Australian Government
The Treasury

Digital and Cyber Security Strategy

2024–26

treasury.gov.au

In the spirit of reconciliation, the Treasury acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Contents

Secretary's foreword

I am proud to present Treasury's Digital and Cyber Security Strategy 2024-26

As the Government's lead economic adviser, Treasury provides timely advice on economic and fiscal issues. Treasury uses rigorous analysis, evidence and data to effectively communicate and collaborate with our stakeholders and partners. We use digital technology to ensure our information and systems are secure, resilient, responsive and fit-for-purpose.

The Digital and Cyber Security Strategy 2024–26 (DCSS) sets out how we will achieve this goal. It builds on a foundation established in recent years and demonstrates Treasury's commitment to continuous improvement, learning and adaptation.

The DCSS describes a set of strategic priorities and actions to ensure Treasury remains agile and responsive to digital challenges and opportunities. It provides flexibility to refine and adapt our approach as we progress. One strategic imperative set by the DCSS is to maximise the return on technology investments by embedding and enhancing what we already have. This means empowering employees to adopt and use digital solutions confidently and securely.

The DCSS also supports Treasury's commitment to building and sustaining trust through our pro-integrity culture. It emphasises the importance of continuing to mature our information management and record-keeping practices to contribute to this strategic priority.

While our digital solutions are an important enabling element, it is up to each one of us to ensure we understand our responsibilities and are effectively fulfilling them in this important area.

I welcome the DCSS and encourage everyone to incorporate digital opportunities and cyber security into the work you do. This could be following good cyber hygiene practices, providing feedback on the digital solutions you use, or finding new ways to leverage data and technology. For example, I stepped cautiously into the AI universe using generative AI to help create the first draft of this foreword.

We use and depend on digital workspaces and tools daily. A strong digital capability, underpinned by robust cyber security, will enable us to continue providing the Government with the best possible advice for improving economic and fiscal outcomes for all Australians.

Dr Steven Kennedy PSM
Secretary

Digital and cyber at Treasury

Introduction: the digital and cyber landscape

Information and communications technology (ICT) extends to all aspects of work at Treasury. To make the most of technology while keeping employees and information safe and secure, Treasury must continually balance and coordinate investment. The department must also commit to ongoing improvement across its people, practices and technology.

The focus of the Digital and Cyber Security Strategy

Treasury's new *Digital and Cyber Security Strategy 2024–26 (the DCSS)* outlines the direction Treasury is taking and why. The DCSS focuses on maximising the return on recent technology investments by embedding and enhancing what the department already has. This means ensuring our employees are individually supported in the adoption and use of digital solutions. It also means evolving and adapting Treasury's practices and ways of working.

The DCSS has four focus areas:

1

The digital workplace

2

Core business functions and systems

3

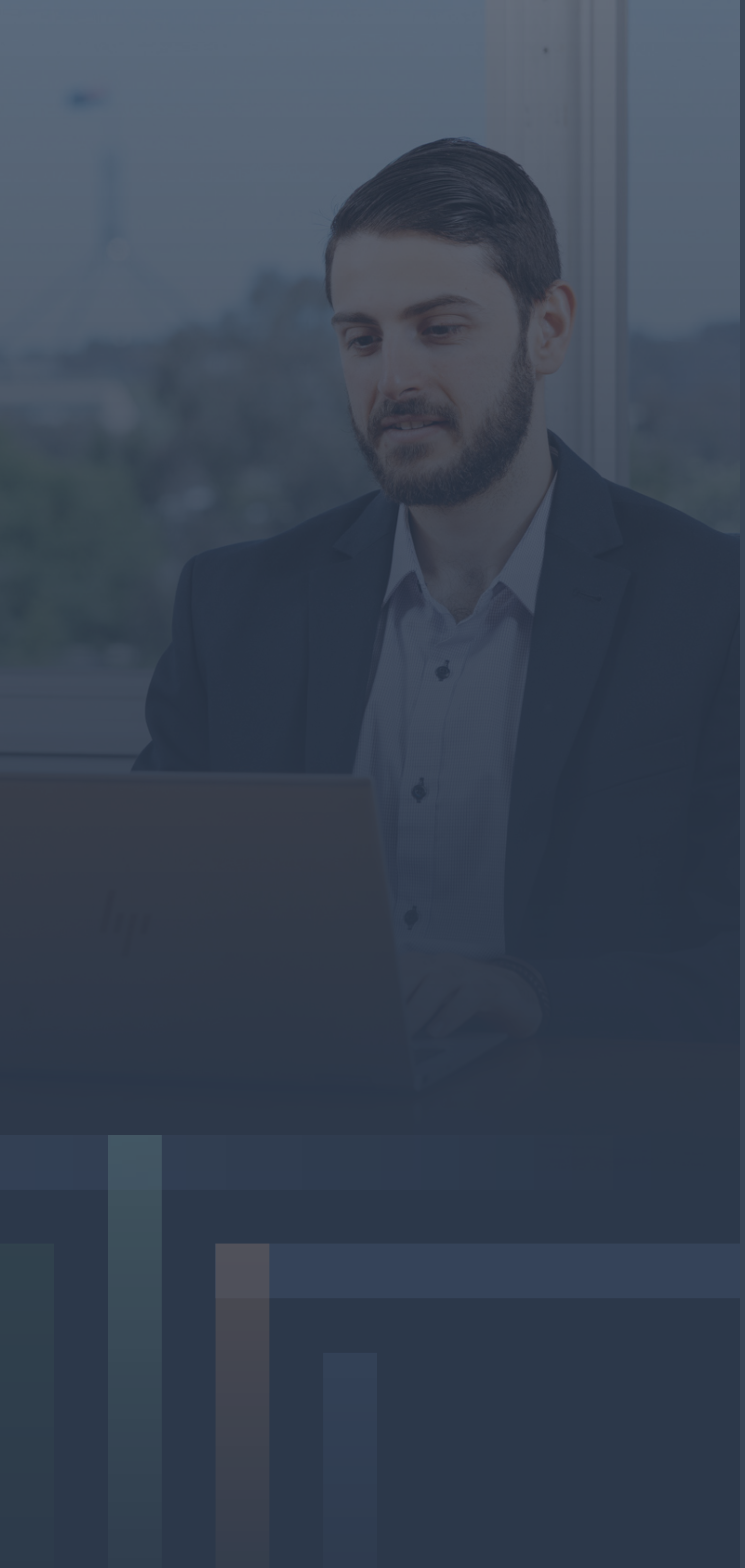
Information integrity

4

The ICT function and technology estate

Each focus area contains goals and actions that give Treasury flexibility to refine and adapt its approach over the life of the Strategy and beyond. Well-planned action in each of these areas will see Treasury continue to succeed in the digital age.

Investment must be balanced across a range of areas and the level of ambition must be aligned with funding and resource availability. Not all opportunities can be pursued, and expectations must be set and managed accordingly. The DCSS actions account for this and have been developed in a way that allows the level of ambition to adjust based on funding availability.



Cyber security

Cyber security has not been isolated into its own focus area within the DCSS. Instead, it is embedded in each of the 4 focus areas. Cyber security underpins the DCSS and, embedding it as part of all IT initiatives, aligns Treasury with whole-of-government strategic directions in this area.

Just as cyber threats constantly evolve to become more sophisticated and diverse, so too does cyber security at Treasury. Cyber security is a dynamic and ongoing process that requires constant vigilance, collaboration and adaptation. Treasury cannot afford to be complacent or reactive. It must continually assess its cyber risks, strengthen its cyber shields, and enhance its cyber capabilities.

Treasury's data capability

No digital or cyber security strategy is complete without acknowledging the importance of data. An abundance of data is a defining feature of the digital age. Organisations are increasingly realising the importance of investing in their data capability and the necessity of having robust data management and governance practices in place. More focus is being placed on building data literacy across the workforce, breaking down data 'silos', and treating data as an enterprise asset that needs to be actively curated.

Treasury has a dedicated Chief Data Officer who led the development of the department's inaugural *Enterprise Data Strategy 2023–25* which is in its initial stages of implementation. While some aspects our data capability – particularly the technologies supporting it – are mentioned in the DCSS, any action taken must be done so within the context of the *Enterprise Data Strategy.*

The *Enterprise Data Strategy* serves as Treasury's primary strategic vehicle for directing data uplift efforts. A strong partnership between the Chief Data Officer, Chief Information Officer, and the teams they lead is imperative for progress in the digital and data domains and the mutual success of the *Enterprise Data Strategy* and DCSS.

