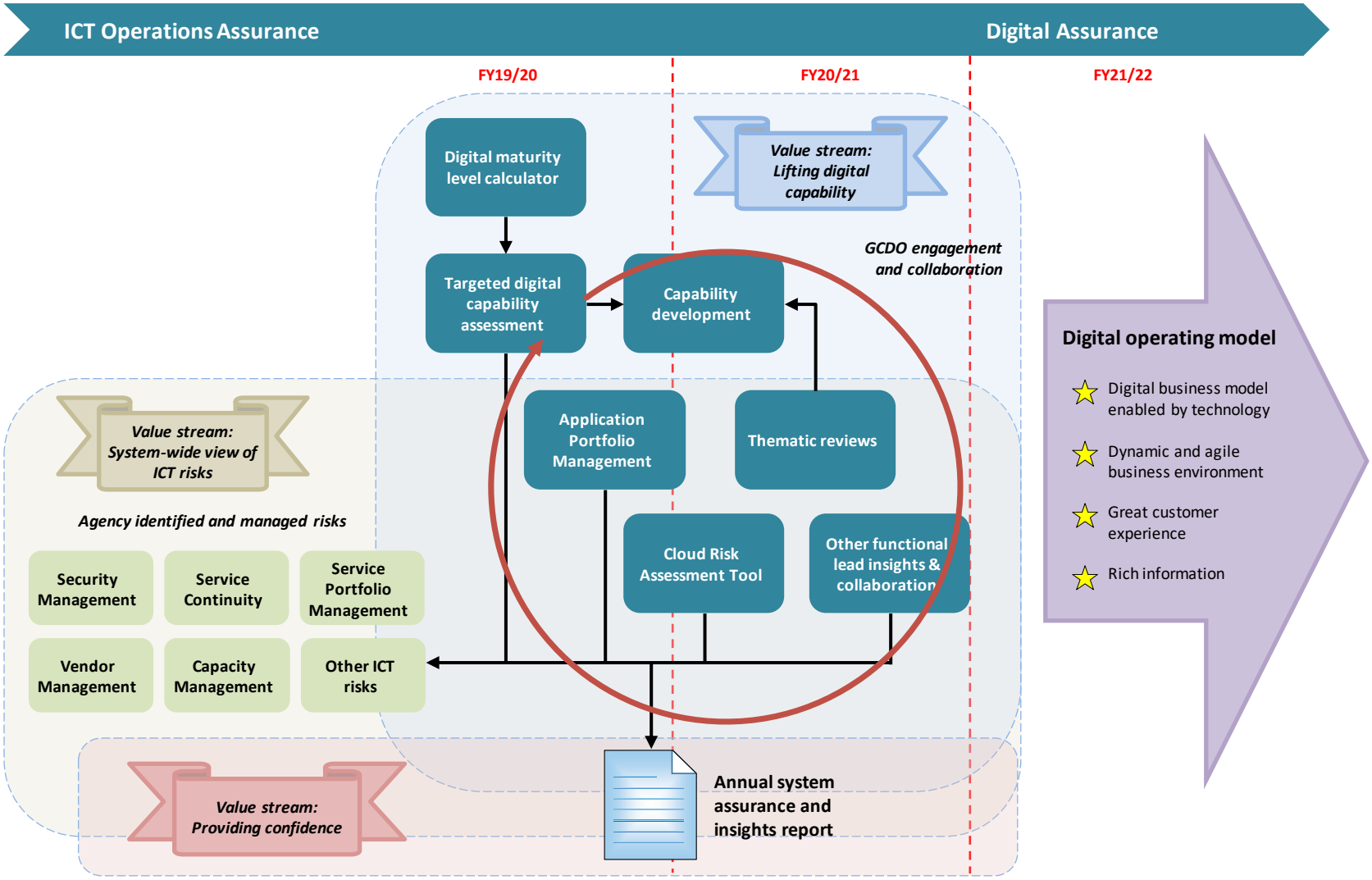


*Figure 1: Digital Assurance Roadmap*

To successfully deliver the Digital Assurance Roadmap, the System Assurance team will need to become digital itself and look at how we can use technology to help government organisations better manage the risks they face. We are developing new ways of working so that we are more integrated, automated and data-driven in our independent assurance oversight role and the insights we provide to government organisations.

