Targeted Assessment of the Reserve Bank Information and Transfer System

May 2023

Contents

ISSN 2201-1226 (Online)

1. Executive Summary

The Reserve Bank Information and Transfer System (RITS) is Australia's high-value payments system. It is used by banks and other approved institutions to settle their payment obligations on a real-time gross settlement basis. RITS is owned and operated by the Reserve Bank of Australia (the Bank).

Following the technology outage in October 2022 that disrupted the payments system, the Payments System Board endorsed the Bank's Payments Policy (PY) Department undertaking a targeted assessment of RITS observance of the Principles for Financial Market Infrastructures (PFMI).[1] PY is the functional area responsible for oversight of the Australian payments system, including RITS. The relevant Principles are Governance (Principle 2), Framework for the Comprehensive Management of Risks (Principle 3) and Operational Risk (Principle 17). The assessment is intended to identify opportunities to augment and uplift governance, operations, and risk management frameworks to continue to provide a highly available and resilient RITS. The objective of publishing this assessment is to increase the transparency of the management of RITS.

The ratings in this assessment are endorsed by the Payments System Board. The assessment draws on recent external reviews including by Deloitte into the October 2022 incident.[2] Information has also been provided by the Bank's relevant business areas including Payments Settlements (PS), Information Technology (IT), Risk Management (RM), Audit, and Workplace Departments. This assessment has been prepared on an exceptions basis, in that it only focuses on opportunities for uplift assessed by reference to the Principles.

RITS is critical national infrastructure for the Australian economy and management of RITS sits within an increasingly complex and fast changing external environment. Many aspects of the governance, risk management and approach to managing operational risk for RITS are working well. Consistent with the Deloitte Review, the assessment found that staff working across the RITS ecosystem have a strong sense of purpose and commitment to ensuring the resilience of a key piece of national infrastructure.

This assessment has focused on specific opportunities to uplift capabilities, to consistently and effectively embed accountabilities, processes, systems and controls, and better identify, monitor and manage risk. The assessment of RITS has downgraded the observance of the relevant Principles, identifying several areas for improvement (Table 1).

Table 1: RITS Ratings[3]

Principle for Financial Market Infrastructures	2023 Assessment
Principle 2 Governance	Broadly observed (↓)
Principle 3 Framework for the Comprehensive Management of Risks	Partly observed (↓↓)

1 Principles for Financial Market Infrastructures (PFMI) (bis.org).

2 See Deloitte report: https://www.rba.gov.au/publications/reviews/pdf/rba-independent-review-oct-2022-rits-outage-21042023.pdf and the Bank's response: https://www.rba.gov.au/media-releases/2023/mr-23-12.html.

3 For explanation of the ratings, please see here: Principles for financial market infrastructures: Disclosure framework and Assessment methodology (bis.org), p 10.

Principle 17 Operational Risk	Partly observed (↓)

These Principles are partly or broadly observed. Consequently, the identified opportunities to uplift capabilities should be afforded a high priority or undertaken within a defined timeline. The heightened operational risks associated with the Head Office (HO) Upgrade reinforces the importance of timely action. The assessment also includes recommendations to enhance the governance, management and operation of RITS in a manner which supports observance of the relevant PFMI.

2. Key Developments

The key developments in relation to RITS since the June 2022 assessment[4] include the October 2022 incident and ongoing works in relation to the Bank's HO Upgrade.

October 2022 Incident

On Wednesday 12 October 2022, at around 7pm, the Bank experienced a major system incident that impacted the Fast Settlement Service (FSS) and the Low Value Clearing and Settlement Services (LVCS and LVSS). The root cause was an operational error during a planned change which applied an incorrect setting to the software that manages the Bank's virtual servers. This took a number of the Bank's production and non-production servers out of service, including some underpinning RITS and FSS.

Settlement notifications for FSS transactions were either delayed or not sent for over two hours. This resulted in around 500,000 unique payments for the New Payments Platform (NPP) (17 per cent of the daily average volume for a Wednesday) being delayed by between four hours and five days. RITS was also unable to receive LVSS File Settlement Instructions (FSIs) for over three hours, which prevented members from submitting FSI's to RITS through the normal channel.[5]

Head Office Upgrade

In 2022, work was commenced to deliver necessary upgrades to the Bank's HO building. During the HO Upgrade, there may be an increased risk of operational disruption to the HO datacentre and therefore critical PS systems such as RITS will operate mostly from the Bank's Business Resumption Site (BRS), which has the same operational capacity as HO.

The June 2022 assessment identified heightened operational risk for RITS associated with the HO Upgrade as an area of oversight focus. Since then, the operational risk emanating from the HO Upgrade has increased as the project time horizon has been extended and the arrangements related to the occupancy of HO during the building works have been revised.