Where Treasury is at

Treasury commences the DCSS in a favourable position. It has a solid digital foundation in place and is protecting our information and employees from cyber security threats. Recent years have seen significant investment that has helped:

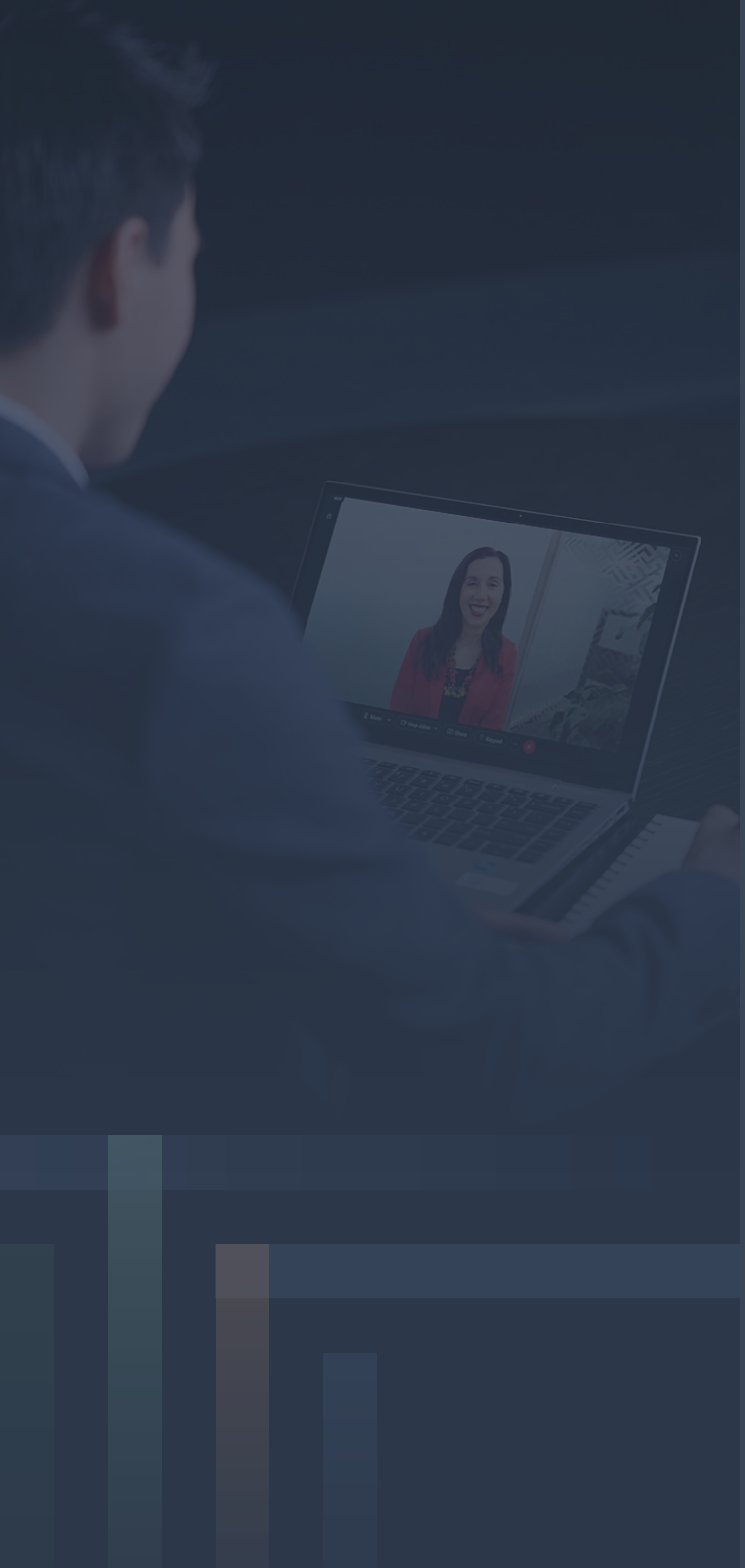
- Stabilise systems
- Pay down legacy technical debt
- Introduce contemporary digital tools
- Uplift information management practices, and
- Mature our cyber security controls.

Importantly, employees report having a positive service experience when consuming digital services at Treasury, particularly in comparison to prior experiences in other workplaces.

What now?

Rather than disrupting or transforming how Treasury operates, the DCSS focuses on making iterative progress. Consultation and analysis have identified opportunities and areas needing improvement.