Embedding good risk management and assurance practices into your ICT operations continues to be a core expectation of government organisations in order to provide confidence to your Chief Executive that ICT risks are being managed effectively (refer to 4.8 Core expectations of government organisations). This expectation defines the scope of this current version of the ICT Operations Assurance Framework.

We plan to transition to a Digital Assurance Framework by 30 June 2022.

# 3 Value of assurance

## 3.1 Improving ICT portfolio management

***Case study – Ministry of Business, Innovation and Employment (MBIE)***

*MBIE plays a central role in shaping and delivering a strong New Zealand economy. Its diverse business units are supported by a complex ICT landscape, including legacy systems.*

*The ICT leadership team faced the challenge of a large number of low-level risk statements that added to the confusion between issues and risks. To help support better risk conversations at leadership/management levels, the team adopted a portfolio approach to risk management that focused on risk expressed as a 'top event' rather than numerous risk causes with the same result. Control assurance considers control effectiveness creating opportunities for improved management insight.*

***Mark Brown – Acting CIO***

*"Risk management is viewed as a management activity no different from budgeting, recruiting or communicating. We plan an annual programme of risk reviews and assurance activity that drives better risk conversations and managerial decisions. Risk informs our activity choices and frequently provides the rationale for prioritisation."*

Strategic risk management and assurance are critical components of ICT portfolio management enabling government organisations to make risk-informed investment decisions.

Often there is a disconnect between the business and ICT which means that executives and ICT governance bodies don't understand the business impacts of ICT risks or the opportunities they might present to improve business performance.

Lifting the conversation to a strategic, portfolio view of ICT investment can help the business and ICT to develop a shared view of ICT risk with a focus on business outcomes.

This shared understanding enables better conversations about critical ICT risks, including the challenges of moving to a digital operating model, and how to manage them to acceptable levels based on the organisation's risk appetite. This includes balancing the costs and benefits of managing ICT risk. In this way, assurance can help inform future investment decisions in people, process, data and technology to achieve business outcomes.

## 3.2 Improving service delivery

Assurance can help improve service delivery by identifying opportunities for improvement.

It is easy to get caught up in the day-to-day activity of providing services to customers. Assurance provides an objective and evidenced-based view of the likelihood of key ICT risks occurring and their potential impact on service delivery. In this way, assurance can help identify the areas of greatest risk to service delivery and ensure adequate arrangements are in place should they arise.

Assurance can also help identify the root causes of key ICT risks and ensure actions appropriately address these. For example, opportunities for improvement may include lifting capabilities in people and processes, the lack of which are often at the heart of ICT risk failures.

## 3.3 Improving risk ownership

### *Case study – Ministry of Social Development (MSD)*

*The MSD ICT environment is complex with more than 440 different applications/tools/technologies in various stages of their lifecycles that deliver business services to more than 1 million MSD clients, partners and non-government organisations (NGOs) and 10,000 internal users. Gaining and maintaining assurance over ICT risks is key to ensuring that services are available and up to standard throughout the product and technology lifecycles.*

### *Paul Weyers – Manager IT Performance & Risk*

*"Recording our ICT operational risks in a single authoritative repository enables a clear view of MSD's ICT risk landscape. This also enables us to assign clear accountability and ownership for control over technical risk back into the business. This supports more informed decision-making and investment decisions."*

Assurance can help improve business ownership of key ICT risks by clarifying goals and objectives for how ICT supports business outcomes. Every ICT system should have a Business Owner who is accountable for ensuring ICT systems are fit-for-purpose based on the business outcomes they support. This includes obtaining assurance over the effective operation of ICT systems.

Engaging with Business Owners to understand their key ICT risks, potential business impacts and assurance needs, enables better management of ICT risks and improves business performance. Improving risk ownership also enables better management of changes to ICT systems, as Business Owners engage early to assess the likelihood and impact of future changes on business outcomes.

## 3.4 More efficient use of resources

Assurance can help prioritise resources by identifying areas that are overcontrolled and redirecting resources to those areas of greatest risk and value.

