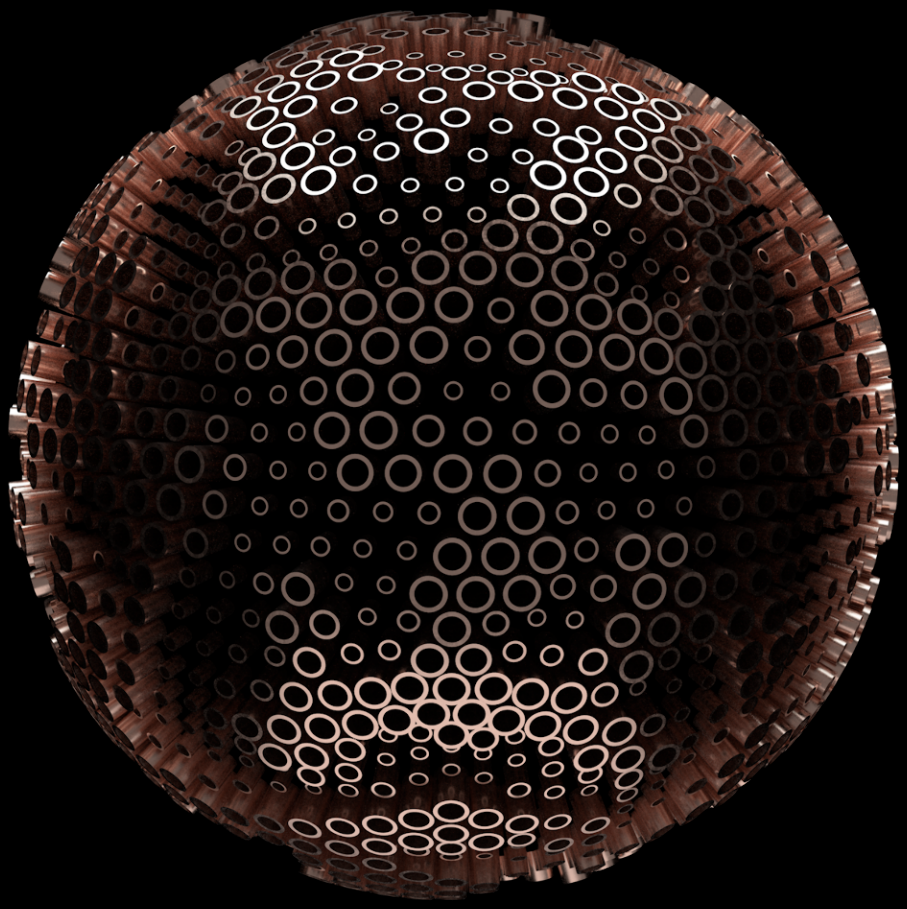
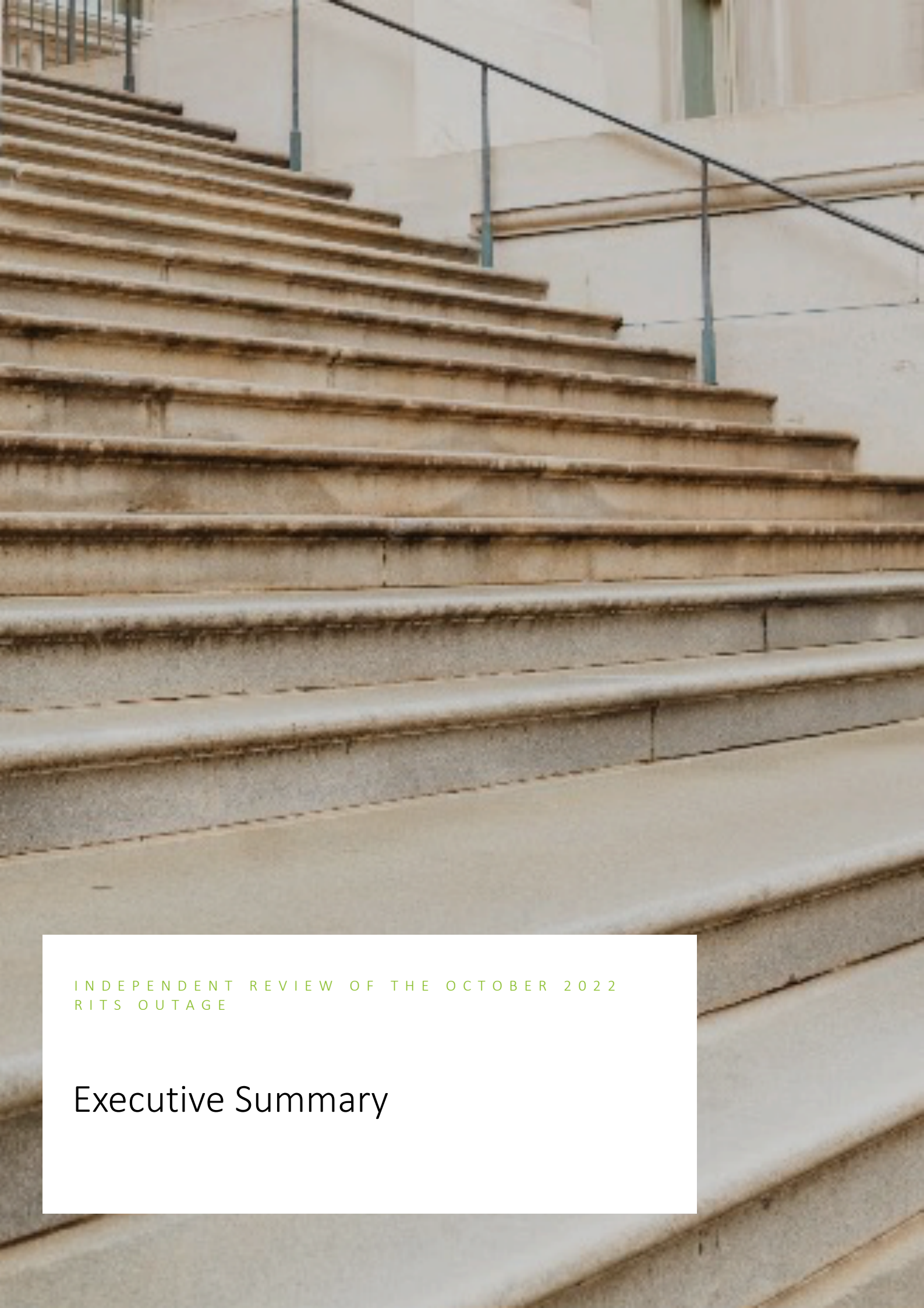
Deloitte.



Independent Review of the October 2022 Reserve Bank Information and Transfer System (RITS) Outage – Final

APRIL 2023

CONTENTS



INDEPENDENT REVIEW OF THE OCTOBER 2022 RITS OUTAGE

Executive Summary

1. Executive summary

1.1. Background

The Reserve Bank of Australia (**the Bank** or **RBA**) has a range of responsibilities. It conducts monetary policy, works to maintain a strong financial system, issues the nation's currency, provides selected banking and registry services to a range of Australian government agencies and to a number of overseas central banks and official institutions, and manages Australia's gold and foreign exchange reserves. In addition, the Bank has an important operational role in payments through its ownership and management of the Reserve Bank Information and Transfer System (**RITS**), Australia's real-time gross settlement (**RTGS**) system.

On 12 October 2022, the Bank experienced a Bank-wide technology issue (**the 12 October 2022 incident** or **the incident**) that affected services provided by RITS, including the Fast Settlement Service (**FSS**) and the RITS Low Value Settlement Service (**LVSS**), collectively known as the RITS ecosystem[1].

The Bank's objective for RITS is to provide highly available and resilient settlement services to payment participants and various securities and property settlement systems. Payment participants include banks and non-banks participating in the Direct Entry, BPAY, EFTPOS, and high-value clearing streams.

The RITS ecosystem is national infrastructure for the Australian financial ecosystem. The Bank has to ensure continuous availability with settlement services needing to meet, or exceed, a 99.95% availability target.

RITS is part of the Bank's broader technology environment and the RITS applications are supported by dedicated technology teams and a shared services model. The RITS ecosystem comprises the Payments Settlements (**PS**) department (the functional area responsible for operating RITS), significant proportions of information technology (**IT**), including most shared services teams, and other Bank-wide departments including Risk and Compliance (**RM**).

A significant proportion of the Bank's employees are involved in delivering and supporting the RITS ecosystem. The 12 October 2022 incident occurred within a shared services team that supports other critical Bank functions.

1.2. Scope and approach

The 12 October 2022 incident, along with other incidents in the last three to four years, have prompted the Payments System Board (**PSB**) to ask the Bank to commission an external review.

Deloitte was engaged by the Bank on 20 January 2023 to assess non-technical factors which either contributed to the incident or present ongoing operational risks for RITS as Australia's RTGS system. A separate independent external review was commissioned by the Bank into the technical factors of the incident. That report was delivered to the Bank in February 2023. For the avoidance of doubt, the technical review was not performed by Deloitte.

The scope of the Deloitte non-technical review covered the following scope areas:

- Operating framework, processes, roles and responsibilities
- People and culture
- Risk management and governance.

Our review was primarily undertaken through stakeholder interviews, document / artefact analysis as well as a risk culture survey, using Deloitte's Risk Culture Framework, of employees across the RITS ecosystem. This report is prepared primarily on an exception basis, highlighting only those findings and associated recommendations that have the potential to present ongoing operational risks. Further, while the scope of our review was focused only on the RITS ecosystem (not broader bank governance and control environment), it is worth noting that several of our findings and recommendations apply more broadly to the Bank.

Our final report was issued on 21 April 2023.

