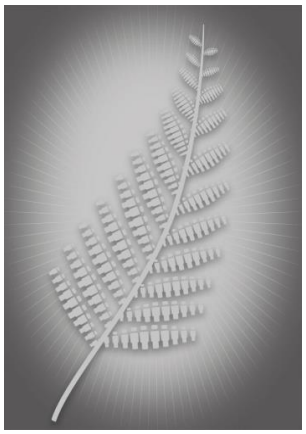
INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Government

All-of-Government ICT Operations Assurance Framework



Information Pack

Version 2.0 May 2015

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.

Contents

1. Introduction and background

1.1 Government agencies are moving to increasingly digital channels to help improve citizen interactions with government, which is being driven by the Better Public Service result areas 9 and 10:

- Result area 9: “New Zealand businesses have a one-stop online shop for all government advice and support they need to run and grow their business.”
- Result area 10: “New Zealanders can complete their transactions with the Government easily in a digital environment.”

1.2 Prior to June 2013, there was no single agency with the responsibility for providing a system-wide view of Information and Communications Technology (ICT) risks and assurance.

1.3 In order to provide confidence to stakeholders that ICT risks and processes are identified and effectively managed, in June 2013, Cabinet agreed (CAB Min (13) 20/13) that, as part of the ICT functional leadership role, the Government Chief Information Officer (GCIO) has responsibility for coordinated oversight and delivery of system-wide ICT assurance. As a result, the GCIO ICT Assurance function and framework is being implemented within the Department of Internal Affairs Service and System Transformation (SST) branch.

1.4 The GCIO ICT Assurance function and framework is intended to:

- Provide coordinated delivery of system-wide ICT assurance.
- Report to Ministers on a system-wide view of the status of information management, technology infrastructure, and technology-enabled business processes and services across government.
- Identify areas where interventions may be needed.
- Take actions to support agencies to improve their ICT assurance processes and intervene where necessary.
- Coordinate, develop and mandate common ICT assurance and information management standards.

1.5 The GCIO’s mandate for system-wide ICT assurance includes the ICT-related activities of the following groups of agencies:

- Public Service Departments.
- Non-Public Service Departments.

1.6 A proposed Whole-of-Government Direction under the Crown Entities Act 2004 regarding ICT functional leadership, including ICT assurance, is currently being consulted on to extend the mandate into the wider State Services.

Scope of the GCIO ICT Assurance Framework

1.7 The scope of the GCIO ICT assurance function and framework includes the ICT-related activities of agencies of the State Services, which encompasses:

- Information management (including security and privacy).
- Technology infrastructure.
- Existing ICT-enabled services.
- New ICT-enabled projects and programmes.

2. Document scope

GCIO ICT Operations Assurance Framework

2.1 The purpose of this document is to describe the ICT Operations Assurance framework. It is not intended to be detailed guidance for executing the Assurance activities. The assurance approach for ICT-enabled projects and programmes is covered in the *'All-of-Government ICT Projects & Programmes Assurance Framework Information Pack'*.

2.2 The scope of this document, the All-of-Government ICT Operations Assurance framework includes:

- Overview of the framework.
- Application of the framework.
- Overview of the process.
- Roles and responsibilities.

2.3 The content of this framework has been developed based on a range of information sources and methods including industry standards, industry experience, and conducting interviews and workshops with a selection of Agency representatives during the design phase. These sources have been adapted to fit a New Zealand all-of-government context and scope.

Agencies

2.4 The current scope of this framework includes Public Service Departments and Non-Public Service Departments. A Whole-of-Government Direction under the Crown Entities Act 2004 regarding ICT functional leadership, including ICT assurance, is currently being consulted on to extend the mandate into the wider State Services. [See www.ssc.govt.nz/whole-of-govt-directions-dec2013.] Therefore an updated framework that outlines the roles and responsibilities of Monitoring Departments and Crown Entities will be published once these have been confirmed.

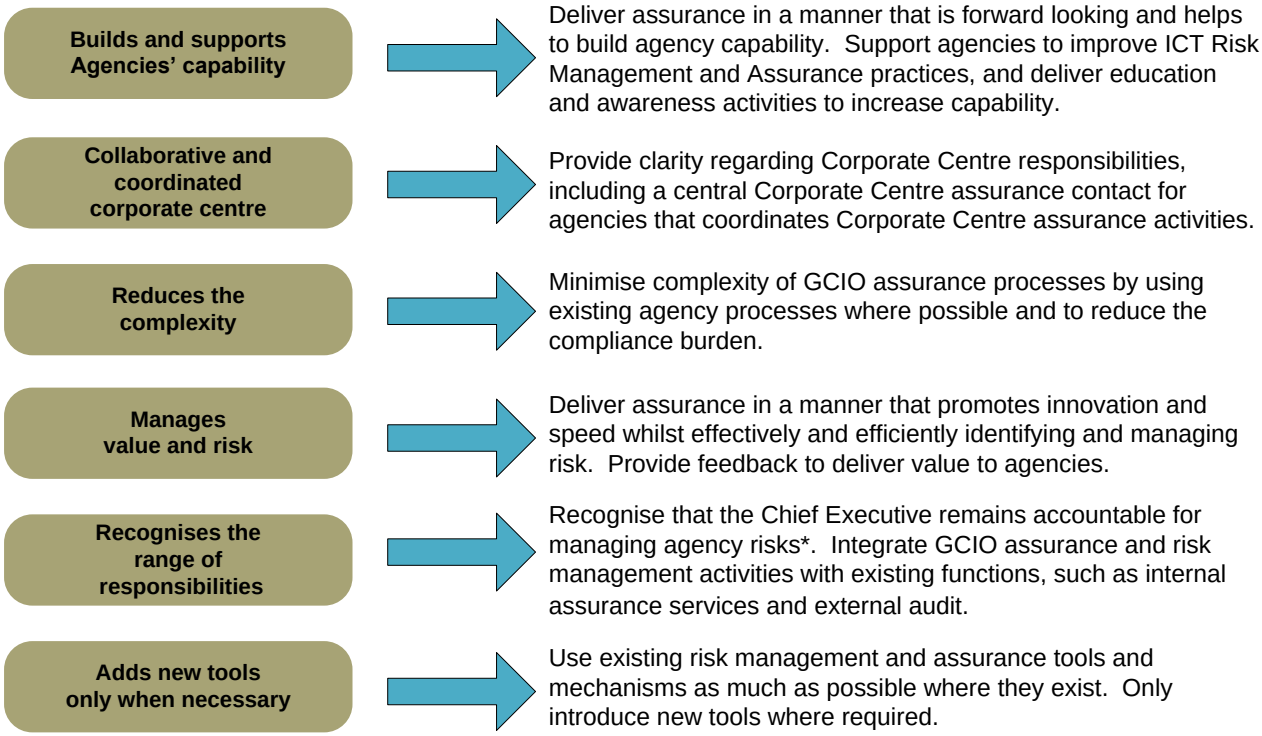
3. Overview

3.1 This section provides an overview of the ICT Operations Assurance Framework. Maps for the underpinning processes are provided in Appendix A.

3.2 The way in which agencies implement the responsibilities and activities outlined within this framework (such as the development of a combined assurance plan) should be integrated into the agency's overall Risk and Assurance strategy, which is outside the scope of the ICT Assurance framework.

Design Principles

3.3 The All-of-government ('AoG') ICT Assurance Framework has been developed based on several design principles, which are relevant for both ICT Operations and ICT-enabled projects and programmes:



Objectives

3.4 The objectives of the ICT Operations Assurance Framework are to:

- Provide a system-wide view of ICT risks.
- Provide stakeholders with confidence that ICT processes and risks within the State Services are identified and effectively managed.
- Improve system-wide ICT risk management and assurance through lifting capability.

---

* The Chief Executive remains accountable for the successful delivery of their ICT Operations and for ensuring risks are managed and kept at an acceptable level.