For example, developing an integrated risk-based assurance plan can help government organisations gain a better understanding of the roles and the scope of work that is undertaken by both internal and external assurance providers. In this way, an assurance plan may identify overlaps in assurance activities which could be combined or better coordinated to improve the overall efficiency and effectiveness of the assurance process.

It also helps to reduce the compliance burden on delivery teams and to maximise value for money. This is becoming increasingly important as government organisations are expected to do more with less resources.

### *Case study – Department of Internal Affairs*

*In 2017/18 Government Information Services (GIS) adopted a coordinated approach to complete security assessments across the GIS portfolio, which provides products for All-of-Government. In the past each product was managed independently. The team started by identifying which products required certification in the current year. They then consolidated these products into a single certification exercise, preparing a pack of refreshed artefacts for Certification team (vendor).*

### *Christine Bennett – General Manager*

*"While the process took a little longer than initially planned, GIS was able to significantly reduce the cost of certification. Now that we better understand the process, we plan to make the upkeep of all related artefacts across the entire portfolio a priority, further reducing the time and cost involved. These artefacts also feed into continuity planning helping us to further reduce our risk footprint."*

# 4 Overview of framework

## 4.1 Purpose

The purpose of the All-of-Government (AoG) ICT Operations Assurance Framework is to support government organisations to implement a fit-for-purpose assurance approach for managing their ICT risks.

***"Effective assurance provides confidence to your Chief Executive and other key stakeholders, including Ministers, that ICT risks are effectively managed to achieve business outcomes."***

The framework is supported by detailed guidance and templates to help you apply the principles of good assurance. Links to the guidance can be found at the end of this document.

## 4.2 Audience

The target audience for the framework is:

- Business Owners and ICT governance bodies
- Chief Information Officers (CIOs) and Chief Digital Officers (CDOs)
- ICT leadership teams
- Internal Audit functions
- Security and risk practitioners.

## 4.3 Our definition of assurance

***"An independent and objective assessment that provides credible information to support decision-making."***

The key words in our definition are 'independent and objective'. There are varying degrees of independence and objectivity, but assurance is most effective when integrated across all 'three lines of defence.'

## 4.4 Three lines of defence model

- The **first line of defence** is the day-to-day operational management processes and controls you have in place for identifying and managing ICT risks. This includes business management and line managers who are responsible for the design and implementation of business processes and controls.

- The **second line of defence** is the governance and oversight arrangements that exist for ongoing monitoring of ICT risks. This includes oversight functions who provide advice and guidance to ensure that correct organisational settings are in place to manage risk e.g. Finance, Human Resources, Procurement, Security and Risk, Privacy, etc.
- The **third line of defence** is the independent assurance you obtain from Internal Audit and third-party assurance providers, including External Audit, that ICT risks are effectively managed.

The focus of our framework is on assurance that is performed by competent and impartial people outside of the ICT operations team (i.e. at the second and third lines of defence). Examples of assurance activities within the scope of our framework include:

- Regular governance and oversight activities e.g. governance meetings, executive reporting, Audit and Risk Committee oversight
- Regular reporting to the ICT Leadership team
- Risk reviews performed by an internal Security and Risk function
- Internal audit reviews
- Third-party assurance reviews
- Annual external audits.

## 4.5 Applicable government organisations

The framework is mandated for the following government organisations:

- Public service departments
- Non-public service departments
- District health boards
- Certain crown entities (ACC, EQC, NZQA, NZTA, HNZC, NZTE, TEC).

**Note:** The framework is not limited to the above government organisations. It can be used by any government or private sector organisation as a guide to good assurance practice to support improved business resilience and the management of ICT risks to grow New Zealand's economy and enhance the wellbeing of its people.

## 4.6 Applicable risks

The framework applies to all ICT risks.

As a guiding principle:

***"ICT risk refers to the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within the department[7]."***

The term 'ICT risk' is used here to mean both traditional ICT operational risk as well as new and emerging risk from adopting digital technologies.

Based on a survey[8] conducted by the GCDO, the top five ICT risks faced by government organisations are:

- Information security
- Service continuity
- Service portfolio management, including legacy ICT risk
- Vendor management
- Capacity management, including resource capacity and capability constraints.