[1] *https://www.rba.gov.au/media-releases/2022/pdf/mr-22-40-final-incident-report-rits-and-fss-incident-12-october-2022.pdf*

1.3. Our Perspectives

The Bank, similar to its financial system counterparts, has over the past few years needed to navigate the complexities and operational realities associated with the COVID-19 pandemic whilst also delivering its duties to contribute to the stability of the currency, full employment, and the economic prosperity and welfare of the Australian people.

COVID-19 also had a profound impact on consumer behaviour, with a considerable increase in the use of digital payments.

Our review observed many strengths that support the Bank's RITS ecosystem. We observed a strong sense of care for the national infrastructure the Bank manages, particularly in PS and amongst longer serving team members. People working across the RITS ecosystem demonstrate high technical competence; it is a work environment characterised by people aligned behind a common purpose, who are proud of their job and role at an iconic Australian institution. This contributes to the Bank having many long serving employees with practical experience of core business practices. This is an important factor supporting the limited incident history across the RITS ecosystem.

However, notwithstanding investments to enhance the operational maturity of the Bank, the RITS risk and control environment subject to this review was found to require uplift to be effective, which is essential for maintaining the high level of system availability required.

Management of the RITS ecosystem sits within an increasingly complex and fast changing external environment. Whilst the Bank has many underlying strengths, it has not continuously strengthened the resilience of processes and controls supporting national infrastructure.

Consistently, we identified that while the Bank has designed and developed a significant volume of frameworks and documentation, many require strengthening and have not been effectively implemented and embedded into business-as-usual operations. This has contributed to a number of the root causes identified in this report and presents operational risk to the RITS ecosystem.

Our findings are summarised below. Full details are included in the body of the report.

Operating framework, processes, roles and responsibilities

The Bank has invested heavily in enhancing its IT capability over the past decade by implementing an industry standard IT operating model and business aligned teams directly supporting Bank departments and shared service teams to provide infrastructure and service management support.

However, considerable work is required to transition from conceptual design to detailed implementation in order to effectively govern and control the RITS ecosystem. For example, we found:

- Insufficiently targeted and clearly documented processes, services, service levels, roles and accountabilities for the RITS ecosystem
- A highly manual and complex technology control environment with limited controls testing
- A lack of comprehensive disruption scenario testing within RITS' business continuity arrangements.

People and culture

The Bank's RITS people are strongly aligned with its core purpose and this contributes to many long serving employees. The depth of experience of these people is highly valued and contributes to knowledge and familiarity across systems, processes and practices. Over recent years, there has been a significant investment in enhancing the 'speak up' culture. There is also a strong culture of employees focusing on 'getting things done'.

While these are organisational strengths, they also have the potential to expose the Bank to risk. We found:

- An insufficient approach to prioritisation, both for projects and IT work requests, which when combined with a lack of strategic resource planning in some areas and limited onboarding, leaves many people feeling overwhelmed by their workload
- Silos between IT and PS, and communication challenges, are perpetuated by unclear accountabilities and responsibilities, and dependence on tenure over documented process
- There is conflicting understanding about what 'speaking up' means, particularly in the context of risk management .

Risk management and governance

The RITS ecosystem is governed within the Bank's risk management and governance arrangements. Our review did not set out to undertake a governance review of the Bank, rather considered how those governance arrangements support the RITS risk environment. We acknowledge the broader governance review of the RBA underway at the time of this report.

The Bank has taken steps to uplift risk frameworks and arrangements over recent years. This has included enhancing the Risk Management Framework, embedding Line 1 risk teams in departments and introducing formal risk goals in performance management. However, further action is required to embed and to uplift the Bank's risk management practices:

- The Bank's risk management and operational risk frameworks have gaps and underlying policies and procedures lack sufficient and consistent detail
- The Bank's Three Lines of Accountability Model is not yet fully operationalised
- In some instances, the Bank's management committees do not operate as intended, impacting the effective oversight, and response to risk information.

1.4. Recommendations

We have made a series of recommendations to strengthen the RITS ecosystem. Our recommendations are summarised below.

Operating framework, processes, roles and responsibilities

- Develop, agree, and implement a formal documented operating model for the RITS ecosystem (covering internal providers, third parties, service levels, and service users)
- Review the technology policies and procedures supporting the RITS ecosystem and update to ensure consistency in the quality of documentation and alignment with the operating model
- Enhance the ability of the Investment Committee to prioritise the delivery of projects through formalising existing criteria and embedding into decision-making process.

People and culture

- Undertake a strategic resourcing review of the RITS ecosystem to assess the level of capability and allocation of resourcing, to ensure alignment with the agreed operating model
- Review the IT shared services approach to triaging and prioritising requests to determine effectiveness, and update where appropriate
- Build a program of work to expand the understanding of 'speaking up' within the RITS ecosystem, with leaders promoting effective challenge and the raising of issues and concerns on a day-to-day basis
- Formalise and embed the process for considering the impact on people from technology change management activities
- Create a consequence management framework and approach, communicate this and upskill leaders in how to use it effectively.

Risk management and governance

- Ensure the Chief Risk Officer has the right access to management forums, has appropriately defined accountabilities for operational risk management, and is sufficiently independent
- Perform an assessment and define the relevant standards that the Bank will align its Risk Management framework, policies, and procedures to, with reference to the objectives of RITS
- Establish a program to implement and embed the Three Lines of Accountability model
- Review and uplift RITS governance arrangements of the Bank's management committees to ensure appropriateness of remit and effectiveness of communication between committees to enable the accurate and transparent provision of RITS risk information
- Establish a program of work to deliver an uplift to the Bank's Risk Management Framework, policies and procedures and ensure that these changes are effectively embedded.

1.5. Acknowledgements

We would like to acknowledge the cooperation of the Governor, Deputy Governor, Senior Management and People of the RBA in undertaking our work.

2. Operating framework, processes, roles and responsibilities

2.1. Background and context

National infrastructure environments are complex and involve a number of teams working together effectively to deliver reliable and secure services. Within the RITS ecosystem, operational teams in PS are supported by IT via a PS aligned application support team, and IT shared services teams. The RITS ecosystem is also supported by other Bank-wide departments including Risk and Compliance and Workplace.

Effective delivery of national infrastructure requires operating models that incorporate a set of well-defined services that are offered based on service-levels agreed with the business departments and supported by standard technology processes. This is augmented by controls, and roles and responsibilities across the services being offered.

Our review identified findings across the operating model for the RITS ecosystem that impact the ability to reliably deliver critical infrastructure.

2.2. Operational Framework

A clearly defined operating model for the RITS ecosystem has not been embedded, impacting clarity of accountabilities, decision making, prioritisation and escalation of issues

Findings

The delivery of the RITS national infrastructure reliably to the Australian financial system is highly dependent on an effective operating model with clearly defined services, service levels, performance metrics and governance. This must be supported by documented operations and technology processes, detailed system documentation and augmented by controls, supporting systems and clearly defined roles and responsibilities.

Our review has found that whilst the Bank has done work to design and document systems and processes, considerable effort is required to transition from design to detailed implementation in order to effectively govern and control the RITS ecosystem. For example:

- The accountabilities, roles and responsibilities, services, processes and defined service catalogue with service levels for the Bank's RITS operating arrangements have not been comprehensively documented
- A Memorandum of Understanding (MoU) was agreed between PS and IT in 2013. This document does not sufficiently detail a clear operating model for the RITS ecosystem including the services to be provided to PS by IT under the IT shared services model and is not used in practice
- While the operational arrangements are understood in principle, a lack of clarity in relation to roles and responsibilities was consistently expressed in interviews with IT shared services employees. This is a contributing factor to workload pressures across the RITS ecosystem.

Why is this important

An operating model that clearly documents accountabilities, roles and responsibilities, and the services and service levels provided by teams is a key component of an operational framework for critical infrastructure. This is required to provide clarity between teams, supporting decision making, prioritisation and fast escalation and remediation of issues and incidents.

2.3. Technology Process Effectiveness

The processes operated by the IT shared services teams supporting RITS are inconsistently documented and applied

Findings

National infrastructure must be supported by common technology processes to ensure that systems can remain available, reliable and secure. These processes must be consistently documented and implemented across all national infrastructure components. Furthermore, processes should be adhered to and supported by effective tools, monitoring and governance to ensure effective management of operational risk. There are a number of gaps in relation to the Bank's technology processes that impact on their effectiveness. In particular, we have noted:

- The technology processes operated by the IT shared services team supporting the RITS ecosystem are not consistently documented. This impacts the quality of information to guide the effective operation of processes, delivery of training, and the consistent and effective onboarding of new staff
- The technology processes operated by the IT shared services team supporting the RITS ecosystem are not consistently embedded. Specifically:
  - The Bank's technology change management process relies on manual effort and has limited automated controls in place to prevent unauthorised changes. As such, there is an increased risk that unapproved changes can be deployed directly into the production environment. It was also noted through several interviews that impacted system owners are not consistently consulted prior to infrastructure changes
  - Infrastructure is not included in the Software Development Life Cycle (SDLC) Standard (2015) and no evidence was available of a consistent SDLC methodology specific to the infrastructure layer prior to the incident. Several disparate software development standards were provided and we observed that the Infrastructure team members lacked clarity on how and when to apply these standards. Adherence to a consistent SDLC and associated controls and processes can support with mitigating the risk of failed changes and incidents
  - The consistent application of IT Service Level Management across the IT Service landscape was not demonstrable. The Bank is currently developing framework documents, roadmaps and the service levels for Information Technology Infrastructure Library (ITIL) processes and key responsibilities to address this. We understand that there is an in-flight project that plans to optimise IT service management processes.
- Technology processes are not underpinned by an effective Configuration Management Database (CMDB). Various excel workbooks are used which are not consistently maintained and governed. As a result, it is not possible to accurately map the impact of changes to systems, applications, infrastructure, their respective owners, and the interrelationships between components. This impacts the ability to understand the impact of changes. We understand that there is a program in-flight that plans to deliver a CMDB; the implementation will need to include an appropriate CMDB operating model that is effectively embedded to enable sustainable process uplift
- Some of the technology processes require uplift to address key gaps. Specifically:
  - Disruption scenario testing is not sufficiently comprehensive to cover key potential scenarios. Testing is generally limited to assessing ability to cut over between production and disaster recovery sites
  - There is no formal process to monitor the resolution of identified problems (i.e. as part of Problem Management processes) outside of an annual review
  - The current technology delivery process does not include the assessment of quality of implementation and alignment to technology strategy and target architecture post implementation
  - The Architecture Review Board does not reconcile delivered architecture to the agreed target state. The responsibility to perform this is not included in the charter
  - There are currently no processes to feedback or assess whether the technology strategy is being developed, adhered to, and delivering the intended business outcomes.