- Treasury must continue embedding the investments it has already made, driving adoption, and building proficiency in the use of our existing digital tools and workspaces.
- Treasury must seek to continually improve and refine its digital solutions and their usage based on feedback and evolving needs.
- Treasury must investigate and adopt new technologies in a targeted and business driven way. At the time of writing, generative artificial intelligence is a prime example with organisation's worldwide exploring and assessing the benefits it promises.
- Treasury must continually balance requirements for digital safety, resilience, integrity and compliance with enabling employees to do their jobs.
- Aligned with the Australian Government Cyber Strategy 2023–2030, we must continue to deliver, evolve, and invest in cyber security.
- Treasury must be disciplined in the upkeep of our digital solutions and the underlying platforms, core technology services, infrastructure, and networking that make up our technology estate. The department has worked hard to put itself in a favourable position, and our digital environment is modern, reliable, and secure. However, things can quickly degrade without continued attention, effort, and investment.



The APS data, digital, and cyber landscape

The Australian Government's two strategy documents for digital and cyber security are the:

- Data and Digital Government Strategy 2023–2030, and
- Australian Cyber Security Strategy 2023–2030.

These strategies fit into a broader APS 'data and digital landscape' made up of related strategies, policies, frameworks, standards, and schemes which are depicted in the *Data and Digital Government Strategy* (page 31 'APS Reform Agenda'). Treasury's DCSS objectives align with these whole-of-government strategies.

1

Focus 1: The digital workplace

Providing employees with a streamlined set of digital tools and platforms that enable them to get their work done while maximising productivity, providing a positive user experience, promoting sustainable work patterns, and supporting employees to operate safely and securely.

What it is and why it's important

The 'digital workplace' encompasses the digital platforms and tools we use to do our work. At Treasury it includes the physical spaces such as workstations and meeting rooms supplemented with technology to provide a digital experience. It also extends to the arrangements, structures, and guidance that help employees use these capabilities.

An organisation's digital workplace directly influences productivity. An effective digital workplace empowers employees to work efficiently and is simple, stable and easy to operate. It should also be flexible to allow remote, hybrid and cross-organisational work to occur in seamlessly. It is secure and empowers Treasury employees to operate safely and securely online.

Importantly, in an increasingly connected and flexible work environment, a mature digital workplace should support staff in establishing sustainable work patterns. This includes providing teams, managers, and HR specialists with data-driven insights around these patterns to help inform discussions and initiatives focused on employee wellbeing.

1

Where we're at and what we'll focus on

Treasury's digital workplace is well positioned. The foundational pieces are in place and our digital environment is stable and easy to access – including remotely.

Treasury has implemented collaboration and creation platforms such as Microsoft SharePoint Online and Microsoft Teams, and options are available to support most activities. However, consultation and analysis to develop the DCSS identified challenges and areas needing improvement.

- Tools that support quantitative analysis and analytics need streamlining. This extends to refining our ways of working, including how we manage code and data.
- Information search and discovery capabilities need to be better.
- Enhancements to Microsoft Teams allowed employees to chat with peers in other agencies but we can improve collaboration with government partners on key information products.
- Minor but compounding performance, stability and usability issues exist. Over time, this can lead to reduced employee productivity and a frustrating experience.
- Employees need better resources and support to identify the digital workplace solutions available to them. This extends to choosing the most appropriate solution for the task at hand and building proficiency in its use.

Noting these challenges, Treasury will focus on maximising recent investments and embedding our digital tools and workspaces into how we work. To do this, we must invest in better supporting employees in the adoption and use of digital workplace products and in developing sustainable work patterns. Treasury must also continuously improve and streamline the tools and solutions we have and reduce the barriers to their effective use.

1

Actions

Action 1.1 – Continue to invest in better supporting employees to identify, adopt, and build proficiency in digital tools and workspaces.

Action 1.2 – Continue maturing our digital workplace by enhancing and streamlining existing platforms and tools and introducing new solutions, where appropriate.

Action 1.3 – Embody a 'continuous improvement' mindset to address minor-but-compounding issues relating to performance, stability and usability.

Action 1.4 – Continue building a proactive, cyber-aware culture to embed principles of secure-by-design and secure-by-default.

2

Focus 2: Core business functions and systems

What it is and why it's important

> Optimise and integrate Treasury's key activities and data to maximise productivity in delivering Treasury's remit as the Government's lead economic adviser.

This focus area looks at the specialised solutions used to support core business functions in different parts of Treasury. These specialised solutions ensure Treasury can deliver its key activities by enabling the:

- capture, storage and presentation of critical data and information
- automation of calculations and quality checks, and
- capture of records of completion.

While some teams in Treasury can rely solely on standard digital workplace tools to complete their work, others require specialised solutions and, in many cases, cannot do their job without them.