This list is not exhaustive, and while the technology landscape may change, with increasing use of digital technologies, our experience is that these risks are enduring. However, as government organisations begin to digitally transform, new risks are emerging related to new ways of working and attracting digital talent.

Refer to our ICT Risk Management Guidance[9] for an example of an ICT risk universe that will help you identify other ICT risks.

## 4.7 GCDO system-wide assurance oversight role

The GCDO has a core responsibility to provide Ministers and other key stakeholders with confidence that the system of assurance supporting digital government outcomes is effective. To enable the GCDO to fulfil this responsibility, the System Assurance team has an independent assurance oversight role to ensure government organisations are managing their ICT risks effectively.

We work closely with government organisations to make sure they:

- Manage the health of their critical business applications and ICT infrastructure
- Have the right skills and capabilities to manage their ICT risks, including the transition to a digital operating model

[7] Queensland Government Chief Information Office

[8] https://www.digital.govt.nz/dmsdocument/124-gcio-top-5-ict-risks-march-2014-pdf

[9] https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-ict-operations-assurance-framework/ict-risk-management-guidance

- Follow ICT risk management and assurance good practice, including the GCDO's guidance for information security[10] and using cloud services[11]
- Understand new and emerging risks in a digital world and what good risk management and assurance looks like.

The Digital Assurance Roadmap sets out how we now intend to engage with government organisations to provide independent assurance oversight. Our approach will enable us to be more flexible and responsive, so we can be more effective in helping government organisations meet the challenges of digital transformation.

## 4.8 Core expectations of government organisations

The following core expectations apply to all government organisations:

- Key ICT risks and controls are identified and regularly reviewed by the ICT Leadership team e.g. on a quarterly basis.
- Top ICT risks (i.e. those rated Critical or High) are escalated and monitored by the Executive Leadership team (ELT).
- An integrated assurance plan exists for key ICT risks which is approved annually by the Chief Executive and/or an appropriate ICT governance body.
- Cloud Risk Assessments and related Cloud Endorsement by Agency are submitted to the GCDO.
- Where appropriate, the GCDO Security and Related Services Panel and/or the GCDO Assurance Services Panel[12] is used for third-party assurance reviews.
- Government organisations will respond to requests for specific information to enable the GCDO to fulfil its independent assurance oversight role in line with the Digital Assurance Roadmap.

[10] https://www.ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/

[11] https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/

[12] https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/gcdo-assurance-services-panel/

# 5 Applying the principles of good assurance to ICT operations

The System Assurance team has developed a set of principles for good assurance practice based on our lessons learned. When applied, these principles support good practice assurance planning.


*Figure 2: Principles of good assurance*

In moving to a principles-based framework, assurance becomes less about compliance and more about demonstrating good assurance thinking based on a clear understanding of ICT risks and their potential impacts on business outcomes.

The principles should be tailored to enable a fit-for-purpose assurance approach based on the risk and complexity of your organisation's ICT operation.

***"A principles-based approach provides confidence in the delivery of business outcomes without resulting in excessive levels of assurance."***

## 5.1 Assurance by design

***"Assurance is not a one-time activity. It's the way we do things here…"***

- Budget for assurance activities over the areas of greatest risk to service delivery.
- Ensure assurance is integrated and operating effectively across all 'three lines of defence':
    - The **first line of defence** is the day-to-day operational management processes and controls you have in place for identifying and managing ICT risks
    - The **second line of defence** is the governance and oversight arrangements that exist for ongoing monitoring of ICT risks
    - The **third line of defence** is the independent assurance you obtain from Internal Audit and third-party assurance providers, including External Audit, that ICT risks are effectively managed.
- Analyse the root causes of ICT risks and issues, implement responses and incorporate them into the assurance plan and approach going forward.
- Undertake risk assessments when designing new systems, processes and policy, including for core delivery partner activities.
- Adopt data-driven approaches to risk management and assurance e.g. continuous auditing and monitoring techniques based on operational management processes and data.