4 Assessment of the Reserve Bank Information and Transfer System - June 2022 (rba.gov.au).

5 For more information regarding the incident, please see: Final Incident Report RITS and FSS Incident – 12 October 2022 (rba.gov.au).

3. Assessment

The assessment identifies opportunities for improvement on an exceptions basis and accords an observance rating for each of the Principles assessed. The assessment also includes recommendations to strengthen observance of the Principles.

Principle 2: Governance

The assessment, informed by the external reviews, has identified several opportunities to augment the governance arrangements for promoting the safe and efficient operation of RITS. Given this, observance of *Principle 2 Governance* has been downgraded to 'broadly observed'.

Accountability for the design and implementation of an effective risk management framework

Consistent with the findings in the external reviews, our assessment is that further activity is required to embed an effective risk management framework. This will require significant focus, oversight, investment, and executive accountability. An accountable senior risk executive will need to drive change and be sufficiently independent to enable effective challenge and focus. They need to provide an integrated view of risk, embed an evolving risk management program, and consider the full spectrums of risk relevant to RITS, including in relation to the management of non-financial risks.

Clear and transparent governance

The governance arrangements which relate to RITS include the involvement of four Bank management committees: the Executive Committee (ExCo), Risk Management Committee, Investment Committee and Technology Committee. However, the role of each committee in the oversight of specific risks associated with RITS, and defined escalation and risk reporting between these committees, is unclear. In addition, the role of Committee Chair in promoting the voice of risk in respect to RITS should be more clearly defined in each of the Committee Charters.

Our assessment, consistent with the external reviews, is that, at both a staff and senior executive level, accountabilities, roles, and responsibilities for RITS are sometimes unclear, insufficiently documented and widely diffused across sometimes siloed teams. This affects decision-making and the escalation of issues of concern or potential future risks relating to the resilience and stability of RITS. This is exacerbated by communication challenges and a dependence on long tenured staff rather than documented process.

Culture of risk awareness

To better and consistently embed risk management frameworks and bolster a strong culture of risk-management, staff knowledge of risk management needs to be deepened. Staff should also be able to effectively voice risk-based concerns and provide challenge. Staff need to have a better understanding of the risk appetite with respect to RITS, how it translates to their work, what controls might apply, and expectations for good risk management behaviours. Despite investment in this area, and a number of in-flight initiatives, there is not yet a fully effective speak-up culture within the RITS ecosystem. Ineffective channels to voice concerns regarding RITS impact the ability to manage risk and proactively

monitor and improve controls. To embed a strong risk-culture and accountabilities, there should also be a more consistent and balanced approach to consequence management, complementing an effective speak-up culture.

Prioritisation

Consistent with the findings in the external reviews, our assessment is that more effective and strategic prioritisation of resources with respect to RITS is needed to proactively manage risk and operate critical infrastructure reliably and safely. There is also sometimes a bias towards action, reflective of a strong culture to 'get things done' with a sometimes insufficient focus on prioritisation and implementation. The completion of tasks also often attracts greater recognition from leaders than does the reliable delivery of business-as-usual activities (BAU) or the adoption of positive risk processes and behaviours. Allocation of resources and frameworks for prioritisation of BAU and project work, including for IT shared services could be improved. There are certification standards for staff working on critical systems, however staff allocation is sometimes based on urgency of need rather than capability or experience. This can increase workload pressures on staff and result in either poor or inefficient outcomes.

Principle 3: Framework for the Comprehensive Management of Risks

The assessment, informed by the external reviews, has identified significant improvement opportunities in the risk-management frameworks for RITS. A high priority should be accorded to addressing these issues. Given this, observance of *Principle 3 Framework for the Comprehensive Management of Risks* has been downgraded to 'partly observed'. Principle 3 should be considered holistically with the observations on Principle 2 (above) and Principle 17 (below).

Risk frameworks, policies and procedures

A risk management framework includes risk identification, risk assessment, controls (including control design, testing and assessments), risk policies and procedures, issue and incident management, risk monitoring (including key risk indicators) and risk reporting. Our assessment, informed by the external reviews, identified opportunities to uplift risk management frameworks, policies and risk practices to be more effective in proactively identifying, measuring, monitoring and managing risk for RITS. This finding also applies to operational risks material to the continued operation of RITS. Risk frameworks are also not always fully aligned to industry standard frameworks.

Consistent with the findings in the external reviews, our assessment found that risk management policies and procedures lack sufficient detail to be effectively embedded. This includes requirements for analysing and managing incidents, communication strategy and escalation to governance forums. Updates to documented risks and controls for PS and IT are made reactively to incidents with comprehensive reviews undertaken on an annual and self-assessment basis. There is also an inconsistent approach between PS and IT to assign ratings for the effectiveness of controls, which are used as an input into residual risk ratings.