Behaviours

3.5 The success of the ICT Operations Assurance framework is premised on a set of behavioural characteristics that are required of the GCIO ICT Assurance team and Agencies, examples of which include:

	Trust	Value	Capability
GCIO ICT Assurance Team commits to	• Providing clarity regarding the purpose of information being collected when requested. • Enabling sufficient time to allow agencies to inform their stakeholders regarding information requests.	• Sharing ICT risk and assurance insights and results of analysis with agencies. • Being responsive to Agency requests and queries.	• Helping agencies to lift ICT risk management and assurance capability by coordinating education and awareness activities. • Acting as a critical friend to agencies to support them to lift their ICT risk management and assurance capability.
GCIO Expectation of Agencies	• Be open and transparent regarding the ICT risk landscape. • Keep key stakeholders informed about ICT risks and assurance, including information that is being provided to the GCIO.	• Be responsive to GCIO ICT Assurance requests and queries. • Share ICT risk management and assurance insights and observations with the GCIO and other agencies.	• Provide advice to other agencies in order to help them lift their capability. • Engage actively in system-wide ICT risk management and assurance initiatives.

Escalation

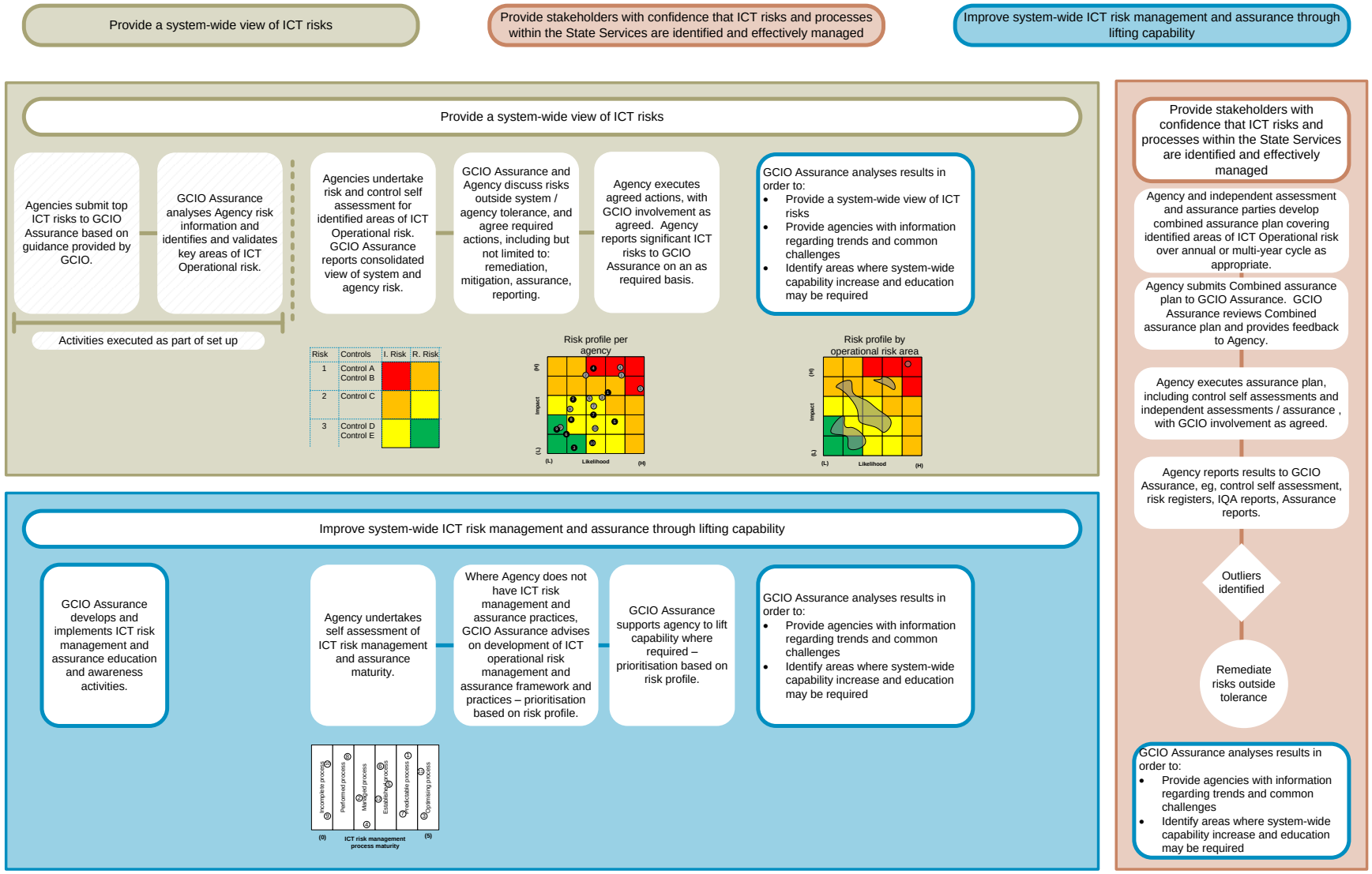
3.6 One of the uses of the ICT Operations framework outputs will be to drive discussions between agencies and GCIO ICT Assurance regarding remediation activities for risks that sit outside the agency and / or system tolerance.

3.7 Where agreement regarding the appropriate response to these risks is not reached between the agency and GCIO, the functional leadership escalation path will be used to help attain agreement. In order to attain agreement on appropriate responses, GCIO ICT Assurance and the Agency should consider gaining Chief Executive, Head of State Services and / or responsible Ministers' perspectives.

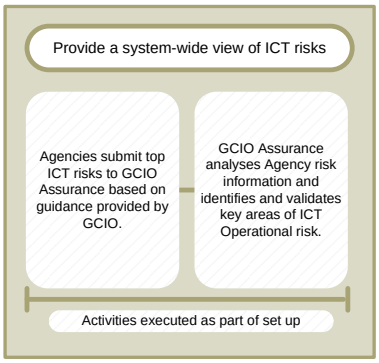
3.8 Where GCIO ICT Assurance and / or Agencies do not demonstrate the behaviours described above, where needed the functional leadership escalation path will also be used.

3.9 Refer to Appendix A, section V, for the escalation procedure.

3.10 The following diagram sets out the ICT Operations Assurance approach, which will be performed on a cyclical basis. Each element is described in more detail in the following pages.



Element 0: Set up



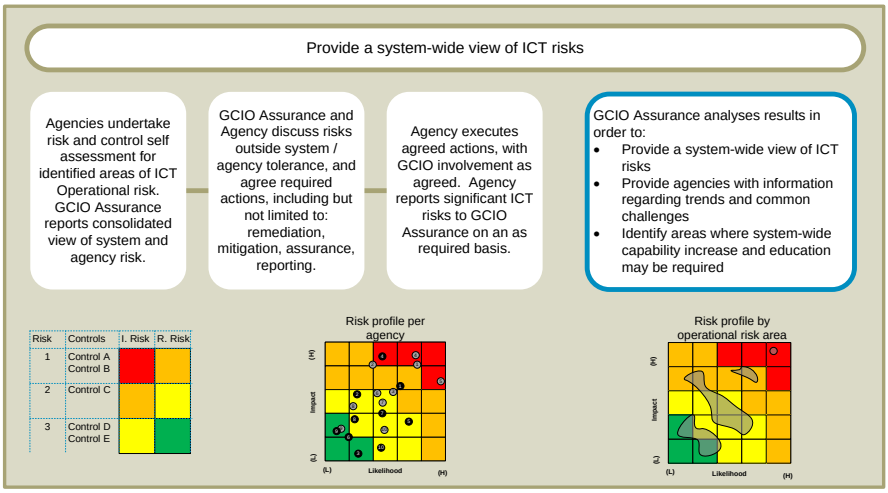
3.11 The following outputs are generated and used for the purpose described:

Outputs	Purpose of the outputs
Key areas of ICT Operational risk	The key areas of ICT Operational risk are designed to identify the 'risks that matter' across the State Services, and drive the focus of GCIO ICT Assurance activities. This enables the GCIO to provide a high level view of key ICT operational risks to Ministers; drive system-wide actions to address pervasive risks where required; provide feedback to Agencies regarding key ICT operational risks; focus areas across the system to help inform Agency ICT operational risk management and assurance activities.