## 5.2 Flexible

***"Assurance is adaptable to meet changes in the operating environment, service delivery approach, or risk profile."***

- Regularly review the operating environment, both internal and external, to ensure risks remain current and that any significant changes trigger a review of the assurance plan.
- Tailor assurance to the service delivery approach e.g. continuous delivery through Agile/DevOps approaches require greater reliance on assurance activities embedded into day-to-day operations.
- Ensure assurance extends beyond the boundaries of your organisation to include key dependencies on core delivery partners, cloud providers and shared platforms that support inter-agency, sector or AoG outcomes.
- Establish metrics to monitor key ICT risks and, where possible, integrate into existing Key Performance Indicators to provide early warning of changes to the risk profile.
- Use the results of assurance activities to inform the forward assurance plan.

## 5.3 Informs key decisions

***"Assurance provides timely, credible information to inform key decisions."***

- Ensure there is a clear relationship between planned assurance activities and key decisions. For example:
    - Obtain assurance for business cases for all significant ICT investment decisions
    - Perform due diligence on new vendors to identify risks to delivery, such as capacity, capability, over-reliance on key people, and location of vendor (offshore, onshore)
    - Make sure reviews performed at project handover include ICT operational readiness and acceptance of residual risks.
- Be clear about the purpose of assurance reviews; avoid a long list of objectives and ensure terms of reference are framed around specific areas of concern, including those raised by key stakeholders.
- Consider the organisation's risk appetite when making key decisions, i.e. the amount of risk an organisation is willing to accept in the pursuit its of business objectives and outcomes.
- Formalise the process for integrating ICT risk management into the strategic planning process, including capturing risks that threaten the achievement of strategic business outcomes.

## 5.4 Risk and outcomes-based

***"Assurance assesses the risks to successful service delivery and their impact on business outcomes."***

- Ensure assurance is risk-based, i.e. there is a clear link between planned assurance activities and key ICT risks, including:
    - Information security
    - Service continuity
    - Service portfolio management, including legacy ICT risk
    - Vendor management
    - Capacity management, including resource capacity and capability constraints.
- Engage with Business Owners to ensure they understand their key ICT risks, potential business impacts and assurance needs.
- For top ICT risks (i.e. those rated Critical or High), conduct a deep dive analysis to embed accountability and gain a better understanding of the nature and scope of the risk as well as the sources and strength of controls and assurance activities.
- The ICT Leadership team regularly reviews top risks to ensure they are being managed in accordance with the organisation's risk tolerance level.

## 5.5 Independent and impartial

***"Assurance is performed by competent people independent of the operation of the process or control who are not unduly influenced by key stakeholders."***

- Proactively engage oversight functions such as Finance, Human Resources, Procurement, Security and Risk, and Privacy teams to ensure assurance activities are fit-for-purpose and timely.
- Ensure that third-party assurance providers have the right skills and experience for the risk and complexity of your organisation's ICT operation.
- Follow formal procurement processes to engage third-party assurance providers. Where appropriate, the GCDO Security and Related Services Panel and/or the GCDO Assurance Services Panel should be used for third-party assurance reviews.
- Ensure any conflicts of interest are clearly identified and managed, including:
    - Ensuring personal relationships between government organisations and providers don't threaten independence and objectivity
    - Performing an assurance review where the provider has or is currently providing design or implementation services for the process or controls under review
    - Fixing issues identified during course of an assurance review.

## 5.6 Accountability

***"Risk management and assurance roles and responsibilities at the governance level are clearly understood."***

- Clearly document ICT risk management and assurance roles and responsibilities in role descriptions and/or ICT governance body terms of reference.
- Establish a formal process for risk acceptance and escalation to ensure ICT risks are managed and owned at the right level within the organisation.
- Ensure top ICT risks are escalated and monitored by the Executive Leadership Team.
- Ensure an integrated assurance plan exists for key ICT risks which is approved annually by the Chief Executive and/or an appropriate ICT governance body.
- The ICT Leadership team regularly reviews the assurance plan to ensure it continues to be fit-for-purpose and that the agreed assurance activities are undertaken.
- The ICT Leadership team regularly reviews the status of issues raised in assurance reports.



# 6 Engaging with us

While the GCDO no longer requires government organisations to submit their annual assurance plan to the System Assurance team, we are happy to provide advice to support government organisations in managing their ICT risks. We encourage you to contact us if there has been a significant change in your ICT operations or key leadership roles.

