



All-of-Government ICT Projects & Programmes Assurance Framework



Information Pack

Version 2.0 August 2014



Crown copyright ©. This copyright work is licensed under the Creative Commons Attribution 3.0 New Zealand licence. In essence, you are free to copy, distribute and adapt the work, as long as you attribute the work to the Department of Internal Affairs and abide by the other licence terms. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/nz/>. Please note that neither the Department of Internal Affairs emblem nor the New Zealand Government logo may be used in any way which infringes any provision of the [Flags, Emblems, and Names Protection Act 1981](#) or would infringe such provision if the relevant use occurred within New Zealand. Attribution to the Department of Internal Affairs should be in written form and not by reproduction of the Department of Internal Affairs emblem or New Zealand Government logo.

Document History

Version	Issue Date	Description of Changes
Version 1.0	February 2014	Initial version
Version 2.0	August 2014	Updated assurance plan template (Appendix B)

Contents

1. Introduction and background	4
2. Document scope	6
3. Overview	10
4. Roles and responsibilities	18
Appendix A Process Maps	21
Appendix B Projects and programmes assurance plan template	27
Appendix C IQA / TQA Terms of reference template	32
Appendix D Glossary of abbreviations and terms	35

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 As part of the overall response to improving programme and project performance, in November 2013, the Central agencies also transitioned the State Services Commission’s (SSC) Major Projects Monitoring (MPM) function from SSC to The Treasury, and established a new Portfolio Performance Management (PPM) function. The overall design of this PPM function is still being developed, and it is expected that changes to the overall assurance frameworks across ICT-enabled and non-ICT enabled projects and programmes will be completed during 2014.
- 1.5 The new assurance framework will be rolled out in phases. This document outlines the process for the first phase, whereby the framework will be applied only to **ICT** projects and programmes that are assessed as either **high** or **moderate risk / value**. This interim *All-of-Government ICT Projects & Programmes Assurance Framework* has been jointly developed by the GCIO and the PPM team.
- 1.6 This approach involves the provision of enhanced ICT assurance at a project and programme level, at an agency level, and at system level. This means that every part of the ICT assurance system needs to play its part and improve performance.
- 1.7 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.
- 1.8 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.

- 1.9 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. [See www.ssc.govt.nz/whole-of-govt-directions-dec2013.]

Scope of the GCIO ICT Assurance Framework

- 1.10 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

All-of-Government ICT Projects & Programmes Assurance Framework

- 2.1 The purpose of this document is to describe the interim processes and requirements associated with introducing the All-of-Government ICT Programmes and Projects Assurance framework. It is not intended to be detailed guidance for executing the Assurance activities. The assurance approach for ICT Operations is covered in the '*All-of-Government ICT Operations Assurance Framework Information Pack*'.
- 2.2 The scope of this document, the interim All-of-Government ICT Projects & Programmes 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 including utilising 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 and context and scope.

Definition of an ICT-enabled programme or project

- 2.4 Programmes and projects have variable levels of ICT change. Defining when a project or programme has sufficient level of ICT change to constitute an ICT-enabled programme or project is therefore problematic. But as a guiding principle, a programme or project may be considered 'ICT-enabled' when the ICT change:
- Presents medium to high risk to the success of the programme or project; and /or
 - Is a primary lever for achieving the anticipated benefits.
- 2.5 To assist agencies to know when the All-of-Government ICT Projects & Programmes Assurance Framework applies the Corporate Centre agencies will jointly assess and advise the outcome when the agency submits the Gateway Risk Profile Assessment (RPA)¹.

Agencies

- 2.6 The current scope of this framework includes Public Service Departments and Non-Public Service Departments.
- 2.7 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. [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.

Alignment with the State Services Monitoring Major Projects and Programmes framework

- 2.8 In 2001, Cabinet required that the Treasury and the State Services Commission (SSC) monitor major ICT projects by Departments to assure Ministers that these projects will

¹ The RPA can be accessed through www.ssc.govt.nz/gateway-rpa-agency-responsibilities.

succeed. In 2010, the monitoring role was extended to all major projects (ICT and other) that meet the defined criteria outlined in Cabinet Circular CO(10)2.

2.9 Cabinet mandates, through this circular and the Guidance for Monitoring Major Projects, that a programme / project shall be monitored when it is defined as a new initiative, an ongoing development or acquisition project, or other type of project which meets any one or more of the following conditions:

- Is assessed as High Risk, using the Gateway Risk Profile Assessment (RPA) tool - this is the primary means of identifying projects that require monitoring.
- Has projected total life-cycle costs of \$25 million or more².
- If not delivered in line with the projected functionality requirements, cost and timelines, would expose the department to significant risk of impaired operational capability or expose the Government to significant fiscal or ownership risk.
- Will impact significantly on more than one department or agency.
- Has been nominated for monitoring by the responsible Minister.

2.10 Generally only departmental projects are monitored by the central agencies, unless a Minister specifically requests that a Crown Entity / Agent project be monitored. These projects are usually monitored by the department responsible for overall monitoring of the Crown Entity / Agent (e.g. Ministry of Transport (MoT) for New Zealand Transport Agency or the Ministry of Health (MoH) for District Health Board (DHB) projects).³

Key Changes

- 2.11 There are two key differences between the current Major Projects Monitoring (MPM) scope (see Cabinet Circular CO(10)2⁴) and the GCIO's mandate:
- The GCIO is responsible for system-wide assurance that covers **all** ICT-enabled programmes and projects regardless of size and risk.
 - The GCIO's system-wide assurance responsibilities will ultimately include Crown Entities.
- 2.12 This interim All-of-Government ICT Projects & Programmes Assurance Framework introduces a number of changes, including but not limited to:
- The introduction of 'value' into the initial risk assessment to inform the extent of Corporate Centre monitoring involvement.
 - The development of a tailored risk-based Assurance plan that addresses key elements of risk and assures the value throughout the investment's lifecycle from initiation through to and including benefits realisation.
 - The introduction of a 'lead assurance' role within the Corporate Centre agencies, that is determined at the time of submission of a risk profile assessment (RPA).
- 2.13 The 'lead assurance' agency will be the primary interface between the Corporate Centre and the monitored agency and for the Corporate Centre with Ministers. The 'lead assurance' agency will be responsible for providing the monitored agency with guidance and oversight during development of the assurance plan, approval of the final plan, and monitoring of the plan. Monitoring activities themselves will be undertaken by the most appropriate Corporate Centre agency on behalf of the 'lead assurance' agency. For ICT-enabled projects and programmes, the lead agency assurance contact will typically be from the GCIO; for non-ICT enabled projects and programmes (e.g. construction), the lead assurance contact will typically be from the PPM team.

² For a complete definition of 'whole of life costs' (WoLC), refer to the 'Instructions' tab of the Gateway Risk Profile Assessment: www.ssc.govt.nz/gateway-rpa-agency-responsibilities.

³ www.ssc.govt.nz/major-projects-monitoring.

⁴ www.dpmc.govt.nz/cabinet/circulars/co10/2.html.

- 2.14 Transition of the MPM group to the Treasury and establishment of the PPM function means that some changes are likely to the scope and remit of the current major projects monitoring function. These changes are expected to be gradually phased in from the middle of 2014.
- 2.15 In the interim, the current major project/programme identification and risk assessment will follow the current process, where departments are required to provide their RPA to PPM when a programme or project is deemed to be medium or high risk/cost.
- 2.16 The existing MPM requirements continue to apply to non-ICT projects, such as construction. It is expected that changes to the overall assurance frameworks across both ICT-enabled and non-ICT enabled projects and programmes will be completed during the latter half of 2014

2.17 The new assurance framework will be rolled out in phases. This document outlines the process for the first phase, whereby the framework will be applied only to **ICT** projects and programmes that are assessed as either **high** or **moderate risk / value**.

2.18 The application of the framework to low risk / value projects and programmes will be addressed in the second phase of the roll out. An updated framework document will be published as part of the second phase.

