Department of Customer Service

Digital Assurance Framework

Version number: Final v3.1

March 2024

NSW GOVERNMENT

Acknowledgement of Country

The NSW Department of Customer Service acknowledges the Traditional Custodians of the lands where we work and live. We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

We pay our respects to Elders past and present and acknowledge the Aboriginal and Torres Strait Islander people that contributed to the development of this Policy.

We advise this resource may contain images, or names of deceased persons in photographs or historical content.

Published by the NSW Department of Customer Service

nsw.gov.au/customer-service

First published: Jan 2017

More information

Digital Strategy, Investment and Assurance

Digital NSW

NSW Department of Customer Service

McKell Building

2/24 Rawson Place

Haymarket NSW

Copyright and disclaimer

Contents

Version name	Date	Purpose
Internal Draft version 0.1	24/4/2020	Internal ICT Assurance working draft
Draft version 0.2	24/4/2020	Draft for Treasury, Infrastructure NSW and Agency comment
Final Draft v0.3	26/08/2020	Final Draft for DaPCo Submission
Final Draft	6/01/2021	Included revision to incorporate Digital Restart Fund
Version 2 Final	5/07/2023	Minor edit to remove references to obsolete governance forums
Version 3 Final Draft	12/01/2023	Updates to framework title and risk criteria descriptions in Appendix A including reference to Artificial Intelligence risk.
Version 3.1 Final	15/05/24	Change Infrastructure, Services and Strategic Investment Working Group (ISSI) governing committee name change to Digital Assurance Risk Advisory Group (DARAG)

Summary

Name	Digital Assurance Framework (DAF)
Responsible Minister	Minister for Customer Service and Digital Government
Cluster	Customer Service
Gateway Coordination Agency	Department of Customer Service
Sponsor contact details	Laura Christie, Government Chief Information and Digital Officer, Deputy Secretary, Digital.nsw
Priority	High
Objectives	The objective of the Digital Assurance Framework is to ensure NSW Government's ICT projects are delivered on time and on budget through the implementation of this risk-based independent assurance framework.
Relationship with Government policies	NSW Gateway Policy NSW Treasury Guidelines for Capital Business Cases[1] Commercial Policy Framework NSW Recurrent Assurance Framework (REAF) Infrastructure Investor Assurance Framework (IIAF) Benefits Realisation Management Framework (BRM)[2] NSW Government Expert Reviewer Panel Framework NSW Cyber Security Policy NSW Government Artificial Intelligence Assurance Framework
Proposed commencement	Ongoing

[1] Reference to NSW Treasury Business Case Guidelines https://www.treasury.nsw.gov.au/information-public-entities/business-cases

[2] Reference to Benefits Realisation Management Framework: https://www.finance.nsw.gov.au/publication-and-resources/benefits- realisation-management-framework

Glossary

Term	Definition
Clearance of gate	Notification to a Delivery Agency by DCS that a Gateway Review or Health Check for a project has been cleared, i.e. an appropriate Close-out Plan is in place to assist with project development or delivery and critical recommendations are met.
Close-out Plan	Document outlining actions, responsibilities, accountabilities and timeframes that respond to recommendations identified in Gateway Review and Health Check Reports.
Complex project	A number of elements contribute to project complexity, such as delivery in multiple stages, varying time periods for stages, the degree of business change, and/or a number of inter-dependencies. Individual project stages may be identified during the development phase or during the procurement and delivery phases (when individual project stages are being procured and delivered under different contracts and potentially over different time periods). In some cases, these individual project stages may have a different Project Tier to the overall complex project.
Deep Dive Reviews	Deep Dive Reviews are similar to a Health Check but focus on a particular issue or limited terms of reference rather than the full range of issues normally considered at a Health Check. These Reviews are generally undertaken in response to issues being raised by key stakeholders to the project or at the direction of the relevant Government Minister.
Delivery Agency	The Government agency tasked with developing and / or delivering a project applicable under this Framework and the NSW Gateway Policy.
DCS Assurance Unit	The dedicated team within DCS responsible for implementing and administering the DAF including organising reviews.
Digital Restart Fund (DRF)	The purpose of the Digital Restart Fund (DRF) is to accelerate whole of government digital transformation. It has been designed to enable iterative, multi-disciplinary approaches to digital/ICT planning, development and service provision and complements existing investment approaches in IDIA. https://www.digital.nsw.gov.au/funding/digital-restart-fund
Estimated To Complete (ETC)	The financial performance index and project management measure that shows you the remaining cost you expect to pay in order to complete a project
Total Cost of Ownership (TCO)	Total capital spend (including from capital envelopes) and recurrent spend of the project/program (including the non-ICT components) -over the period of time defined in the project/program business case.
Expert Reviewer Panel	Panel comprising independent highly qualified Expert Reviewers established to cover all aspects of Gateway Review needs.
Gate	Particular decision point(s) in a project/program's lifecycle when a Gateway Review may be undertaken.

Term	Definition
Gateway Coordination Agency (GCA)	The agency responsible for the design and administration of an approved, risk-based model for the assessment of projects/programs, the coordination of Gateway Reviews and the reporting of performance of the Gateway Review Process, under the NSW Gateway Policy.
Gateway Review	A Review of a project/program by a Review Team at a specific key decision point (Gate) in the project/program's lifecycle. A Gateway Review is a short, focused, independent expert appraisal of the project/program that highlights risks and issues, which if not addressed may threaten successful delivery. It provides a view of the current progress of a projects/programs assurance and that it can proceed successfully to the next stage with any critical recommendations addressed.
Gateway Review Manager	The Gateway Review Manager guides the implementation of the Gateway Review or Health Check. The Manager facilitates the Review but does not participate in the Review.
GCA Framework	A framework designed and operated by a GCA, that assesses the risks associated with a project or program of a particular nature in order to determine the application of Gateway. A GCA Framework defines the roles and responsibilities to deliver Gateway and aligns with the Gateway Review process outlined in the NSW Gateway Policy.
Health Check and Agile Health Check	Health Check is an independent review carried out by a team of experienced practitioners seeking to identify issues in a project/program which may arise between Gateway Reviews. For projects following an Agile methodology, a more suitable and flexible Health Check, the Agile Health Check, is carried out as an independent review by a team of experienced practitioners.
High Priority (High Risk/High Profile) Projects	High Priority projects receive greater scrutiny – that is more reporting is required and more assessments are conducted. Projects are determined as high priority determined assessing the project risk. All Tier 1 projects are treated as High Priority projects.
ICT	The infrastructure and components that enable modern computing. The term is generally accepted to mean all devices, networking components, applications and systems that combined allow people and organizations to interact in the digital world. This may include stand-alone Operational Technology projects and programs as agreed with Infrastructure NSW.
ICT and Digital Assurance Portal	ICT Assurance online portal for DAF project registration and risk profiling, and reporting.
ICT and Digital Leaders Group (IDLG)	Made up of Chief Information/Digital Officers from every cluster. The primary governance forum for ICT and Digital including strategy, key decisions and work programs in the NSW Government.
Digital Assurance Risk Advisory Group (DARAG)	Made up of Chief Information/Digital Officers from every cluster and representatives from the ICT and Digital Assurance Branch from DCS. Responsible for supporting the operation of the DAF by providing advice to the Government Chief Information and Digital Officer (GCIDO) and the IDLG and for monitoring projects by taking a Whole of Government perspective.

Term	Definition
Independence	Characterises a role or a process within the DAF that is not influenced or controlled by the delivery agency or the delivery agency's project team. A conflict of interest test should be undertaken with the delivery agency's project to ensure that the specific role(s) commissioned have no conflict of interest with the project nor its sponsoring agency.
Investor	The Government, representing the State of NSW.
Mixed project	A project or program that contains a material combination of elements relating to multiple GCA frameworks.
Modified Project Assurance Plan	Document prepared by Delivery Agencies and lodged with DCS for endorsement after completion of a particular Gateway Review, after which a program or complex project may be considered in its component parts. For complex projects this would be individual stages, for programs this would be individual projects or sub-programs. The Modified Project Assurance Plan outlines the proposed Delivery Agency assurance arrangements for future Gateway Reviews for each individual component of work initiated (stage/project/sub-program).
Operational Technology	Systems used to control critical infrastructure. Can include systems that relate to service delivery, such as tolling systems, rail signalling or technology to support a new school or hospital.
Policy Owner	For the purpose of the NSW Gateway Policy, the Policy owner is NSW Treasury.
Portfolio	The totality of an organisation's ICT investment program.
Program	A temporary, flexible organisation 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 the organisation's strategic objectives. A program could be longer term and have a life that span more than 1 year. Projects that form part of a program may be grouped together for a variety of reasons including spatial co-location, the similar nature of the projects or projects collectively achieving an outcome. Programs provide an umbrella under which these projects can be coordinated. The component parts of a program are usually individual projects or smaller groups of projects (sub-programs). In some cases, these individual projects or sub-programs may have a different Project Tier to the overall program.
Project	A temporary organisation, usually existing for a shorter duration than a program, which will deliver one or more outputs in accordance with an agreed business case. Projects are typically delivered in a defined time period on a defined site. Projects have a clear start and finish. A particular project may or may not be part of a program. Where a project is delivered in multiple stages and potentially across varying time periods it is considered a 'complex project'. Refer to the definition for 'complex project'.
Project Assurance Plan	Document prepared by Delivery Agencies and lodged with DCS for GCIDO confirmation when registering projects via the ICT Assurance Portal.

Term	Definition
	Project Assurance Plans detail proposed Delivery Agency initiated project assurance arrangements in line with the DAF requirements.
Project Risk Profile Tool	Online tool as part of the ICT Assurance Portal available to Delivery Agencies to self- assess risk profile of projects/programs.
Project Sponsor	The Delivery Agency executive with overall responsibility for ensuring that a project meets its objectives and delivers the projected benefits.
Project Sponsor-Commissioned Review	The Project Sponsor commissioning an independent milestone or health check review on the project using the relevant Gateway Review Toolkit as part of its internal assurance arrangements. These are required at certain gates for Tier 3 and Tier 4 projects. Reviewers must be independent of the Delivery Agency and the project team.
Project Tier	Tier-based classification of project profile and risk potential based on the project's estimated total cost and qualitative risk profile criteria (level of government priority, interface complexity, sourcing complexity, agency capability, technical complexity, change complexity and cyber security). The Project Tier classification is comprised of five Project Tiers, where Tier 1 encompasses projects deemed as being the highest risk and profile (Tier 1 – High Profile/High Risk projects), and Tier 5 with the lowest risk profile.
Review Team	A team of expert independent reviewers, sourced from the Expert Reviewer Panel, engaged to undertake a Gateway Review, Health Check or Deep Dive Review.

Acronyms

Abbreviation	Definition
CEO	Chief Executive Officer
CIO	Chief Information Officer
DARAG	Digital Assurance Risk Advisory Group
IDLG	ICT And Digital Leadership Group
DCS	Department of Customer Service
DPC	Department of Premier and Cabinet
DRF	Digital Restart Fund
ERC	Cabinet Standing Committee on Expenditure Review
ETC	Estimated Total Cost
GCA	Gateway Coordination Agency
GCIDO	Government Chief Information and Digital Officer
HPHR	High Profile/High Risk
DAF	Digital Assurance Framework
ICT	Information and Communications Technology
IDIA	ICT Digital Investment and Assurance
INSW	Infrastructure NSW
Portal	ICT Assurance Portal
SOC	State Owned Corporation

1 Introduction

On 8 June 2016, NSW Government agreed to strengthen NSW Government ICT Investment Governance Model to improve ICT investment outcomes and deliver better value ICT projects. This model requires all ICT projects/programs to be assessed under a new risk-based Digital Assurance Framework (DAF) in accordance with the NSW Gateway Policy.