## 6.1 Digital Assurance Roadmap tailored engagement

As we roll out the Digital Assurance Roadmap, it will help us to understand how much collaboration and engagement we will need to have with government organisations. For each initiative, we will develop a tailored engagement approach in consultation with government organisations.

If we require additional information from government organisations to enable our independent assurance oversight role, we make the purpose and value of the data collection clear to you and, where possible, we will use existing data sources.

## 6.2 How to contact us

The System Assurance team can be contacted for ICT risk management and assurance queries, advice and guidance at systemassurance@dia.govt.nz

# Guidance and Templates

1

**Managing your ICT risks**

These resources will help you to design and implement a risk management process that enables key ICT risks to be effectively identified, managed and governed:

- **ICT risk management guidance:** https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-ict-operations-assurance-framework/ict-risk-management-guidance
- **Risk register template:** https://www.digital.govt.nz/dmsdocument/122-risk-register-template-xlsx
- **Heat map template:** https://www.digital.govt.nz/dmsdocument/137-heat-map-template-pptx
- **GCDO ICT Risk Survey:** https://www.digital.govt.nz/dmsdocument/124-gcio-top-5-ict-risks-march-2014-pdf

2

**Developing your assurance plan**

These resources will help you to develop a fit-for-purpose assurance plan based the risk and complexity of your organisation's ICT operation:

- **Principles of good assurance and lessons learned for ICT operations pocket guide:** https://www.digital.govt.nz/dmsdocument/136-principles-of-assurance-and-lessons-learned-ict-ops-pg-pdf
- **ICT operations assurance plan quality review checklist:** https://www.digital.govt.nz/dmsdocument/146-ict-ops-assurance-plan-quality-review-checklist-docx
- **ICT operations assurance plan template:** https://www.digital.govt.nz/dmsdocument/132-assurance-plan-template-docx

3

**Maximising the value of independent assurance**

These resources will help you to create a comprehensive engagement terms of reference for an independent assurance review, and select the right provider with the right experience to deliver a high quality review:

- **GCDO Panel pocket guide:** https://www.digital.govt.nz/dmsdocument/90-gcdo-assurance-services-panel-pocket-guide
- **GCDO assurance services guide:** https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/gcdo-assurance-services-panel/assurance-report-executive-summaries/gcdo-assurance-services-guide/
- **ICT operations terms of reference quality review checklist:** https://www.digital.govt.nz/dmsdocument/138-ict-ops-terms-of-reference-quality-review-checklist-docx
- **ICT operations terms of reference template:** https://www.digital.govt.nz/dmsdocument/133-terms-of-reference-template-docx

4

**Ensuring high quality assurance information**

The quality of assurance reports is critical to make well informed decisions. Use this resource to review the quality of assurance reports:

- **ICT operations assurance report quality review checklist:** https://www.digital.govt.nz/dmsdocument/139-ict-ops-assurance-report-quality-review-checklist-docx

5

**Overseeing assurance activities and recommendations**

Consider:

- How will progress against the assurance plan be monitored at the governance level?
- How will the status of issues raised in assurance reports be tracked and reported at the governance level?

6

**Capturing lessons learned**

We would like you to share your ICT risk management and assurance lessons learned with us to help inform a system-wide view of trends and share examples of working 'smarter' for other government organisations to use.

If you are keen to share your lessons learned, contact us at systemassurance@dia.govt.nz

# Glossary of abbreviations and terms

| Term or Abbreviation | Definition |
|---|---|
| Business Owner | A Business Owner is responsible for making sure any ICT system they own is fit-for-purpose based on the business outcomes they support. |
| Functional lead | Functional leads are assigned by the State Services Leadership Team to chief executives to drive performance across the state services in functional areas such as policy, finance, data and analytics, communications, procurement, digital, property, human resources, health and safety, legal, and investment management and asset performance. |
| ICT governance body | A governance body that oversees the overall direction of ICT and ensures that ICT risks are effectively managed. |
| Risk appetite | Risk appetite is a high-level (usually narrative) expression of the amount and type of risk that an organisation is willing to take in the pursuit of its business objectives and outcomes. |
| Three lines of defence model | The three lines of defence model is used as a clear and effective way to strengthen communications on risk management, assurance, and control by clarifying essential roles and duties for various parts of governance, management, and day-to-day operations. |