Why is this important

Consistent execution of processes is essential to effectively manage operational risk in national infrastructure environments. Where processes are not adhered to there is a significant increase in the risk of incidents, potentially impacting the stability, reliability and

security of systems. Consistent documentation is a foundational requirement for process adherence. This must also be supported by effective tooling.

With technology processes, effective tooling, including a well maintained and governed CMDB is critical to enable effective process delivery. A CMDB enables teams to understand and manage the linkages between technology assets to ensure core technology processes (e.g. technology change management, incident management) can be executed safely.

2.4. Knowledge Management

The Bank does not have a standardised approach for knowledge management in place, resulting in incomplete and inconsistently applied process documentation

Findings

Knowledge management practices and a centralised knowledge management solution are critical components for the effective operation of critical infrastructure. Technical teams require easily accessible and searchable documentation to understand the configuration of systems, processes for maintaining systems, making changes or troubleshooting incidents and problems proactively. Knowledge management is also a key input for effective onboarding and training to ensure employees understand the why, what and how of the national infrastructure that they are supporting. We found that the Bank has a number of weaknesses in relation to its knowledge management practices:

- The Bank does not have in place a standardised approach for knowledge management. We observed various technology solutions utilised inconsistently resulting in an overreliance on experienced team members to provide knowledge and information. Specifically:
  - Inconsistent use of informal tools such as Confluence Wikis
  - Reliance on the Bank's document management solution, TRIM, as a knowledge management solution, despite its limited search, knowledge tagging and collaboration features
  - Insufficient technical training and handover processes for new staff
- There are gaps in the technical documentation to support the RITS ecosystem. For example:
  - Architectural documentation to detail the segregation of the RITS's operational infrastructure and the Bank's wider enterprise systems is not in place
  - While incident reports document recovery steps from prior incidents, there is no easily accessible knowledge management repository to retrieve the specific steps that were used to recover from these.

Why is this important

Processes and system documentation needs to be easily accessible and searchable to enable consistent processes, and allow effective response to incidents, problems and events in the ecosystem. These are key components to enable effective management of operational risks in the RITS ecosystem.

Effective disruption scenario planning and testing is essential to ensure teams are sufficiently prepared for, and can respond to incidents. This will enable reduced recovery times and lower the impact of outages.

2.5. Technology Control environment

The technology control environment is largely manual and detective in nature, with insufficient control testing and limited tooling to support automated process execution

Findings

Technology processes require effective controls to be embedded to ensure process objectives are met and operational risks are mitigated. Automated controls enable a more proactive and robust control environment. While manual controls will always be required, they can be complex and time consuming. The current industry focus is towards an efficient set of controls, aligned to process and risk objectives, which are automated where possible.

A standard technology control framework supports consistent application of policies, alignment with standards and effective management of risk. Testing these controls on a regular basis is critical to understand the risk profile, the exposure to threats and vulnerabilities and to effectively plan remediation. We found that the technology control environment supporting the RITS ecosystem requires significant uplift:

- The Bank's IT control library contains approximately 170 controls. One library control is recorded as automated, 76% are recorded as manual and the remainder are recorded as semi-automated. Industry standard IT Key Control frameworks contain a rationalised control set with a more balanced blend of automated and manual controls adapted to the risk profile of the organisation. Overall, we observed that:
  - Controls are not consistently documented with a number of key attributes of a technology control library missing. For example, control owner and frequency of operation
  - The Bank is heavily reliant on manual IT controls to govern key technology processes supporting the RITS ecosystem. This includes technology change management, where we observed limited use of automated controls to manage changes being deployed into production
  - Tooling to support automation of controls is also limited. We understand that some tools have been deployed as part of the Bank's Technology Simplification project to manage aspects of automation for configuration management and Virtual Machine building. However, there is no comprehensive automation of technology processes.
- Control effectiveness ratings are provided by staff attestation and are not supported by control testing
- There is limited controls testing in place for either PS or IT, and a reliance on internal audits to assess control effectiveness, which does not provide regular or effective assessment for the RITS ecosystem. Consequently, the Bank has a limited view of where control gaps and issues may occur, how policies have been implemented and the effectiveness of controls in key applications.

Why is this important

An effective technology control environment will enable the Bank to reduce the frequency and severity of incidents and lower the operational risk profile of the RITS ecosytem. Control testing will enable issues to be identified in a timely manner, and highlight where effort, resources and funding are required to mitigate risk, before incidents occur.

3. People and culture

3.1. Background and context

All organisations exist as a collection of the skills, knowledge and experience of its people working together to achieve common objectives, supported by their structures, systems and processes. The way people come together is driven by the values, attitudes, beliefs and norms that influence behaviours, defining its culture.

Our review identified common people and culture-related themes, which co-exist across teams and departments within the RITS ecosystem. These themes influence how people interact and perform their roles, ultimately impacting the Bank's operational risk profile.

3.2. Culture and Collaboration

The Bank's culture of risk awareness requires additional support to encourage people to 'speak up' and, improve inter-departmental collaboration, underpinned by stronger performance and consequence management

Findings

To support the operation and reliability of national infrastructure, it is essential that the Bank has a strong risk culture reinforcing the behaviour and decision-making of its people. A strong risk culture needs to be supported by a number of elements including leadership, risk awareness, safety to 'speak up' or challenge others, effective collaboration, and aligned performance and consequence management.

In respect of the RITS ecosystem, we have noted a number of gaps in relation to these key cultural elements that have a strong interdependency upon one another:

A. Risk Awareness and Leadership

Risk awareness refers to the extent to which people are aware of the importance of managing the risks associated with their role and keeping the Bank safe. Within the Bank, the heightened sense of duty and risk awareness towards critical systems and infrastructure is known as the 'culture of care'. Our review noted that:

- People working across the RITS ecosystem have a strong culture of purpose, risk awareness and culture of care consistent with its responsibilities of ensuring the resilience of Australia's financial system. This mindset was demonstrated most strongly amongst those in PS and longer-serving employees (i.e. those commencing prior to 2015)
- Some employees perceive leadership on risk to be insufficient, specifically as it relates to technical knowledge, consultation on decision-making, coaching, and in some instances performance and consequence management.

B. Safety to 'Speak Up'

'Speak up' culture refers to a collective belief among people that they can confidently 'speak up', share ideas, ask questions, take risks or challenge decisions without fear of being judged, ridiculed, or punished. Our review found that the Bank has invested in dedicated 'speak up' programs over recent years. We have observed the following in relation to 'speaking up':

- Across the Bank, there is conflicting understanding about what 'speaking up' means. This may be due to formal initiatives on 'speaking up' in recent years[2] which have focused primarily on fraud and other wrongdoings and professional workplace conduct, with less focus on challenging decisions or raising issues on operational risks
- While the majority of survey respondents agreed they feel safe to 'speak up', those who were longer-tenured employees (i.e. those employed before 2015) and those *substantially* involved in RITS (but RITS was not their *entire role*) reported weaker confidence in 'speaking up'
- People expressed some concerns about challenging the key decisions of senior leaders or other teams. A range of factors impact on their ability to 'speak up', including: believing that managers sometimes do not take action when concerns are

[2] Since 2018 there have been several 'speak up' initiatives at the Bank, including the creation of a speak-up network, speak-up awareness sessions and a speak-up intranet site.

raised; believing leaders sometimes override decisions; having a fear of potential adverse consequences; and employees not wanting to create additional workload for themselves and team members.

C. Collaboration

A strong risk culture requires people to be able to productively collaborate with others across teams and departments. While collaboration between the PS and IT departments is crucial to support the operating model adopted by the Bank, we found that it is not optimised to support the Bank's critical infrastructure. There are several elements that hinder collaboration between these critical functions:

- The Change Advisory Board includes representatives from both PS and IT and has a documented schedule of IT-related changes and impacts. However, there is no evidence of regular communication of these changes outside of this forum. There is a perception, particularly amongst more junior people who are impacted, that changes relate to shared systems and infrastructure are not consistently communicated in advance
- There is an over-reliance on the empirical knowledge of long-tenured employees to direct processes and decision-making in respect of critical IT systems and infrastructure, rather than job role or responsibility
- There is a lack of formal documentation setting out clear responsibilities and accountabilities, processes for engagement and agreed service levels between IT and PS
- There is a reported lack of trust between the PS department and the IT shared services team in relation to matters impacting the RITS system and associated infrastructure.

D. Performance and Consequence Management

Performance and consequence management are essential components of an organisation's accountability framework. By implementing an effective performance and consequence management system, organisations can establish a culture of accountability where employees understand their roles and responsibilities and are held responsible for their actions. The Bank's risk culture is not adequately promoted through robust performance and consequence management settings. The specific areas requiring further attention are set out below:

- While the Bank has a performance management framework, it requires additional, explicit embedment of risk considerations. A risk goal was rolled out across the business in mid-2022, but is yet to be reflected in the Performance Management Guideline for managers or fully embedded across the business, with many saying it is not discussed in their performance appraisals and they do not regularly receive feedback on their ability to manage risk
- The Bank has an inconsistent approach to consequence management, with few formal frameworks or procedures in place to guide the management of issues regarding poor performance or behaviour[3].