This framework document sets out the principles and arrangements for the DAF, and covers:

- Gateway Assurance Review of ICT projects as per NSW Gateway Policy
- Application of best practice in project/program governance and delivery such as due diligence and milestone reviews requested by a Project Sponsor. In these cases, the review is commissioned by and for the Project Sponsor using the DAF Gateway Review Toolkit
- Strategic imperatives, Business Outcomes and delivery-focused investment principles that NSW Government ICT investments must comply with

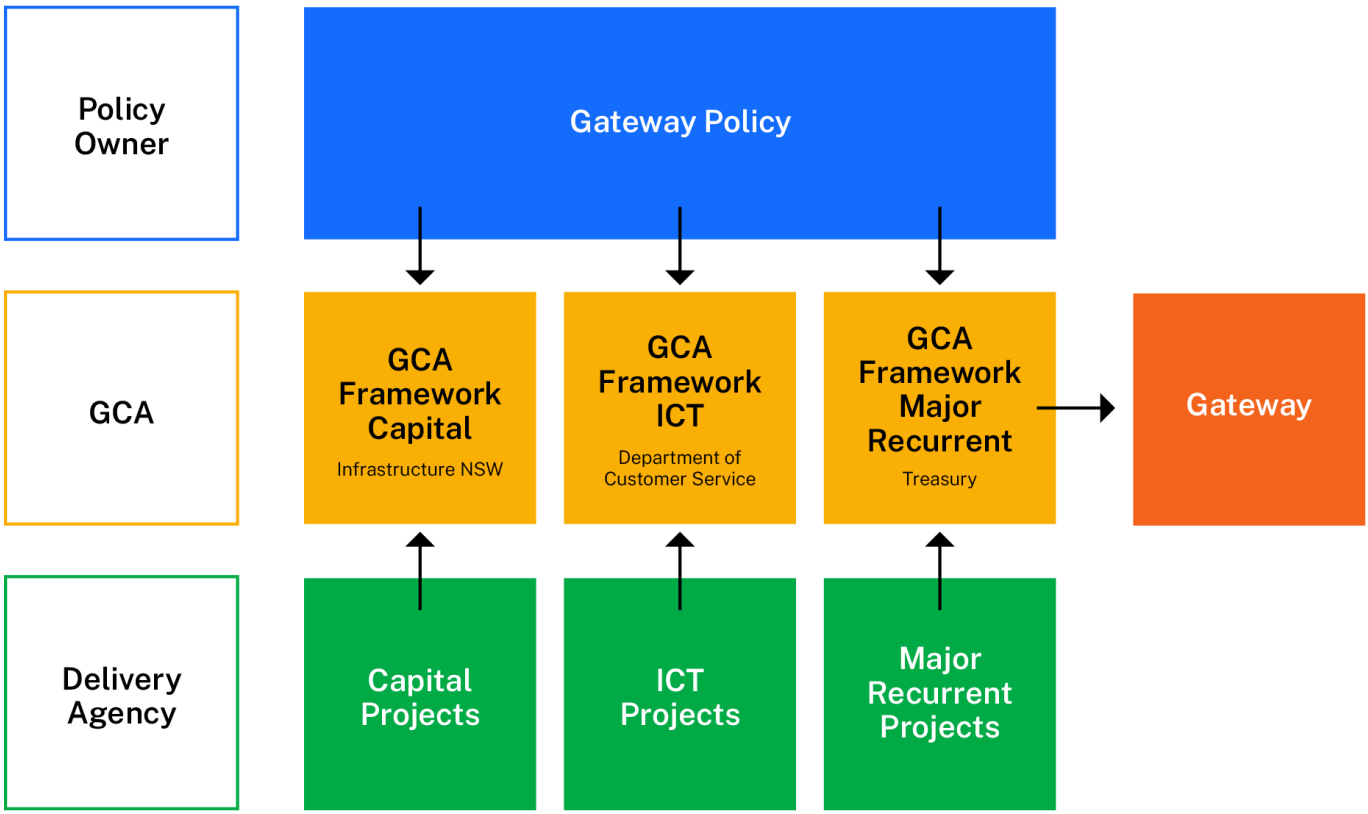
The aim of the DAF is to ensure NSW Government's ICT projects are delivered on time, on budget and deliver outcomes through the implementation of this risk-based independent assurance framework. The DAF provides the NSW Government effective tools to monitor this investment, receive early warning of emerging issues, and act ahead of time to prevent projects from failing.

1.1 Relationship between the DAF and NSW Gateway Framework

Under the proposed NSW Gateway Policy, three risk-based assurance frameworks focus on specific areas of investment, with Infrastructure NSW – the coordinating agency for capital infrastructure projects, DCS – the coordinating agency for ICT and Digital projects (capital and recurrent funded), and Treasury for major recurrent programs.

Figure 1 summarises the interaction between the NSW Gateway Policy[3], Gateway Coordination Agency (GCA) Frameworks and delivery of Gateway reviews.

Figure 1. NSW Gateway framework



[3] NSW Gateway Policy.

2 Framework Principles

2.1 Digital Assurance

The *Digital Assurance Framework* (DAF) is an independent[4] risk-based assurance process for the State's capital and recurrent ICT and Digital projects. It identifies the level of confidence that can be provided to Cabinet and Cabinet sub-committees that the State's ICT and Digital projects are being effectively developed and delivered in accordance with the Government's objectives.

The framework's key features are categorised under the following headings:

Accountability -

- a single point of accountability for independent assurance across all NSW Government ICT and Digital projects/programs
- ensuring collective accountability among Delivery Agency Secretaries/CEOs/CIOs for best-for-Government outcomes through the ICT governance arrangements, reporting through DCS to the Minister for Customer Service and Cabinet/ERC
- Delivery Agencies retaining direct accountability for particular projects and programs

Transparency -

- ensuring alignment to the NSW Government ICT and digital strategic direction, the NSW Government Enterprise Architecture and other relevant government reforms, also enabling opportunities to reduce risk and cost through better collaboration, re-use or shared solutions
- ensuring alignment with ICT and Digital strategic imperatives and investment principles
- ensuring Digital Assurance is effectively conducted for relevant digital projects e.g. through the DRF

Agility -

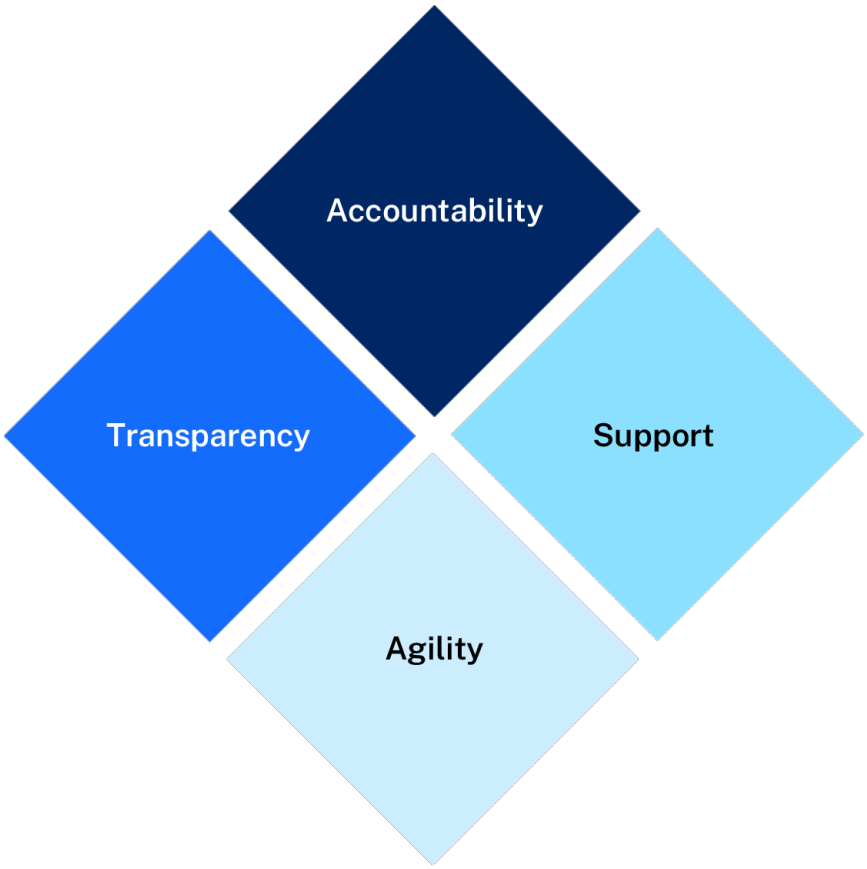
- a focus on what matters by taking a tiered approach based on project/program risk assessment

Support -

- escalating the levels of scrutiny and/or interventions applied to projects as and when emerging risks are reported/detected
- improved reporting and data collection through the ICT and Digital Assurance portal
- ensuring Project Sponsors complete project sponsor training coordinated by DCS

[4] Independent means independent of a Delivery Agency and a project unit.

Figure 2: Key features of DAF



The DAF is applied through a range of products and services delivered by DCS including:

- a portfolio level review of each Cluster's current and planned ICT and Digital investment
- a series of focused, independent reviews at key project/program milestones, which are independent of Delivery Agencies and projects and include Gateway Reviews and periodic Health Checks/Deep Dives
- a series of focused independent digital assurance showcases
- risk-based project reporting provided by Delivery Agencies and
- risk-based project monitoring conducted by DCS

The DAF does not take away from delivery Agency assurance requirements to meet internal governance arrangements or the need to prepare business cases to support funding decisions in the event that a project does not require a Gateway Review under the DAF.

2.2 Benefits of the DAF

Using a risk-based approach, managed by a centralised independent body achieves the following benefits:

Whole of Government:

- a consistent whole-of-government approach to investor assurance for ICT and Digital projects providing confidence in the portfolio
- provide a portfolio/account level view of the Government's ICT and Digital investment to drive strategic whole of government opportunities and reduce risk and cost through better collaboration, re-use or shared solutions
- foster the sharing of skills, resources, experience and lessons learned within and across the government sector including state digital assets/infrastructure

Taxpayer Value:

- a focus on return on investment outcomes, not outputs
- more systematic and transparent metrics which adds value and weight to decision making and risk reduction
- greater analytic support for the Government as an investor, before and after an investment decision has been made, rather than project-level assurance only

Risk Management:

- a regular level of due diligence that reflects the level of budget risk and complexity for each project, focusing investor assurance resources towards high-risk complex projects
- increasing transparency regarding project development/delivery risks and progress
- contributing to improved levels of compliance with the Gateway Review process applied from the commencement of project development to project implementation, providing confidence to Cabinet

Public Good:

- improving public confidence in the timely provision of value for money ICT and Digital investments, and
- contributing to job growth and the State's competitiveness through ICT and Digital

2.3 Application

The DAF applies to all ICT and Digital projects being developed and/or delivered by:

- general Government agencies and Government Businesses State Owned Corporations (SOCs) as required by NSW Treasury under NSW Treasury's Commercial Policy Framework

Secretaries and Chief Executives are accountable for ensuring all ICT and Digital projects meet the requirements of the DAF.