3.12 The following tables describe the key considerations for each of the activities within element 0 of the framework.

Key activities	Agencies submit top ICT operational risks to GCIO Assurance based on guidance provided by GCIO. GCIO analyses information and identifies and validates key areas of ICT Operational risk.
Many agencies have a view of their top ICT operational risks, therefore this information is used to inform the focus of GCIO ICT Assurance activities. In order to achieve this, agencies submit existing information to GCIO ICT Assurance regarding their: • Top ICT operational risks based on the inherent ('uncontrolled') risk assessment. • Top ICT operational risks based on the residual ('controlled' or current) risk assessment. If agencies do not have an existing view of their ICT operational risks they submit a 'NIL' return. GCIO ICT Assurance analyse the information and provide a summary report of system-wide ICT operational risks to Ministers and Agencies, and use the information to inform the scope of ICT Operational risk areas that system-wide ICT risk management and assurance activities focus on. The scope of these activities is also informed by the ICT Risk Universe contained within Appendix B.	

Element 1: Provide a system-wide view of ICT operational risks



3.13 The following outputs are generated and used for the purpose described:

Outputs	Purpose of the outputs
A consolidated system-wide and sector view of ICT Operational risk	The consolidated system-wide view of ICT operational risks and their status helps to identify areas where system-wide capability increase and education and awareness activities may be required. The view informs discussions within agencies, and between agencies and GCIO ICT Assurance, regarding agency and system risk tolerance and the level of risk management and capability to help inform remediation activities. The key ICT operational risks, trends and challenges, and potential remediation strategies form part of the system-wide view and will help inform agency ICT risk management and assurance activities.
Agency view of ICT Operational risk	The Agency view of ICT operational risks drives discussions within agencies, and between agencies and GCIO ICT Assurance, regarding agency and system risk tolerance and the level of risk management and capability to help inform remediation activities.
Agency remediation plan for risks outside system / agency tolerance	Remediation plans are designed to help improve ICT risk management within agencies and across the system, and provide confidence to stakeholders that ICT operational risks are being effectively managed.

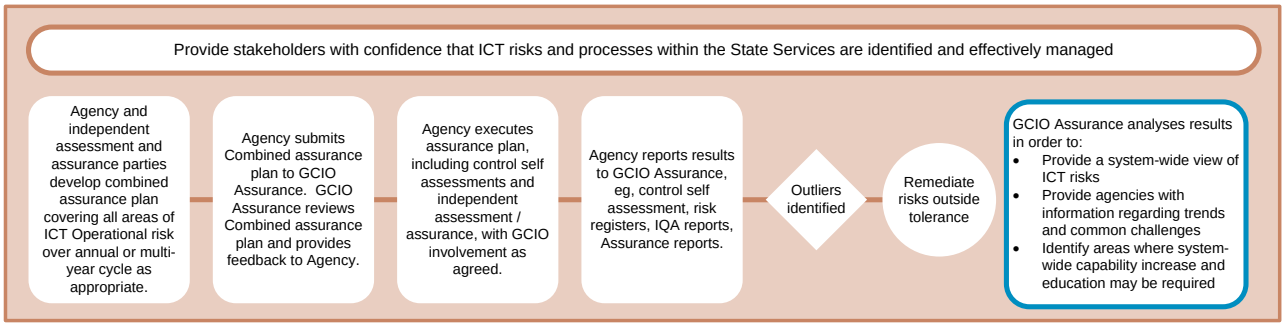
3.14 The following tables describe the key considerations for each of the activities within element 1 of the framework.

Key activities	Agencies undertake risk and control self assessment for identified areas of ICT Operational risk. GCIO reports consolidated view of system and agency risk.
Agencies undertake a risk and control self assessment using guidance and templates provided by GCIO ICT Assurance (refer Appendix C for the template). The scope of the assessment includes the 'in-scope' ICT Operational risk areas identified as part of set up, as well as other significant agency ICT operational risks if they are not covered by the 'in-scope' risk areas. Other significant Agency ICT operational risks are included in the assessment to help keep focus on the 'risks that matter' for the Agency, and also inform changes to the scope of system-wide ICT risk management and assurance activities over time. For each risk area Agencies assess the inherent ('uncontrolled') risk, and residual ('controlled') risk based on identified controls. Agencies submit the assessment to GCIO ICT Assurance. GCIO ICT Assurance analyse the information provided by agencies to provide system-wide and sector views of ICT operational risks by ICT Operational risk area. This analysis is used to inform GCIO ICT Assurance reporting and feedback to Ministers and Agencies on areas of ICT risk, trends and challenges. A critical component of this reporting includes providing context (such as remediation activities underway) particularly for ICT operational risks that are assessed as 'Significant'.	

Key activities	GCIO ICT Assurance and Agency discuss risks outside system / agency tolerance, and agree required actions. Agency executes agreed actions, with GCIO involvement as agreed.
Agencies and GCIO ICT Assurance jointly identify key ICT operational risks that require immediate attention, management and / or remediation. Actions may include, but be not limited to: • Remediation of ICT operational risks and / or control issues. • Implementation or identification of mitigation strategies. • Independent assessment of and assurance over the identified risk. • Acceptance and reporting to appropriate Agency and system governance and oversight functions regarding the level of ICT risk. The remediation effort and activities should be commensurate to the risk profile and appetite of the Agency as well as the system. Agencies own and execute the agreed actions, with GCIO ICT Assurance involvement and support as agreed.	

Key activities	Agency reports significant ICT operational risks to GCIO Assurance on an as required basis.
In order to keep the view of the 'risks that matter' (the key system-wide and agency risks) up to date, Agencies report significant ICT operational risks along with proposed responses to GCIO ICT Assurance as they arise. The activities described in the table above regarding required actions are then undertaken. Should risks become issues (i.e., an incident occurs), Agencies will provide relevant information to their GCIO contact who will assist the agency to respond to the incident and advise the GCIO ICT Assurance team.	

Element 2: Confidence that ICT risks and processes are identified and effectively managed



3.15 The following outputs are generated and used for the purpose described:

Outputs	Purpose of the outputs
Combined assurance plan	The combined assurance plan is a risk-based plan developed by the Agency to determine the involvement of different parties in the development, monitoring and execution of assurance over ICT Operations. The level and nature of the assurance is based on the risk associated with the Operational area, and the risk profile of the Agency. The assurance plan drives what assurance activities will occur over time, and is amended in response to emerging risks and issues internal and external to the Agency.
Results of assurance activity	Results of assurance activity, such as assurance reports, are used by the Agency to inform remediation activities (refer Element 2 for more information), and to provide confidence to stakeholders that ICT operational risks and issues are identified and effectively managed. The results help to identify areas where system-wide capability increase and education and awareness activities may be required. Results of assurance activities should be copied to the GCIO Assurance lead.

3.16 The following tables describe the key considerations for each of the activities within element 2 of the framework.

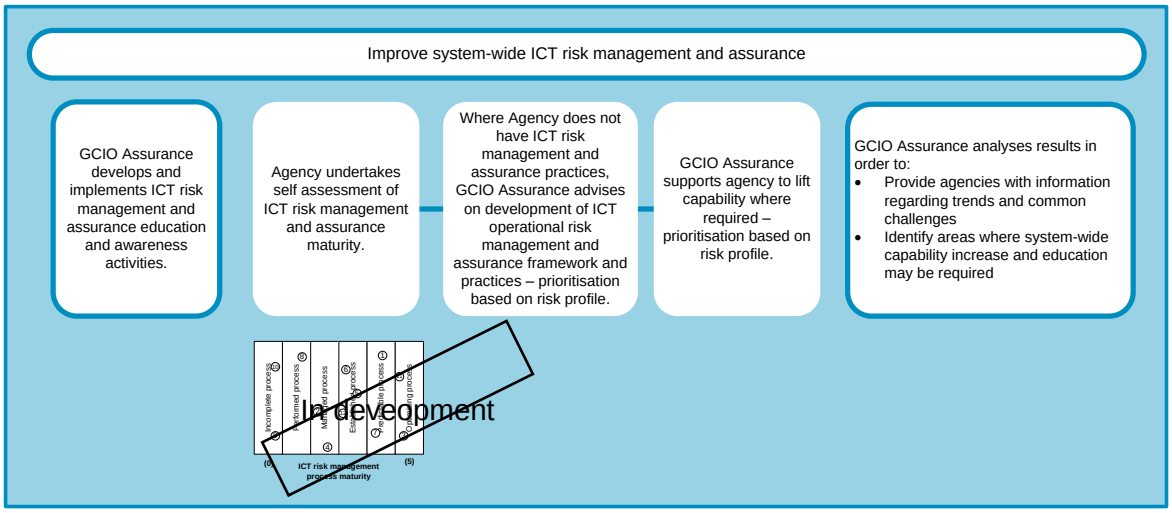
Key activities	Agency and independent assessment and assurance parties develop combined assurance plan covering all areas of ICT Operational risk over annual or multi-year cycle as appropriate.
The Agency and their independent assessment and assurance parties (such as Internal Assurance Services) develop a combined assurance plan. The plan aims to address key ICT Operational risks and put adequate assurance activities / strategies in place. The plan identifies the assurance providers and activities that will be used to provide assurance, and the high level objectives of each assurance activity. Refer to Appendix E for an Assurance plan template.	