2

Where we're at and what we'll focus on

With limited resources available, Treasury's ICT function must focus on balancing its attention between supporting the teams relying on specialised solutions (for example non-enterprise, line-of-business software applications), against the priorities of the whole of Treasury.

Consultation and analysis to develop the DCSS did not identify any major gaps, however opportunities do exist to better support some teams performing specialised functions. Where appropriate, Treasury should further investigate and pursue these opportunities.

Treasury's existing portfolio of specialised solutions is largely functional but far from optimised. While some teams have received investment to modernise their systems, other teams still rely on sub-optimal solutions.

The DCSS consultation process found that to optimise Treasury's existing portfolio of specialised solutions we need to:

- expand and enhance functionality
- improve integration, and
- improve use and adoption by employees.

Some specialised solutions are ageing and need plans in-place to either modernise, replace, or retire them as they move closer to end-of-life.

Some teams in Treasury rely on legacy utility solutions that are smaller in scale and less visible to Treasury employees. In some cases, these utilities support critical business processes and, if unavailable or compromised, present a risk of significant delay or disruption. Treasury should formalise the existence of these utility solutions and agree to their ongoing management and/or replacement.

Aspects of Treasury's digital governance need attention, namely the process of identifying and introducing new solutions and managing existing ones. For example, we need to document how Treasury identifies, assesses and funds new opportunities, and ensures appropriate governance during their implementation.

2

Actions

Action 2.1 – Partner with business areas to create digital roadmaps for the department's line-of-business applications and utilities. This mapping exercise should consider unmet needs and/or pain points that are most likely to require investment and should include considerations for enhancing or replacing legacy solutions as appropriate.

Action 2.2 – Establish and embed a decision-making approach and guidance to support the identification, assessment and funding of investments in non-enterprise, line-of-business applications. This should extend into the oversight of their implementation.

Action 2.3 – Pursue opportunities to better support Treasury's core business functions by addressing gaps, improving existing systems to ensure they are fit-for-purpose, and better integrating and automating processes and information flows. This should build on insights from Action 2.1 and the consultation and analysis done to develop the DCSS.

Action 2.4 – Continue maturing and optimising the structural arrangements and digital practices related to the management of Treasury's application portfolio and development of individual solutions.

3

Focus 3: Information integrity

> Robust information management and record-keeping practices that underpin defensible and transparent Treasury business activity, contribute to our culture of integrity and capability, and ensure our information assets remain accessible and useable.

What it is and why it's important

Treasury undertakes research and analysis across many policy domains. The department develops information that informs critical decision making and is subjected to much scrutiny. These information holdings are vast and continue to grow in size and complexity. Without the appropriate structures and processes it becomes difficult to find and validate past information.

Some Treasury information is highly sensitive in nature, although this can change over time. Treasury's information management obligations must be maintained to ensure information risks are appropriately managed, to meet government and community expectations, and to comply with policies and legislation. Sound information management and governance are essential for maintaining and contributing to a culture of integrity.

3

Where we're at and what we'll focus on

Treasury is progressively developing and refining its ability to securely manage its information and fulfil record-keeping obligations. The department is establishing robust information management and governance practices.

However, consultation and analysis has identified several areas that need focus and further improvement.

- Teams are struggling to locate, leverage, and manage historical information, particularly in areas where historic information is spread across multiple repositories.
- Some teams still rely on corporate file shares as a digital workspace to create and store information. Further analysis is needed to understand why and how these file shares are being used so that more appropriate solutions and practices can be discussed.
- Teams have reported mixed experiences with metadata tagging and the transition to a flattened, metadata-driven information storage and management system.
- Education, awareness raising and training about the information lifecycle is needed so that employees understand their responsibilities beyond initial information creation and storage. Employees and teams should understand their obligations and be equipped to fulfil them.
- Information management considerations should be factored into digital-solution design and decision-making. The implications of unavoidable trade-offs on information management policies and strategic directions should be explicit.

3

Actions

Action 3.1 – Continue embedding and refining recent information management capability uplift, including a focus on improvements to the functionality and usability of our information management systems, to ensure good information management practices and behaviours are maintained across Treasury (particularly for employees holding formal roles as defined under the Information Governance Framework).

Action 3.2 – Shore up historical information holdings and move away from legacy solutions that lack the safeguards and functionality to support good information management practices.

Action 3.3 – Work through the backlog of records to assess what needs to be retained, transferred or disposed of. As part of addressing these records management obligations, this effort should seek to identify and reduce redundant, obsolete and trivial information (frequently referred to as ROT).