Interim Framework

- 2.19 Until such time that the AoG Programme and Project Assurance framework design is confirmed by the Corporate Centre⁵, the following interim protocol will operate.
- 2.20 Assessing the risk / value of the programme and project will follow the current process, where departments are required to provide their RPA to Treasury/PPM when a programme or project is deemed to medium or high risk with the inclusion of a 'value'⁶ component for ICT-enabled projects and programmes. This 'value' component will be extended in the broader framework.
- 2.21 Treasury/PPM group will work with the GCIO to determine which programmes and projects are ICT-enabled. Treasury/PPM (on behalf of the Corporate Centre) will advise agencies if their programme or project has been classified in this category
- 2.22 Coordination of Corporate Centre engagement with high and selected medium risk / value programmes and projects that are deemed to be ICT-enabled will typically be undertaken by the GCIO.
- 2.23 The Corporate Centre will apply the interim framework outlined in this document for high and selected medium risk / value ICT programmes and projects.
- 2.24 Programmes or projects led by DIA will be monitored by the Treasury/PPM, including those assessed as medium risk / value. Programmes or projects led by the Treasury will be monitored by the GCIO, including those assessed as medium risk / value
- 2.25 Until the independent IQA / TQA panel is established the existing procurement practices of agencies will apply.
- 2.26 Department's medium and high risk / value ICT-enabled programme and projects will be expected to develop an appropriate Assurance Plan and specific terms of reference for each assurance activity.
- 2.27 A proposed Whole-of-Government direction regarding functional leadership of ICT, including ICT assurance, is currently being consulted on with Crown Entities under the Crown Entities Act 2004.

⁵ 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.

⁶ See section 3.12.

Following enactment of this direction it is envisaged that the GCIO's role as ICT functional leader, including associated powers in relation to ICT assurance, which currently applies to Public Service and Non-Public Service departments, will be extended to relevant entities within the wider State Services.

Updates and enhancement

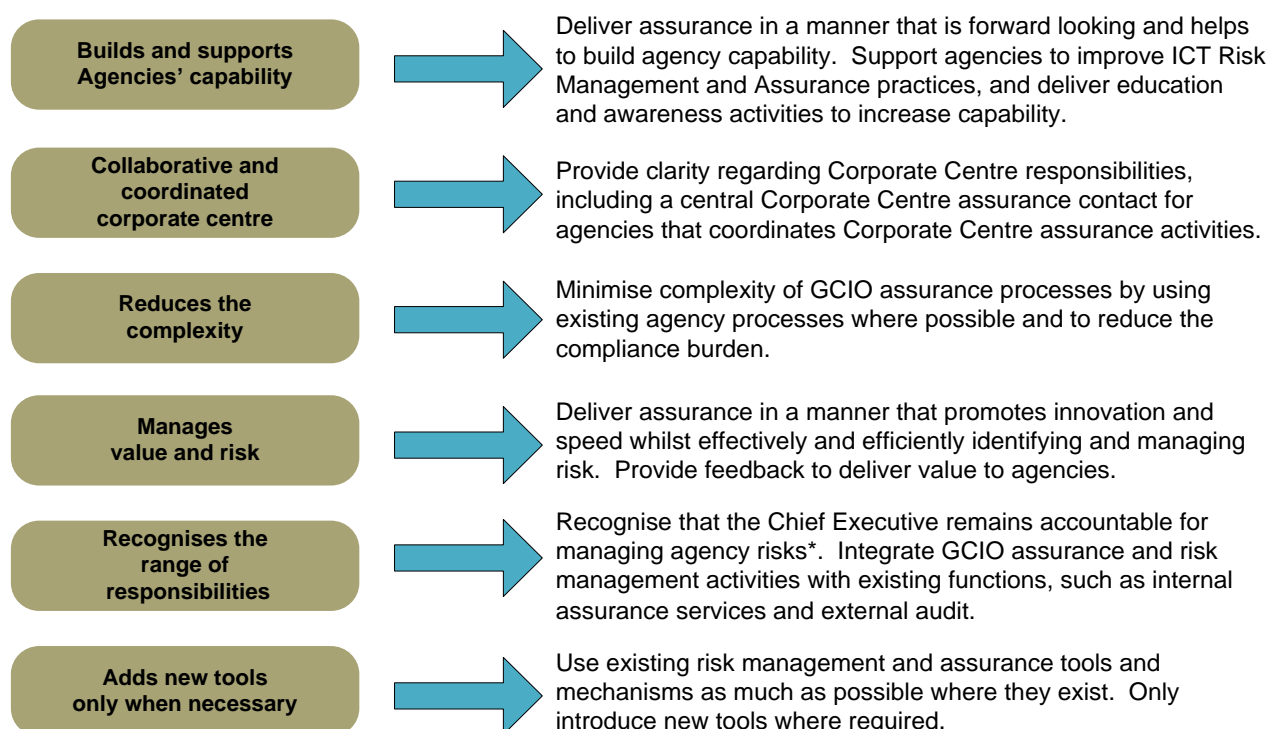
- 2.28 As noted, this framework is an interim operating model for embedding and developing ICT assurance of projects and programmes across the State services. As Corporate Centre agencies complete their review of the overall assurance arrangements for all projects and programmes, it is expected that this interim operating model will be updated. It is expected that this review will be completed by April 2014, and the recommendations will be subsequently phased in over a transition period that will be discussed and communicated across the State services.
- 2.29 This framework will therefore be updated and enhanced based on lessons learned whilst applying the framework to ICT projects and programmes. This process will operate until such time as the Corporate Centre has completed the design of the all-of-government framework. Although enhancements have not been confirmed, they may include:
- A consistent framework for ICT and non-ICT projects and programmes.
 - Further enhancement to concept of 'value' when assessing the relative importance of a project or programme, in addition to the traditional cost and risk lenses.
 - Update to the Risk Profile Assessment tool.
 - Addition of low risk / value projects and programmes to the framework.

3. Overview

- 3.1 This section provides an overview of the ICT Projects & Programmes 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 an 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 Projects & Programmes Assurance Framework are to:
- Provide a system-wide view of ICT risks.
 - Provide stakeholders with confidence that ICT-enabled projects and programmes within the State Services are effectively managed to deliver expected outcomes.
 - Improve system-wide ICT risk management and assurance through lifting capability.

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

Behaviours

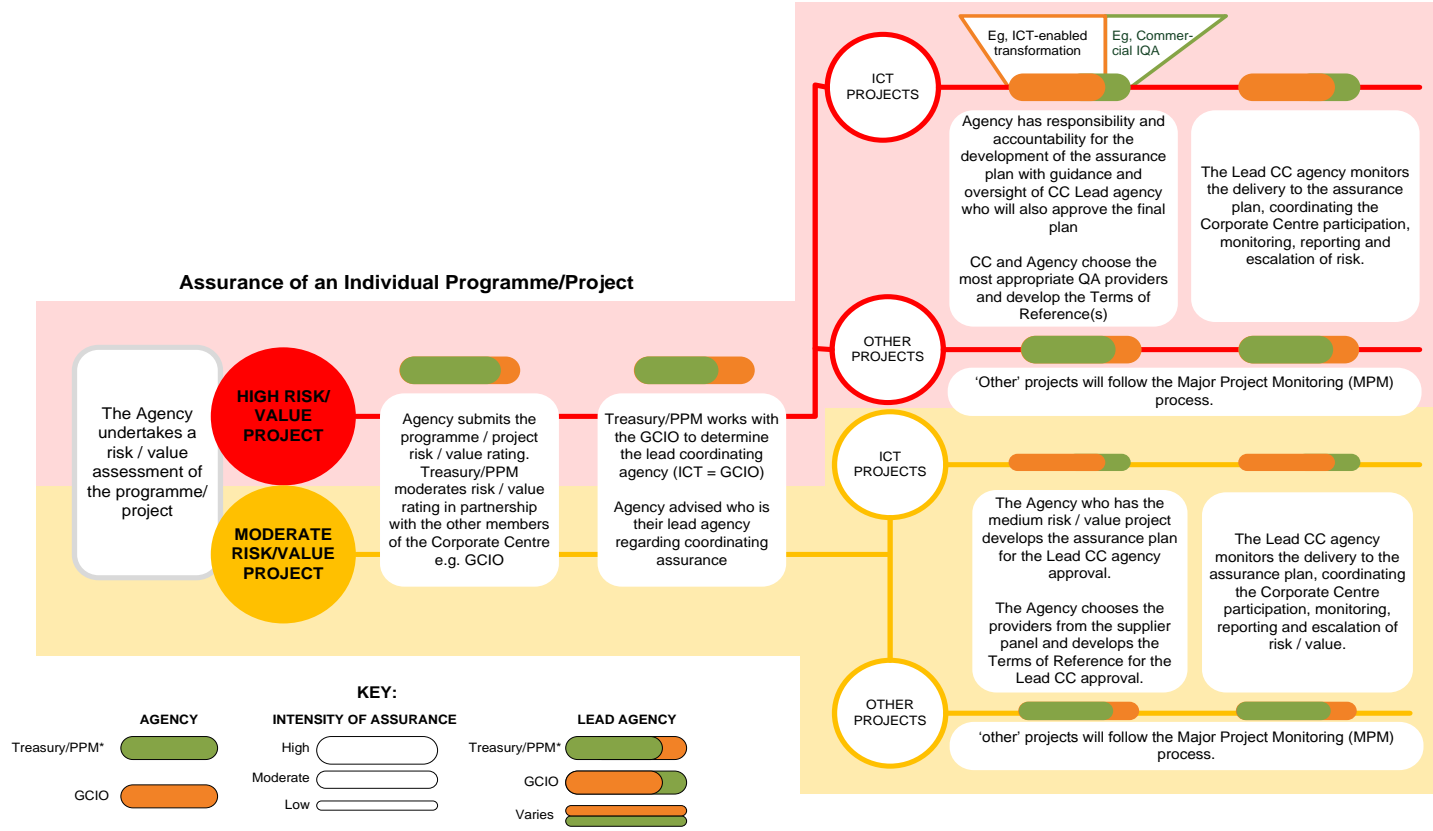
- 3.5 The success of the ICT Projects and Programmes Assurance framework is premised on a set of behavioural characteristics that are required from the GCIO ICT Assurance team and Agencies, examples of which include:

	Trust	Value	Capability
GCIO ICT Assurance Team commits to	<ul style="list-style-type: none"> • Providing clarity regarding the purpose of information being collected when requested. • Enabling sufficient time to allow agencies to inform their stakeholders regarding information requests. 	<ul style="list-style-type: none"> • Sharing ICT risk and assurance insights and results of analysis with agencies. • Being responsive to Agency requests and queries. 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Be responsive to GCIO ICT Assurance requests and queries. • Share ICT risk management and assurance insights and observations with the GCIO and other agencies. 	<ul style="list-style-type: none"> • Provide advice to other agencies in order to help them lift their capability. • Engage actively in system-wide ICT risk management and assurance initiatives.

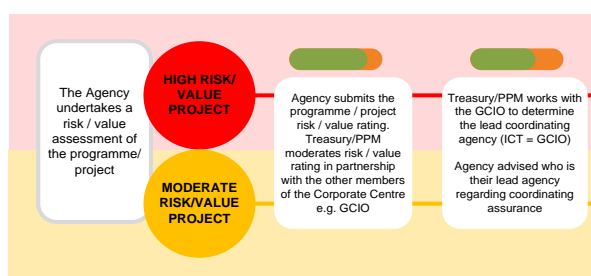
Escalation

- 3.6 One of the uses of the Projects and Programmes Assurance framework outputs is to drive discussions between agencies and GCIO ICT Assurance regarding recommendations to address project risks, issues and / or delivery challenges.
- 3.7 Where agreement regarding the appropriate response to these risks, issues or challenges is not reached between the agency and GCIO, the functional leadership escalation path is 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 VI, for the escalation procedure.

3.10 The following diagram sets out ICT Projects & Programmes Assurance framework. Each element is described in more detail in the following pages.



Element 1: Risk/Value Assessment



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

Outputs	Purpose of the outputs
Criteria for undertaking an AoG risk / value assessment	Due to the large portion of projects and programmes a well structured criterion is necessary to determine which particular projects and programmes require a risk / value assessment. In the interim, the existing Major Projects Monitoring (MPM) protocol will be used to determine which projects and programmes require a risk / value assessment.
Project/ Programme risk / value rating	<p>The risk / value rating is generated through the Gateway Risk Profile Assessment tool (RPA), accessible through the SSC website^[1]. The RPA produces an indicative risk / value rating.</p> <p>In phase 1 (this phase), a value component of ICT projects and programmes will also be assessed (where the definition of value includes alignment with the Government's ICT Strategy & Action Plan, and multi-agency benefits as well as to an individual agency).</p> <p>As part of broader changes to the PPM function beginning in the middle of this year, the Corporate Centre will be working with agencies to more formally define 'value', and update the risk profile assessment as appropriate.</p> <p>In phase 2 it is anticipated that the RPA tool will be revisited to include an enhanced assessment of value where the definition of value includes the benefits and value to the system as well as to an individual agency.</p> <p>The risk / value rating defines which assurance process the project will travel through.</p> <p>The Agency will re-submit the RPA if there are significant changes to the project / programme that impact the RPA rating.</p>

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

Key activities	Entry point: move into initiation phase, and criteria for undertaking an AoG risk / value assessment.
Due to the large number of projects and programmes that are part of the Government	

^[1] www.ssc.govt.nz/gateway-rpa-agency-responsibilities.

portfolio, criterion for undertaking an AoG risk / value assessment is essential to obtain the maximum value and optimal use of resources when managing risks within projects and programmes. An effective criterion also contributes to appropriate focus being placed on the different projects and programmes across AoG. The criteria used for MMP will continue to be used for all projects and programmes, with the addition of a 'value' component for ICT-enabled projects and programmes.

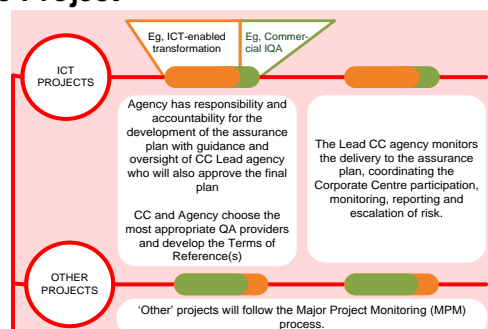
Key activities	The Agency undertakes a risk / value assessment of the programme/project.
<p>The risk / value assessment involves the Agency determining the risk / value rating of the project or programme using the guidelines provided by Treasury/PPM. Programmes / projects are rated as High, Moderate or Low based on the risks and/or value that are relevant to them. Support and guidance is provided by Treasury/PPM to enable Agencies to classify projects and programmes appropriately.</p> <p>Assessing the risk / value of the project / programme will follow the current process, where agencies are required to provide their RPA to Treasury/PPM when a programme or project is deemed to be medium or high risk and/or value.</p> <p>In this interim framework, for ICT-enabled projects and programmes, the Corporate Centre will include consideration of a 'value' component when assessing the level of assurance to be applied to a particular project or programme. This value assessment will use information provided in the RPA, that describes:</p> <ul style="list-style-type: none"> • Alignment of the project or programme and its impact on delivering components of the Government's ICT Strategy & Action Plan • To what extent a project or programme involves multiple agencies or delivers benefits across the entire system, as well as benefits to a specific agency or department <p><i>Generally, over the short to medium-term it is our expectation that many high-value ICT-enabled projects and programmes will likely also be high-cost and/or high-risk.</i></p>	

Key activities	Agency submits the programme / project risk / value rating. Treasury/PPM moderates risk / value rating in partnership with the other members of the Corporate Centre e.g. GCIO.
<p>After assessing the risk / value of the project/programme, the Agency submits the Risk Profile Assessment (RPA) to Treasury/PPM. Treasury/PPM objectively assesses whether this rating is appropriate to the project/ programme in partnership with other members of the Corporate Centre in order to make an informed decision.</p>	

Key activities	Corporate Centre determines the lead coordinating agency. Agency advised who is their lead assurance agency regarding coordinating assurance.
<p>The Corporate Centre agencies determine which programmes and projects are deemed ICT-enabled.</p> <p>The lead Corporate Centre assurance agency for each high and selected medium risk / value project / programme is determined by the Corporate Centre.</p> <p>For projects and programmes that are deemed to be ICT-enabled the GCIO will typically be</p>	

the lead Corporate Centre assurance agency (refer section 2.4 for further information on the definition of an ICT-enabled programme or project). The Treasury/PPM advises the Agency who their lead Corporate Centre assurance agency is and the personnel who will be coordinating assurance for the project / programme.