Key activities	Agency submits combined assurance plan to GCIO. GCIO reviews combined assurance plan and provides feedback to Agency.
In order to obtain confidence that the Assurance plan covers key areas of ICT Operational risk, GCIO ICT Assurance reviews and provides feedback on the combined assurance plan to the Agency, who incorporate and update the plan as appropriate. The Agency and GCIO ICT Assurance agree the extent of engagement required with GCIO ICT Assurance during the execution of the plan.	

Key activities	Agency executes assurance plan, including control self assessments and independent assessments / assurance, with GCIO involvement as agreed. Agency reports results to GCIO, e.g., control self assessment, risk registers, IQA reports, and Assurance reports.
The Agency is responsible for executing the combined assurance plan (refer Appendix E for an example combined assurance plan). In order to obtain the maximum value and optimal use of resources when assessing ICT operational risks, it is anticipated that assurance activities include a combination of self assessments, internal assurance reviews, supplemented by specialist external assessments and assurance where required. The Agency sends the results of agreed assurance activities, such as particular Assurance reports, to GCIO ICT Assurance as agreed during planning. GCIO ICT Assurance analyse the information provided by Agencies to enhance and update the system-wide and sector views of ICT operational risks and mitigation strategies. This analysis is used to inform GCIO ICT Assurance reporting and feedback to Ministers and Agencies on areas of ICT risk, trends and challenges. A critical component of this reporting includes providing context (such as remediation activities underway) particularly for ICT operational risks and issues that are assessed as 'Significant'.	

Key activities	Outliers are identified, and risks outside system / agency tolerance are remediated.
Where risks that are outside system / agency tolerance are identified, agencies are responsible for defining and executing remediation plans. The key considerations are the same as those for the remediation activities undertaken as part of the risk and control self assessment (detailed in Element 2 section above). These risks and remediation plans should be discussed with the GCIO Assurance Lead.	

Element 3: Improve system-wide ICT risk management and assurance



3.17 The following outputs are generated and used for the purpose described:

Outputs	Purpose of the outputs
A consolidated system-wide and sector view of ICT risk management and assurance maturity	The consolidated system-wide view of ICT risk management and assurance maturity helps to identify areas where system-wide capability increase and education and awareness activities may be required.
Agency view of ICT risk management and assurance maturity	The Agency view of ICT risk management and assurance maturity drives discussions within agencies, and between agencies and GCIO ICT Assurance, regarding what activities may be required in order to increase Agency maturity in these areas (where needed – recognising that most agencies will not need to achieve highest maturity level).
ICT risk management and assurance education and awareness activities	The purpose of the education and awareness activities is to improve system-wide ICT risk management and assurance through lifting capability where required.

3.18 The following tables describe the key considerations for each of the activities within element 3 of the framework.

Key activities	GCIO develops and implements ICT risk management and assurance education and awareness activities.
One of the key objectives of the ICT Assurance framework is to improve system-wide ICT risk management and assurance through lifting capability, and to help achieve this GCIO ICT Assurance will develop and drive education and awareness activities. Activities will be designed to cater for the varying needs of agencies. Agencies will engage actively in these activities, including, but not limited to: • Providing advice to other agencies in order to help them lift their capability; and • Sharing experiences and practices regarding risk reduction and mitigation.	

In mid-late 2014 the GCIO ICT Assurance team expect to publish an ICT Risk management maturity model self-assessment guide and survey to help agencies understand their ICT Operations and wider ICT risk management maturity. The maturity assessment tool will help agencies to clearly define their current and required maturity level and any activities needed to meet that level.

From a system-wide perspective this will provide a baseline from which to help build risk management capability across the system and guiding agency development as required.

Following the baseline assessment the GCIO will assess progress and report improvements across the system. Following the baseline assessment maturity targets may be set in order for agencies to meet a minimum level of risk maturity.

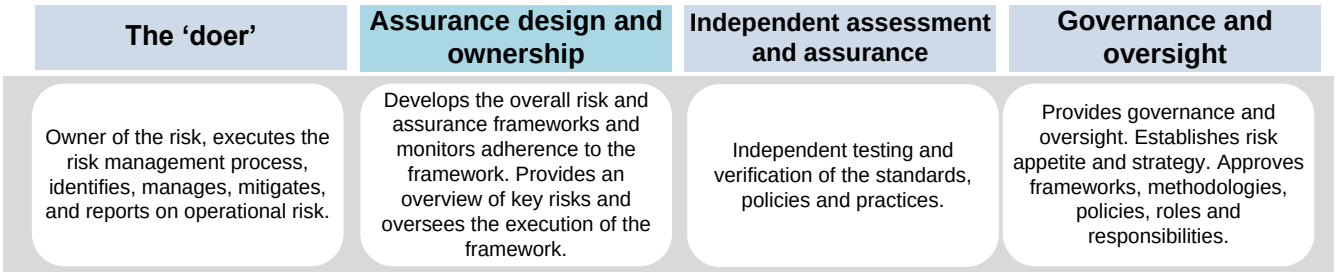
Key activities	Agency undertakes self assessment of ICT risk management and assurance maturity.
Agencies undertake an ICT risk management and assurance self assessment using guidance and templates provided by GCIO ICT Assurance. This assessment is undertaken in conjunction with the risk and control self assessment described in element 1. Agencies assess their current state maturity and desired state maturity (recognising that it is neither appropriate nor achievable for all Agencies to achieve a high state of maturity) to identify areas where capability uplift is required. Agencies submit the assessment to GCIO ICT Assurance. GCIO ICT Assurance analyse the information provided by agencies to provide system-wide and sector views of ICT risk management and assurance maturity (refer Appendix D for heat map template). This analysis is used to inform GCIO ICT Assurance reporting and feedback to Ministers and Agencies, and drive education and awareness activities.	

Key activities	Where Agency does not have ICT risk management and assurance practices, GCIO advises on development of ICT risk management framework and practices. GCIO supports Agency to lift capability where required. Prioritisation based on risk profile.
Typically education and awareness activities will be provided to groups of Agencies rather than individual Agencies. However there will be times when individual support will be appropriate in order to lift Agency capability. Individual requirements will be determined on a case by case basis, and supported by the ICT risk management and assurance standards and templates published by GCIO ICT Assurance. In order to prioritise GCIO ICT Assurance resources, priority will be given to those agencies with a higher residual risk profile.	

4. Roles and responsibilities

4.1 The roles and responsibilities within the ICT Operations Assurance framework are based on the industry standard 'lines of defence' model. The separation of responsibilities within the model is key to delivering robust risk management. The model has been tailored specifically for the all-of-government ICT assurance framework.

4.2 The following diagram sets out the key roles and associated risk management responsibilities within the model:



4.3 This 'System of Assurance' requires a number of parties to play their part. Across government, there are a number of teams and functions that fulfil the roles and responsibilities within each of these lines. The table in section 4.6 describes some of the entities that may undertake these roles, along with the key responsibilities within the ICT Operations assurance framework.

4.4 The role of the GCIO ICT Assurance function is 'Assurance design and ownership' for system-wide ICT risk management and assurance, which includes ensuring that the framework is followed to deliver system-wide assurance.

4.5 Agencies remain responsible and accountable for owning, identifying, managing, mitigating and reporting on ICT operational risks within their agency. Agencies will support the GCIO by providing the GCIO with the information needed to provide a system-wide view of ICT risk and assurance.

4.6 The following tables set out:

- The example functions that undertake each of the roles – note that these functions are illustrative only, and not all agencies will have the teams or functions described.
- The key responsibilities within the ICT Operations assurance framework – note that this is not intended to be an exhaustive list of risk management and assurance responsibilities.