Action 3.4 – Ensure the ongoing confidentiality, integrity, and availability of our information within an evolving cyber landscape by proactively hunting threats and monitoring the digital environment to identify unusual and/or suspicious patterns.

Focus 4: The ICT function and technology estate

A capable and empowered ICT workforce delivering high quality services while proactively sustaining a modern, secure, and responsive technology estate.

What it is and why it's important

Treasury's 'ICT function' is underpinned by its workforce of ICT specialists that support and serve employees. Treasury's 'technology estate' refers to the platforms, core technology services, infrastructure and networking that underpin digital tools, workspaces and business applications.

Treasury's ICT workforce and technology estate are critical to providing an effective digital offering that supports the department's operations. Both need ongoing attention to ensure the ICT function continues to offer Treasury employees high quality, fit-for-purpose products and services.

4

Where we're at and what we'll focus on

Treasury's ICT function is mature with key processes and practices relating to digital service delivery and the solution lifecycle in place. Feedback during consultation indicated that in most cases, employees have positive service experiences. Investments in the technology estate have allowed the establishment of a modern and secure hybrid-cloud capability, providing greater choice and sophistication in where and how we run digital solutions.

However, there are pressure points and challenges.

- Recruiting, developing and retaining a suitably skilled and experienced ICT workforce with an appropriate ratio of APS employees is a challenge. There is intense competition to attract talented individuals with the required skills and expertise. Treasury is not alone in this challenge and its resolution is a whole-of-government priority.
- Cloud governance, cost optimisation and transition-to-sustainment capabilities need attention to keep pace with demand for new solutions and improved responsiveness.
- Parts of Treasury's technology estate need to be redesigned or refined to better suit a hybrid-cloud reality and maximise the return on recent investments.

4

Actions

Action 4.1 – Build workforce capability in line with whole-of-government efforts and Treasury's Strategic Workforce Plan 2024–2030 by investing in the recruitment and retention of talented, experienced people with the skills to operate, maintain, and defend Treasury's digital environment.

Action 4.2 – Mature the processes and practices that deliver, operate, sustain and protect digital solutions and the technology estate.

Action 4.3 – Continue developing our technology estate for a hybrid-cloud reality and be disciplined and proactive with its upkeep.

Success and tracking progress

Determining success

The topics and success measures below have been set out to give an indication of what success looks like for the DCSS. As action plans are developed and delivered, the definition and measures of success may evolve to match the shifting operating context and greater level of planning and detail available.

1

The digital workplace

2

Core business functions and systems

3

Information integrity

4

The ICT function and technology estate

Focus 1: The digital workplace

Topic/measure	What success looks like and how it will be determined
Employee awareness of digital workplace solutions available and level of confidence in their use.	Treasury staff are aware of the digital workplace solutions available to them and are confident in their ability to use these solutions, feeling adequately supported as they seek to adopt and build proficiency in them. This item will be assessed via insights from the APS Census and Delphi survey and incident data with additional, targeted staff surveys to fill gaps as needed.
Employee experience when consuming digital services and solutions at Treasury.	Treasury staff have a positive service experience when engaging with ISB and other digital service owners at Treasury and positive user experiences when leveraging Treasury's digital workplace offering to deliver their remit. This extends past usability to the fitness-for-purpose of the digital workplace to support them in their work. This item will be assessed via insights from the APS Census and Delphi survey and incident data with additional, targeted staff surveys to fill gaps as needed.
Staff cyber hygiene awareness and behaviours.	Treasury staff understand their role in protecting Treasury from Cyber security threats and are exhibiting good cyber hygiene behaviours. This item will be assessed via a targeted survey as part of other cyber awareness activities during Cyber Security Awareness week each October. Other quantified metrics regarding specific cyber hygiene areas may also be explored.