Element 2: High Risk/Value Project



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

Outputs	Purpose of the outputs
Assurance plan	The assurance plan is used to determine the involvement of different parties in the development, monitoring and execution of assurance across the programme/project's life. The level and nature of the assurance is project specific. The assurance plan drives what assurance activities will occur over the life of the project and is amended as changes in the project occur. The assurance plan is a part of the costed and resourced project plan.
Terms of Reference for assurance activities	The terms of reference describes how a specific assurance activity, such as an IQA, will operate. The terms of reference describes the purpose of the assurance activity, the scope, the depth of the review, who will be involved and who will have access to the resulting reports/feedback. The Corporate Centre, by default, will have access to any draft and final reports.

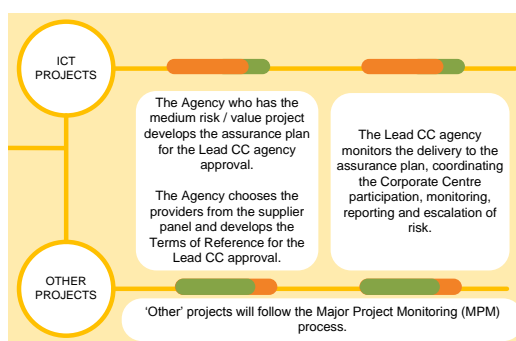
3.14 The following tables describe the key considerations for each of the activities within element 2 of the framework.

Key activities	Agency has responsibility and accountability for the development of the assurance plan with guidance and oversight of CC Lead assurance agency who will also approve the final plan. Corporate Centre and Agency choose the most appropriate QA providers and develop the Terms of Reference(s).
<p>The development of the assurance plan involves the Lead Corporate Centre assurance agency, Agency and other involved Corporate Centre parties working collaboratively to develop an assurance plan. The assurance plan is resourced and budgeted for as part of the project plan.</p> <p>The GCIO will apply the framework outlined in this document for high risk / value programmes and projects that are deemed to be ICT-enabled.</p> <p>Following the development of the assurance plan, the Corporate Centre agency and Agency work together to select the most appropriate Independent Quality Assurance (IQA) providers (when the plan has identified the requirement for this type of assurance). Until the AoG IQA /</p>	

TQA panel is established, the existing procurement practices of the specific departments will apply. The terms of reference is also developed collaboratively by the lead Corporate Centre agency and Agency to enable the assurance activity to meet the needs of the Agency and the Corporate Centre. Refer Appendix B for an Assurance Plan template and Appendix C for a Terms of Reference.

Key activities	The Lead Corporate Centre agency monitors the delivery to the assurance plan, coordinating the Corporate Centre participation, monitoring, reporting and escalation of risk.
<p>The Lead Corporate Centre agency consistently monitors the delivery to the assurance plan. Support, guidance and involvement of the Corporate Centre (including the GCIO) is provided as and where necessary.</p> <p>The lead Corporate Centre agency is also involved in coordinating the involvement of the Corporate Centre participation. The lead Corporate Centre agency is responsible for flagging concerns within the Agency and, where appropriate, to Ministers.</p> <p>Where there are material changes to the project / programme that impact the risk / value elements, the RPA and Assurance plan are to be updated and resubmitted outlining the responses to these changes.</p> <p>Agencies must ensure that outputs of assurance activities are provided to the GCIO Assurance Lead.</p>	

Element 3: Moderate Risk/Value Project



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

Outputs	Purpose of the outputs
Assurance plan	<p>Moderate risk / value projects produce the same outputs as the high risk / value project outputs detailed above. The outputs will also serve the same purpose as that of high risk / value projects. Moderate risk / value project outputs will be tailored to reflect the needs of these projects (i.e. the criteria, project / programme risk / value rating, assurance plan and terms of reference will be based on moderate risk / value projects).</p> <p>While all moderate risk / value ICT-enabled projects and programmes are expected to have a tailored costed and resourced assurance plan, only those selected by the Corporate Centre will need to submit their plan for approval by the lead Corporate Centre</p>
Terms of Reference	

Outputs	Purpose of the outputs
	assurance agency.

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

Key activities	The Agency who has the selected moderate risk / value project develops the assurance plan for the lead Corporate Centre assurance agency approval. The Agency chooses the providers from the supplier panel and develops the Terms of Reference for the lead Corporate Centre agency approval.
<p>The Agency leading the project / programme develops the assurance plan based on the risk / value assessment that was carried out. The lead Corporate Centre assurance agency (typically GCIO for ICT projects) reviews the assurance plan and provides feedback to the Agency. This process aims to address key risks and put adequate assurance activities / strategies in place. The lead Corporate Centre assurance agency works together with the Agency to check that the assurance plan is comprehensive and fit-for-purpose.</p> <p>Following the development of the assurance plan, the Agency selects the most appropriate IQA providers and develops the Terms of Reference. The Terms of Reference is reviewed by the lead Corporate Centre assurance agency. Again, the lead Corporate Centre assurance agency works together with the Agency to check that the Terms of Reference is comprehensive and fit-for-purpose.</p>	

Key activities	The lead Corporate Centre assurance agency monitors the delivery to the assurance plan, coordinating the Corporate Centre participation, monitoring, reporting and escalation of risk.
The considerations for the lead Corporate Centre assurance agency monitoring the delivery to the assurance plan, coordinating the Corporate Centre participation, monitoring, reporting and escalation of risk will reflect the same considerations as that of high risk / value projects (detailed in the Element 3 section above).	

Low Risk/Value Projects

3.17 Presently the framework does not apply to low risk / value projects. However, the GCIO recommends that Agencies follow good practice and develop a tailored Assurance plan for such projects / programmes.

4. Roles and responsibilities

- 4.1 The roles and responsibilities within the Projects and Programmes 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:

The 'doer'	Assurance design and ownership	Independent assessment and assurance	Governance and oversight
Owner of the risk, executes the risk management process, identifies, manages, mitigates, and reports on operational risk.	Develops the overall risk and assurance frameworks, and monitors adherence to the framework. Provides an overview of key risks and oversees the execution of the framework.	Independent testing and verification of the standards, policies and practices.	Provides governance and oversight. Establishes risk appetite and strategy. Approves frameworks, methodologies, policies, roles and responsibilities.

- 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 Projects and Programmes 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 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 Projects and Programmes 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)
	<ul style="list-style-type: none"> Programme / project team and sponsor. Vendors. 	<ul style="list-style-type: none"> All-of-government delivery, e.g., DIA Commercial Strategy and Delivery. All-of-government ICT vendors.
Key responsibilities within the Projects and Programmes assurance framework	<p>The primary responsibility of the 'doer' is to achieve the project / programme objectives and therefore own the associated risk management process on a day to day basis. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to:</p> <ul style="list-style-type: none"> Identify risks and implement appropriate mitigations. Keep governance and oversight functions informed about risks, 	

The 'doer'	
	<p>mitigations and alignment to the governance group's risk tolerance.</p> <ul style="list-style-type: none"> • Submit the risk rating to the Corporate Centre, and inform the Corporate Centre of any changes to the risk rating. • Engage with the Corporate Centre to develop the appropriate assurance practices over the programmes and projects (high to medium risk / value projects). • 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)
	<ul style="list-style-type: none"> • Enterprise Project Management Office. • Risk function. 	<ul style="list-style-type: none"> • Treasury Better Business Case. • Treasury Vote Analysts. • GCIO ICT Assurance. • Treasury/PPM.
Key responsibilities within the Projects and Programmes assurance framework	<p>Assurance Design (GCIO and Corporate Centre)</p> <p>The responsibility of the assurance design role is to develop an overall ICT Projects and Programmes Assurance Framework. In order to achieve the objectives set out within this framework, key responsibilities include, but are not limited to:</p> <ul style="list-style-type: none"> • 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. <p>Assurance Ownership (GCIO and Corporate Centre)</p> <p>The responsibility of the assurance ownership role is to monitor the 'doers' adherence to the ICT Projects and Programmes 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:</p> <ul style="list-style-type: none"> • Support agencies to lift capability, provide tools, and address key risks as required • Provide agencies with advice and guidance around the execution of the framework. • Provide support and approval of the agency's design and execution of the project's / programme's assurance plan (medium and high value / risk programmes and projects). • Provide support and approval of the agency's design and execution of the terms of reference for the project's / programme's assurance activities (medium and high value / risk programmes and projects). • Engage with the agency in any escalation process. • Analyse results of various assessments in order to provide a system-wide view of ICT risks. • Provide agencies with information regarding trends and common challenges. 	