The 'doer'		
Example functions	**Agency function (illustrative)**	**System-wide functions (illustrative)**
	• ICT team. • Business line teams. • ICT vendors.	• All-of-government delivery, e.g., DIA Commercial Strategy and Delivery. • All-of-government ICT vendors.
Key responsibilities within the ICT Operations assurance framework	The primary responsibility of the 'doer' is to achieve the business objectives and therefore own the associated operational risks by implementing the risk management frameworks, and identifying, managing, mitigating and reporting on ICT operational risks. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to:	

The 'doer'	
	ICT risk identification, management and reporting • Identify and manage ICT operational risks, and submit ICT risk information to the GCIO ICT Assurance Team. • Periodically undertake risk and control self assessments, and submit the results to the GCIO ICT Assurance team. • Discuss risks outside system and agency tolerance with agency governance and oversight functions, and agree required actions. • Discuss risks outside system tolerance with the GCIO ICT Assurance team, and agree required actions. • Define and execute actions to improve risk mitigation, and engage with the GCIO ICT Assurance team as required. *ICT risk management capability* • Undertake ICT operational risk management maturity self assessment, and submit the results to the GCIO ICT Assurance team. • Engage with GCIO ICT Assurance and other Agencies to improve ICT risk management practices where required. • Communicate and report effectively with all lines throughout the model, where required.

Assurance design and ownership		
Example functions	**Agency function (illustrative)**	**System-wide functions (illustrative)**
	• Risk function. • Chief Information Security Officer.	• GCIO ICT Assurance. • New Zealand Security Intelligence Service. • Government Communications Security Bureau.
Key responsibilities within the ICT Operations assurance framework	***Assurance Design (specifically GCIO ICT Assurance responsibilities)*** The responsibility of the assurance design role is to develop an overall ICT Operations Assurance Framework. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to: • Support agencies to lift capability. • Develop the appropriate frameworks, guidance and tools. • Identify areas where system-wide capability increases and education may be required. • Communicate and report effectively with all lines throughout the model, where required. ***Assurance Ownership (specifically GCIO ICT Assurance responsibilities)*** The responsibility of the assurance ownership role is to monitor the 'doers' adherence to the ICT Operations Assurance Framework, providing an overview of key risks and supervising the execution of the framework. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to: • Support agencies to lift capability. • Help address key risks as required. • Provide agencies with advice, guidance and tools around the execution of the framework.	

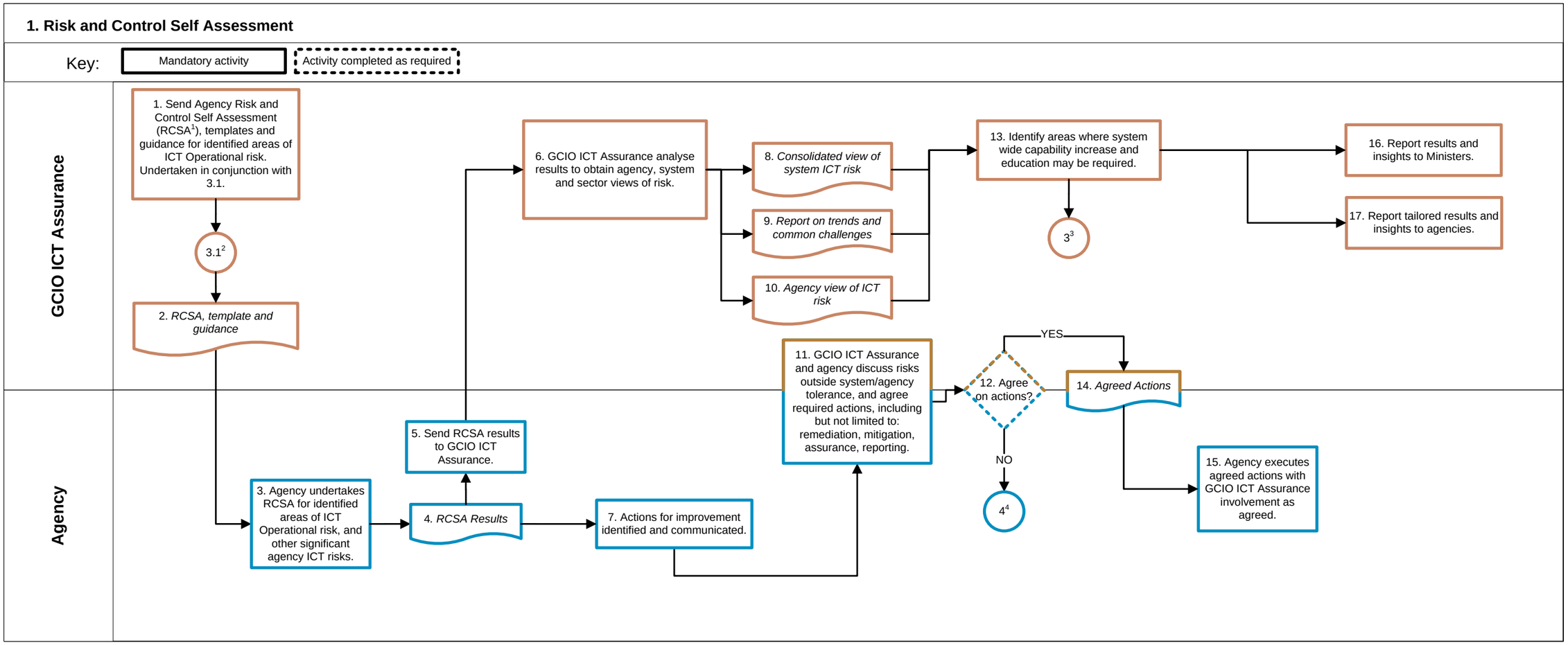
Assurance design and ownership	
	• Provide support to the agencies with regard to the design and execution of the combined assurance plan. • Engage with the agency in the escalation process for significant risks. • Analyse results of various assessments in order to provide a system-wide view of ICT operational risks. • Provide agencies with information regarding trends and common challenges. • Communicate and report effectively with all lines throughout the model, where required.

Independent assessment and assurance		
Example functions	**Agency function (illustrative)**	**System-wide functions (illustrative)**
	• Assurance services. • Internal Audit. • OAG-appointed External Auditor. • Other sources of Assurance.	• All-of-government IQA / TQA panel. • GCSB (for Top Secret systems).
Key responsibilities within the ICT Operations assurance framework	The independent assessment and assurance role is responsible for the independent testing and verification of standards, policies and practice. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to: • Develop and maintain the combined assurance plan. • Execute independent assurance and assessment activities as part of the combined assurance plan. • Provide assurance with regard to delivery of successful ICT operations and services. • Communicate and report effectively with all lines throughout the model, where required.	

Governance and oversight		
Example functions	**Agency function (illustrative)**	**System-wide functions (illustrative)**
	• Chief Executive. • Executive Leadership Team. • Audit and risk committee.	• Cabinet. • DPMC.
Key responsibilities within the ICT Operations assurance framework	The 'Governance and Oversight' line provides governance and oversight over framework operations, and will act as the overarching source of approval over framework design and operations. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to: • Establish risk appetite and strategy for ICT Operations. • Approve frameworks, methodologies, policies, roles and responsibilities. • Approve responses to the key risks identified as a consequence of the application of the framework. • Accountable for the successful delivery of Agency operations. • Communicate and report effectively with all lines throughout the model, where required. • Ensure IT Operations Assurance Plan integrates and aligns to the overall agency risk framework.	