Why this Is important

A strong sense of purpose and risk awareness is a crucial area of strength and a foundational element of a strong risk culture, but alone is insufficient to safeguard national infrastructure. It needs to be supported by effective leadership, with strong supporting frameworks and processes. Included in this is the effective design and embedment of accountabilities and responsibilities. By having clarity on roles and purpose, teams can work in harmony and collaborate to align objectives and outputs, optimise resource management to priorities, and manage risks.

People also need to feel safe to 'speak up', by contributing their ideas or challenging the ideas of others. By supporting team members to feel empowered, collaborate and contribute, they are able to enhance the flow of information that influences decision-making and alert the business to identified risks.

Finally, a strong risk and 'speak up' culture needs to be supported by effective performance and consequence management. A risk goal helps people understand the importance of risk to the business and to their success. While an effective consequence management framework provides the guardrails to ensure people are held to account for their actions when they have fallen short of expectations. Inconsistent performance and consequence management may contribute to a perception that positive risk behaviours are not appropriately valued, or a fear amongst employees of how they might be treated if they make a mistake, preventing 'speaking up'.

[3] While the Performance Management Guideline has reference to an underperformance process, this is relatively high level with little detail on how poor behaviour is managed.

3.3. Impact of Resourcing and Prioritisation on Operational Risk

There is elevated operational risk from employees across the RITS ecosystem feeling overwhelmed by their workload due to insufficient prioritisation practices, a lack of strategic resource planning, and insufficient people change management and onboarding processes

Findings

Effective resourcing enables an organisation to achieve its strategic objectives. By having the right resources with the right capability and training, an organisation can perform its operations successfully, improve productivity, and minimise unnecessary costs. Effective resourcing can help an organisation to attract and retain the best talent, and respond to changing market conditions and demands. In respect of the RITS ecosystem, we observed a range of factors which influence the operational risk environment associated with its people:

A. Workload and employee retention

When working with critical infrastructure, it is essential that people have the appropriate workload to optimise performance, manage quality delivery and ensure stability of systems. People that experience consistently high workloads are more prone to error and can risk feeling 'burnt out', resulting in productivity loss and potentially causing high levels of turnover. To understand the workload pressures at the Bank it is important to note that:

- A majority of employees surveyed, that work on RITS, feel overwhelmed by their workload, and do not feel they have enough people in the right roles to help them operate technical systems effectively. Across the RITS ecosystem, some people report burnout and fatigue due to overwork, which is resulting in people bypassing policies and creating workarounds to get the job done, increasing the risks of operational failures.
- A maximum headcount was instituted between FY18 to FY21, which influenced workload pressure to meet increasing demands, particularly within the IT department. While the headcount cap was regularly mentioned by employees as a key contributing factor to why the workforce felt overwhelmed; other factors are also likely to have contributed to perceived staff shortages during the period in the lead-up to the RITS outage, including:
  - A significant pipeline of project initiatives and systems enhancements requiring experienced people to deliver projects successfully, often resulting in temporary roles being used to backfill business-as-usual roles while more experienced people served to deliver projects
  - The loss of key experienced employees in critical roles, compounded by historical restrictions on renewing temporary staff contracts
  - High workload demands and frequent movement of people around the department, across functional teams and between project and operational tasks in response to urgent needs
  - High job vacancy rates and slow recruitment processes
  - An influx of new employees in FY22, combined with higher exit rates amongst short-tenured staff (0-5 years).

B. Prioritisation and decision making

Prioritisation is a key element of leadership and a critical component of achieving an organisation's objectives. Prioritisation is an essential consideration for decision-making in relation to projects, initiatives and tasks. Effective prioritisation needs attention in order to manage operational and people risk. In particular, we noted that:

- The Bank's Investment Committee makes decisions without a formally endorsed prioritisation framework or a holistic view of available resources, often relying on business cases that lack sufficient data to understand the impact of the investment upon the business. While an informal prioritisation framework exists, it is not embedded, rigorously applied or fully understood by all Committee members
- The IT shared services team have no formally endorsed framework for assessing the prioritisation of IT-related operational tasks, and the approach taken is unclear and applied inconsistently in practice. This puts daily workload pressure on IT shared services employees to manage conflicting demands from management and business stakeholders, with reports that people are pressured to perform tasks based on which stakeholder is most demanding, rather than which task is most critical
- There is a perception that people are recognised for 'getting things done', which in practice means that the completion of tasks is often recognised by leaders over the reliable delivery of business-as-usual activities or for adopting positive risk processes and behaviours.

C. Strategic resource planning

Strategic resource planning enables the business to plan its resources around the strategic priorities of the business.

We found that some areas of the Bank lacks sufficient strategic resource planning, with some people referencing a lack of tools and capability to plan the resourcing and capability needs of their departments and teams to delivers on their objectives.

In relation to a lack of strategic resource planning we noted that:

- Spans of management: Some junior managers within the IT Infrastructure and Operations team have been leading very large teams (+25 people). People reported as a result managers are failing to consistently invest in onboarding, training or mentoring to new or junior staff, engage in effective performance management processes, or appropriately deal with risks and issues raised by team members
- Shuffling people to meet demands: There is a general lack of strategic resource planning, particularly in IT, which when combined with poor prioritisation, means that some IT shared services team members reported they are allocated to projects or business-as-usual tasks based on urgency of need, rather than on their capability or experience. While there are certification standards for people who work on critical systems, the sub-optimised allocation of shared resources can increase operational risk by: requiring staff to perform unfamiliar roles, support unfamiliar systems and processes, or leaving teams short staffed.

D. People change management

Effectively supporting people through change is crucial to supporting BAU teams to successfully embed new systems, processes and developments into their operations. It is important that impacted teams are aware of upcoming change activity, understand what capability will be necessary to support the ongoing operation of the activity, and can plan their workload and resourcing to absorb the change.

There is a perception, particularly amongst more junior people who are impacted, that changes relating to shared systems and infrastructure are not communicated in advance. This limits the ability of managers to allocate resources and manage the impacts of change on their people, and may result in employees having to absorb unexpected changes while already under considerable workload pressure. We heard from some employees that there is:

- A perceived lack of notice or consultation for some about how upcoming or delivered changes to systems or processes will affect their day-to-day work. A driving factor of this was reported to be a lack of understanding of end-to-end processes and the interconnectivity of systems to assess the impact of changes.
- A perceived lack of consideration when technology changes are rolled out of how it will impact upon people's workload, how it will affect resourcing or whether the change will require new capabilities to be successfully delivered across the RITS ecosystem. This is made more difficult by a lack of inter-departmental collaboration.

At the time of the incident, there was no people change management framework to support the embedment and adoption of change from projects into the business-as-usual environment. This framework has since been introduced but remains an inconsistent practice.

E. Onboarding and capability

Onboarding is an important step for new employees to become acclimated to their role responsibilities and performance expectations; understand the organisation's objectives, culture and values; and build relationships with co-workers and managers.

With increasing technology demands, the Bank has onboarded a large number of people into its IT Department in recent years and has had to uplift capability to develop their workforce to meet the business needs. Through our review work, we found that:

- While the Bank has a group-wide onboarding program, it is high-level and not sufficient in preparing new starters for their roles without significant support and development
- A structured certification regime within the IT Department is constructive, but insufficient alone to prepare new employees to work on national infrastructure without the depth of knowledge or confidence to perform their role effectively
- Some people within IT shared services are often allocated to tasks on other systems, which may not be appropriate for their capability or experience to meet immediate resourcing needs
- The professional development of managers is ad hoc and does not consistently support people stepping into management roles. Instead, it was reported there is a reliance on on-the-job experience and an assumption of leadership capability over a formalised program of training and development of managers.

Why this is important

Effective prioritisation combined with strategic workload management is critical for the RITS ecosystem (and the broader Bank) to manage the people and capabilities to meet its goals and objectives, and to identify potential resourcing constraints or inefficiencies.

High workloads within the RITS ecosystem increase the likelihood of incidents via human errors and can influence staff to bypass processes to meet business deliverables. This also impacts the ability to effectively onboard and develop team members, impacting capability and reducing productivity. High workload can also be a factor affecting employee retention, resulting in loss of critical knowledge and experience.

With the recent expansion of the Bank's IT workforce, efficient and effective onboarding is essential to support critical capability while minimising business disruption and reducing operational risk. Onboarding processes need to cover both the technical and non-technical components of the role, including to develop foundational knowledge of core processes supporting the role deliverables and an understanding of the Bank's "ways of working" to meet business requirements and expectations.

The RITS ecosystem exists in a resource constrained environment. Effective utilisation of resources in this environment, requires prioritisation at both the project and BAU level to ensure that resources are effectively utilised to deliver national infrastructure reliably and safely. Effective utilisation is reliant on consistent and effective onboarding of new employees into the RITS environment, to ensure that they understand the why, what and how of managing national infrastructure and build effective capability to manage operational risk.

4. Risk management and governance

4.1. Background and context

Effective risk management and governance are foundational capabilities for managing critical infrastructure. Resilience is achieved through the implementation of focused risk management activities.

The Bank has a strong culture of risk awareness and has taken steps to uplift risk frameworks and arrangements over recent years. However, further action is required to effectively implement, embed and uplift the Bank's risk management practices.

In undertaking our work, we have considered various risk management standards relevant to other Australian financial services entities, systemically important banks and entities providing national infrastructure with careful consideration of the nature of the Bank's role and accountabilities to the Australian financial system[4].