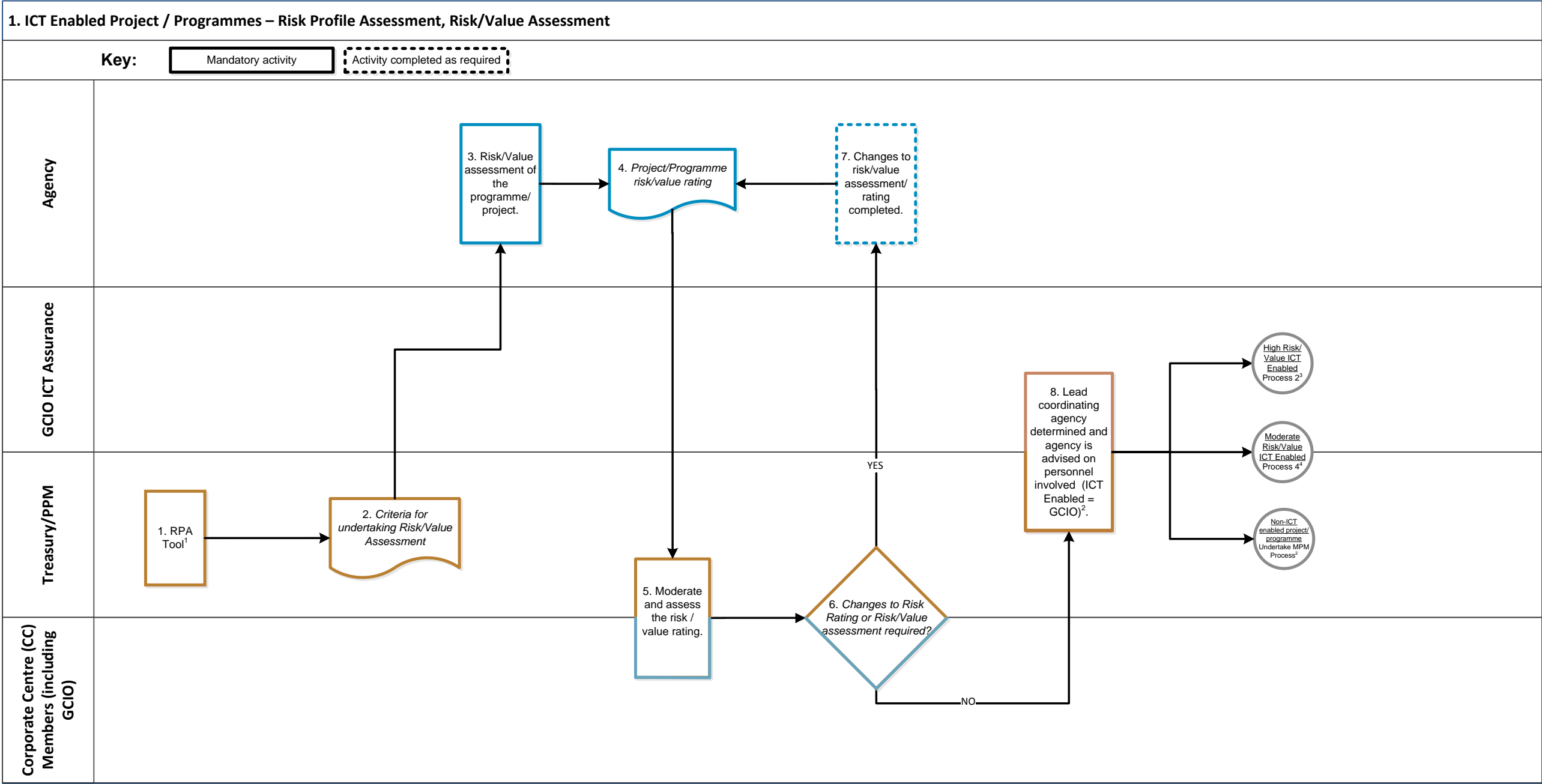
Assurance design and ownership	
	<ul style="list-style-type: none"> Communicate and report effectively with all lines throughout the model, where required.

Independent assessment and assurance		
Example functions	Agency function (illustrative)	System-wide functions (illustrative)
	<ul style="list-style-type: none"> Assurance services. Internal Audit. OAG-appointed External Auditor. Other sources of Assurance. 	<ul style="list-style-type: none"> All-of-government IQA / TQA panel. Gateway – delivery confidence. GCSB (for Top Secret systems).
Key responsibilities within the Projects and Programmes assurance framework	<p>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:</p> <ul style="list-style-type: none"> Assist in the development of the assurance plan. Execute the independent assessment to the terms of reference. Provide assurance with regard to delivery of successful outcomes. Communicate and report effectively with all lines throughout the model, where required. 	

Governance and oversight		
Example functions	Agency function (illustrative)	System-wide functions (illustrative)
	<ul style="list-style-type: none"> Chief Executive. Executive Leadership Team. Audit and risk committee. 	<ul style="list-style-type: none"> Cabinet. DPMC.
Key responsibilities within the Projects and Programmes assurance framework	<p>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:</p> <ul style="list-style-type: none"> Establish risk appetite and strategy. 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 overall oversight and success / failure of the programme and / or project. Communicate and report effectively with all lines throughout the model, where required. 	

Appendix A Process Maps

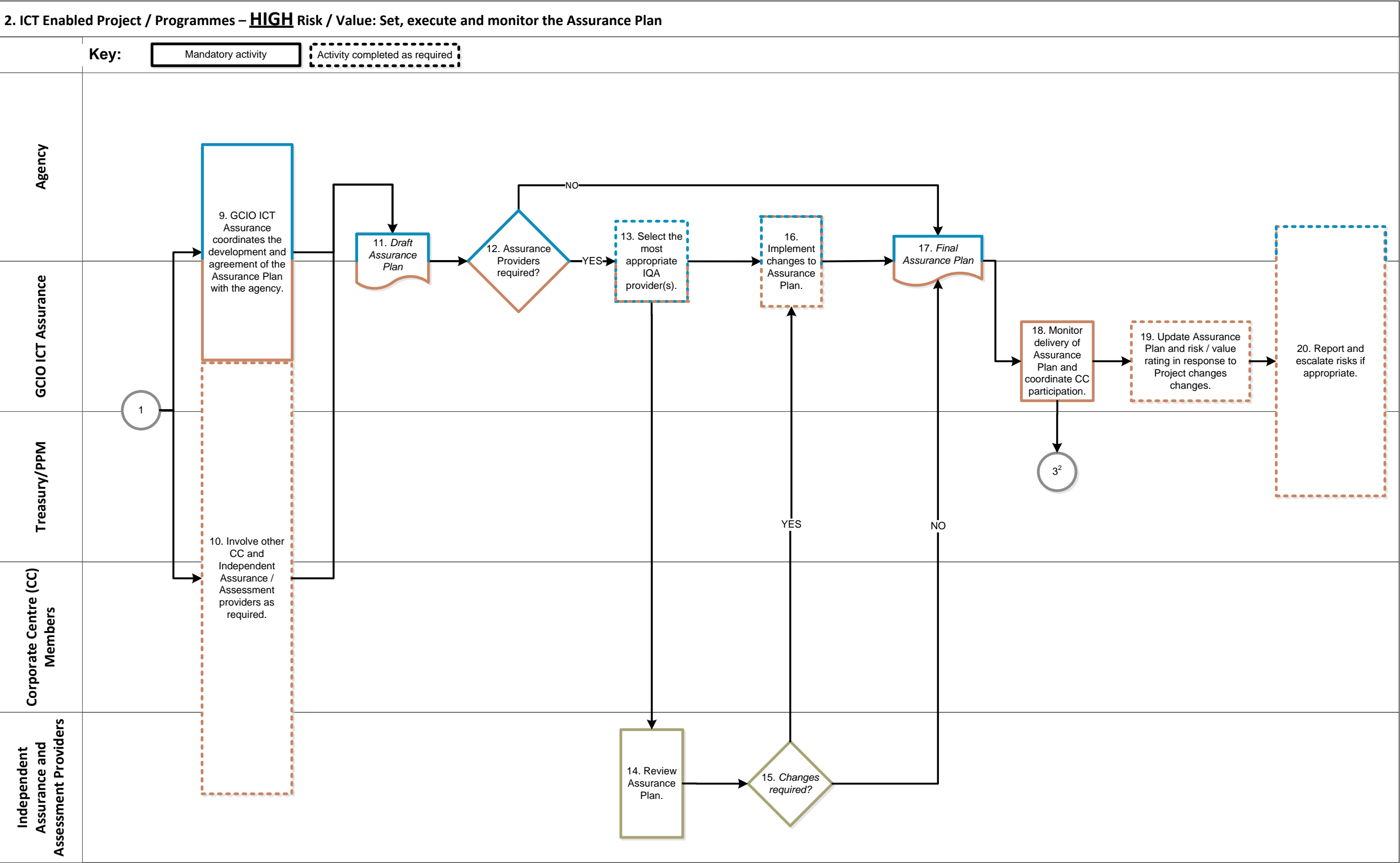
I. ICT Enabled Project / Programmes – Risk / Value assessment