ICT and Digital projects include:

- ICT
- Digital Investments
- Operational Technology (BAU[5]), or
- other projects or programs as directed by Cabinet.

Projects will fall within the scope of the DAF if they meet the following criteria:

- all ICT and Digital projects with a cost of more than $5M, regardless of funding source
- projects funded by the Digital Restart Fund
- projects yet to submit a business case to NSW Treasury, unless excluded by the GCA
- projects currently in procurement or in delivery, unless excluded by the GCA, and
- projects otherwise nominated by the Policy Owner/Sponsor

The ICT and Digital component of a mixed project or program administered by other GCAs will be referred by the GCA to DCS for assessment:

- An ICT and Digital component that is discrete enough to be treated as a separate project may be transferred to DCS. If an Assurance Gateway Review is required for the ICT and Digital component, Section 4.3 (Treatment of projects and programs) applies.
- When an ICT and Digital component cannot be treated as a separate project, the GCA will undertake a joint review, with DCS informing the review's terms of reference for the ICT and Digital component and supplying reviewers from their Expert Reviewer Panel. This will enable an optimal review outcome of the overall project.

Digital Projects funded through the Digital Restart Fund, are subjected to its prescribed Digital Assurance arrangements as per the DRF funding guidelines.

[5] BAU – In IT, BAU stands for "Business as Usual." A BAU project refers to a project that involves regular, ongoing operational activities or maintenance tasks within an organisation's IT infrastructure. These projects focus on ensuring the smooth functioning of existing systems, applications, and services rather than implementing major changes or new initiatives. Examples of BAU projects include routine system updates, patch management, user support, server maintenance, and network monitoring. The goal is to maintain stability, reliability, and security in the IT environment.

2.4 Threshold

All ICT and Digital projects valued at an Estimated Total Cost (ETC) of $5 million or above regardless of funding source are to be registered with DCS via the Assurance Portal. It is mandatory for these projects to be reviewed to consider the Project Tier and the Project Assurance Plan. This is to determine the applicability of Gateway Reviews and level of project reporting and monitoring required. Projects funded through the Digital Restart Fund (regardless of value) are also required to be registered with DCS via the Assurance Portal.

ICT and Digital Projects with ETC under $5 million that are of strategic importance or of concern may be subjected to Gateway Reviews and other assurance arrangements if nominated by the Premier, Treasurer, Minister for Customer Service, Responsible Minister, Delivery Agency, the GCIDO, or IDLG. For purposes of determining Project Tier, projects under $5 million will be assessed under the $5m-$10m category.

2.5 Project Tier and Project Assurance Plan

Initial project tier assessments are made by Delivery Agencies through an online Project Risk Profile Tool when registering a project on the ICT and Digital Assurance Portal. Delivery agencies also lodge an initial Project Assurance Plan for endorsement when registering. The Project Assurance Plan must meet the minimum requirement for Gateway Reviews outlined in this Framework.

Following review by DCS Assurance Team and advice from the ICT and Digital Working Group, the GCIDO will confirm the Tier and Project Assurance Plan for each project. Delivery agencies will then be notified of the endorsed Project Tier and Project Assurance Plan for each project.

Delivery agencies are to update the Project Tier on the Portal, in consultation with DCS, for all projects within the approved threshold:

- where there are material changes to project risk/profile criteria, scope, procurement or budget, or
- upon request by DCS

2.6 Confidentiality

ICT and Digital Assurance is a confidential process. Gateway Review and Health Check reports are confidential between the nominated Delivery Agency Project Sponsor and DCS.

Regular project reporting and the reporting of findings from final Gateway Review and Health Check reports[6] are provided to Cabinet Committees and are therefore Cabinet Sensitive.

The outcomes of Gateway Reviews and Health Checks may be provided to the Secretaries Board, ICT and Digital Leaders Group, and DARAG. Refer to Section 4.1 Reporting for details.

[6] Final Gateway Review and Health Check Reports refers to reports that have been reviewed by the nominated Delivery Agency.

2.7 Ownership

Expert reviewers, engaged by DCS, prepare Gateway Review and Health Check Reports on behalf of DCS. These reports remain the property of DCS until finalised. Once finalised, reports become the property of relevant Delivery Agencies. Project Sponsors (as owners of reports) are able to distribute reports at their discretion, having regard to the confidential nature of the reports.

2.7.1 ICT Digital Investment and Assurance (IDIA) Unit

The ICT Digital Investment and Assurance (IDIA) Unit has been established within DCS to conduct the assurance functions required under the DAF. Senior staff within the Assurance Unit are assigned to particular portfolio of agencies to provide a single point of contact for Delivery Agencies and central government. The IDIA Unit responsibilities include:

- regularly meeting with Project sponsors, Delivery Agency Program Managers, Project Directors, project
- teams, stakeholders/customers
- liaising with Delivery Agencies in the preparation for ICT and Digital portfolio reviews
- organising Gateway Reviews, Health Checks and other due diligence reviews as required
- refer projects to CyberNSW, Information Privacy Commissioner and AI Review Committee as per the Digital Restart Fund Guidelines and the AI Assurance Framework requirements.
- preparing summary reports post-Gateway Reviews/Health checks
- overseeing close-out plan sign-off and reporting
- overseeing regular project reporting
- reporting to Cabinet Committees; and
- providing a single point of contact for Delivery Agencies and central government.

The IDIA Unit facilitates Assurance Reviews by:

- liaising with the project sponsor regarding the selection of Expert Reviewer Panel members to conduct reviews and assembling the Assurance Review Team and assisting with logistics and administrative arrangements for the planning meeting.
- briefing the program/project team on the requirements of an Assurance Review
- providing the Assurance Review Team with relevant templates
- responding to queries and providing advice to the entity and the Assurance Review Team as required
- Reviewing draft reports from the Assurance Review Team before distributing them to the sponsor
- ensuring that procedural requirements have been met
- collating evaluations on the Assurance Review Team’s performance; and
- analysing review reports and recommendations to identify non-attributable lessons learned.

2.7.2 Expert Reviewers

Assurance Reviews are conducted by an independent Assurance Review Team appointed by DCS. An Assurance Review Team usually consists of a Review Team Leader (RTL) and up to two Review Team Members (RTMs).

Reviewers may be sourced from the public or private sector. Public sector reviewers have the unique and strategic learning opportunity to work across government and contribute their experience to provide assurance to important programs/projects. It is important to note that public sector reviewers are selected for their expertise, and not to represent their entity (e.g. cluster, agency or project).

Similarly, private sector reviewers are selected for their expertise, not to represent their firm, and may not use the Assurance Reviews process to actively solicit business for themselves or their firm.

Further guidance on the management of the Expert Reviewers is provided through the **Expert Reviewer Panel Framework.**

2.8 Responsibilities

The responsibilities of the various bodies involved in the DAF are described in Table 1.

Table 1 DAF Responsibilities

Group	Responsibilities/Decision Rights
Government Chief Information and Digital Officer (GCIDO)	Responsible for DAF oversight and performance, including: • approves Project Tier ratings and corresponding Project Assurance Plans • monitors Tier 1 and High Priority (High Profile/High Risk) projects, Tier 2 and Tier 3 (Gate 1) project performance through independent Gateway Reviews and Health Checks • maintains oversight of Close-out Plans • approves projects to proceed at certain gates for Tier 1 and Tier 2 projects: – Tier 1 – require GCIDO approval at Gates 1, 2 and 3. – Tier 2 – require GCIDO approval at Gates 1 and 3 **GCIDO approval may be subjected to conditions checked at the next gate or withheld until conditions are met. DCS Secretary approval is required to withhold endorsement.** • provides independent analysis and advice on key risks and any corrective actions recommended for Tier 1 and High Priority (High Profile/High Risk), Tier 2 and Tier 3 projects • escalates projects to IDLG, and then Secretaries Board, and Cabinet committees by exception, where projects present 'red flag issues' and where corrective action is needed. Low and Medium Assurance reviews are also escalated under the same conditions. • provides advice to ERC on all ICT and Digital projects being considered by ERC, based on Gateway Review and Health Check reports, to ensure effective investor-level assurance advice and risk mitigation strategies • may nominate Tier 3 and lower project for closer scrutiny (e.g. treat as Tier 2 for future gates) • commissions Gateway and other assurance reviews • works with Delivery Agencies to ensure all ICT and Digital projects and other projects of concern or strategic importance are registered and ensures they are risk profiled and assigned a risk-based project tier with an endorsed Project Assurance Plan
Secretaries Board	The primary role for the Secretaries Board in relation to the DAF is to consider any strategic, whole-of-government issues escalated by the ICT and Digital Leadership Group or the GCIDO. By exception, the Board also considers red or deteriorating status for Tier 1 and 2 and High Priority (High Profile/High Risk projects), Assurance Reviews (Medium and Low rated), and changes to Tier ratings. The Board may provide advice to Cabinet Committees if required.
Expenditure Review Committee (ERC)	The role of the Expenditure Review Committee (ERC) is to assist Cabinet and the Treasurer in: • framing the fiscal strategy and the Budget for Cabinet's consideration • driving expenditure controls within agencies and monitoring financial performance • considering proposals with financial implications brought forward by Ministers ERC periodically receives updates and details of issues relating to projects under the DAF. By exception, ERC also considers red or deteriorating status for Tier 1 and 2 and

Group	Responsibilities/Decision Rights
	High Priority (High Profile/High Risk projects), Assurance Reviews (Medium and Low rated), and changes to Tier ratings.
ICT and Digital Leadership Group (IDLG)	The ICT and Digital Leadership Group (IDLG) is the primary governance forum for ICT and Digital decisions and work programs in the NSW Government. It provides a forum for developing a whole of government strategic approach to ICT and digital government, including: • developing, and implementing actions of, the NSW ICT and Digital Strategy • providing assurance for ICT and Digital investment to support greater re-use of existing assets and better overall outcomes for projects • facilitating better collaboration and sharing expertise across the sector. In relation to the DAF: • the Group provides advice on submissions to Cabinet committees. • endorses Tier 1 and 2 and High Priority (High Profile/High Risk) project reports for scrutiny by Cabinet Committees. • IDLG reviews reports prepared by IDIA.
Digital Assurance Risk Advisory Group (DARAG)	Responsible for supporting the operation of the DAF by providing advice to the Government Chief Information and Digital Officer (GCIDO) and the IDLG and for monitoring projects by taking a Whole of Government perspective. • Monitor ICT and Digital program/projects performance based on monthly Portfolio reporting. • Advise IDLG and GCIDO across the program/project lifecycle to ensure effective investor-level assurance advice and risk mitigation strategies. • Advise on the need to escalate the levels of scrutiny to the GCIDO and any additional assurance activities needed on projects, which need to be carried out by IDIA • Assist troubled High-Priority (high risk/high profile) projects by taking a Whole of Government perspective and potentially being part of assurance review panels. • Participate in Review Workshops for Tier 1 and Tier 2 projects. • Invite CIOs to present Tier 1 and 2 project business cases at DARAG and ensure alignment to Whole of Government/Cluster Strategies and Policies (e.g. enterprise architecture, Cyber, Procurement, etc.,). • Refer Tier 1 and 2 projects with high or escalated AI risks as identified by the AI Assurance Framework to the AI Review Board to provide further advice and recommendations on their AI solution(s). Endorse: • Tier 1 and 2, Gate 2 Business Cases. • Tier endorsement ratings and gate exits as per DAF requirements for subsequent approval by GCIDO • Key reports prior to presentation to governance forums (e.g. ERC, Secretaries Board, IDLG, etc.) • Shape ideas/proposals and provide insights/feedback into submissions going up to IDLG. • Socialise information on new initiatives being considered for the DRF and report on approved DRF projects (status, issues, reviews and outcomes).
Executive Director, ICT Digital Investment and Assurance	Responsible for DAF administration and performance including: • conducts Tier 1 (High Profile/High Risk), High Priority, Tier 2 and Tier 3 (Gate 1) project performance through independent Gateway Reviews and Health Checks