4.2. Accountability for the design and implementation of effective systems of risk

There is no single executive with distinct responsibility for the risk management function and accountability for non-financial risks.

Findings

The Bank's Executive Accountability Framework sets out 10 specific accountability categories in relation to Risk Management, Compliance and Operational Resilience which are assigned to Executives at a Bank-wide level as well as within various functional areas. We observed:

- The Deputy Governor is accountable for risk management, and is also accountable for Audit, Finance, Human Resources and IT
- The Bank recently appointed a Chief Risk Officer (CRO) who is responsible for management of the Risk and Compliance Department (RM), and is accountable for certain aspects of the Bank's risk management. For example, privacy, fraud controls, conflicts of interest, sanctions and business continuity. However, this role does not have sufficient access to the Bank's Executive Committee, Investment Committee or Technology Committee to effectively challenge Management and enable informed decision making
- The Deputy Governor and CRO accountabilities relating to risk management do not include accountability for critical non-financial risks, including operational resilience.

Why this is important

While further design and build activity is required for the Bank to address gaps in risk framework and policies, effective implementation and embedment of those frameworks will require significant focus, oversight, investment, and executive accountability to be successful.

An effective CRO provides an integrated view of risk, embeds an evolving risk management program and considers the full spectrums of risk relevant to the Bank, including in relation to the management of non-financial risks.

The Bank's CRO should be distinct from other executive functions and business line responsibilities, and there generally should be no 'dual hatting' to enable effective challenge, focus and mitigation of potential conflicts of interest.

4.3. Risk frameworks, policies and procedures

The Bank's Risk Management Frameworks and Policies have significant gaps or lack sufficient detail at the procedure level to be effectively embedded

Findings

Uplift in risk management frameworks, policies and risk practices across Australian financial institutions has been driven by a shift in focus from reacting to issues and incidents, to proactively identifying, measuring and managing risks. Better practice risk

[4] These standards include APRA's prudential standards CPS220 Risk Management, CPS510 Governance, CPS230 Operational Risk Management, Bank for International Settlements (BIS) Corporate Governance Principles For Banks, BIS Principles For Operational Resilience and Principles for Financial Market Infrastructure (PFMI).

management policies and procedures include frameworks for issue identification, escalation and resolution, originating from employees, whistle-blowers, ecosystem participants and regulators.

The Bank's frameworks and risk practices are not sufficiently effective in supporting risk management for the RITS ecosystem. Specifically:

- The Bank does not sufficiently detailed risk policies and procedures for material operational risk subcategories defined within the risk appetite, including operational resilience, cyber risk and third-party risk management
- The Bank's risk management policies and procedures lack sufficient detail to be effectively embedded. For example, the risk and compliance management framework and risk management policy do not include incidents, issues, and action management policies covering key definitions of an incident and issue, requirements for analysis and managing incidents and issues, and communication and escalation to governance forums
- The updates to documented risks and controls for PS and IT (including RITS related controls) are generally undertaken only once a year as part of the annual Risk and control self-assessment process. We also observed different approaches in IT and PS to determine control effectiveness ratings used as an input to the residual risk ratings. Further there is no independent review and challenge of PS and IT controls by Line 2 to assess if the controls are operating as intended
- There is an inconsistent practice for ownership of risk policies with some risk policies owned by Line 1, while others by Line 2.

Why this is important

The Bank's RITS ecosystem requires its defined critical operations to operate within defined outage tolerance levels through disruption. Relevant operational resilience frameworks, policies and risk practices must extend to consider the activities, processes, services and their relevant supporting assets where disruption would be material to the continued operation of the Bank or its role in the financial system.

4.4. Three lines of accountability

The Bank has not implemented and embedded an effective Three Lines of Accountability model. This has contributed to unclear accountabilities and responsibilities for managing risk, a lack of effective challenge from the Risk Management department, and a lack of management control testing

Findings

The three lines of accountability (3LoA) framework is a standard industry approach to providing clarity of accountability and responsibility for the ownership and management of risk and performing risk management activities. The Bank has designed an appropriate 3LoA model that is in its early stages of adoption and is not yet implemented or embedded.

Through our review we observed:

- Detailed accountabilities and responsibilities of Line 1 (including Line 1 risk teams) and Line 2 across key risk activities have not been sufficiently defined. For example, detailed roles and responsibilities relating to risk identification, risk assessment, controls (including control design, testing and self-assessments), risk policies and procedures, issue and incident management, risk monitoring (including key risk indicators) and risk reporting
- Line 1 risk teams within PS and IT are not well integrated within a broader risk management program
- There is limited demonstrable evidence of effective Line 2 review and challenge, independent assessment and escalation of risk, including at key management committees
- Those responsible for understanding and escalating risks within the Bank are not consistently heard, particularly as it relates to non-financial risks
- There is no formal approach to Line 1 and Line 2 controls testing.

Why this is important

It is important in a critical Financial Market Infrastructure environment to have a robust 3LoA, especially line 2 that has strong technical capability to challenge operational resilience and stability of IT systems supporting RITS. When 3LoA is effectively implemented:

- Management have responsibility to own and manage risks associated with the Bank's day-to-day operations and the design, operation and implementation of controls

- The second line will enable the identification of emerging risks and provide compliance and oversight in the form of frameworks, policies, tools to support risk and compliance management
- The third line will provide objective and independent assurance reporting to the Board Audit Committee in addition to providing assurance to regulators and external auditors that the control culture across the Bank is effective in its design and operation.

4.5. Governance arrangements that impact RITS

Risk information presented to Management lacks sufficient action

Findings

Our review considered the governance arrangements of the Bank (excluding the Board and its subcommittees) as they relate to RITS. This includes four management committees; the Risk Management Committee (RMC), Executive Management Committee, Investment Committee and the Technology Committee.

While the scope of our review was focused only on RITS governance (not broader bank governance and control environment), it is worth noting that several of our findings and recommendations may apply more broadly to the Bank as the management committees are shared across RITS and Bank functions.

We observed several opportunities to improve the risk oversight of these committees that will benefit the RITS ecosystem. For example, the inclusion of explicit delegations from the RMC to other committees for oversight of specific risks, defined escalation and risk reporting from other committees to the RMC, and clearly defining the role of the Committee Chair within Committee Charters in promoting the voice of risk.

The Bank did identify operational risk as being an issue and outside of its risk appetite in late 2018. While there is evidence that the Bank was assessing the increase in incidents impacting RITS and related systems, including taking steps to understand the related root causes, there is limited evidence to demonstrate sufficient action was taken in response.

- The Bank has identified a number of risk indicators that are monitored and reported regularly to its various risk committees and operational working groups in relation to risks specific to departments, processes and the RITS ecosystem. We observed the provision of relevant risk information that is understood by management. However, there is an opportunity to review, rationalise and define a cohesive and aggregated view of risks specific to the RITS ecosystem in terms of risk matters, risk decisions, risk information and related risk reporting to the four governance committees
- Risk information including risk indicators were reported outside of residual risk targets in multiple months without corresponding time bound actions to remediate risks. These actions were not comprehensively remediated prior to the incident. For example, enterprise risks related to workforce resourcing, technology resilience, cyber risk and access management reported outside of their residual risk target between July 2021 and December 2022 and prior to the incident
- The Bank does not have in place risk reporting specific to the RITS ecosystem that is provided to the Risk Management Committee, Technology Committee or Technology Risk Committee
- We observed that some of the contributing factors of the incident were known to the Bank based on deficiencies identified in prior incident reviews but were not effectively overseen to ensure that these were effectively mitigated. For example, the Bank identified root causes within its 2019 Operational Stability Review related to technology service incidents over a three-year period. The 2019 review highlighted 62% of errors arose due to incorrect configuration parameters being applied to systems that were in production, and resourcing in the Infrastructure Services team where most errors have originated had not aligned with the increase in numbers and types of systems those teams support
- As a practice, certain risk decisions are deferred or escalated to the Executive Committee by the Risk Management Committee. However, committee charters do not define what, when, or how risk matters are deferred, escalated or how actions related to those escalations are reported back to the Risk Management Committee. There is no clearly defined process to communicate risk information between the Investment Committee and the Risk Management Committee. This includes delivery and delivered risks at a Bank-wide or portfolio level and related impacts on bank level investment prioritisation processes.

Why this is important

Risk management metrics including the Bank's key risk indicators should focus on the risk profile of the Bank, including risks specific to the operation of the RITS ecosystem. Care must be taken to ensure the accuracy and transparency of aggregated risk information provided to management including the Bank's Risk Management Committee.

Effective risk governance can be achieved at both the enterprise and ecosystem level provided that those arrangements are underpinned by the reliability of the Bank's management committees including appropriate risk metrics, oversight and action management relating to the risk.

INDEPENDENT REVIEW OF THE OCTOBER 2022 RITS OUTAGE

Recommendations

5. Recommendations

We have made a series of recommendations to strengthen the RITS ecosystem. Our detailed recommendations are provided in the tables below, they have been grouped into themes for ease of delivery.

