Connect › Support › Advance

The Institute of Internal Auditors Australia

# Factsheet: ICT Governance and Assurance

**Updated 2020**

## ICT governance

### What is ICT?

The definition ICT is a term used to holistically include information, communication, and technology (ICT) related matters within an organisation. It is sometimes used interchangeably with more simply the abbreviation IT (information technology).

### What is ICT governance?

Australian Standard 8015 'Corporate governance of information and communication technology' defines ICT governance as:

> *"The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation."*

Australian Standard 8015 was the precursor to international standard ISO 38500 'Corporate governance of information technology'.

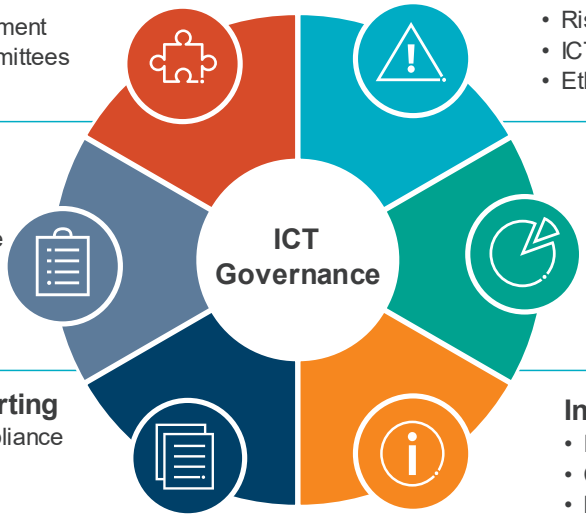
The primary outcomes of effective ICT governance include:

- ICT strategies are aligned with organisation objectives.
- Risks are identified and managed properly.
- ICT investments are optimised to deliver value to the organisation.
- ICT performance is defined, measured, and reported using meaningful metrics.
- ICT resources are managed effectively.

- **ICT Strategic Management** includes a number of governance elements, including implementation of an ICT plan by the chief information officer (CIO) to help ICT contribute to the organisation achieving its objectives. The ICT plan needs to clearly align with the organisation's vision and strategic objectives.
- **Risk Management** is anticipating and managing risks that may have an impact on ICT.

### ICT Strategic Management
- ICT committee
- ICT strategic objectives
- ICT planning
- Performance management
- Governance and committees
- Learning

### Risk Management
- Risk management
- ICT disaster recovery
- Ethical behaviour




### Assurance
- Audit committee
- Project management office
- ICT assurance activities
- Internal audit

### Resource Management
- ICT operations
- Financial management
- Human resource management
- Vendor and contractor management
- Asset and infrastructure management
- ICT project management

### Compliance and Reporting
- Legal and regulatory compliance
- Policy compliance
- Privacy
- Management reporting

### Information Management
- Information management
- Cyber-security
- Data integrity and quality

- **Resource Management** is the efficient and effective use of resources when they are needed for ICT to achieve its objectives. It needs to include focus on vendors, contractors and projects contributing to achievement of ICT objectives. Organisations formally performance manage ICT staff, yet the same does not always apply to contractors and consultants.
- **Information Management** refers to the collection, recording, processing, securing and distribution of information throughout an organisation that is essential for assisting management to make informed decisions. ICT plays a key role with cyber-security, data integrity, quality and information management.
- **Compliance and Reporting** – It is important for ICT to comply with laws, regulations, policies and privacy requirements to show it is ethical and information is secure. ICT reporting needs to be useful to management and aid effective decision-making.
- **Assurance** comprises evaluations of ICT systems, processes, operations, projects, and services. It determines the validity and reliability of information and helps improve ICT effectiveness and accountability.

### Why is an ICT plan important?

Many CIOs seem to believe they do not need a formal plan to manage ICT within an organisation. While it is true that long-term ICT plans tend to be a thing of the past due to changing business environments and rapid technology advancements, including digital disruption, for an organisation to commit large funds to ICT, especially projects, without a coherent justification plan, is surely poor management. An ICT plan may be shorter-term, but should contain such things as:

- Table of contents
- Introduction
- Purpose of the plan
- Organisation profile
- Strategic organisation objectives
- Strategic ICT objectives
- Alignment to organisation vision and objectives
- Role of ICT committee
- Current ICT environment
- Drivers of ICT change
- Current and future issues to be addressed
- ICT environment gap analysis:
  - Industry standards
  - Current environment
  - Gap
- Proposed improvement actions, responsibilities and timings
- ICT strategies
- ICT replacement and upgrade
- ICT resourcing
- Current and future ICT projects
- Current and future ICT costs
- Service standards and performance measures
- Appendices:
  - Glossary
  - Current state ICT environment
  - Future state ICT environment
  - ICT risk assessment
  - ICT Committee terms of reference
  - List of ICT vendors and contracts
  - Supporting references
  - Discussions and workshops

## ICT assurance

### What is ICT assurance?

Assurance is a positive declaration intended to give confidence designed to improve the quality of information to aid informed decision-making.

Organisations and business units have a range of assurance activities, which are often identified as the 3 lines of defence, plus external assurance mechanisms. Ideally, all assurance activities should be visible to senior management and the audit committee.

### What is ICT 3 lines of defence?

Organisations have a range of activities to provide assurance to the audit committee, chief executive officer and senior management.