Notes:

1. Risk Profile Assessment (RPA)
2. The GCIO will serve as the Lead Corporate Centre for ICT Enabled Projects and Programmes (refer section 2 for further information on the definition of an ICT enabled programme or project). The GCIO will always work with Treasury to determine the Lead coordinating agency. Projects/programmes that are not deemed 'ICT enabled' will follow the MPM process.
3. High risk/value projects/programmes, refer to process 2, 'High Risk / Value: Set, execute and monitor the Quality Assurance Plan'
4. Moderate risk/value projects/programmes, refer to process 4, 'Moderate Risk / Value: Set, execute and monitor the Quality Assurance Plan'

II. ICT Enabled Project / Programmes – High Risk / Value: Set, execute and monitor the Assurance Plan

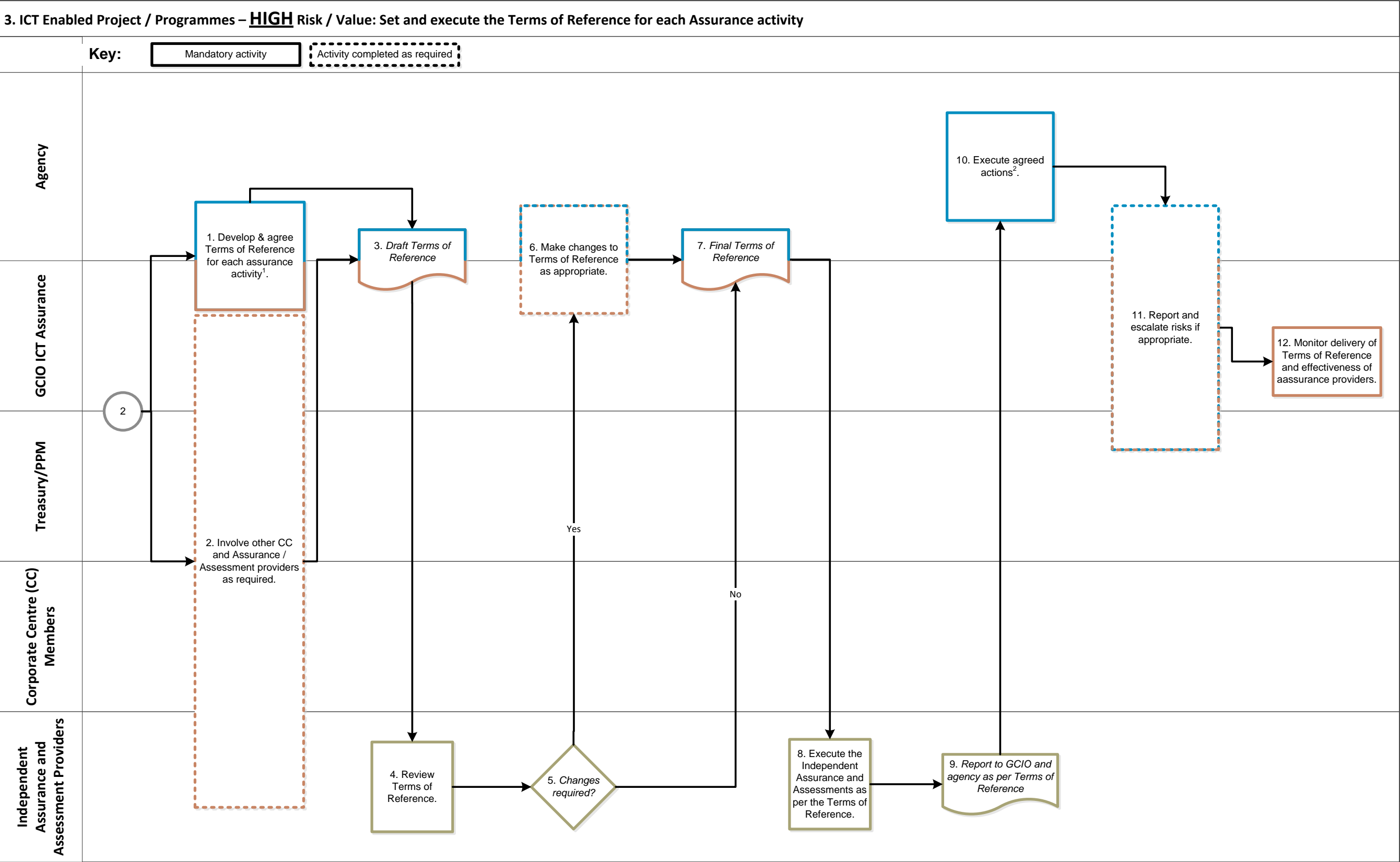


Notes:

1. The GCIO will serve as the Lead Corporate Centre for ICT Enabled Projects and Programmes (refer section 2 for further information on the definition of an ICT enabled programme or project). The GCIO will always work with Treasury to determine the Lead coordinating agency but this joint decision may result in another Lead Corporate Centre Agency being used if the Project/Programme is not deemed to be ICT Enabled.

2. Please refer to Process 3, 'ICT Enabled Project / Programmes – High Risk / Value: Set and execute the Terms of Reference'

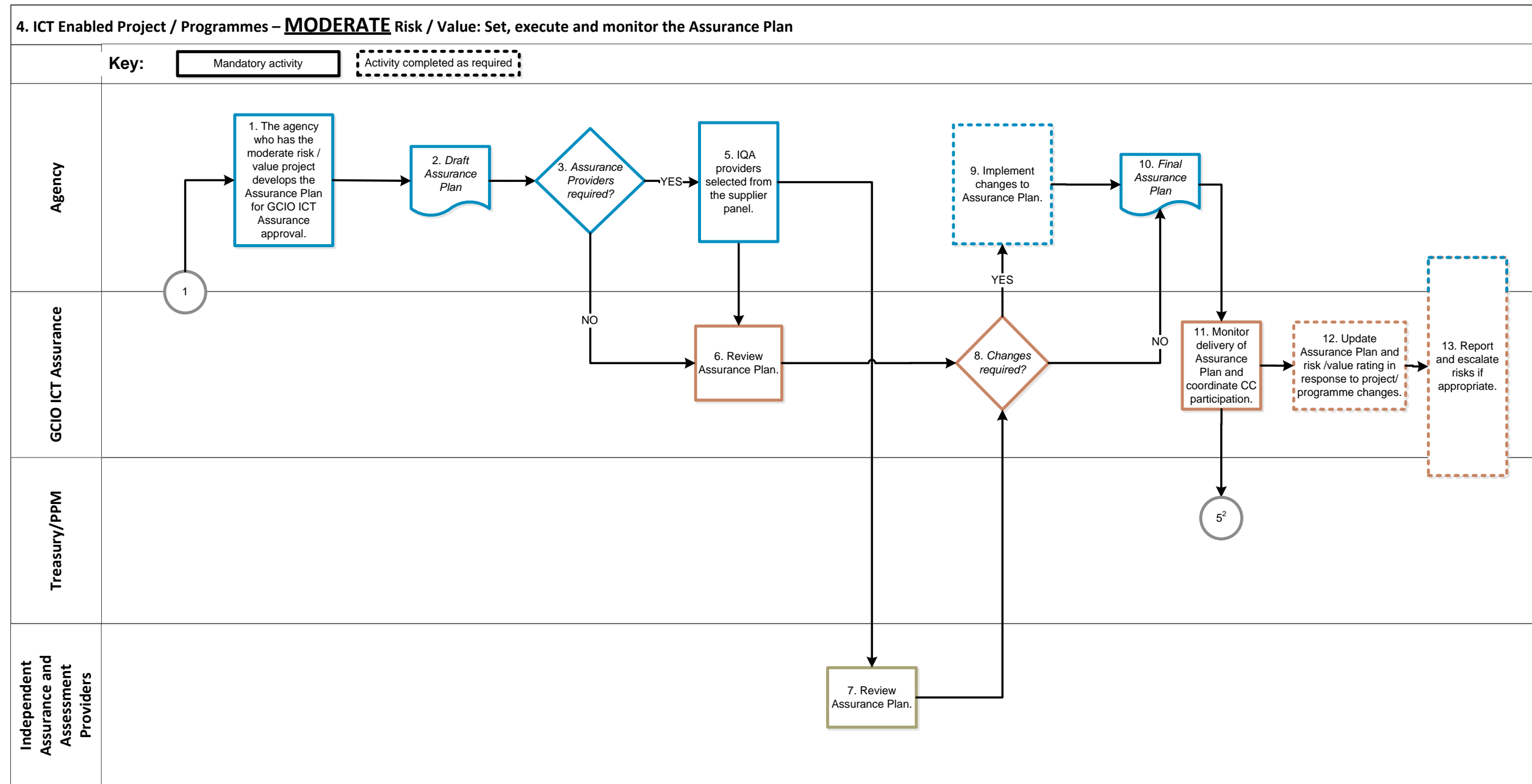
III. ICT Enabled Project / Programmes – High Risk / Value: Set and execute the Terms of Reference for each Assurance activity