Thematic Area 1: Formalise the RITS Operating Model

No.	Title	Description
1.1	RITS Operating Model	• Develop, agree, and implement a formally documented operating model for the RITS ecosystem, covering internal providers, third parties and service users aligned with both business and technology objectives. This should include but not be limited to: – The services provided by IT documented through a detailed service catalogue that defines capabilities, processes, roles and responsibilities and key performance metrics – Defined service levels with an associated service level agreement and governance mechanisms in place to monitor adherence e.g., reporting and governance forums.
1.2	Prioritisation	• Enhance the ability of the Investment Committee to deliver projects into the RITS ecosystem by: – Reviewing the existing criteria for Investment Committee prioritisation, considering alignment to the objectives for RITS, and embedding into the decision-making process – Building the capability of the Investment Committee to apply the prioritisation criteria to both new projects and the existing project pipeline – Revising the business case framework, ensuring quality and consistency in the business case and resource considerations (both for projects and eventual business-as-usual) • Review current and scheduled projects considering the prioritisation framework and determine which projects can continue, be put on hold, slowed down or cancelled • Review the IT shared services approach to triaging and prioritising requests to determine effectiveness, and update where appropriate.
1.3	Technology documentation	• Review and uplift the technology policies and procedures supporting the RITS ecosystem. This should include a consistent quality of documentation and alignment with the operating model • Ensure architectural documentation of the RITS ecosystem remains current and consistent with changes implemented • Uplift operational resilience documentation through identifying severe but plausible disruption scenarios that may impact the RITS ecosystem. These should be captured in documented playbooks that are assessed and tested through an enhanced operational resilience program (see recommendation 5.4). • Incorporate all updated policies and procedures in a knowledge management platform, communicate changes and expected use (refer recommendation 2.3).

Thematic Area 2: Uplift Technology Processes across the RITS ecosystem

No.	Title	Description
2.1	RITS IT Process Effectiveness	• Uplift SDLC policies and processes to incorporate a standard approach across all domains, including infrastructure • Assess whether the current in-flight program of work will deliver an automated Configuration Management Database (CMDB) solution which streamlines technology processes and consolidates management of assets. The implementation of a CMDB should include an agreed operating model to support the solution including: – Documented processes for ongoing updating and maintenance of the database – Clear accountabilities, roles and responsibilities for ongoing updates – Key operational and performance metrics covering completeness and accuracy, and related reporting • Continue to enhance the RITS ecosystem control environment through implementing monitoring controls and metrics that assess ongoing adherence to technology processes e.g., technology change management and incident management • Embed a process to assess process and control candidates for automation into all change activities. This should focus on identifying opportunities for automation to enhance process adherence. We understand that the current Technology Simplification program is intended to achieve some of these outcomes.

No.	Title	Description
2.2	RITS Technology Controls	• Design and implement a Controls Assurance Program for the RITS ecosystem. This should include consideration of controls in scope, the testing approach, frequency, reporting and appropriate resourcing to execute the program. • Refresh the IT Key Control framework based on industry standards. Assess technology processes against this to identify control gaps and where controls can be consolidated or removed. Map technology controls to the Risk Taxonomy and implement the control framework through: – Mapping and documenting controls against processes – Agreeing control owners with defined roles – Uplifting controls to meet the framework • Embed control KPI's into RITS senior management scorecards that incorporate a blend of control metrics across effectiveness and efficiency, including control effectiveness. Implementation should be prioritised for technology controls impacting the RITS ecosystem.
2.3	RITS IT Knowledge Management and Onboarding	• Establish a formal knowledge management capability including a consistent knowledge management solution. Communicate use of the capability and identify champions across the RITS ecosystem to promote implementation and embedding. • Assign accountabilities, roles and responsibilities for maintaining the knowledge repository for the RITS ecosystem. Introduce Key Performance Indicators / incentives to drive adoption and promote knowledge sharing. • Develop a formal onboarding program for IT teams supporting the RITS ecosystem. This should include consistent training which draws on the updated suite of policies and processes (see recommendation 1.3) and the knowledge repository. This should also include formal mechanisms to enable long tenured employees across the RITS Ecosystem to impart knowledge to newer employees, for example, structured mentoring or coaching.

Thematic Area 3: Review RITS ecosystem Resourcing

No.	Title	Description
3.1	RITS Strategic Resourcing	• Undertake a strategic resourcing review of the RITS ecosystem to assess the level of capability and allocation of resourcing across IT and PS, aligned with the right team and fit for purpose to meet the agreed operating model. – Prepare a strategic resourcing plan aligned to the Bank's business plan – Consider increased use of, contractors, or external parties in the short term to relieve the burden on existing team members, while the planning and prioritisation work is undertaken – Consider revising the use of appropriately skilled contractors or external parties in the medium term in alignment with the strategic resourcing plan.
3.2	People Change Management	• Formalise and embed the process for consideration of people impacts from change management activities, review its effectiveness and update the approach within a defined period (for example, 12 months).

Thematic Area 4: Uplift the RITS Culture

No.	Title	Description
4.1	'Speaking Up'	• Build and execute a program of work to expands the understanding of 'speaking up'. This should enable effective challenge and the raising of concerns and ideas in day-to-day roles.
4.2	Leadership and Capability	• Develop and implement a strategic employee listening program, collecting data on employee experiences and perceptions, and report to the executive and leadership at regular intervals. This would involve conducting regular surveys and deep dives of employees, combined with looking at key employee data (e.g. turnover rates, absenteeism rates, whistleblowing thematics, underperformance management etc.) to gain a fuller view of the experiences of RITS people.
4.3	People and Culture	• Create a Bank-wide consequence management framework and approach, communicate this and upskill leaders in how to use it effectively.

Thematic Area 5: Uplift Risk Management and Risk Capabilities across the RITS ecosystem

No.	Title	Description
5.1	Risk Accountability	• Ensure the Executive accountable for risk is sufficiently independent and does not wear other 'hats' that may present a real or perceived conflict of interest. Update Executive Accountability Framework to reflect these changes. • Ensure the Chief Risk Officer has access to Management Committee forums. Update committee charters to reflect these membership changes • Update the Bank's Executive Accountability Framework to include Chief Risk Officer accountabilities for non-financial risks such as operational resilience (operational risk, business continuity and service provider/ third party risk) and cyber risk. These accountabilities should include: – Setting the bank-wide approach for these risks, including defining the risk frameworks, policies and processes – Providing oversight (through review and challenge processes), advice and insight.
5.2	Three Lines of Accountability	• Establish a program to implement and embed the Bank's 3LoA model including, but not limited to: – Defining and documenting the accountabilities and responsibilities of Line 1, (including Line 1 Risk teams) and Line 2 across all existing and planned risk processes and activities. For example, risk identification, risk assessment, etc. – Assess the capability and capacity of risk teams (across Line 1 and Line 2) to meet the updated responsibilities, and ensure the RITS ecosystem has adequate resources to manage, mitigate and monitor material risks – Communicate, implement, and embed the 3LoA model and associated accountabilities and responsibilities across Line 1 and Line 2 – Support this program of work with specific risk training on effective challenge and risk leadership. Implementation activities within the RITS ecosystem should be prioritised, whilst taking into account the other critical roles that the Bank plays.
5.3	Risk Management Standards	• Define the relevant standards that the Bank will align its Risk Management framework, policies, and procedures to with specific consideration of: – Risk Management: APRA CPS 220 Risk Management – Operational resilience: 'BIS Principles for Operational Resilience, 2021', 'APRA CPS230 – Operational Risk Management' – Information Security: APRA CPS 234.
5.4	Risk Management	• Continue uplift activities to the design of the Banks Risk Management Framework, policies and procedures and take steps to ensure that changes are effectively embedded including, but not limited to: *Design Activities* – Update the Risk Management Policy or Risk and Compliance Management Framework to incorporate a policy section on Incident Management, Issue and Action management including defining an Incident, and issue. This policy/ framework should govern all existing incident, issue and action management policies, standards, guidelines and procedures to ensure a consistent and cohesive enterprise approach. – A defined approach and process to govern and manage risks across the RITS ecosystem in line with the Risk and Compliance Management Framework. This will include a single, combined end to end risk register of all risks and controls, combined risk indicators and risk profile leading to combined risk monitoring and reporting across the RITS ecosystem (i.e., across internal departments, third party service providers and participants/ service users). – A defined approach to assess, monitor, and report delivery and delivered risk across projects at a portfolio and Bank level and align Bank level prioritisation processes. This should also include an uplift to project risk reporting. *Implementation and Embedment* – An accountable Owner in Line 2 Risk to drive consistent implementation and embedment of Incident Management, Issues and Action Management at an enterprise level – An accountable owner in Line 2 risk to drive implementation and embedment of the approach and process to govern and manage risks across the RITS ecosystem at an enterprise level *Resourcing and Change Management* – A capacity assessment of the Line 2 Risk and Line 1 risk teams to perform the relevant risk management roles and embed this framework, including review and challenge – Change management activities including communication, education and training for risk owners and risk managers aligned to the new policies and procedures.

No.	Title	Description
		Implementation activities within the RITS ecosystem should be prioritised, whilst taking into account the other critical roles that the Bank plays.
5.5	Operational Resilience	• Perform a detailed gap assessment of the Bank's existing operational resilience arrangements against the Bank's defined relevant standards (determined in recommendation 5.3) • Develop a detailed execution plan to address identified gaps across business continuity management, service provider management and operational risk management • Undertake a program of work to deliver on the execution plan. Based on our review of current enterprise level guidelines, frameworks and policies, we anticipate this will include, but not be limited to: • Processes to identify, assess, treat and monitor operational risk where any business decisions are made, or issues and incidents arise that might impact the resilience of critical operations across the end to end value chain i.e., across internal RBA departments, third party service providers and participants/ service users • The comprehensive consideration of critical operations through operational risk profiles • Processes to monitor the age and health of IT infrastructure supporting critical operations and risk management • Guidance, methodologies, standardised tools and templates for consistent BCM implementation across departments • Detailed roles and responsibilities of Line 1 and Line 2 across all BCM sub-activities including business impact assessments, business continuity planning, business continuity monitoring, business resumption testing and BCP training • A clearly defined methodology and approach to identifying and managing material service providers (incl. fourth parties) and their associated risks • Development of a Cyber Risk Management Framework, to be defined and owned by RM, in line with their 2nd line role of setting and defining the enterprise approach to Risk, including risk frameworks, policies and processes. Implementation activities within the RITS ecosystem should be prioritised, whilst taking into account the other critical roles that the Bank plays.
5.6	Risk Governance	• Review and update governance arrangements of the Bank's management committees to enable accurate and transparent provision of RITS risk information between the Bank's committees, including but not be limited to: – Define a process between the four governance committees (RMC, Executive Committee, Technology Committee and Investment Committee) which defines who, what, when, and how risk matters, risk decisions, risk information and related risk reporting will be escalated, deferred reported, and acted upon – Define a risk reporting process from the Executive Committee, Investment Committee and Technology Committee to the Risk Management Committee, and feedback loop to the relevant committee – Revise the scope of the Technology Committee to include oversight of Bank-wide technology related risks including a defined reporting and escalation process to the Risk Management Committee • Update the Charter of the Bank's committees to clearly define the role of the Committee Chair in promoting the voice of risk as an effective counterbalance to the business to achieve an optimised state of governance.