Appendix A. Process diagrams

I. Risk and control self assessment



Notes:

1. Risk and Control Self Assessment (RCSA)

2. Please refer to the 'ICT Risk Management and Assurance Maturity, Education and Awareness' process 3.1

3. Please refer to the 'ICT Risk Management and Assurance Maturity, Education and Awareness' process

4. Please refer to the 'Escalation Procedure' process 4

II. Agency-led Assurance over identified areas of ICT Operational risk

2. Agency-led Assurance over identified areas of ICT Operational risk

Key: Mandatory activity | Activity completed as required

GCIO ICT Assurance

- 3. GCIO ICT Assurance reviews combined assurance plan and provides feedback to Agency. Agree required GCIO involvement.
- 8. GCIO ICT Assurance involvement as agreed.
- 14. GCIO ICT Assurance analyses results to update system wide views of ICT risks.
- 15. *Consolidated view of system ICT risk*
- 16. *Report on trends and common challenges*
- 17. *Agency view of ICT risk*
- 23. Identify areas where system wide capability increase and education may be required.
- 3[1]

Agency

- 1. Independent assessment/ assurance parties develop combined assurance plan covering identified areas of ICT Operational risk with input from agency stakeholders.
- 7.Agency executes control self assessment.
- 9. *RCSA*
- 10. *Risk Register*
- 13. Send results of agreed assurance activity to GCIO ICT Assurance.
- 18. Address outliers and risks outside system tolerance by developing and implementing remediation plan.
- 19. *Remediation Plan*
- 21. Agency executes remediation plan.
- 22. Report results to GCIO ICT Assurance and Independent Assessment and Assurance, as agreed.

Independent Assessment and Assurance (including Internal Assurance Services)

- 2. *Draft Combined Assurance Plan*
- 4. Agency updates Combined Assurance Plan as required, following GCIO ICT Assurance review and feedback.
- 5. *Final Combined Assurance Plan*
- 6. Agency executes combined assurance plan, including assessments/ assurance with GCIO ICT Assurance involvement as agreed.
- 11. *IQA Report*
- 12. *Audit Report*
- 20. Agency receives feedback on remediation plan.

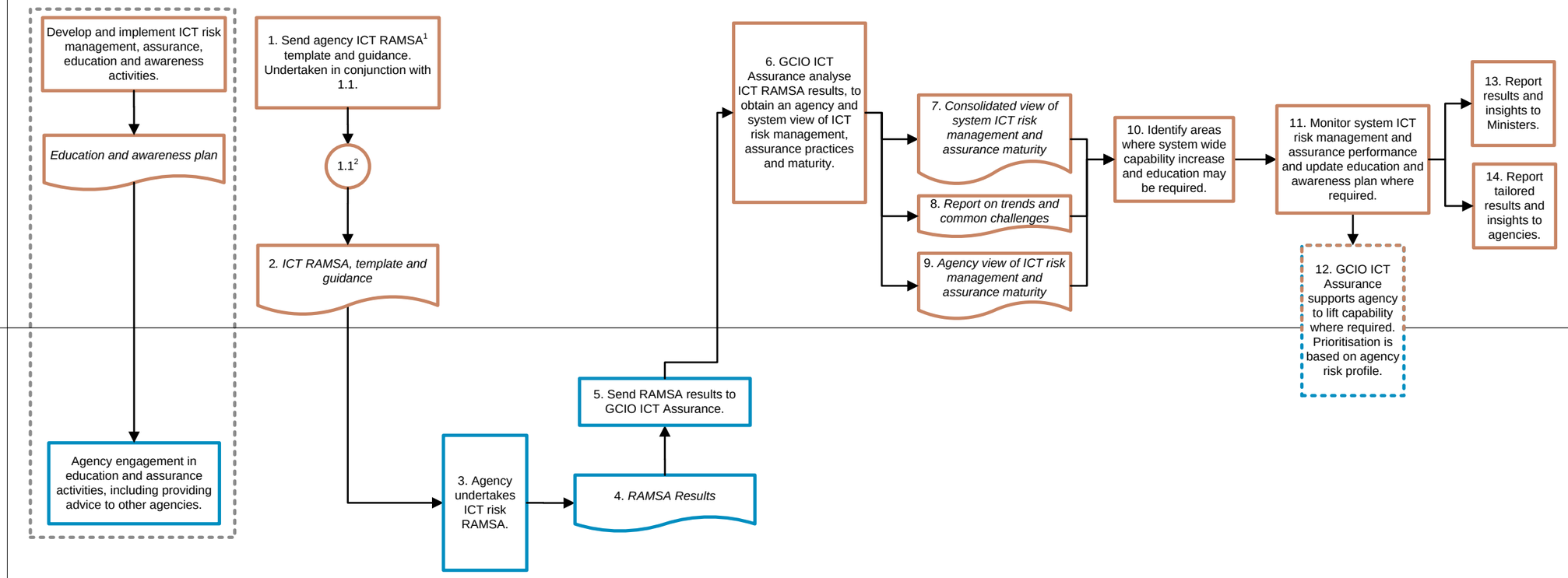
Notes:

1. Please refer to the 'ICT Risk Management and Assurance Maturity, Education and Awareness' proccess.
2. The Assurance Plan is a cyclical and dynamic process in order to address business change, collaboratively decided between the Agency and GCIO ICT Assurance Team.

III. ICT Risk Management and Assurance maturity, education and awareness

3. ICT Risk Management and Assurance Maturity, Education and Awareness

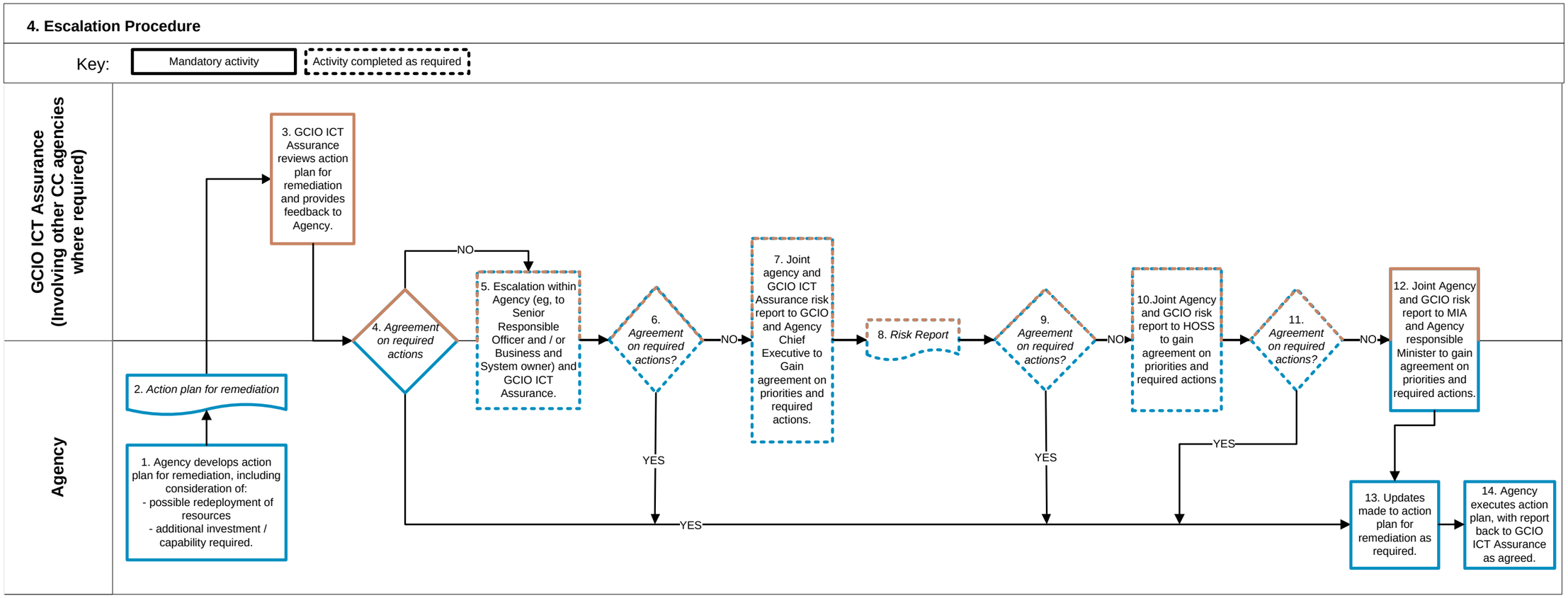
Key: Mandatory activity | Activity completed as required



Notes:

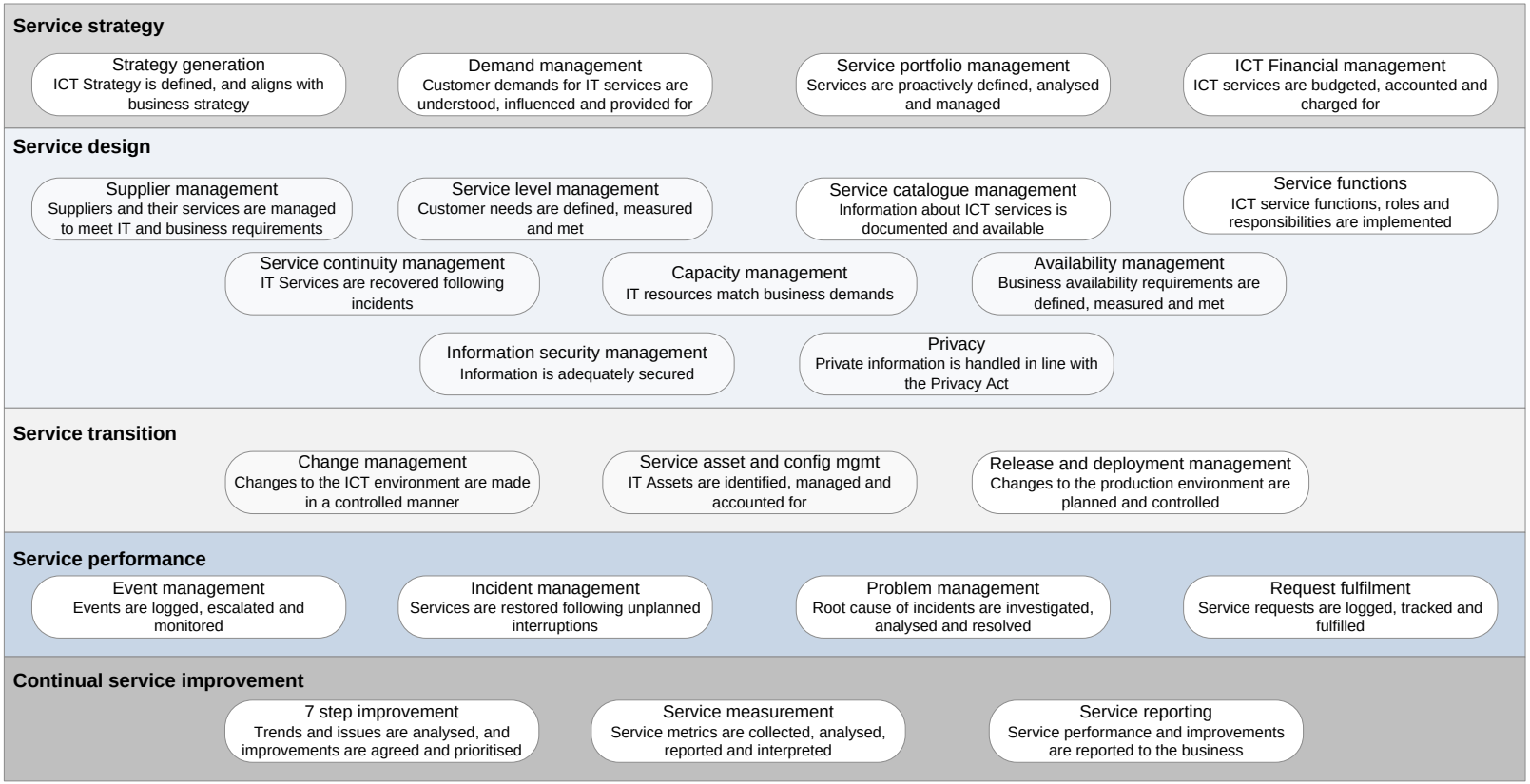
1. Risk Management and Assurance Maturity Self Assessment (RAMSA)
2. Please refer to the 'Risk and Control Self Assessment' process 1

IV. Escalation procedure



Appendix B. ICT Risk Universe

Note these areas are primarily taken from ITIL, with the exception of Privacy, which has been highlighted specifically given the GCIO's mandate



ICT Operational Risk Area	Example risk statement
Service strategy	
Strategy generation	An ICT strategy is not developed or is misaligned to agency strategy, which results in ICT services that are do not meet the needs of relevant stakeholders, resulting in over- or under-investment in ICT services.
Demand management	Ineffective demand management processes result in degradation or interruption of ICT services due to unexpected increases in agency demand and / or hardware and software faults.
Service Portfolio management	Lack of integrated service portfolio management results in a sub-optimal mix of ICT services that do not meet agency requirements. Lack of service documentation impacts ICT's ability to effectively respond to events and incidents resulting in prolonged outages.
ICT Financial management	Ineffective financial management for ICT services results in insufficient investment, overspend or misdirected investment. As a result, ICT services degrade over time, and / or ICT investment and services do not meet the needs of relevant stakeholders.
Service design	
Supplier management	Ineffective ICT supplier management results in the organisation assuming third party technology risks without knowledge or understanding, which may ultimately impact the confidentiality, integrity and availability of information and systems.
Service level management	Ineffective or misaligned service level management practices mean ICT services do not meet agency requirements, impacting agency operations and service delivery requirements.
Service catalogue management	Ineffective service catalogue management practices mean that no comprehensive or accurate view of ICT services exist, which impacts ICT's ability to effectively respond to events and incidents resulting in prolonged outages, and misdirected ICT investment.
Service functions	Lack of integrated ICT service functions results in end user confusion, and impacts ICT's ability to resolve service requests and incidents, ultimately impacting agency operations and service delivery requirements.
Service continuity management	Lack of effective Business and ICT Service Continuity Management plans and associated processes mean that management and ICT may not be adequately prepared to respond to and recover from a business continuity event, reducing their ability to handle the event and ultimately impacting the recovery time following the disruption.
Capacity management	Ineffective capacity management practices result in degraded system performance and / or loss of information when existing capacity is exceeded.
Availability management	Ineffective availability management practices mean that systems are not available when required by the agency, impacting agency operations and service delivery requirements.

ICT Operational Risk Area	Example risk statement
Information security management	Ineffective information security management practices results in private or classified information being disclosed to or accessed by unauthorised persons, resulting in information loss, damage to reputation finances and / or legal proceedings.
Privacy	Ineffective privacy practices results in personal information being handled in a manner that is inconsistent with the Privacy Act 1993, resulting in breaches that impact the confidentiality of citizen information, the organisation's reputation, and / or result in legal proceedings.
Service transition	
Change management (ICT)	Ineffective change management practices may result in defects or unexpected ICT changes being introduced into the production environment, leading to system instability, unscheduled impacts to agency operations and / or loss of system integrity.
Service asset and configuration management	Ineffective service asset and configuration management practices means that asset and configuration information become out of date and / or inconsistent, reducing ICT's ability to manage the impact of service changes and incidents resulting in unintended or unknown consequences that impact agency operations.
Release and deployment management	Ineffective release and deployment management practices means that poorly integrated changes are introduced into the production environment that are not understood or accepted by agency end users, ultimately impacting agency operations and service delivery requirements.
Service performance	
Event management	Ineffective event management practices reduce ICT's ability to identify, analyse and respond to service events, which may result in disruptive or unplanned events going undetected and therefore unresolved.
Incident management	Ineffective incident management practices reduce ICT's ability to respond in the event of a service disruption or adverse event, increasing the risk that issues escalate and become more severe, ultimately impacting agency operations and service delivery requirements.
Problem management	Ineffective problem management practices means that the root causes of incidents remain unresolved, resulting in continued diversion of ICT resources to respond to incidents.
Request fulfilment	Ineffective request fulfilment practices means that user requests are not logged, prioritised or fulfilled, reducing ICT's ability to resolve service requests and incidents, and ultimately impacting agency operations and service delivery requirements.

ICT Operational Risk Area	Example risk statement
Continual service improvement	
7 step improvement	Lack of service improvement practices results in ICT services becoming misaligned with business requirements over time and / or poor performance not being addressed, resulting in over- or under-investment in ICT services and ultimately impacting agency operations.
Service measurement	Ineffective service measurement practices and lack of service performance metrics reduces management's ability to measure and track ICT service performance, meaning that performance issues may not be identified and resolved in line with business requirements.
Service reporting	Ineffective service reporting practices reduces management's ability to assess whether ICT services are meeting and will continue to meet business requirements, resulting in over- or under-investment in ICT services and ultimately impacting agency operations.