Group	Responsibilities/Decision Rights
	• provides independent analysis and advice on key risks and any corrective actions recommended for Tier 1 (High Profile/High Risk), High Priority, Tier 2 and Tier 3 projects • works with Delivery Agencies to ensure all ICT and Digital projects and other projects of concern or strategic importance within the approved threshold are registered and ensures they are risk profiled and assigned a risk-based project tier with an endorsed Project Assurance Plan • undertakes Cluster portfolio reviews of ICT and Digital investments (annual and ad hoc), consistent with the NSW Gateway Policy focusing on business need and project justification, to ensure alignment to NSW ICT and Digital Strategy and other relevant government reforms, identifying/enabling opportunities to reduce risk and cost (e.g. re-use; sharing of solutions) • provides a dedicated Assurance Unit (ICT Digital Investment and Assurance) to coordinate Reviews • oversees an appropriate Expert Reviewer Panel, the performance of individual expert reviewers, and the selection of appropriate expert reviewers, and the scheduling, commissioning and administration of Gateway Reviews and Health Checks • oversees the continuous improvement of DAF processes • supports approaches to improving sector capability such as Project Sponsor/manager training, cross-sector knowledge sharing and skills planning initiatives. Supports insightful monthly or as needed reporting to DARAG, IDLG, Cabinet/ERC: • results of Cluster portfolio reviews • details of approved Project Tier and corresponding Project Assurance Plans • gateway Reviews, Health Checks and Close-out Plans for Tier 1 and 2, High Priority (High Profile/High Risk) projects • project status and mitigation strategies for red flag issues • gateway Reviewer Performance • trends and analysis of the key issues, and • overall performance of the assurance framework. Regularly reports to NSW Treasury on the performance of the DAF.
NSW Treasury	As Policy Owner, NSW Treasury has overarching policy responsibility for NSW Gateway Policy, Economic Appraisals and Business Cases. The role includes: • monitoring the application of the NSW Gateway Policy • reviewing GCA Frameworks submitted for review and where appropriate provide its endorsement prior to final approval by the relevant Cabinet Committee • confirming the applicable GCA Framework and informing the concerned • parties where there is dispute or confusion as to the appropriate GCA to deliver Gateway • determining the appropriate GCA Framework a mixed project should follow (i.e. where it contains a material combination of more than one element of different frameworks) • reporting on the performance of the NSW Gateway Policy, including the performance of the GCA Frameworks, after one year of operation and annually. Treasury will coordinate the review of GCIDO-managed projects within DCS. A GCIDO-managed project is one that is led and/or delivered by a team or unit that has a reporting line to the GCIDO as its Deputy Secretary. For other DCS-managed projects, Treasury may elect to delegate the Gateway Review coordination to the GCIDO.

Group	Responsibilities/Decision Rights
	Service NSW projects are not considered DCS-managed. Treasury retains ability to request independent review where appropriate.
Expert Reviewer Panel	The Panel comprises independent highly qualified expert reviewers established to cover all aspects of Gateway Review needs. A Review Team, for Gates 1 through 6, is drawn from the Panel. A Review Team conducts Gateway Reviews and Health Checks/Deep Dives/Rapid Reviews. Panel members can also be drawn upon to provide advice to DCS on projects and to the various assurance committees on an as-need basis. Panel member performance is to be reviewed regularly and membership updated.
Delivery Agency	The Delivery Agency must identify the appropriate GCA Framework for a project/ program and adhere to the approach in the relevant GCA. The Delivery Agency is responsible for meeting DAF requirements, including: • registration and risk profiling of projects: – registers all ICT and Digital projects with ETC of $5 million and above, and other projects of concern or strategic importance. This applies to projects being planned, developed and/or delivered – self-assesses Project Tier and prepares corresponding Project Assurance Plan – updates DCS on changes of project risk criteria that may affect the Project Tier, and – updates DCS on proposed changes to Project Assurance Plan requirements. • DAF Gateway Reviews, Health Checks – registers in a timely manner for Gateway Reviews and Health Checks – provides in a timely manner all relevant information to support Gateway Reviews and Health Checks – assist with organising interviews of personnel required by the Review Team and with sourcing the required documentation – responds to requests for fact checks of the draft Reports in a timely manner – provides a Delivery Agency endorsed response to recommendations in a timely manner – prepares formal Close-out Plan, for endorsement by DCS, for each Gateway Review or Health Check – implements Close-out Plans – provides regular updates to DCS on the status of Close-out Plans, and • regular reporting: – provides timely and comprehensive project reports consistent with Project Tier frequency reporting requirements and agreed format. • ensuring Project Sponsors within the Delivery Agency complete the required training coordinated by DCS. The Delivery Agency is responsible for paying any direct costs of Gateway Reviews, Deep Dive Reviews and Health Checks. This includes time and expenses relating to the engagement of independent reviewers, as well as disbursements relating to a Review such as venue hire, catering and administrative support services. DCS will initially pay for these direct costs. These will then be recovered in full by invoicing the Delivery Agency at the completion of a Gateway Review, Health Check or Deep Dive Review. The Delivery Agency is responsible for ensuring that appropriate internal assurance arrangements, distinct from the Gateway Review process, are designed into the project to ensure its successful delivery.

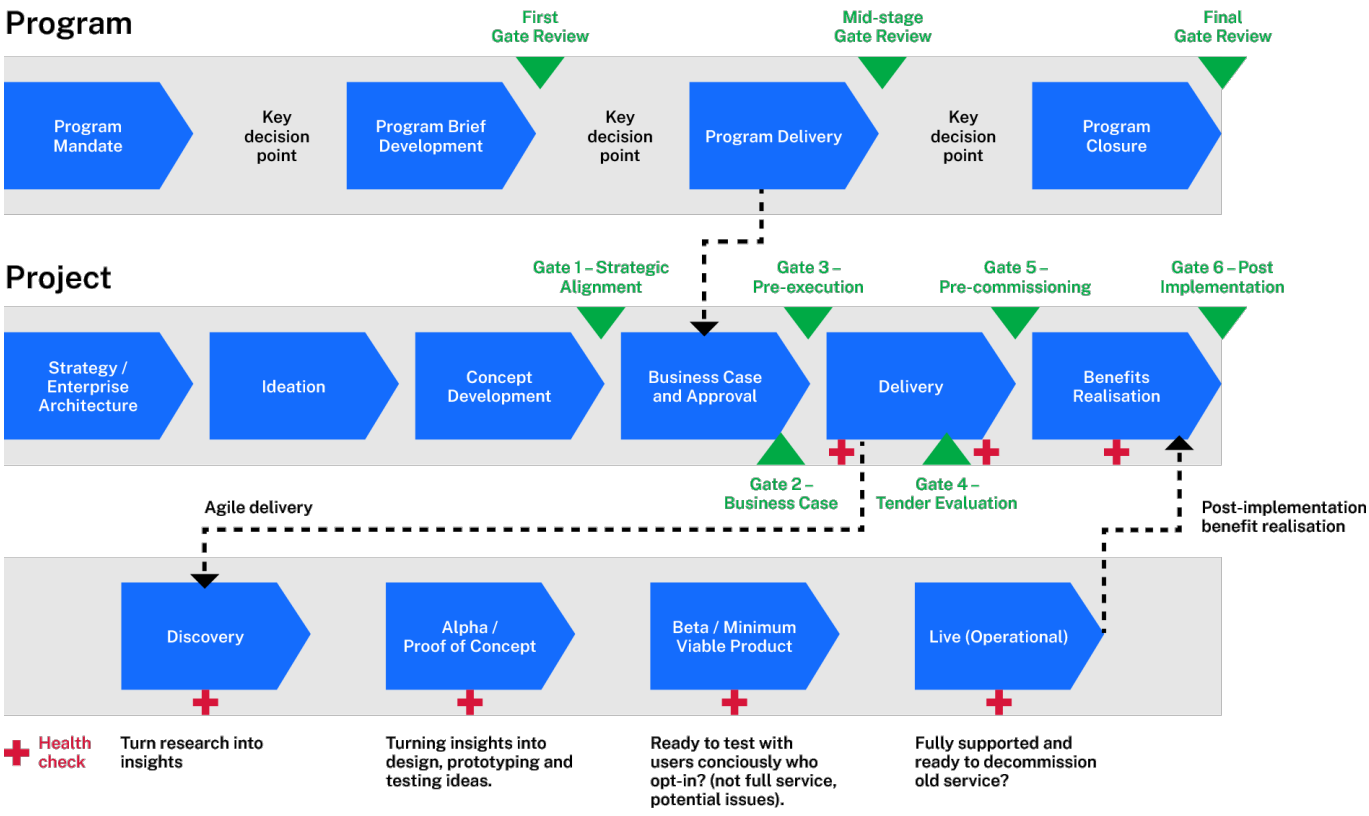
Group	Responsibilities/Decision Rights
Project Sponsor	• ensures that the project is focused throughout its life on achieving its objectives and delivering a product that will achieve the forecasted benefits • ensures that the project gives value for money • participates in Gateway Reviews and Health Checks • commissions an independent review at specified gates for Tiers 3 and 4 (Project Sponsor-Commissioned Review) and reports to DCS. • ensures the project meets the objectives of the business case and may initiate due diligence checks as required • responsible for DAF related actions and reporting for their Delivery Agency • completes the required Project Sponsor training coordinated by DCS

3 Framework Arrangements

3.1 Framework Outline

The DAF incorporates a risk-based approach to ICT Digital investment assurance consistent with NSW Gateway Policy. Assurance arrangements for the state's ICT and Digital investment supports the Premier, the Treasurer, the Minister for Customer Service, and Cabinet/ERC in ensuring that this investment is maximised and programs are delivered effectively. The DAF is designed to support both the Delivery Agencies' own decision-making and assurance processes and to support Budget processes throughout the project/program lifecycle as shown in Figure 4.

Figure 4 Project/Program Lifecycle Assurance



3.2 Risk-based approach to investor assurance

Risk-based assurance means that different levels of assurance and reporting are applied proportionate to the risk profile. The qualitative risk profile criteria are outlined in Table 2 below.

