Principles of good assurance and lessons learned for 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 government organisations with good practice assurance planning.

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."

Government Chief Digital Officer System Assurance Team

New Zealand Government

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 get from Internal Audit and third party assurance providers, including External Audit, that ICT risks are effectively managed.
- Analyse the root cause 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.

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 capabilities 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.

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 of its 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.

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 the top risks to make sure they are being managed in accordance with the organisation's risk tolerance level.

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 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, use the GCDO Security and Related Services Panel and/or the GCDO Assurance Services Panel 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 is currently providing design or implementation services for the processes or controls under review
  - » Fixing issues identified during course of an assurance review.

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.

Contact us

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

Additional guidance and templates can be found on the GCDO's website: bit.ly/2ZQCCbo

Information on the GCDO Assurance Services Panel can be found on the GCDO's website: bit.ly/2FCsxaC