Notes:

1. For the Assurance activities that The CC and GCIO involvement has been agreed as per the Assurance Plan. This process excludes Assurance actions for which there is no GCIO involvement required.
2. Support, guidance and involvement of the Corporate Centre (including the GCIO) will be provided as and where necessary.

IV. ICT Enabled Project / Programmes – Moderate Risk / Value: Set, execute and monitor the Assurance Plan

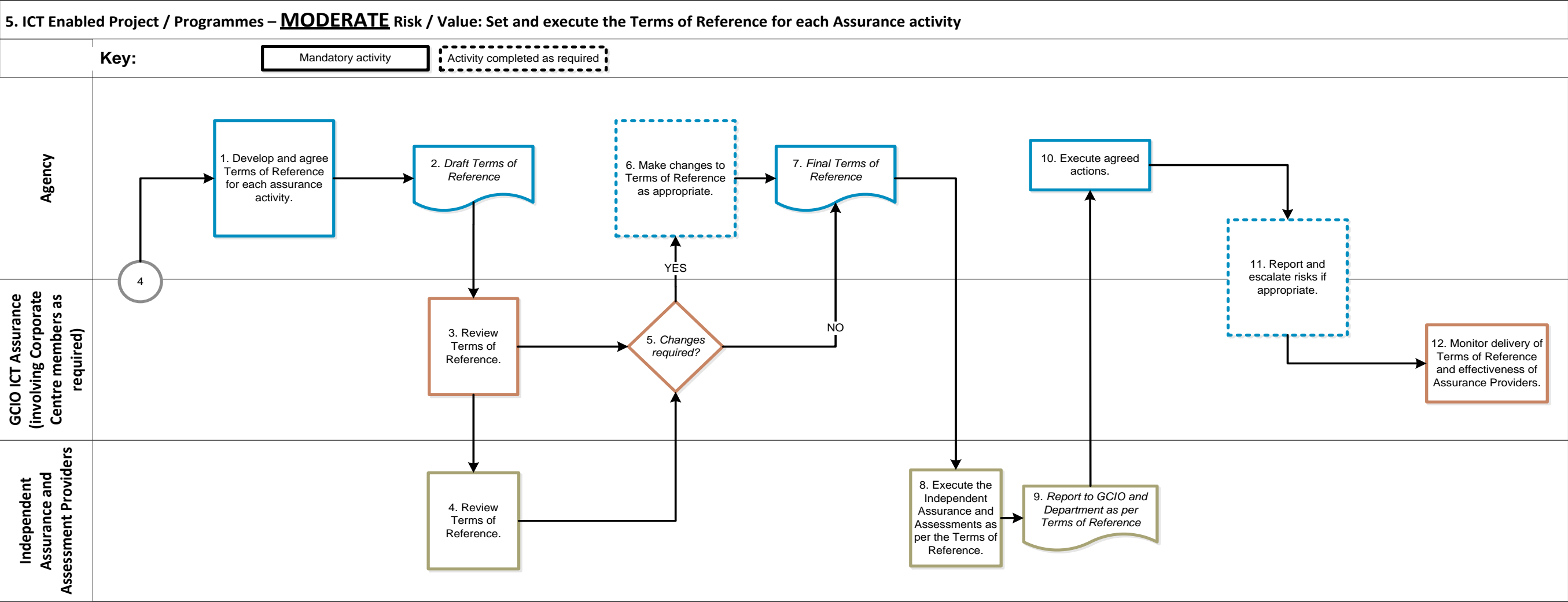


Notes:

1. The GCIO will serve as the Lead Corporate Centre (CC) Agency for ICT Enabled Projects and Programmes (refer section 2 for further information on the definition of an ICT enabled programme or project). The GCIO will always work with Treasury to determine the Lead Corporate Centre Agency but this joint decision may result in another Lead Corporate Centre Agency being used if the Project/Programme is not deemed to be ICT-enabled.

2. Please refer to Process 5, 'ICT Enabled Project / Programmes – Moderate Risk / Value: Set and execute the Terms of Reference for each Assurance Activity'

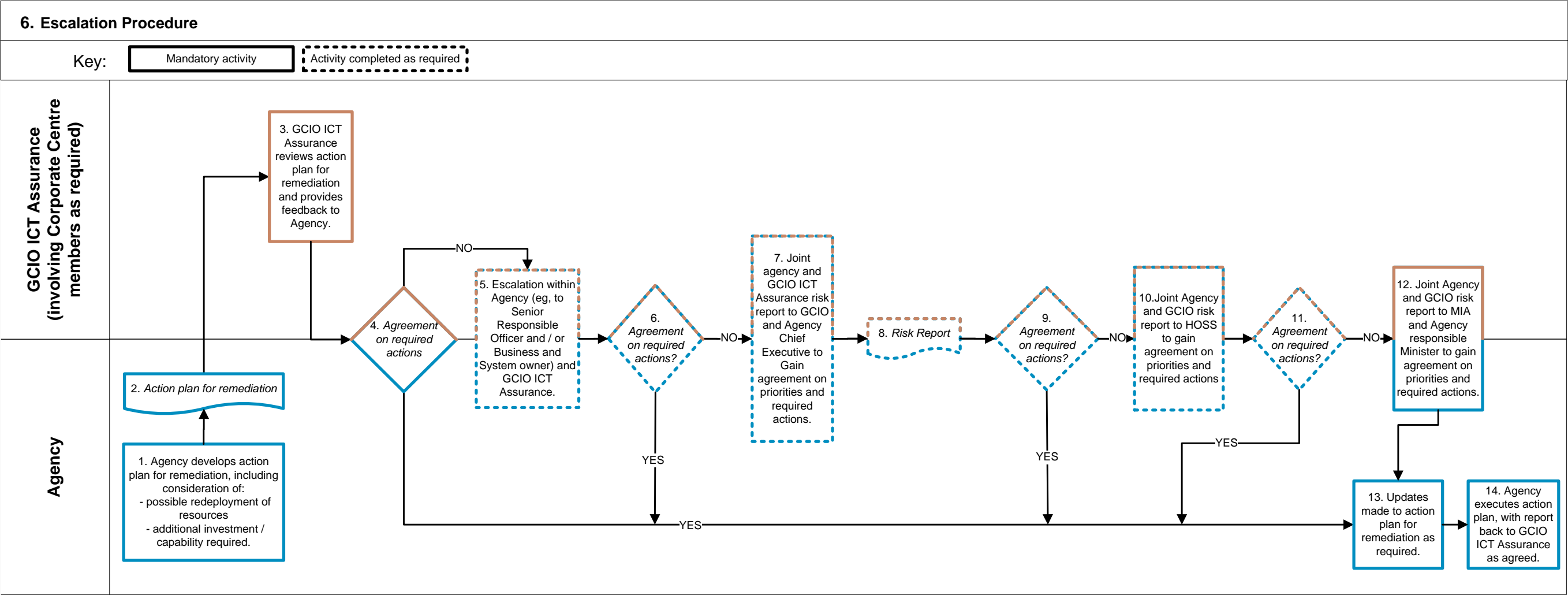
V. ICT Enabled Project / Programmes – Moderate Risk / Value: Set and execute the Terms of Reference for each Assurance activity



Notes

1. Support, guidance and involvement of the Corporate Centre (including the GCIO) will be provided as and where necessary.