2

Focus 2: Core business functions and systems

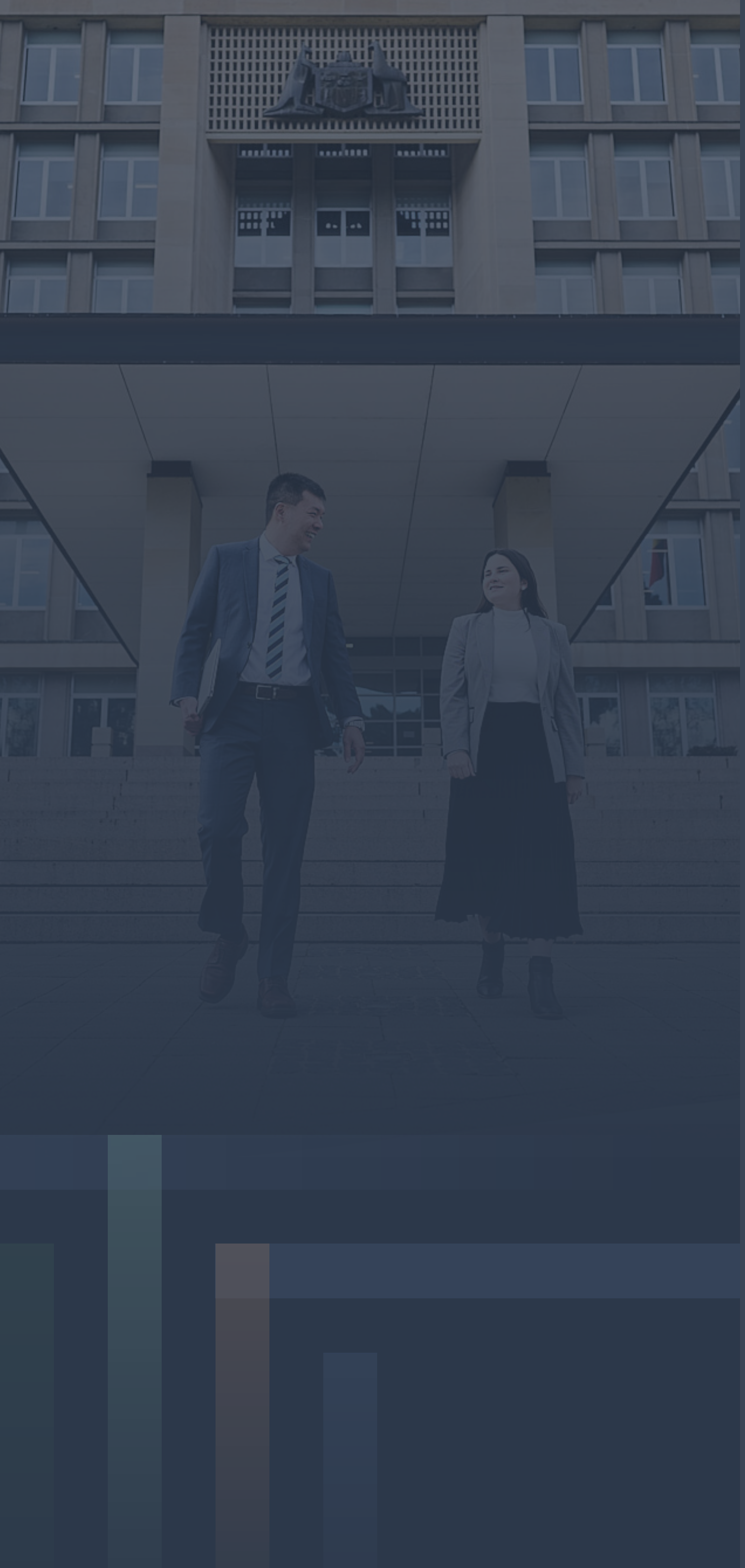
Topic/measure	What success looks like and how it will be determined
Shared understanding of Treasury's digital landscape and agreement on the pressure points and areas likely to require investment.	ISC, ISB, and relevant business areas have a common view of the systems and utilities supporting Treasury's core functions. Building on this, they have a shared understanding of the pressure points and areas likely to require investment. There is also agreement on the priorities, or on how these will be established, which helps facilitate investment decision-making. This item will be assessed via the establishment of formal, endorsed digital needs statements and supporting roadmaps for prioritised functional areas and their associated systems.
Benefits realised by business areas from initiatives targeting core system uplift.	Treasury business areas are actively benefiting from the core system uplift initiatives that Treasury chooses to invest in. These benefits will come in many forms and may relate to operational efficiency and productivity, risk mitigation, and/or the efficacy of the functions and the quality of their key deliverables. This item will be assessed via a summary of the benefits resulting from individual initiatives and will draw on insights from the standard project and benefit management products developed by the initiatives.
Level of collaboration and ongoing engagement between business and technical teams	ISB and business areas are proactively partnering, early in the solution development journey, to identify and understand business needs and explore the different solution options available. Treasury's full portfolio of applications and utilities is understood and insights from the associated analysis are being fed into the discussion. Success in this area will be assessed via feedback in staff surveys, an assessment of engagements and subsequent initiatives that arise throughout the DCSS' lifespan, and the establishment and completeness of the application portfolio catalogue.