REVIEW OF THE OCTOBER 2022 RITS OUTAGE

Appendices

6. Appendices

6.1. Appendix 1 – Stakeholders

Interviews

In undertaking our work, we conducted interviews with a number of stakeholders relevant to the RITS environment, in order to assess the non-technical factors which either contributed to the incident or present ongoing operational risks for RITS as a wholesale Real-Time Gross Settlement (RTGS) system.

Our interviews included interviews with executives and employees. Our employee interviews included the Heads of various Bank departments and general Team Members, Team Leads, Managers, Senior Managers (Levels 3-6). The External Parties interviewed were the Clearing system owners for the associated settlement systems.

Group	Number of stakeholders interviewed
RBA - Executives	6
RBA - Information Technology	28
RBA - Payments Settlements	19
RBA - Risk and Compliance	9
RBA - Workplace Department	1
External Parties	2

Survey

A risk culture survey was designed in alignment with Deloitte's Risk Culture Framework. The survey was sent to 645 stakeholders within 3 departments: Information Technology, Payments Settlements and Risk and Compliance, covering 12 sections and 7 levels (Levels 3, 3/4, 4, 5, 6, prefer not to say, other), and was open between 1st and 10th February 2023. We received 279 responses achieving a 43.2% response rate. Of the responders, 51.2% had an involvement in RITS over the past two years.

Statistical analysis was performed on the response rate to ensure that findings are based on a sample that is representative of the population of interest (in this case it is statistically interpreted as having a Confidence Level of 95%) and is as precise as practically possible in interpretation (in this case it is statistically as having at least a Confidence Interval of ±10 in our findings). The minimum computed sample size based on a CL of 95% and a CI of ±10 of 84 responses for 645 individuals was achieved.

Insights from the survey findings have been used in conjunction with data from interviews and document review to support the findings in this report.

6.2. Appendix 2 - Documentation Reviewed

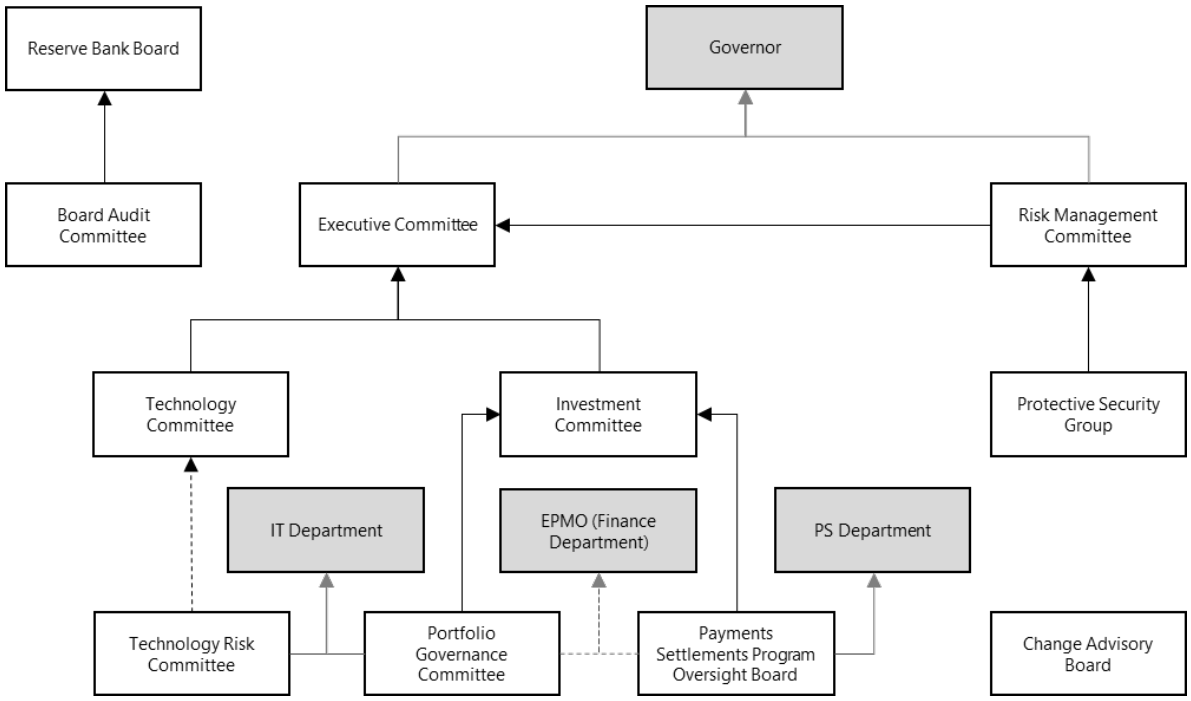
In undertaking our work, we reviewed a number of documents relevant to the RITS environment, in order to assess the non-technical factors which either contributed to the incident or present ongoing operational risks for RITS as a wholesale Real-Time Gross Settlement (RTGS) system.

The quantity of documents reviewed by scope area are:

Scope Area	Number of documents received
General Documents – all scope areas	6
Operating framework, processes, roles and responsibilities	33
People and culture	5
Risk management and governance	20
Multiple scope areas: – Operating framework, processes, roles and responsibilities – Risk management and governance.	19
Total	**83**

6.3. Appendix 3 – Board and Committee Definitions

Boards and Committees



Committee	Members
Board Audit Committee	Three or more members, who are either non-executive members of the Board or external appointments; the Chair is a non-executive member of the Board. The DG represents the Bank's management at meetings, but is not a member of the Committee.

PURPOSE

The Audit Committee assists the Governor (as the Reserve Bank's accountable authority) and the Reserve Bank Board to fulfil certain obligations under the Reserve Bank Act 1959 and the Public Governance, Performance and Accountability Act 2013 (PGPA Act), namely:

- It assists the Governor and the Reserve Bank Board by reviewing the appropriateness of the Reserve Bank's financial reporting, including the financial statements in the annual report
- It assists the Governor by reviewing the appropriateness of the Reserve Bank's:
  - Performance reporting, including the annual performance statement in the annual report
  - Systems of risk oversight and management
  - Systems of internal control.

Risks associated with the formulation of monetary and payments policies are the direct responsibility of the Reserve Bank Board and the Payments System Board, and so are not considered specifically by the Audit Committee. The Boards review management of these risks annually and as part of their regular decision-making processes.

The responsibilities of the Audit Committee include, but are not limited to, the following:

Risk oversight and management

- Review the Bank's approach to risk management as established in its risk and compliance management framework, which is overseen by the Risk Management Committee (chaired by the Deputy Governor), and the appropriateness of systems of risk oversight and management
- Review the key risks to which the Bank is exposed, the actions taken by management to mitigate those risks and the overall effectiveness of the risk and compliance management framework and internal control environment
- Review the Bank's fraud control arrangements, including the processes and systems in place to prevent, detect and effectively investigate instances of fraud

- Review reports by management on significant instances of fraud and investigate such instances, if necessary
- Review the Bank's policy on reporting fraud and unethical behaviour and reports of significant instances of whistleblowing
- Participate in the appointment of the Head of the Risk and Compliance Department. The Head of the Risk and Compliance Department reports on risk and compliance matters to the Deputy Governor and the Audit Committee
- Meet with the Head of the Risk and Compliance Department without other management present as required.

Executive Committee	Chair - Governor; Members - DG and all AGs; Secretary (attends all meetings)

PURPOSE

The role of the Executive Committee is to assist and support the Governor in fulfilling their responsibilities to manage the Bank (in particular under the Reserve Bank Act 1959 and the Public Governance, Performance and Accountability Act 2013). The Executive Committee is the principal committee in the Bank at which matters that have a strategic or Bank-wide significance are discussed by the Bank's senior executives.

The Executive Committee's agenda includes the following:

- Regular reviews of the achievements, challenges and strategic issues in each area of the Bank (quarterly for Banking, Finance, Human Resources, IT, Payments Settlements and Workplace, and semi-annually for all other areas)
- The formulation of the Bank's annual budget and regular budget reviews (quarterly)
- Regular reviews of the Bank's projects (quarterly)
- Consideration of papers for the Reserve Bank Board, Payments System Board and Audit Committee that are not reviewed through other processes
- Operational and staffing matters that have Bank-wide implications
- Approval of a number of the Bank's major policies, including the Code of Conduct and other Bank-wide HR policies.

Members are expected to bring to the Executive Committee for discussion important issues affecting their area or the Bank as a whole. Members are also expected to bring proposals for significant changes to their operations to the Executive Committee.

Members should consult the Governor or the Deputy Governor if it is not clear whether a matter should be discussed by the Executive Committee.

Significant breaches of the Code of Conduct should be tabled at the Executive Committee.

A member of the Executive Committee is able to request that an issue be tabled for discussion.