VI. Escalation procedure



**Appendix B Projects and programmes assurance plan
template [Version 2.0] – [CLICK HERE TO ACCESS A WORD
DOCUMENT VERSION OF THE TEMPLATE \[80kb, Word\]](#)**

[Agency Name]

[Project / Programme Name]

Assurance Plan

Version Number

Date

Document Approval

	Name / Title	Sign-off Date
Approved by Senior Responsible Officer		
Endorsed by the Project / Programme Board		
Endorsed by GCIO ICT Assurance		

1. PROJECT / PROGRAMME CONTEXT

1.1 Key Objectives and Outcomes

[Outline the key objectives, scope, outcomes, benefits and success criteria of the project / programme. For programmes only, include a high level overview of how the programme is structured in terms of tranches and/or projects.]

1.2 Costs and Benefits

[Insert the estimated whole-of-life cost and expected monetary benefits of the project / programme.]

	NZD \$
Estimated Whole-of-life Cost (WOLC)	
Expected Monetary Benefits	
WOLC Duration	

1.3 Risk Rating

[Insert the indicative risk rating from the Risk Profile Assessment (RPA).]

Indicative Risk Rating from Risk Profile Assessment (RPA)	
---	--

[Outline the strategic and delivery risks identified for the project / programme.]

1.4 Referenced Documents

Document Name	Version Number
[Provide details of documents referenced in the assurance plan.]	

2. ASSURANCE PLAN OVERVIEW

2.1 Assurance Approach

[Outline the overall assurance approach for the project / programme, including any specific methodologies to be followed.]

2.2 Lessons Learned

[Outline any specific lessons learned from similar projects / programmes (either internally or publicly available) and how you have incorporated these into assurance activities. Refer also to Gateway Lessons Learned⁷ and GCIO ICT Assurance Top 10 Lessons Learned from ICT-enabled projects and programmes⁸.]

2.3 Key Assurance Activities

[Outline the key internal and external assurance activities for the project / programme e.g. Management Oversight, Internal Audit, Independent Quality Assurance (IQA), Technical Quality Assurance (TQA), Gateway, etc.]

Assurance Activity	Purpose	Audience

2.4 Assurance Roles and Responsibilities

[Outline roles and responsibilities at the governance level with respect to assurance activities. For example,

- Who is responsible for reviewing and updating the assurance plan?
- How will progress against the assurance plan be monitored at the governance level?
- Who will receive copies of assurance reports?
- How will the status of findings recommendations raised in assurance reports be tracked and reported at the governance level?]

2.5 Assurance Budget

[Insert the estimated cost of the assurance activities covered by the assurance plan and state whether the cost is included in the project / programme budget.]

	NZD \$
Estimated Assurance Cost	

⁷ <http://www.ssc.govt.nz/gateway-lessons-learned>

⁸ <http://ict.govt.nz/ict-system-assurance/ict-assurance-frameworks/ict-projects-and-programmes-assurance-framework/guidance-and-templates>

3. DETAILED ASSURANCE PLAN⁹

3.1 Critical Project / Programme Milestones

Outlined below are the assurance activities that will be performed over the critical project / programme milestones and decision points:

Milestone	Indicative Due Date	Assurance Activity / Purpose	Assurance Provider	Status
[Insert key milestones that represent a key deliverable or programme / project transition]	[Insert indicative milestone / delivery due date]	[Insert assurance activity / purpose]	[Insert assurance provider e.g. Internal Audit, IQA provider]	[Insert status of assurance activity]

3.2 Ongoing Project / Programme Assurance Activities

Outlined below are assurance and oversight activities that will occur at regular intervals over the project / programme risks:

Assurance Activity / Purpose	Key Risks	Assurance Provider	Frequency
[Insert assurance activity / purpose]	[Insert the key risks covered by the assurance activity]	[Insert assurance provider e.g. Internal Audit, IQA provider]	[Insert how often the assurance activity will occur e.g. monthly]

3.3 Critical Project / Programme Dependencies

Outlined below are critical project / programme dependencies (external to the project / programme) and associated assurance activities:

Dependency	Key Date	Assurance Activity	Assurance Provider
[Insert critical dependency and the nature of the dependency]	[Insert the date / period the dependency impacts on the project / programme]	[Insert assurance activity / purpose]	[Insert assurance provider e.g. Internal Audit, IQA provider]

⁹ Each assurance activity is supported by a specific terms of reference. The terms of reference should be referred to for detailed information regarding the assurance activity.

4. DECISION MAKING AUTHORITY

Outlined below is the decision making authority for all parties involved in the design and approval of the specific **terms of reference** for each type of assurance activity.

	Decision Making Authority
R	Recommend(s) the terms of reference for the assurance activity
A	Approve(s) ¹⁰ the terms of reference for the assurance activity
C	Consulted in reaching the terms of reference for the assurance activity
I	Informed of the terms of reference for the assurance activity

Assurance Activity	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]	[Insert Name or Role / Group]
[Insert assurance activity]									

¹⁰ GCIO ICT Assurance will review and endorse the terms of reference for IQA / TQA reviews for monitored projects.

Appendix C IQA / TQA Terms of reference template [Version 1.0]

[Agency name]

Terms of Reference for [insert name of
assurance type/activity]

[Project/programme name]

[Date and version number]

Name/title and Organisation	
Prepared by:	
Approved by:	
Issued to:	
Key Contacts:	Name/title and Contact Details
Senior Responsible Owner	
Project/Programme Manager	
Assurance Providers	

1. Assurance assessment

1.1 Purpose and objectives

[Outline the key purpose/objectives of the assurance activity]

1.2 Scope of the assessment

The following documents should be read in conjunction with this Terms of Reference:

In scope	Out of scope
[Insert what is in scope for the assessment]	[Insert what is out of scope for the assessment]

1.3 Approach to the assessment

[Outline the approach to the assurance activity/assessment]

1.4 Timeline

The time line for the assurance assessment is outlined below:

Activity	Start date	Finish date
[Insert action]	[Insert start date]	[Insert completion date]

1.5 Interviews

Listed below are the people to be interviewed:

Name	Title/organisation	Role in the project
[Insert the person's name]	[Insert the person's title/organisation]	[Insert the person's relationship to the project]

1.6 Documents

Listed below are the documents to be reviewed:

Document
[Insert the document to be reviewed]

1.7 Resources assigned

Listed below are the people who are assigned to undertake this assessment:

Name	Title/organisation
[Insert the person's name]	[Insert the person's title/organisation]

1.8 Deliverables

[Describe the deliverables from the assurance activity/assessment]

Outlined below are who will receive each deliverable (include drafts as a separate deliverable):

Deliverable	Person/Title/Organisation	Secure action	Reviewed prior to release	Provided for their information
[Insert deliverable]	[Insert the person's name title & organisation]	[Yes/No]	[Yes/No]	[Yes/No]

Appendix D Glossary of abbreviations and terms

Term	Description
Agency	<p>Term used to describe entities within the New Zealand state sector, including:</p> <ul style="list-style-type: none"> • Public Service Departments. • Non-Public Service Departments. • Crown Entities. • Public Finance Act Schedule 4 Organisations. • Reserve Bank of New Zealand. • Offices of Parliament. <p>Refer State Services Commission list of Central Government Agencies - http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf.</p>
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	<p>An organisation that forms part of New Zealand's state sector established under the Crown Entities Act 2004.</p> <p>Refer State Services Commission list of Central Government Agencies - http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf.</p>
Department	<p>Term used to describe Public Service Departments and Non-Public Service Departments within the state sector.</p> <p>Refer State Services Commission list of Central Government Agencies - http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf.</p>

Term	Description
External Audit	<p>An independent statutory audit (typically annual) of the financial reports of organisations in order to express an independent opinion on whether the report:</p> <ul style="list-style-type: none"> complies with the recognised framework of generally accepted accounting practice (known as “GAAP”); and fairly reflects the entity’s financial performance and financial position. <p>(Controller and Auditor General).</p>
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	<p>Information and Communications Technology, which spans:</p> <ul style="list-style-type: none"> 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	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 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.
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 and the Board are willing to accept on an aggregate basis in relation to strategic and business objectives.
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).