Table 2 Qualitative risk profile criteria

Criteria	Definition
Level of government priority	The level **and** timing of project or program priority, where: • the level of priority for a project is specifically mandated (or where a Ministerial authority has been given to mandate that a project is a priority) in documents such as the NSW Budget, Premier's Priorities, State Infrastructure Strategy, NSW ICT and digital strategy, Election Commitment, or is a response to a Legislative Change, or • the project is a direct enabler of a mandated priority project.
Interface complexity	The extent to which the project or program's success will depend on the management of complex dependencies with other: • agencies, portfolio of agencies or non-government sector organisations: contributing to the funding of the project; operational responsibility; and/or cross cluster/agency delivery of the project • projects or services - there are fundamental interdependencies with other projects or services that will directly influence the scope and cost of the project.
Sourcing complexity	The extent to which a project or program requires sophisticated, customised or complex procurement methods (non-traditional), thereby increasing the need for a careful assessment and management of risk. Sourcing complexity may also be influenced by contractual complexity, especially if multiple suppliers are involved in the delivery of the solution with varying service levels. Sourcing complexity may also be influenced by the extent of agency experience and capability. For example, some procurement methods (e.g. Early Contractor Involvement) may be used more commonly by some agencies and represent a lower procurement risk.
Agency capability and capacity	The extent to which the sponsor agency has demonstrated capability (skills and experience) or can access through recruitment or procurement the required capability in the development and / or delivery of the type of project or program proposed and/or its delivery strategy.
Technical complexity	The extent to which a project or program requires new or unproven technology, customised technology, or complex or lengthy integration with other solutions, thereby increasing the need for a careful assessment and management of risk.
Cyber security	The extent to which a compromise of this product could result in an impact to services, loss of confidence in government (reputational, trust) or personal safety. The degree to which an attack against this product would impact significant state-wide infrastructure, and An identification of the classification level or volume of data traversing this product (to assess impact of a cyber-attack)
Change complexity	Sensitivity to the degree of business change required for the success of the project. This could be complex business or process changes internal to government or in the service delivery to government customers. Risk or perception of risk to service delivery, security and privacy, or similar issues that may impact the change management aspects. The degree of criticality of services impacted by the project such as front-line services to citizens. The degree of unknowns involved with the chosen approach.

A weighted score for the above criteria is determined based on the weightings and scores outlined in Appendix A. This weighted score is compared against ETC to determine a preliminary Project Tier based on the matrix shown in Table 3.

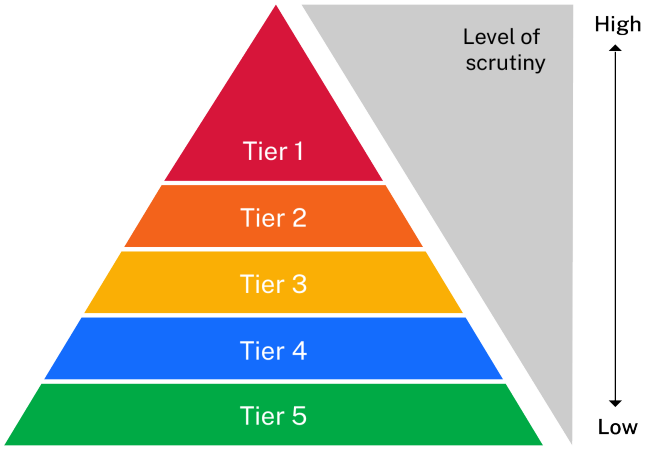
Table 3 DAF project tier weighted risk score matrix

Risk score	ETC ($m)						
	200+	>100-200	>50-100	>20-50	10-20	5-10	<5
4.0 – 5.0	Tier 1	Tier 1	Tier 1	Tier 1	Tier 1	Tier 2	Tier 3
3.0 – 3.9	Tier 1	Tier 2	Tier 2	Tier 2	Tier 2	Tier 3	Tier 4
2.5 – 2.9	Tier 1	Tier 2	Tier 2	Tier 2	Tier 3	Tier 4	Tier 5
2.3 – 2.4	Tier 2	Tier 2	Tier 2	Tier 3	Tier 4	Tier 5	Tier 5
2.1 – 2.2	Tier 2	Tier 2	Tier 3	Tier 3	Tier 4	Tier 5	Tier 5
0.0 – 2.0	Tier 2	Tier 3	Tier 3	Tier 3	Tier 4	Tier 5	Tier 5

The initial risk profiling self-assessment process is by Delivery Agencies through the online tools on the ICT and Digital Assurance Portal. The process involves giving each project a risk-based score against these criteria, and undertaking further qualitative analysis, enabling projects to be grouped into risk-based tiers to which different levels of project assurance can be applied. The risk-based tiers are as follows:

- Tier 1 - High Profile / High Risk
- Tier 2
- Tier 3
- Tier 4
- Tier 5

Figure 5: Tiered Approach



This tiered approach (Figure 5) is designed to ensure that the right balance is struck between a robust approach correctly focused on highest risks and achieving value for money.

Throughout their lifecycle, projects may move between tiers depending on changing risk profiles. A project may be nominated as a Tier 1 project by the:

- Premier, Treasurer, Minister for Customer Service and Digital Government, Responsible Minister,
- relevant Delivery Agency Secretary, Chief Executive Officer, or Project Sponsor[7], or
- the GCIDO.

For a project to be removed as a Tier 1, before it is operational, the relevant Delivery Agency Secretary or Chief Executive Officer must request the removal in writing to the GCIDO. The request may also be referred to the Digital Assurance Risk Advisory Group (DARAG) for advice.

[7] and /or in accordance with individual Delivery Agency policy.

3.3 Assurance requirements

The DAF Gateway Review process provides for a series of focused, independent expert reviews, held at key decision points in a project's lifecycle (as depicted in Table 4). The Gateway Reviews are appraisals of ICT and Digital projects/program, that highlight risks and issues, which if not addressed may threaten successful delivery.

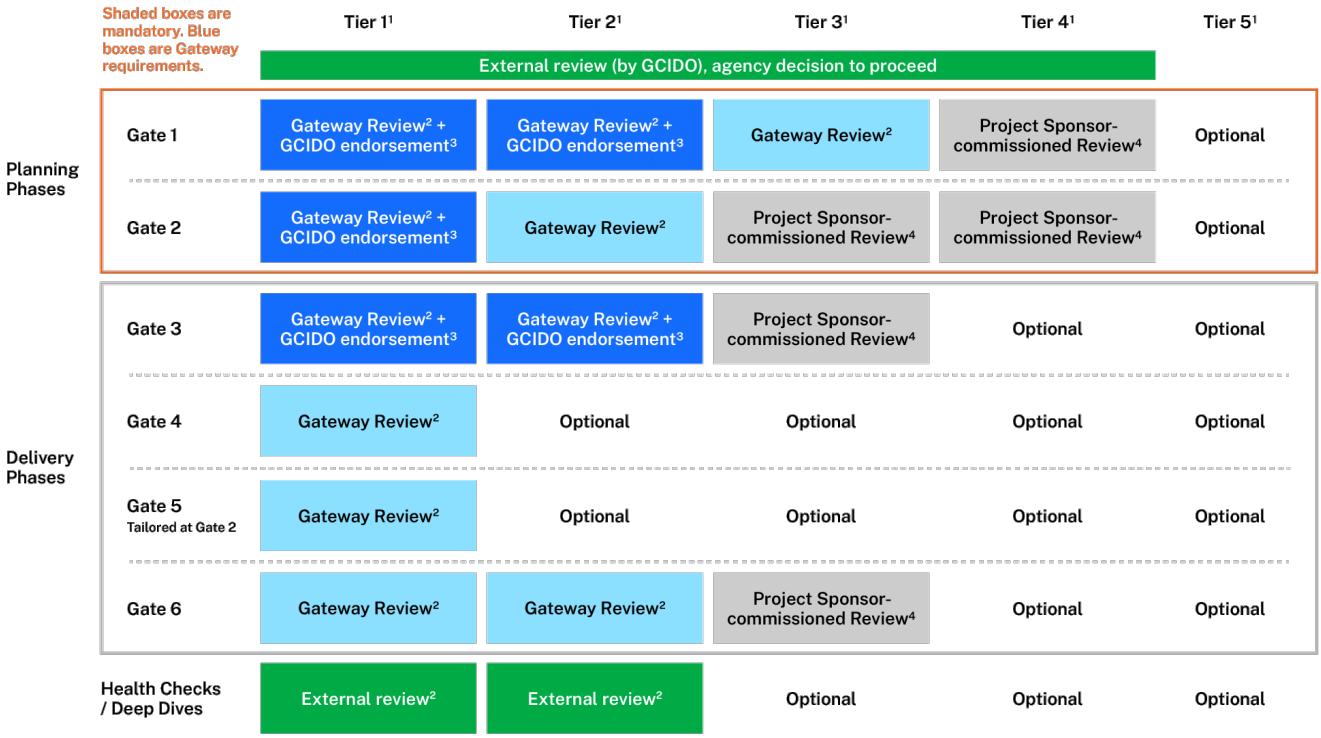
The Gateway Review process is in place to strengthen governance and assurance practices and to assist Delivery Agencies to successfully deliver major projects and programs. Gateway Reviews are part of an assurance process which provides confidence to Government in the information supporting their investment decisions, the strategic options under consideration, and the Delivery Agency's capability and capacity to manage and deliver the project.

Gateway Reviews are supported by Health Checks which assist in identifying issues which may emerge between decision points. Health Checks will be carried out by an independent team of experienced practitioners (peers, industry experts including from the private sector), appointed by the ED IDIA.

For projects following an Agile methodology, a more suitable and flexible Health Check, the Agile Health Check, is carried out in lieu of the delivery Gate or Health Check reviews. In addition, for projects funded by the DRF, where funding request is less than $5 million, a lean investment assurance is conducted against the lean business case.

The risk-based application of Gateway Reviews and Health Checks under the DAF are depicted in Table 4. Delivery agencies can nominate additional Gateway Reviews and Health Checks beyond those mandated by the DAF.

Table 4 Application of Gateway Reviews and Health Checks under the DAF



1. Risk tier at Gate 1 using risk assessment tool completed by agency; Confirmed / revised at subsequent gates as additional information becomes available.
2. Review commissioned by the GCA and conducted by a party other than or "external" to the agency in question; may include a mix of GCIDO, peer and independent resources depending on the tier. Accredited IQA organisations can perform external reviews.
3. GCIDO endorsement may be subject to conditions checked at next gate OR withheld until conditions are met. DCS Secretary approval required to withhold endorsement.
4. Project Sponsor-commissioned Reviews are due diligence reviews rather than part of the Gateway Review process, but will use Gateway Review toolkit.
5. Optional: will be required if project is deemed high risk.

3.3.1 Gate 1 – 6 Reviews

Reviews include interviews with significant project stakeholders and the examination of project documents. Review Teams assess the progress of projects against the criteria set out in the guidance material for the relevant Gateway Reviews and are conducted in accordance with the DAF Gateway Review Toolkit. Appendix B details the purpose of each Gate.

DCS will develop Terms of Reference for a Review in consultation with the responsible Delivery Agency and key stakeholders including sponsor. The Terms of Reference are used to guide the selection of appropriate reviewers and will be provided to reviewers in advance of the Review.