Risk Management Committee	Chair - DG; Members - AGs of Business Services, Corporate Services, Financial Markets; CFO; CIO; Heads of RM, Audit, HR, Information Departments; General Counsel

PURPOSE

RMC is responsible for overseeing the Bank's approach to the management of risks as established in its risk management framework, the assessment of the key risks to which the Bank is exposed and overseeing the actions taken by management to mitigate those risks.

The Committee assists and supports the Governor in fulfilling his/her responsibilities to manage the Bank, including by having an appropriate system of risk oversight and management and an appropriate system of internal control as required under section 16 of the Public Governance, Performance and Accountability Act 2013.

Protective Security Group (PSG)	Head of IT (for IT security); Head of Workplace Department (for physical security); Head of Information Department (for information security); Head of HR (for personnel security)

PURPOSE

PSG shall oversee the implementation of the Bank's protective security arrangements, assess new and emerging security threats and risks and provide the Risk Management Committee (RMC) with updates and strategic direction for protective security.

Protective security for this purpose is the protection and security of the Bank's people, information and assets.

Technology Committee	Chair - AG of Corporate Services; Members - CIO; Heads of Banking, Domestic Markets, HR, Payments Policy, PS Departments

PURPOSE

The purpose of the RBA Technology Committee is to provide oversight and governance of the role of technology in executing the Bank's strategy, on behalf of the Executive Committee.

Specific objectives are to:

- Review and report from a Bank-wide perspective to the Executive Committee, on:

- Alignment of the RBA Technology Strategy to the Bank's business priorities and implementation progress
- Business readiness required to ensure successful implementation of the business-aligned RBA Technology Strategy
- Business prioritisation of material technology investments
- Best practice' developments in technology and their potential to be applied to the Bank's operating environment
- Ensure IT services are delivered to the Bank in a cost effective, secure and stable manner
- Approve Bank-wide technology strategies, policies and material standards.

Technology Risk Committee	14 members who are all part of IT Department, including: CIO, CISO, Deputy Head, Infrastructure & Ops, Senior Manager, Strategy Architecture and Governance

PURPOSE

The Committee meets to discuss current risks facing the IT department and agree on activities within the department to manage them.

The Technology Risk Committee (TRC) oversees and monitors the Information Technology (IT) department's risk management and internal control framework with the objective of ensuring effective management of the various risks facing the IT department.

In doing so, the committee assists and supports the Chief Information Officer (CIO) in fulfilling their responsibilities of effective, efficient and compliant operations of the Bank's risk management framework within IT and in relation to IT services across the Bank.

Investment Committee	Chair - DG; Deputy Chair - AG of Corporate Services; Members - AGs of Business Services, Financial Markets; Advisors - CFO; Head of HR; CIO

PURPOSE

Investment Committee is responsible for the oversight of the bank's project portfolio.

Its primary role is to support the Governor and Executive Committee in recommending how the bank should best prioritise its spending on projects efficiently & to ensure the portfolio is delivering target outcomes.

Its objectives include - make recommendations to Executive Committee on the Bank's Strategic and Operational Projects Portfolio, evaluating & prioritising the bank's spending on projects to maximise the benefits subject to the overall budget and headcount constraints determined by the Governor.

Portfolio Governance Committee	Chair - CIO; Deputy Chair - Head of Portfolio and Delivery; Members - Deputy Head of Business Engagement; Deputy Head of Infrastructure and Operations; CSIO; Senior Manager, Strategy Transformation and Governance; Advisors - Manager, Finance Representative (IT Partner); Manager, Procurement Representative (IT Partner); Senior Manager, EPMO; Manager, HR (IT Partner); Manager, IT Led Portfolio; Manager, Business Led Portfolio; Secretary - IT Delivery and Portfolio Practice Lead

PURPOSE

The IT Portfolio Governance Committee (IT PGC) exists to support and inform the IT senior leadership team on the investment and governance decisions for the Bank's IT-enabled projects and programs by providing strategic oversight, advice, and a platform for decision making.

The PGC will measure the progress of the IT enabled projects portfolio by:

- Monitoring how well the portfolio is delivering to its stated strategic objectives; and
- Understanding portfolio capacity constraints and prioritisation impacts.

It will also seek to advance the portfolio vision by aligning strategy, implementation, and budget by:

- Maintaining the portfolio vision
- Revealing budget guardrails
- Reviewing portfolio metrics
- Reviewing portfolio roadmaps including pipeline.

The decisions the ITP GC are expected to make should address:

- Systematic roadblocks
- Capacity constraints
- Systematic risks and issues.

Payments Settlements Program Oversight Board (PS POB)	Chair - AG of Business Services; Deputy Chair - Head of PS; Members - Deputy Head, Portfolio Delivery (PS); Deputy Head, Business and Operations (PS); Deputy Head, IT Infrastructure (or delegate); Senior Management of PS; Senior Manager, IT Payments Systems

PURPOSE

The purpose of the POB is to provide oversight of the PS project portfolio and to guide and support the work of project teams by identifying and considering key focus areas, raising questions in respect to material project activities, and providing advice on important matters that may have a significant impact on the success of PS's projects. This includes considering various strategies for completing key project deliverables on time, and identifying and clarifying important project dependencies and options for dealing with risks or issues that may adversely impact the success of a project (e.g., staffing shortages, dealing with competing project priorities, issues found in penetration testing or vendor problems).

Monitoring and providing guidance on effective management of emerging issues and risks. This includes ensuring strategies to address potential risks to the project's success have been identified, appropriate control plans are in place, and that threats are regularly re-assessed

Enterprise Project Management Office (EPMO)	EPMO Resource Pool

PURPOSE

The purpose of the Enterprise Portfolio Management Office is to provide effective governance of the Banks Project Portfolio through appropriate application of the Project Management Framework (PMF) and to report to the Executive Committee and Investment Committee on the status and progress of these projects. The EPMO also facilitates the evaluation and prioritisation of the Project Portfolio to ensure alignment with the Bank's Strategic Plan by the Investment Committee.

Change Advisory Board (CAB)	Chair - Manager, IT Service Management; Backup Chair - Senior Change Administrator, IT Service Management; Members - Senior Manager, IT Operational Services (Operational oversight); Senior Manager, IT Workplace and Corporate Systems1 (Workplace oversight); Manager, IT Network Services (Infrastructure network oversight); Manager, IT Systems Services (Infrastructure systems oversight); Manager, IT Operations (Operations oversight); Manager, IT Service Desk (Service Desk oversight); Manager, IT Mitigation and Response (Security oversight); Manager, IT Shared Application Systems (Shared services oversight); Manager, Electronic Distribution Services 2 (BK oversight); Manager, PS Operations 2 (PS oversight); Manager, FM Business Operations or Manager, FM Market Data Platforms 2 (FM oversight).

PURPOSE

The Change Advisory Board (CAB) is a body that exists to support the approval of changes and to assist Change Management in the assessment and prioritisation of changes along with assessing and agreeing on acceptable technology risk. The CAB's purpose is to assess changes to ensure the stability of the Bank's technology services are not adversely impacted by technology changes. This is measured by meeting the agreed operational targets for change related incidents. The CAB will scrutinise scope, implementation plan, testing, scheduling, communication and overall clarity to achieve its objective.

6.4. Appendix 4 – Glossary

Abbreviation	Definition
3LoA	Three Lines of Accountability
APRA	Australian Prudential Regulation Authority
BAU	Business As Usual
BCP	Business Continuity Policy
BIS	Bank of International Settlements
BK	RBA Banking
CAB	Change Advisory Board
CMDB	Configuration Management Data Base
CRO	Chief Risk Officer
EPMO	Enterprise Portfolio Management Office
FSS	Fast Settlement Service
IT	RBA Information Technology Department
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
KRI	Risk monitoring
Level 1	Depending on the department, Bank employees in positions including business support, assistant business officer
Level 2	Depending on the department, Bank employees in positions including analyst, information officer
Level 3	Depending on the department, Bank employees in positions including analyst, IT operator, executive assistant
Level 4	Depending on the department, Bank employees in positions including team leader, lead analyst and architect
Level 5	Bank employees in manager positions
Level 6	Bank employees in senior manager positions
Line 1	Business and Support Functions: Own and manage the risks of that business including ownership of related risk management
Line 2	Risk Management: Develop risk management policies, systems, and processes. Provide review, challenge, and SME support on risk matters
Line 3	Internal Audit: Provide independent assurance over the effectiveness of Line 1 and Line 2.
LVSS	Low Value Settlement Service
PFMI	Principles for Financial Market Infrastructure
PS	RBA Payments Settlements Department
PSB	Payments System Board
RBA	The Reserve Bank of Australia
RITS	The Reserve Bank Information and Transfer System
RM	RBA Risk and Compliance Department
RMC	Risk Management Committee
RTGS	Real-time Gross Settlement
SDLC	Software Development Lifecycle
'The Bank'	The Reserve Bank of Australia
TRC	Technology Risk Committee
TRIM	A Record Management System Software

Inherent Limitations

The Services provided are advisory in nature and have not been conducted in accordance with the standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions under these standards are expressed.

Because of the inherent limitations of any internal control structure, it is possible that errors or irregularities may occur and not be detected. The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made.

Our work is performed on a sample basis and we cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Any projection of the evaluation of the control procedures to future periods is subject to the risk that the systems may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Recommendations and suggestions for improvement should be assessed by management for their full commercial impact before they are implemented. We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy, or reliability is given in relation to the statements and representations made by, and the information and documentation provided by the Reserve Bank of Australia's personnel. We have not attempted to verify these sources independently unless otherwise noted within this report.

Limitation of Use

This report is intended solely for the information and internal use of the Reserve Bank of Australia with our engagement letter and is not intended to be and should not be used by any other person or entity.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities(collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com