Appendix C. Risk and control self-assessment template

Risk assessment criteria

Likelihood	Description
5. Almost Certain	Is expected to occur in most instances (> 95% chance of occurring)
4. Highly Probable	Will probably occur in most circumstances (75% < x < 94% chance of occurring)
3. Possible	Might occur at some time (50% < x < 74% chance of occurring)
2. Possible But Unlikely	Could occur at some time (20% < x < 49% chance of occurring)
1. Almost Never	May occur only in exceptional circumstances (<19% chance of occurring)

Impact	Description
5. Severe	• Business operations, information integrity, confidentiality or security is seriously compromised. High external scrutiny and concern is expected. Major and extended adverse national media campaign. Could seriously undermine or damage the Agency and/or Government's reputation. Impacts most NZ citizens and residents.
4. Significant	• Business operations, information integrity, confidentiality or security is seriously compromised. Adverse national media coverage over a period. Widespread complaints from stakeholders. Significant number of people impacted.
3. Moderate	• Major refocus of agency resources required. Operations are significantly impacted. Adverse national media coverage. Widespread complaints from stakeholders. Multiple incidents impact a significant number of people over time.
2. Minor	• Manageable within existing agency team. Additional costing requiring reprioritisation and / or reallocation of available funds. Widespread complaints from stakeholders. Multiple incidents impact groups of people over time.
1. Minimal	• Manageable within existing agency team and budget. Localised complaints from stakeholders. Adverse local media. Single incident impacts a small group of people.

Risk and control self-assessment template

#	Process	Risks	Likelihood	Impact	Inherent risk	Controls	Treated Likelihood	Treated Impact	Residual risk	Comments / issues	Owner
1	*Privacy*	*Personal information is disclosed to or accessed by unauthorised individuals*	*4*	*4*	*21*	*Technical security controls implemented in line with NZISM. Privacy policy and practices implemented and monitored across the organisation.*	*2*	*3*	*9*	*Annual Independent Assurance undertaken*	*DCE is responsible for Privacy*

Appendix D. Heat Map template

5- Severe	15	19	22	24	25
4- Significant	10	14	18	① 21	23
3- Moderate	6	9 ❶	13	17	20
2- Minor	3	5	8	12	16
1- Minimal	1	2	4	7	11
	1- Almost Never	2- Possible But Unlikely	3- Possible	4- Highly Probable	5- Almost Certain

Key

⚪ Inherent risk assessment

⚫ Residual risk assessment

Zone	Escalation path	Escalated to[1]
Extreme	Risk must be escalated to the Deputy Chief Executive via the Executive or Business / System owner at the first possible opportunity. GCIO Assurance Lead updated on the risk.	DCE Business Owner via previous escalations first
High	Risk must be escalated to the Business / System Owner	Business / System Owner via Operational Manager if appropriate
Medium	Risk can be managed and monitored by the operational manager (ICT and Business)	Operational Manager (ICT and Business)
Low		

[1] Note that the escalation path may vary from that described but must effectively highlight the risk to the appropriate level of management.

Appendix E. Combined assurance plan template

Please visit https://www.ict.govt.nz/ict-system-assurance/ict-operations-assurance/guidance-and-templates/ for the current operations assurance plan template.

Appendix F. Glossary of abbreviations and terms

Term	Description
Agency	Term used to describe entities within the New Zealand state sector, including: • Public Service Departments. • Non-Public Service Departments. • Crown Entities. • Public Finance Act Schedule 4 Organisations. • Reserve Bank of New Zealand. • Offices of Parliament. Refer State Services Commission list of Central Government Agencies - http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf.
AoG	"All of Government" refers to the entire New Zealand state sector.
Assurance	Objective examination of evidence for the purpose of providing an independent assessment on risk management, control, or governance processes for an organisation (Institute of Internal Auditors).
Assurance Plan / Combine Assurance Plan	Document that sets out the assurance strategy and related assurance activities, role and responsibilities for executing assurance activities over Projects and Programmes and ICT Operations. The approach should be integrated into the agency's overall Risk and Assurance strategy.
Corporate Centre (CC)	The Corporate Centre refers to the three Central Agencies (The State Services Commission, Treasury and the Department of the Prime Minister and Cabinet) and the Cabinet Mandated Functional Leaders for Property Procurement and ICT.
Combined Assurance Plan / Assurance Plan	Document that sets out the assurance strategy and related assurance activities, role and responsibilities for executing assurance activities over Projects and Programmes and ICT Operations.
Crown Entity	An organisation that forms part of New Zealand's state sector established under the Crown Entities Act 2004. Refer State Services Commission list of Central Government Agencies - http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf.
Department	Term used to describe Public Service Departments and Non-Public Service Departments within the state sector. Refer State Services Commission list of Central Government Agencies - http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf.

Term	Description
External Audit	An independent statutory audit (typically annual) of the financial reports of organisations in order to express an independent opinion on whether the report: • Complies with the recognised framework of generally accepted accounting practice (known as “GAAP”); and • Fairly reflects the entity’s financial performance and financial position. (Controller and Auditor General).
GCIO	Government Chief Information Officer describes the role undertaken by Chief Executive of the Department of Internal Affairs to provide leadership on ICT matters within Government.
GCIO ICT Assurance	The function responsible for the integrity of AoG ICT assurance that resides in the Service and System Transformation branch of the Department of Internal Affairs.
GCSB	Government Communications Security Bureau.
ICT	Information and Communications Technology, which spans: • Information management. • Technology infrastructure. • Technology-enabled business processes and services.
ICT Assurance Framework	The framework implemented by GCIO ICT Assurance to deliver integrity of AoG ICT assurance.
Inherent Risk	The risk derived from the environment without the mitigating effects of internal controls (Institute of Internal Auditors). Also referred to as “gross risk” or “uncontrolled risk”.
Internal Audit / Assurance Services	A department, division, team of consultants, or other practitioner(s) that provide independent, objective assurance and consulting services designed to add value and improve an organisation's operations (Institute of Internal Auditors).
IQA	“Independent Quality Assurance” - an independent assessment undertaken by a team of consultants, or other practitioner(s) to provide independent, objective assurance and consulting services to add value and improve the outcomes of projects and programmes.
Mandate	An official order or commission to carry out an action.
Monitoring Department	Function within a Ministry or other government Department that oversees and manages the Crown’s interests in Crown Entities on behalf of a Minister.
PPM	Portfolio and Performance Management function residing within Treasury.
Programme	Temporary flexible organisation structure created to coordinate, direct and oversee the implementation of a set of related projects and activities in order to deliver outcomes and benefits related to an organisation's strategic objectives (MSP).

Term	Description
Project[2]	Temporary organisation that is created for the purpose of delivering one or more business products according to an agreed Business Case (PRINCEII).
RAMSA	“Risk Management and Assurance Maturity Self-Assessment”.
RCSA	“Risk and Control Self-Assessment”.
Remediation Plan	The plan that is formulated to address risks and issues that have been identified during the course of business, or as a result of self assessments and / or assurance activities.
Residual Risk	The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk (Institute of Internal Auditors). Also referred to as “net risk” or “controlled risk”.
Risk	The possibility that an event will occur, which will impact an organisation’s achievement of objectives (Institute of Internal Auditors).
Risk Universe	Collection of risk types and categories that could affect an organisation.
Risk Tolerance	The level of risk executive management and the Board are willing to accept relative to variation or variability around specific business objectives.
Risk Appetite	The level of risk executive management are willing to accept on an aggregate basis in relation to strategic and business objectives.
Risk Register	A register of risks that have been identified as part of a process, entity, project or programme, including description, cause, likelihood, impact, identified controls, proposed response, and owner.
RPA Tool	The SSC Gateway Risk Profile Assessment Tool, which is the primary means of assessing project risks and identifying projects that require monitoring within the New Zealand state sector. http://www.ssc.govt.nz/sites/all/files/nzrpa-template-sept2013.XLS
SSC	State Services Commission.
SST	Service and System Transformation branch within the Department of Internal Affairs.
Terms of Reference	For the purposes described within this framework, a Terms of Reference describes the purpose, structure, roles and responsibilities for undertaking assurance activities.
TQA	“Technical Quality Assurance” - an independent assessment undertaken by a team of consultants, or other practitioner(s) to provide independent, objective assurance and consulting services to assess technical delivery aspects of a project or programme (such as source code reviews).

[2] Where the term Project has been used in the document the term also covers Programmes.