Focus 3: Information integrity

Topic/measure	What success looks like and how it will be determined
Empowerment in, and ease of, managing information at Treasury.	Employees are clear on their information management responsibilities and feel empowered to fulfil them. This item will be assessed via employee feedback either as additional questions as part of National Archives of Australia's (NAA) annual Check-up Survey, via insights from the APS Census, or via an additional, targeted staff survey.
Maturity of Treasury's information management capability.	Treasury's information management capability is sufficiently mature given Treasury's requirements and operating context and taking into consideration maturity benchmarks established across government. This item will be assessed via the NAA's annual Check-up Survey.
Size and status of Treasury's historical information holdings.	Treasury is actively managing its historical business content. A good understanding of what is held has been established. Proactive, ongoing discussions are being held between central information management areas and Treasury teams to preserve and retain what is necessary and to dispose of what is redundant, trivial or obsolete, in line with best practice as established the National Archives of Australia. The footprint of these holdings and associated costs are reducing accordingly. This item will be assessed via the completeness of Treasury's information asset register, the completeness of assessment activities such as records sentencing, and the storage footprint (size and file volume) of Treasury's historical holdings.
Cyber security threats and vulnerabilities detected and remediated.	Treasury's cyber defence and response posture shifts from a reactive to a proactive model. The department is dynamically detecting and responding to emerging threats, actively minimising the likelihood of data breaches and disruptions to business operations. Success for this item will be determined via an assessment of the threats proactively detected and vulnerabilities identified and remediated.

Focus 4: The ICT function and technology estate

Topic/measure	What success looks like and how it will be determined
Understanding of skill and expertise gaps and commencement of pilot actions to resolve.	Treasury is contributing to addressing the Whole-of-Government digital skills challenge and has made progress in identifying and filling its most pressing digital/ICT skill and expertise gaps. Success in this area will be assessed based on the finalisation of a gap analysis and identification and commencement of several pilot response actions.
Presence of the necessary framework(s) and processes for prioritised functions and capability areas.	ISB has the appropriate frameworks and other guidance materials in-place which set out and clarify the approach for, and processes involved in, priority functions such as cloud governance and cost-optimisation. This measure will be assessed based on the finalisation of these products and the active execution of the new/refined processes as part of ongoing operations.
Volume of legacy patterns and technical debt in Treasury's technology estate.	Treasury's technology estate has continued to evolve, with legacy patterns that run counter to a hybrid-cloud reality remediated and technical debt managed to acceptable levels. Success in this area will be assessed via a stock-take of the changes made and an assessment of their contribution to reducing Treasury's 'tech debt'.



Implementing the Strategy and tracking progress

In order to implement the DCSS, and to track progress of the implementation, additional levels of planning and decision making are first required. The DCSS will be supported by an action plan(s) which, for the chosen planning horizon, will set out the agreed concrete action areas being targeted and the steps that will be taken to progress realisation of the Strategy. The Action Plan will be published alongside the DCSS in addition to the supporting information (for example, discussion papers and session summaries from the strategy development working group) that helped inform the Strategy. The action planning effort will effectively translate the DCSS into an agreed set of tangible initiatives and steps forward which will then allow progress against the DCSS focus areas and actions to be demonstrated and reported on.

This action planning will consider Treasury's investment management approach and the availability of funding. Action plans developed for the DCSS will help inform, and be informed by, Treasury's annual ICT investment plan, the *IT and Cyber Security Work Program*. Levels of ambition will be aligned to funding availability, and the organisation's capacity for change, while still being driven by business need and requirements.

A progress review will be carried out at the end of year 1 of strategy implementation. This will draw on the Action Plan and the additional detail that informed the Strategy to provide an update on progress made. It will include a narrative around any significant changes in the operating environment that are relevant to the DCSS's intent and/or its implementation. The review will also capture any useful insights or key learnings from the first year of the Strategy's implementation. This will then inform a revised action plan which will guide the Strategy through to its completion.

In addition to the year 1 review, quarterly reporting through to Treasury's Information Strategy Committee (the ISC) on DCSS implementation will be carried out. This reporting will be lightweight and focus on highlighting key achievements as well as raising any noteworthy challenges or dynamics that arise.

Noting the design and flexibility of the DCSS, Treasury leadership may decide to extend its lifespan with updates to the narratives and priorities of each focus area made as needed.