Good governance and project/program assurance calls for the need to have an individual as the single point of accountability and strategic responsibility: the Project Sponsor.

To enable a successful Review to take place, it is essential that the Delivery Agency's Project Sponsor participates in the Gateway Review process.

Optional Gateway Reviews or a Project Sponsor-commissioned Review can be called for at the direction of any of the following:

- Premier, Treasurer, Minister for Customer Service, Cabinet/ERC
- the GCIDO
- IDLG
- Project Sponsor

3.3.2 Project Sponsor-commissioned Reviews

Agencies are responsible for putting in place appropriate internal assurance arrangements, and

the Project Sponsor may initiate due diligence checks as required to ensure the project meets the objectives of the business case.

Tier 3, Tier 4 and Tier 5 projects are required as part of their internal assurance arrangements to carry out sponsor-initiated reviews, called Project Sponsor-commissioned Reviews, for the following gates:

- Tier 3 – at Gates 2, 3 and 6
- Tier 4 – at Gates 1 and 2
- Tier 5 – Optional

A Project Sponsor-commissioned Review is defined as:

- An independent review, i.e. reviewers must be independent of the Delivery Agency and the project team.
- A review that uses the relevant DAF Gateway Review Toolkit.

The Project Sponsor is required to provide a copy of the Review report to DCS as part of the oversight of projects.

3.3.3 Health Checks and Deep Dive Reviews

At least one Health Check is mandatory for Tiers 1 and 2, tailored at Gate 2 for each project. Health Checks should be conducted at regular intervals (minimum 6 months) for Tier 1 – (High Profile/High Risk) projects when in the delivery phase of the project lifecycle. Independent reviewers forming the Review Team can include individuals currently employed with the NSW Government if they are independent of the Delivery Agency and project team.

Triggers for optional Health Checks may include:

- Where a Gateway Review Team recommends a Health Check be completed before the next Gateway Review.
- If there is overall low or medium delivery confidence and there are a significant number of critical and essential recommendations raised at a Gateway Review or Health Check. The Health Check would focus on ensuring recommendations have been closed effectively.
- If insufficient progress is being demonstrated in closing out recommendations from a previous Gateway Review or Health Check.
- If there is a major incident or major event or major change in the project or its environment. including change of governance or change in Delivery Agency responsibility.
- If a Delivery Agency self-nominates.

Optional Health Checks can be called for at the direction of any of the following:

- Premier, Treasurer, Minister for Customer Service, Cabinet/ERC
- the GCIDO
- IDLG
- Project Sponsor.

Deep Dive Reviews are similar to a Health Check but focus on a particular issue or limited terms of reference rather than the full range of issues normally considered at a Health Check. These are generally undertaken in response to issues being raised by key stakeholders to the project as a result of a Gateway review or at the direction of the relevant Government Minister.

3.3.4 Rapid Assurance Review (RAR)

Gated Assurance reviews in the delivery phase of a project are more suitable to projects following a Waterfall methodology.

For projects following an Agile methodology, such as a product delivery model, the Rapid Assurance Review is a more suitable and flexible risk-based assurance review, in lieu of the standard delivery Gate reviews.

The RAR is characterised by:

- Iterative assessments.
- Conducted on a periodic basis, depending on the needs of the project and visibility to IDIA.
- Focusing on progress to treat the identified risks.
- Reviewers as integral advisors to the project to ensure continual reviews and feedback to the project.

Independent reviewers forming the Review Team can include individuals currently employed with the NSW Government if they are independent of the Delivery Agency and project team.

RAR are mandatory for Tier 1 and 2 projects following an Agile methodology, tailored at Gate 2 for each project.

The timing and frequency of the RAR should be agreed on with the Delivery Agency, based on the cadence of the project when in the delivery phase.

Additional, optional RAR can be directed by the same people as optional Health Checks, using the same triggers (refer 3.3.3, above).

When completing the RAR, the Assurance Partner may ask for documentation from the project team to demonstrate the achievements and outcomes of the funded project phase – this may include research, technical and design documentation and reports. The Assurance Partner will also review and consider advice and recommendations from:

- NSW Design Standards,
- Information and Privacy Commission,
- AI Review Committee,
- NSW Data Analytics Centre (DAC).

Once the Assurance Partner has completed the RAR, the results of the assessment may be made available to Project Sponsor, Cabinet/ERC and other relevant NSW Governance committees.

3.4 Delivery agency assurance

The DAF Gateway Reviews and Health Checks relate to those conducted under the DAF and do not relate to reviews and checks conducted under individual Delivery Agency arrangements.

3.5 Independent reviewers

Reviews are to be conducted by a highly experienced independent Review Team where independent refers to the individuals being independent of a Delivery Agency and a project team. Reviewers could be drawn from a number of sources both internal and independent from government.

The selected review team will possess the skills, capability and experience to enable it to provide relevant assessment and advice.

For Tier 1 – (High Profile/High Risk), Tier 2 and High Priority projects, independent reviewers forming the Review Team should be drawn from high profile industry experts and may, with the approval of the ED IDIA, involve a NSW Government expert.

For Tier 3, 4 and 5 projects, independent reviewers forming the Review Team may include individuals currently employed with the NSW Government if they are independent of the Delivery Agency and project team.

Further guidelines on the management (including section, interview and remuneration) of Expert Reviewer Panel can be found in the NSW Government Expert Reviewer Panel Framework. Contact ICTAssurance@customerservice.nsw.gov.au for more information.

3.6 Gateway Review / Health Check / Deep Dive Reports

The results of each Gateway Review, Health Check and Deep Dive are presented in a report that provides a snapshot of the project's progress with recommendations to strengthen the project.

3.7 Close-out Plans

Close-out Plans are required to be prepared in response to the recommendations set out in each Gateway Review, Health Check and Deep Dive report. Close-out Plans are supplied by Delivery Agencies as approved by the Delivery Agency Secretary, Chief Executive Officer or nominated Project Sponsor[8]. These Plans detail specific actions, timelines and accountabilities that respond to the recommendations provided in these reviews. DCS will:

- endorse the Close-out Plans and the closing out of recommendations
- monitor the progress towards closing out these actions and recommendations, and
- report on this activity.

3.8 Confirmation of clearance of Gate

The GCIDO will provide a confirmation of clearance that a project can move to the next Gate or Health Check. This clearance reflects that a Delivery Agency has completed a Gateway Review for a particular stage of the project and an appropriate Close-out Plan is in place to assist with project development or delivery. Gateway Reviews are independent reviews and the project remains the responsibility of the Delivery Agency.

For Tier 1 and Tier 2 projects, the GCIDO will endorse projects to proceed at certain gates:

- Tier 1 – require GCIDO endorsement at Gates 1, 2 and 3
- Tier 2 – require GCIDO endorsement at Gates 1 and 3.

GCIDO endorsement may be subject to conditions checked at the next gate or withheld until conditions are met. DCS Secretary approval is required to withhold endorsement.

[8] and /or in accordance with individual Delivery Agency policy.

4 Framework Performance and Reporting

Performance and reporting are important components to the independent investor assurance process. Project reporting is based on inputs provided by the Delivery Agencies and DCS monitors these projects/program on a monthly basis.

4.1 Regular project reporting (traffic lights)

Reporting will be conducted for projects and programs, with data gathered for all Tiers and maintained by DCS in a central repository called the ICT and Digital Assurance Portal. These reports will record and assess implementation against time, cost, benefits, risks and issues to project development/delivery. Alerts for management attention and/or intervention will be based on analysis of data as well as Gateway Reviews and project Health Checks.

It is therefore required that the Delivery Agencies provide a sufficient level of data, including RAG (Red/Amber/Green) status and associated descriptive commentary for each of the time, cost, benefits, risks and issues categories.

High Priority (high profile/high risk) projects can be any Tier (all Tier 1 projects are treated as High Priority projects) and are determined using a combination of the Project RAG (Red/Amber/Green), Agency Capability category rating, and DAF assessment:

- Monitor – on-going monitoring of the health of the project for adverse changes/deterioration.
- Engage – assist the project in resolving their RAG status/issues via active engagement mechanisms e.g. health checks.
- Escalate – continuing issues with project RAG status; serious project issues, poor review ratings and outcomes, and unresolved engagement concerns (or a combination) can result in the need to escalate. Escalation can include to Senior Executive Management and Governance forums including DARAG, IDLG, and ERC.

Reporting will reflect the tiered approach with greater analysis and strategic advice provided for Tier 1, 2 and High Priority (High Profile/High Risk) projects on a monthly basis.

Regular project reporting (traffic light reports) for Tier 1, 2 and High Priority (High Profile/High Risk) projects (monthly) is provided to the DARAG and IDLG, and by exception to ERC .

4.1.1 Summary of reviews

A summary of the outcomes of Gateway Reviews and Health Checks for Tier 1, 2 and High Priority (High Profile/High Risk projects) is provided to IDLG for noting and submitted to Cabinet/ERC (by exception only).

Advice will be provided to Cabinet/ERC on Tier 1 and 2 projects' business cases based on Gateway Reviews and Health Check reports.

The Project Sponsor commissions reviews at most Gates for Tiers 3 and Tier 4 projects with summary reports provided to the GCIDO.

4.1.2 Distribution of reports

DCS will only distribute reports for the following as indicated in Table 5:

- final regular project reports (traffic light)
- summary of the outcomes of Gateway Reviews and Health Checks, and
- summarised final Gateway Review and Health Check reports

Table 5 Distribution of regular project reports and Gateway Review and Health Check reports

Stakeholder/Forum	Final regular project reports	Summary of outcomes of Gateway Reviews and Health Checks	Final Gateway Review and Health Check reports
NSW TREASURY	Yearly	Yearly	To support investment or financing decisions made by ERC, when required
DELIVERY AGENCY SECRETARIES / CEOS[9]	Routinely	Routinely	Routinely[10]
SECRETARIES BOARD	On request	By exception	On request
MINISTER FOR CUSTOMER SERVICE AND DIGITAL GOVERNMENT	On request	By exception	On request[11]
EXPENDITURE REVIEW COMMITTEE (ERC)	Yearly	Yearly	On request
ICT AND DIGITAL LEADERSHIP GROUP (IDLG)	Monthly	Monthly	On request
DIGITAL ASSURANCE RISK ADVISORY GROUP (DARAG)	Monthly	Monthly	On request
DRF WORKING GROUP	On request and to support decisions re DRF projects	On request, and to support decisions re DRF projects	On request, and to support decisions re DRF projects

To support reporting arrangements, Delivery Agencies are required to provide:

- Timely and comprehensive project reporting in the agreed format
- Close-out Plans which document actions and accountabilities that respond to recommendations identified in Gateway Review and Health Checks
- Mitigation Plans for very high/high issues identified in Tier 1, Tier 2 or High Priority (High Profile/High Risk) project status reports.

[9] Only for projects within the Cluster.

[10] Copies are initially provided to the nominated Delivery Agency Project Sponsor.

[11] On request to the GCIDO.