An ICT 3 lines of defence combined assurance model defines the ICT assurance environment:

- The 1st line of defence originates or initiates risk, and owns those risks; it needs to have mechanisms in place to demonstrate controls are working effectively.
- The 2nd line of defence monitors, reviews and tests effectiveness of 1st line control and management of risks.
- The 3rd line of defence independently evaluates and gives an opinion on the adequacy and effectiveness of both 1st line and 2nd line risk management approaches.

This approach demonstrates how assurance activities co-ordinate to provide assurance. It needs to be considered that, if 2nd line of defence assurance activities are strong, there may be a case for less internal audit. Likewise, if 2nd line of defence assurance activities are weak, more internal audit may be necessary. This can be illustrated as:

The Institute of Internal Auditors Australia

| ICT 3 lines of defence | | | |
|---|---|---|---|
| 1st line of defence | 2nd line of defence | 3rd line of defence | External assurance |
| Own and manage risk | Monitor risk | Assure risk is managed | External risk oversight |
| Real-time focus | Real-time focus and review of 1st line | Review of 1st line and 2nd line | Review of all 3 lines of defence |
| Review compliance and implement improvements | Confirm compliance and recommend improvements | Recommend improvements | Direct improvements be implemented |
| *Organisation*<br>- Organisation internal control framework.<br>- Project management methodology and controls. | *Organisation*<br>- Organisation corporate governance.<br>- Business continuity and business impact analysis.<br>- Project management office.<br>- Corporate quality management. | *Organisation*<br>- Audit committee.<br>- Internal audit.<br>- Continuous auditing. | *External*<br>- External auditor.<br>- Regulators. |
| *ICT*<br>- ICT internal control framework.<br>- ICT policies and procedures.<br>- ICT management controls.<br>- System controls.<br>- Change and release management.<br>- Project management methodology and controls. | *ICT*<br>- ICT committee.<br>- Performance reporting.<br>-Risk registers.<br>- ICT security.<br>- Network security.<br>- Cyber-security and penetration testing.<br>- Technical compliance.<br>- Disaster recovery and testing.<br>- ICT Project management office.<br>- Data analytics and continuous monitoring.<br>- Quality management. | | |

**Why have an ICT assurance strategy?**

The purpose of an ICT assurance strategy is to:

- Assess assurance coverage against key ICT strategies, risks and assurance requirements.
- Ensure there are comprehensive ICT governance and assurance arrangements in place.
- Minimise duplication of effort.
- Identify assurance gaps.
- Minimise assurance cost.
- Provide comfort to stakeholders about the level of ICT assurance.
- Help to understand where ICT governance and assurance roles and accountabilities reside.
- Identify skills required to deliver necessary assurance as a guide to resourcing.

Key components of an ICT assurance strategy would be:

- ICT 3 lines of defence combined assurance model, showing assurance activities.
- An ICT assurance map to assess effectiveness of the 3 lines of defence, and identify where improvements can be made.
- ICT assurance activities that assign responsibilities for assurance activities to improve the control environment – these may be 1st line or 2nd line assurance activities, or 3rd line audit services from internal audit.
- Providing assurance on such things as project delivery and ICT security roadmap implementation.

**What might an ICT assurance strategy look like?**

An ICT assurance strategy identifies the ICT 3 lines of defence and rates its effectiveness. It results in a plan to improve assurance across all lines of defence, from where the work is done through to review activities such as internal audit.

| ICT assurance strategy approach | |
|---|---|
| 1 | Identify ICT 3 lines of defence and rate effectiveness |
| 2 | Prepare ICT assurance map |
| 3 | Validate and rate assurance map |
| 4 | Prepare ICT assurance and audit plan<br>Develop improvement actions |
| 5 | Implement improvement actions across all ICT 3 lines of defence |
| 6 | Periodically review and update the strategy |

**A word of caution**

Some 2nd line of defence assurance activities purport to provide assurance, but this is not always so. An example would be a project management office (PMO) providing reporting to management. The management receiving PMO reporting believes it is receiving independently validated assurance reports. That is, the PMO has reviewed projects to assure veracity of the reporting. Often this is not the situation, as many PMOs act as a postbox by accepting self-

The Institute of Internal Auditors Australia

assessed information provided by projects and collating it into management reports. Management then make decisions based on unverified information.

It can be useful for a project to define its 3 lines of defence, rate effectiveness, and implement improvements to improve assurance over projects.

## Helpful references

AS NZS ISO IEC 38500–2010 'Corporate governance of information technology'

Australian Standard AS 8000:2003 'Good Governance Principles', Standards Australia

Australian Standard AS 8015:2005 'Corporate Governance of Information and Communication Technology', Standards Australia

'COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT', ISACA

Fact Sheet '3 Lines of Defence', IIA–Australia

Fact Sheet 'Combined Assurance', IIA–Australia

Fact Sheet 'Corporate Governance', IIA–Australia

Global Technology Audit Guide (GTAG) 'Assessing Cybersecurity Risk: Roles of the Three Lines of Defense', IIA–Global

Global Technology Audit Guide (GTAG) 'Auditing IT Governance', IIA–Global

'ICT Assurance Framework', NSW Government

'Information and Communications Technology Strategic Framework', Department of Local Government Western Australia

'Information and Communications Technology (ICT) Strategic Planning Guideline', NSW Government

'Internal Audit in Australia', IIA–Australia

Practice Guide 'Coordination and Reliance: Developing an Assurance Map', IIA–Global

Practice Guide 'Internal Audit and the Second Line of Defense' IIA–Global

The Institute of Internal Auditors Australia