Three lines of accountability

An operator of critical financial infrastructure should have a robust three lines of accountability (3LoA) model, especially a line 2 function that has strong technical capability to challenge operational resilience and stability of the IT systems supporting RITS.

An effectively implemented 3LoA should consist of business owners and operators (first line) having responsibility to own and manage risks associated with 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 second line should have a sufficiently authoritative voice to effectively identify risks, challenge business areas and escalate these risks as necessary to senior and executive management. The third line will provide objective and independent assurance reporting regarding the effectiveness of control culture, with the capacity to escalate issues to executive (or senior) management as required.

Our assessment, informed by the findings in the external reviews, is that RITS does not have a fully implemented, embedded and effective three lines of accountability model. This has contributed to unclear accountabilities and responsibilities for managing risk. There is a lack of effective challenge from the second line, which does not have the technical capabilities or seniority to challenge operational resilience and the stability of IT systems supporting RITS. There are also some deficiencies in the capabilities and capacity of embedded line one risk teams. Third line could also be enhanced to ensure it operates as an effective last line of accountability.

Knowledge management

There are weaknesses in knowledge management practices for RITS. There is no standardised approach to knowledge management, with various technology solutions being utilised inconsistently. This has resulted in an overreliance on the longevity of key individuals for retaining institutional knowledge. The technical documentation supporting RITS could be uplifted to be consistent, traceable and searchable. There is also no easily accessible knowledge management repository to retrieve incident reports and recovery steps, compromising effective disruption scenario planning.

Reporting of risk indicators to underpin oversight and action management

Risk indicators are monitored and reported regularly to governance committees. However, there is an opportunity to review, rationalise and define a cohesive and aggregated view of risks specific to RITS, in terms of risk decisions, risk information and related risk reporting.

Our assessment, consistent with the external reviews, only found limited evidence to demonstrate that sufficient action has been taken in response to operational risks that have been identified as outside of risk appetite. Notably, some key risk indicators for RITS were reported outside of risk tolerance for several months without sufficient actions being taken by relevant staff to remediate these risks. 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. Risk management remediation actions to address known issues and incidents have not adequately addressed root cause issues. Some of the contributing factors to the October 2022 incident were known to relevant staff, based on issues identified in prior incident reviews, but there was insufficient action and oversight to ensure that these were effectively mitigated.

Principle 17: Operational Risk

The assessment, informed by the external reviews, has identified significant opportunities for improvement in the ability to reduce and mitigate operational risks to RITS and provide a high degree of security, reliability and availability. A high priority should be accorded to addressing these issues. Given this, observance of *Principle 17 Operational Risk* has been downgraded to 'partly observed'.

Operating model

Consistent with the findings in the external reviews, our assessment is that the RITS operating model (the framework, processes, services, service levels, roles and accountabilities) is not sufficiently and consistently documented and embedded. This adversely affects accountability, decision making, prioritisation and the rapid escalation and remediation of issues and incidents. Collaboration between PS and IT is crucial to support the RITS operating model and is not currently optimised. Notably, critical services provided to PS by IT are not provided under a formal service level agreement. There is also a lack of formal documentation setting out clear responsibilities and accountabilities, and processes for engagement between PS and IT.

Technology processes, controls and documentation

The external reviews found that technology processes could be better documented and consistently embedded. Technology change management processes rely on manual effort with limited automated controls to prevent unauthorised change. This increases the risk that unapproved changes can be directly deployed affecting RITS, as occurred in the October 2022 incident.

There is an in-flight project to deliver a Configuration Management Database (CMDB). In its absence, it is not possible to accurately map the impact of changes to systems, applications, infrastructure, owners and the interrelationship between components. In addition, disruption scenario testing could be enhanced.

The external reviews found that the technology control environment is overly complex and largely manual, limiting the ability to apply controls in a complete, consistent and accurate manner. Controls are not embedded into infrastructure services design and operational delivery, nor enforced through automated workflow, inhibiting control effectiveness. Controls are also not explicitly identified, applied, maintained, tested, assured and continuously improved as part of an end-to-end infrastructure services lifecycle framework. Technology controls are generally defined and applied with no linkage to policy, standards, or processes. Lack of traceability to typical determinants of controls limits the ability to determine their adequacy, to assess alignment to the technology strategy and intended business outcomes. It also means gaps in controls can be identified only on a reactive basis following scenarios like major outages. Controls are also not consistently documented with a number of key attributes missing. A lack of consistent role-based access controls also gives rise to a greater risk of harm due to human error, a contributing factor in the October 2022 incident. The gaps in the technology control environment coupled with a lack of segregation of environments in technical infrastructure gives rise to material operational risk. In that regard the architectural documentation to detail the segregation of RITS operational infrastructure and the Bank's wider enterprise systems does not reflect the current state. Our assessment, consistent with the external reviews, is that the technology control environment supporting RITS requires significant uplift to be effective in reducing RITS' operational risk profile.