4.2 Monitoring

DCS will monitor project status (including mitigation plans) and the findings of Gateway Reviews and Health Checks (including Close-out Plans). DCS will provide regular project reports and summary findings of Gateway Review and Health Checks to:

- Digital Assurance Risk Advisory Group (DARAG) for:
  - endorsement of regular project reports, and
  - noting of findings and recommendations of project Gateway Review and Health Checks
- IDLG by exception for findings and recommendations of project Gateway Review and Health Checks
- the Secretaries Board by exception for projects with red status or deteriorating status
- ERC through an annual summary report.

The GCIDO may escalate a project to the IDLG, Secretaries Board and ERC if required, where projects present very high/high issues and where corrective action is needed.

Regular project reports as well as Gateway Review and Health Check summary findings are owned by DCS. In providing this reporting, DCS will undertake the necessary steps to verify the information provided by Delivery Agencies or prepared by Review Teams. This may include:

- detailed assessment of each Tier 1 – High Priority (High Profile/High Risk) project with direct input from Panel experts (this will include Health Checks and the results of Deep Dive Reviews)
- independent analysis and advice on key risks, recommended corrective actions and mitigation strategies.

4.3 Treatment of Projects and Programs

ICT and Digital projects must be registered under the DAF as either a project or a program. After a project or program is risk-profiled and assigned, a Project Tier it is required to comply with the assurance and reporting requirements outlined in Section 4.1 according to its Project Tier.

4.3.1 Modified Project Assurance Plan for complex projects and programs

Under the IDAF, the assurance process for complex projects and programs begins with registration and risk profiling of the project/program in its entirety to establish its Project Tier. For assurance purposes (Reviews, regular reporting and monitoring), a complex project or a program may need to be considered both as a single project or program and in its component parts (project stages, individual projects or sub-programs) at various stages in the program lifecycle.

In some cases, these project stages, individual projects or sub-programs may have a different Project Tier to the overall complex project or program. This may result in the need for a Modified Project Assurance Plan.

As the different component parts (project stages, individual projects or sub-programs) are typically developed and/or delivered over varying timeframes, they may not be able to be considered in a single Gateway Review. It may therefore be necessary to have multiple Reviews to accommodate a program/project's needs. In some cases, a smaller stage of work or individual project may not warrant the application of these separate Gates.

For complex projects, the application of separate tiering for certain identified stages allows the Delivery Agency to access Reviews for a distinct stage (dependent on the risk-profiling of that stage) to accommodate a project's specific needs. For example, larger stages of work within a complex project may warrant the application of certain Gates, particularly at the procurement and delivery stages of a project's lifecycle, whereas a smaller stage of work may not require a Review. This adaptation provides for greater assurance and efficiency across a complex project.

When stages of a complex project are identified as needing separate tiering for assurance purposes, the stages are separated and undergo risk profiling, where each stage is assigned a Project Tier, and subsequently included as such in a Modified Project Assurance Plan. Importantly, a stage's tiering is assessed on its own merits, and therefore may be tiered at any level. Separating a stage of a complex project for risk profiling may occur at any time. Typically, this would be after the complex project's strategic or final business case. A complex project should only be considered as a linear program of staged outputs in accordance with an agreed business case.

This process is similar for programs needing to be considered as separate projects or sub-programs. For instance, a large program that is considered in its entirety during the development of strategic business cases may require the development of a series of separate final business cases for individual projects and sub- programs due to these being progressed and delivered at different times.

Where a complex project has been split into stages or a program into individual projects or sub-programs, and those component parts have their own tier assessment, it is important, for satisfaction of the originating objective of the complex project/program, to return to a single Review step. This occurs as Gate 6 - the benefits realisation stage of its lifecycle, allowing the benefits realisation assessment to be undertaken for the entire complex project or program.

Complex projects/programs include mixed projects/programs.

4.3.2 Endorsement of a Modified Project Assurance Plan

Determining the extent or need to apply the mandatory gates for complex projects or programs to the project stages, individual projects or sub-programs will require:

- Delivery agencies to provide a Modified Project Assurance Plan with self-nominated assurance arrangements for each project stage, individual project or sub-program as relevant
- DCS to assess the Modified Project Assurance Plan may refer to the DARAG for advice and recommend to the GCIDO for endorsement.

4.3.3 Treatment of Programs

Separate from Project Gate Reviews and Health Checks, Programs under all tiers must have a minimum of three program reviews, with tier 1 and 2 programs subject to up to six reviews, including three mid-stage reviews, as agreed between ICT and Digital Assurance and the Program Sponsor.

Program Gateway Reviews include:

- First gateway review
- Mid-stage gateway review
- Final gateway review

Reference should be made to the separate Program Review Guidelines for more information on Program Reviews.

4.4 Assurance Portal

The Assurance Portal provides an online environment to manage assurance information and reporting for ICT and Digital projects under the DAF. The Portal provides a single source of truth in relation to project information and enables portfolio of agencies to report regularly and appointed Gateway Reviewers, governance body members and DCS to actively and efficiently access assurance data within a secure online environment.

4.5 Project Sponsor training

Training will be provided for Project Sponsors and project managers where required.

4.6 Performance

4.6.1 Yearly operational review

After every 12 months of operation from the finalisation of this DAF, IDIA will review the implementation of the DAF with NSW Treasury and Delivery Agencies.

4.6.2 Annual framework performance

A crucial part of the DAF will be to regularly evaluate the performance of the DAF itself and contribute to the analysis of project and assurance issues and trends. To this end, the key aspects of the performance management approach are outlined in Table 6.

Table 6 Performance reporting

Report	Description	Frequency	Primary Audience
Assessment of Expert Reviewer Panel capability	Confirm that reviewers on the Expert Review Panel have the requisite experience and skills set to provide high performing advice for the projects they review. Evaluations will be prepared by DCS.	Annual - to match Cluster Assurance Plans.	IDLG, Treasury
Gateway Reviewer Performance	Continually monitor the robustness and timeliness of individual expert reviewer performance. 360° feedback will be obtained for each expert reviewer at the conclusion of a Gateway Review or Health Check. Collated reports on reviewer performance will be prepared by DCS for the consideration of the Expert Reviewer Panel.	Annual	IDLG, Treasury
Performance of closing out recommended actions for all projects within the approved threshold undergoing a Review	Close-out plans are confirmed by the relevant Delivery Agency and approved by DCS to identify actions and mitigation measures to address review recommendations. A report on the performance of Delivery Agencies and Portfolio of Agencies in closing out Review recommendations will be prepared by DCS.	Annual	IDLG
Trends and analysis of the key issues	Analysis of systemic issues identified in assurance reviews and offer recommendations to address these issues. Trends and analysis reports will be prepared by DCS.	Annual	Cabinet/ERC Minister for Customer Service and Digital Government
DCS performance in the operation of the DAF	Report card on DCS's performance in key areas such as project registration, risk profiling, Gateway Reviews, Health Checks, and project reporting.	Annual	IDLG, Treasury Minister for Customer Service and Digital Government
Efficacy of the DAF	Improvement in project delivery across the sector.	Annual	ERC Minister for Customer Service

5 Appendix A - Project profile/risk criteria, criteria scores and weightings

The below project profile/risk criteria have been extended from the criteria referenced in The Treasury Gateway Policy to be directly relevant for ICT and Digital projects under this framework.

Criteria and Weighting	Priority and Risk level	Score
Government priority: 15% The level **and** timing of project or program priority, where: • the level of priority for a project is specifically mandated (or where a Ministerial authority has been given to mandate that a project is a priority) in documents such as the NSW Budget, Premier's Priorities, State Infrastructure Strategy, NSW ICT and digital strategy, Election Commitment, or is a response to a Legislative Change, or • the project is a direct enabler of a mandated priority project.	Very high Government priority • addresses an urgent and critical service need for the community, mandated priority project, or a direct enabler, and final business case or construction to be completed within within 12 months	5
	High Government priority • addresses a serious deficiency with a high service need for the community, mandated priority project, or a direct enabler, and final business case or construction to commence within Budget Year	4
	Medium Government priority • mandated priority project, or a direct enabler, and final business case or construction to be completed outside forward estimates but within the next 2 to 3 forward estimates	3
	Low Government priority • Government priority project, or a direct enabler, and final business case and construction to commence outside forward estimates but within the next 3-6 years beyond forward estimates.	2
	Very low Government priority • agency priority, or a direct enabler, in Agency Strategic Plan over the next 5-10 years.	1
	Extremely low Government priority • not a documented Government priority or a direct enabler.	0

Criteria and Weighting	Priority and Risk level	Score
Interface complexity: 10% The extent to which the project or program's success will depend on the management of complex dependencies with other: • agencies, portfolio of agencies or non-government sector organisations - contributing to the funding of the project or will be given operational responsibility, and/or • projects or services - there are fundamental interdependencies with other projects or services that will directly influence the scope and cost of the project. The extent to which the project impacts on the success of the program or other project.	Very high interface complexity risk • high degree of external dependencies (Federal, local, private or inter-agency); or • fully interdependent on other projects or services, including cross-government; or • very high degree of impact on the program's or other project's success	5
	High interface complexity risk • many external dependencies with 2 or more entities (Federal, local, private or inter-agency); or • important interdependencies with other projects or services; or • high degree of impact on the program's or other project's success	4
	Medium interface complexity risk • external dependencies - with 1 entity (Federal, local, private or inter-agency); or • some interdependencies with other projects or services; or • moderate impact on the program's or other project's success	3
	Low interface complexity risk • single external dependency (Federal, local, private or inter-agency); or • minor interdependence with other projects or services, or minor impact on the program's or other project's success	2
	Very low interface complexity risk • very little or infrequent external dependency; or • very little interdependence on other projects or services; or • very little impact on the program's or other project's success	1
	Extremely low interface complexity risk • no interface complexity; or • extremely low impact on the program's or other project's success	0

Criteria and Weighting	Priority and Risk level	Score
Sourcing complexity: 10% The extent to which a project or program requires, sophisticated, customised or complex procurement methods (non- traditional), thereby increasing the need for a careful assessment and management of risk. Sourcing complexity may also be influenced by contractual complexity, especially if multiple suppliers are involved in the delivery of the solution with varying service levels. Sourcing complexity may also be influenced by the extent of agency experience and capability. For example, some procurement methods (e.g. ECI) may be used more commonly by some agencies and represent a lower procurement risk.	Very high sourcing complexity risk • highly complex sourcing involving multiple suppliers (including finances using a hybrid financial structure and/or commercialisation (PPP))	5
	High sourcing complexity risk • unconventional complex sourcing. For example an Alliance or hybrid Alliance; and • sourcing of new emerging technology platforms such as AI, quantum, blockchain and any advanced information and communications technologies (eg: advanced optical, RF communication, high performance computing and protective cyber security technologies)	4
	Medium sourcing complexity risk • some sourcing complexity (for example, any type of sourcing as a service – XaaS); or • sourcing 'out of the box' emerging technologies such as AI and quantum and any advanced information and communications technologies (eg: advanced optical, RF communication, high performance computing and protective cyber security technologies)	3
	Low sourcing complexity risk • minor sourcing complexity. For example Directly Managed Contract	2
	Very low sourcing complexity risk • business as usual sourcing. For example sourcing from the ICT Services Catalogue	1
	Extremely low sourcing complexity risk • no sourcing complexity (for example routine procurement method for a routine ICT and Digital solution that is purchased); or • procurement for a study, strategy or planning activities	0

Criteria and Weighting	Priority and Risk level	Score
Agency capability and capacity: 15% The extent to which the sponsor agency has demonstrated capability (skills and experience), or can access through recruitment or procurement the required capability in the development and / or delivery of the type of project or program proposed and/or its delivery strategy.	Very high agency capability and capacity risk • no projects of this type previously procured and delivered over the last 10 years; or • resourcing capacity potentially severely limited in government or industry within the delivery timeframes (eg AI emerging technology)	5
	High agency capability and capacity risk • less than 5 projects of this type previously procured and delivered over the last 10 years; or • resourcing capacity potentially very limited within government or industry to deliver within the intended delivery timeframes (eg AI emerging technology)	4
	Medium agency capability and capacity risk • at least 5 projects of this type procured and delivered over the last 5 years • a record of successful procurement and delivery of these projects; and • resourcing capacity potentially limited within government or industry, requiring early planning and attention (eg AI emerging technology)	3
	Low agency capability and capacity risk • multiple recurring projects; and • a record of successful procurement and delivery of these projects; and • resourcing capacity may be limited within government or industry but is manageable (eg Cyber Security)	2
	Very low agency capability and capacity risk • business as usual type projects; and • a record of successful procurement and delivery of these projects; and • resourcing capacity within government and industry is established and adequate	1
	Extremely low agency capability and capacity risk • no agency capability risk for routine projects; and • a record of successful procurement and delivery of these projects; and • no agency or industry resource capacity risk	0

Criteria and Weighting	Priority and Risk level	Score
Technical Complexity: 15% The extent to which a project or program requires new or unproven technology, customised technology, or complex or lengthy integration with other solutions, thereby increasing the need for a careful assessment and management of risk.	Very high technical complexity • extremely new technology proposed or an unproven solution and/or complex inter-operability requirements across multiple platforms • there are a significantly high level of unknowns and/or assumptions involved which may have a significant influence over successful implementation (for example, automated decision-making systems, generative AI)	5
	High technical complexity • new technology proposed with numerous inter-operability requirements • there are a high level of unknowns and/or assumptions which may influence successful implementation (for example, similar technology solutions which have had at least one implementation completed in Government before)	4
	Medium technical complexity • proven technical solution with several inter-operability requirements. • There are a moderate level of unknowns and/or assumptions involved which may influence successful implementation (for example, similar technology solutions which have had more than one implementation completed in Government before)	3
	Low technical complexity • proven technical solution with few inter-operability requirements. • There are a low level of unknowns and/or assumptions involved which are unlikely to influence the success of implementation	2
	Very low technical complexity • proven solution with known inter-operability requirements • There are a low level of unknowns and/or assumptions involved which are highly unlikely to influence the success of implementation	1
	Extremely low technical complexity • no technical complexity, known and proven solution with no inter-operability requirements. • There are little or no assumptions involved	0

Criteria and Weighting	Priority and Risk level	Score
Cyber Security: 10% The extent to which a compromise of this product could result in an impact to services, loss of confidence in government (reputational, trust) or personal safety. The degree to which an attack against this product would impact significant state-wide infrastructure, and An identification of the classification level or volume of data traversing this product (to assess impact of a cyber- attack).	Very high cyber security risk • Highly valuable asset, operationally critical to achieving entity's mission and/or has critical external dependencies • Incident will have catastrophic impact. Consequences such as large-scale data loss, degradation of security controls, asset integrity and/or access failure could impact organisational operations statewide or multiple agencies and their dependencies. Critical or essential services are disrupted or unavailable • Public safety may be a material risk • Public disclosure causes long term reputational damage, community, client and executive dissatisfaction, financial losses and/or leads to penalties or legal action NB: Very high-risk level should be considered if: • Stores or processes NSW Dissemination Limiting Marker (DLM) Official: Sensitive or 'Protected' and higher • Project technical, interface and change complexity rated high or very high • Enterprise cyber risk appetite is low	5
	High cyber security risk • Highly valuable asset, operationally critical to achieving entity's mission and/or has critical external dependencies • Incident will have major impact. Consequences such as large-scale data loss, degradation of security controls, asset integrity and/or access failure could impact organisational operations to one or multiple agencies and their dependencies • Disruption in providing services and core business functions • Public disclosure causes reputational damage, community dissatisfaction in service, financial losses and/or leads to notification by regulating authority and increased regulatory oversight NB: High risk level should be considered if: • Stores or processes NSW DLM Official and/or Personally Identifiable Information (PII) or higher • Project technical, interface and change complexity rated medium or above • Enterprise cyber risk appetite is low	4
	Medium cyber security risk • Medium value asset, supports operationally critical services or processes to achieve entity's mission • An incident will have moderate impact • Consequences such as data loss, asset degradation or access failure could impact operational processes or systems to one agency or multiple dependent agencies • Public disclosure causes limited reputational damage and community dissatisfaction. Any regulatory non-compliance requires management effort to resolve NB: Medium risk level should be considered if: • Stores or processes NSW DLM Official and/or PII • Project technical, interface and change complexity rated medium	3

Criteria and Weighting	Priority and Risk level	Score
	Low cyber security risk • Low value asset, enables business operations but does not support operationally critical services or processes and has no integrations or dependencies • An incident will have minor impact • Consequences such as data loss, asset degradation or access failure limited to localised non-essential service • Highest data classification is NSW DLM Official that is non PII • Minimal disruption or delays to outward facing government or portfolio/agency ICT and Digital Systems • Disclosure causes short term concern in the media and community	2
	Very low cyber security risk • Very low value asset that enables some business operations but does not support operationally critical services or processes, with no integrations or dependencies • An incident will have negligible impact to outward facing government portfolio/agency ICT and Digital Systems • Stores and processes NSW DLM Unofficial and publicly available data. No privacy impact • Any disruption is manageable through BAU practices • No economic impact or reputational damage • No media attention, negligible concern from stakeholders	1
	Extremely low cyber security risk • A very low value asset that does not support business operations and has no integrations or dependencies • An incident will have no impact to outward facing government or portfolio/agency ICT and Digital systems • Stores and processes publicly available data. No privacy impact • Any disruption is manageable through BAU practices • No media attention and no concern from stakeholders	0

Criteria and Weighting	Priority and Risk level	Score
Change Complexity: 25% Sensitivity to the degree of business change required for the success of the project. This could be complex business or process changes internal to government or in the service delivery to government customers Risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects. The degree of criticality of services impacted by the project such as front-line services to citizens. The degree of unknowns involved with the chosen approach.	Very high change complexity risk • transformational changes in business processes with potential impact on service delivery processes • very high risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects • very high degree of criticality of services impacted by the project, or • involving more than one automated decision without human oversight, including cross-government projects/issues	5
	High change complexity risk • significant changes required to business processes with no impact on service delivery processes • high risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects • high degree of criticality of services impacted by the project; or • there is a high level of unknowns and/or assumptions involved • involving one automated decision without human oversight	4
	Medium change complexity risk • changes required to some business processes with impacts to connected systems requiring rework • medium risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects • medium degree of criticality of services impacted by the project, or • involving one or more automated decisions with human oversight	3
	Low change complexity risk • minimal changes required to either business process or service delivery processes. Low technology change • low risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects, or • low degree of criticality of services impacted by the project (for example research data collections using drones and IoT devices)	2
	Very low change complexity risk • no changes required to business or service delivery processes, minimal systems impacted • very low risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects, or • very low degree of criticality of services impacted by the project	1
	Extremely low change complexity risk • no changes required to business or service delivery processes; no other systems impacted • no risk or perception of risk to service delivery, security and privacy or similar issues that may impact change management aspects • extremely low degree of criticality of services impacted by the project	0

6 Appendix B - Gateway Review purpose

	PLANNING		DELIVERY			
	GATE 1 Strategic Alignment	**GATE 2 Business Case**	**GATE 3 Pre-execution**	**GATE 4 Tender Evaluation**	**GATE 5 Pre-commissioning**	**GATE 6 Post-implementation**
	Will the project efficiently deliver on Strategic Imperatives?	*Will the project deliver value for money?* *Is the money being invested wisely?*	*Is the project set up for success?*	*Will delivery be successful?*	*Are the deliverables ready for service?*	*Did the project deliver benefits?* *Are there lessons to be learned?*
PURPOSE	Ensures the business needs for the initiative are clearly defined and aligned with Strategic imperatives, Investment Principles and Enterprise Architecture	Ensures that the business case is robust and there are plans to realise benefits and align with Strategic imperatives, Investment Principles and Enterprise Architecture.	Assesses the procurement and tendering approach, identifies problems early in the initiative and ensures plans for the delivery of the initiative are in place.	Evaluates the solution and preferred option prior to committing funds, ensuring that the initiative will be delivered effectively and checks requirements against milestones.	Assesses whether the organisation is ready to adopt the solution to achieve the planned benefits stated in the business case and implement the change management required.	Assesses whether the anticipated benefits are being delivered, lessons learned have been considered and plans for ongoing improvements in value, service enhancements and performance are in place.
			Potential for multiple or recurrent health checks and milestone reviews.			
			HEALTH CHECKS			
			Are there any leading indicators of project failure?			
			Test leading indicators of problems to catch risks and issues early. *Ensure appropriate measures and checks in place for ongoing assurance.*			
			DEEP DIVES			
			Focus on a particular issue or limited terms of reference rather than the full range of issues normally considered at a Health Check.(for example: penetration testing)			
			RAPID ASSURANCE REVIEW (RAR)			
			Iterative assessment, depending on the needs of the project and visibility to IDIA, focusing on progress to treat the identified risks.			

Gate 1 - Strategic alignment gate. Ensures the project is conceived of in the right way and aligns with relevant Strategic Imperatives, Investment Principles and Enterprise Architecture.

Gate 2 - Business case gate. Ensures the project has a robust business case, with clear plan to realise benefits, aligns with relevant Strategic Imperatives, Investment Principles and Enterprise Architecture.

Gate 3 - Pre-execution gate. Assesses delivery readiness and includes pre-tender review. Ensures the project is set up for successful delivery, identifies delivery problems early, and ensures procurement strategy and other planning is appropriate.

Gate 4 - Tender Evaluation gate. Ensures project will be delivered effectively, checks against specific project requirements at key delivery milestones, includes tender evaluation.

Gate 5 - Pre-Commissioning gate. Assesses the state of readiness to commission the project and implement the change management required.

Gate 6 - Post-implementation gate. Confirms realisation or plan for realisation of benefits against those agreed at business case, ensures lessons learned have been sufficiently considered and documented.

Health Checks: assess whether a project is being managed effectively and assists those responsible for managing a project between Gateway Reviews.

Deep Dives: Focus on a particular issue or limited terms of reference rather than the full range of issues normally considered at a Health Check.(for example: penetration testing)

Rapid Assurance Review: Iterative assessment, depending on the needs of the project and visibility to IDIA, focusing on progress to treat the identified risks.

Department of Customer Service

McKell Building
2/24 Rawson Pl
Haymarket NSW 2000

GPO Box 7075
Sydney NSW 2001

Office hours:
Monday to Friday
9am to 5pm

E: ICTAssurance@customerservice.nsw.gov.au
W: digital.nsw.gov.au

NSW GOVERNMENT