Resilience, scenario planning and business continuity

Business continuity management is a key component of an operational risk management framework. Business continuity plans should be subject to periodic review and testing and consider a range of different scenarios which simulate wide-scale or major disruption. Comprehensive disruption scenario testing within RITS' business continuity arrangements could be uplifted. Effective disruption scenario planning and testing is also essential to ensure teams are sufficiently prepared for, and can respond to, incidents.

All critical systems and key enterprise-wide systems will operate primarily out of the Bank's BRS for an extended period during the HO Upgrade. The HO data centre will continue to operate as a second site for RITS. This may result in RITS operating with reduced resiliency, as the secondary site will be located within a building undergoing extensive renovations. There is an elevated risk that an outage could occur at the HO data centre during the HO Upgrade.[6] Consequently, the HO site may not be able to provide the required level of redundancy continuously, impeding RITS' ability to remain fully functional in the event of an outage at BRS. The RITS business continuity plan could be more fully documented, maintained, updated and tested, particularly to reflect the increased operational risk associated with the HO Upgrade.

Recommendations to facilitate observance of the Principles

The assessment, drawing on recent external reviews, highlights some material opportunities for improvement to observe the Principles. Implementation of these recommendations would build on the many aspects of the governance, risk management and approach to managing operational risk for RITS that are working well, and in-flight initiatives to improve governance arrangements and technical controls. It would also enhance capabilities and resilience to promote the safe and efficient operation of critical national infrastructure. To ensure each recommendation is progressed, implemented, embedded and (if relevant) continuously improved there should be regular reporting to the Bank's Executive Committee by the relevant Department, Steering Committee or senior executive.

	Recommendation	**Deloitte Recommendation**	**Principle (P) and Key consideration (KC)**
1.	Implement a formally documented RITS operating model including a detailed service level agreement, IT service catalogue and resource management.	**1.1**	**P 2** KC 2 **P 17** KC 5
2.	Develop and execute a detailed plan (including accountabilities and timeframes) to address identified operational gaps, including business continuity management, service provider management and operational risk management.	**5.3 & 5.5**	**P 17** KC 1 & 6
3.	Develop and execute a detailed plan (including accountabilities and timeframes) to address identified gaps in the RITS risk management framework, policies and procedures.	**5.4**	**P 3** KC 1 **P 17** KC 1
4.	The senior executive accountable for risk should be responsible for implementing and embedding the risk management framework for RITS, including an effective 3 Lines of Accountability model for RITS.	**5.1 & 5.2**	**P 2** KC 2 & 5 **P 3** KC 1 **P17** KC 1

6 A physical incident occurred in August 2018, where the Bank experienced a disruption to the power supplying the data centre at one of its sites. The power loss abruptly cut off all technology systems operating from that data centre, including those supporting RITS. Experience from the August 2018 incident reinforces the importance of conducting regular testing of backup arrangements and maintenance on critical systems (particularly as the parameters of the HO Upgrade are subject to change) and the need to have robust arrangements in place for system restoration (which address all risks associated with the extended period that BRS will operate as the primary site)(see 2019 Assessment of the Reserve Bank Information and Transfer System (rba.gov.au)).

5.	Develop and execute a detailed plan (including accountabilities and timeframes) to address the identified gaps in RITS technology documentation, technology controls and processes to reduce design complexity. Emphasis should be on ensuring RITS has an efficient set of controls that are aligned to processes, risk objectives and are a more effective balance of automated and manual controls.	**1.3, 2.1, 2.2 & 5.4**	**P 3** KC 1 **P 17** KC 1 & 2
6.	Identify, plan for and document a range of severe but plausible disruption scenarios that may impact the RITS ecosystem. This also requires an uplift to operational resilience documentation.	**1.3**	**P17** KC 6
7.	The relevant Departments, Steering Committee and the senior executive accountable for risk should each promptly escalate serious issues of concern relating to the resilience and stability of RITS to the Bank's Executive Committee. Additionally, a horizon scan for emerging or possible challenges to the resilience of RITS should be a standing agenda item in periodic strategic updates by relevant Departments to the Executive Committee.	**1.2 & 5.1**	**P 2** KC 1, 2 & 5
8.	The Risk Management Committee, Investment Committee and Technology Committee should update their governance and reporting arrangements to ensure that the committees have mechanisms in place to facilitate timely, accurate and transparent provision of information on RITS-related risks, including to other committees.	**5.6**	**P 2** KC 2 **P 3** KC 1