SUMMARY OF RITS BUSINESS CONTINUITY AND SECURITY ARRANGEMENTS

The security, resilience and reliability of RITS and RITS Members is critical to the smooth functioning of the Australian payments system. This document sets out at a high level the business continuity and security arrangements in relation to the operation of RITS.[1]

The Reserve Bank Information and Transfer System (RITS) is Australia's interbank settlement system used by banks and other approved institutions to settle their payment obligations. Final and irrevocable settlement is achieved by the simultaneous crediting and debiting of Exchange Settlement Accounts (ESAs) held at the Reserve Bank of Australia (RBA). Transactions are entered into RITS directly or delivered via external feeder systems including SWIFT and Austraclear, and the New Payments Platform which delivers to the RITS Fast Settlement Service (FSS). Low-value clearings are settled periodically throughout the day on a multilateral netted basis for cheques, direct entry, cards, and some asset transactions (equities and some property-related transactions).

Business Continuity Framework

As part of its overall approach to risk management, the RBA has developed business continuity arrangements for RITS that enhance its resilience and minimise the likelihood and impact of operational disruptions. These arrangements prepare for major contingency events such as:

- Loss of access to an operating site
- Disruptions affecting systems or supporting infrastructure
- Unavailability of critical staff to support its operations.

The RBA's Business Continuity Management Policy sets out the high-level policy for maintaining its critical functions, consistent with its overall risk management framework, and is overseen by the RBA's Risk Management Committee. Under the risk management framework, all departments within the RBA prepare and maintain their own risk register, business impact analysis (BIA) and business continuity plan (BCP).

The risk register identifies the range of risks that might affect the RBA's ability to operate RITS in a safe and efficient manner, and the associated controls to mitigate those risks. Important business operations of the RBA and the facilities, staff and IT systems and infrastructure that are required to

[1] Whilst the RBA does not provide detailed information on sensitive security and business continuity matters, the annual RITS Assessment includes a report of the RBA's compliance with relevant industry standards. Similarly, the RBA is not a vendor or third-party supplier to RITS Members and therefore does not provide detailed information that could typically be sought by Members under third-party compliance arrangements. The legal arrangements between the RBA and a RITS Member are set out in the RITS Regulations and the associated RITS Membership Agreement.

support them are identified and the recovery of various systems prioritised in the BIA. RITS, as a critical system, has a very high recovery priority.

The BCP sets out how the RBA would respond to a disruption that affects RITS. It outlines business continuity responsibilities, operational arrangements for staff and systems (including backup facilities), communication channels and facilities, contingency roles, contingency scenarios and key considerations, key processes, priority of systems recovery and dependencies, shelter-in-place arrangements and evacuation plans, management of a contingency including the restoration of normal operations, review and mitigation arrangements, and employee awareness and training. The BCP is supplemented by detailed procedures for the operation of RITS, systems failovers, incident management and communications.

The RBA's Risk Management Policy sets out incident reporting requirements. Incident reports are sent to the Risk and Compliance Department and are reviewed by the Risk Management Committee.

Security

The RBA maintains a high level of vigilance over the adequacy of its security controls in relation to RITS. These are aligned to the *Australian Signals Directorate's Information Security Manual* and the *International Organization for Standardization (ISO) 27001 - Information Security Management Standards.* The RBA maintains ISO 27001 certification for the systems supporting RITS. Regular reviews ensure that appropriate security controls are maintained.

A comprehensive range of security controls employed to protect the RITS ecosystem include: network infrastructure segregation, tight access controls, regular software patching, comprehensive system monitoring, and robust physical security arrangements. Security arrangements are regularly tested. The RBA does not provide detailed information about the RITS security controls and testing arrangements.

The SWIFT Customer Security Program is a suite of security initiatives introduced by SWIFT to provide a baseline of security standards and an associated assurance framework for the global SWIFT community. The Bank commissions independent assessments of its compliance with the SWIFT controls, and compliance is reported in the RITS Assessment annually.

Infrastructure Resilience and Failover

The RBA maintains permanent, 24/7 operational and technical support staff for RITS at two geographically remote operating sites. This allows RITS operations to be conducted from either site, and ensures that operations can continue seamlessly in the event of a disruption affecting one site. Critical operational and technical support personnel are also able to connect to RBA systems remotely to perform essential functions.

RITS (and the FSS) has been designed with a high degree of technical redundancy, including appropriate automatic failover of components. Multiple versions of critical components, including infrastructure, network, database and application technologies, exist at each of the two sites. RITS data from the active site is synchronously replicated to the systems at alternate sites to ensure that transactional information is protected in the event of a failure. In the event of equipment/component failure, the systems will failover to the redundant equipment operating at the active site. For RITS, the Bank's recovery time target (the time taken between confirmed system failure at one site and resumption at

the alternate site) is up to 40 minutes, depending on the nature of the operational disruption. Cross-site failover of the FSS will occur within 2 minutes.

The RBA rotates the operation of core RITS between the two sites during the year, with each site acting as the active site for part of each year. These planned system rotations are transparent to Members.

Testing

To help ensure that business continuity arrangements, including contingency procedures, are up to date and effective, the RBA performs regular reviews and testing. The testing covers various contingency scenarios relating to component failure at a site, total systems failure at the active site with failover to the alternate site, remote access to a site's systems, external infrastructure outages, and a total site outage (staff and systems). Regular contingency simulations are conducted throughout the year, including desktop exercises and test system drills.

Contingency Incident Management and Communications

The RBA has in place robust incident management procedures. The *RITS Member Contingency Procedures* document (available to RITS members on the RITS Information Facility) sets out for Members how the RBA will manage various contingency events affecting all or part of RITS operations, and provides high-level information on procedures to be followed by Members in those events.

The RBA uses an internet-based communications facility to enable efficient dissemination of important messages regarding RITS during significant incidents, by email and SMS, even if the RBA's normal communications infrastructure is affected. Contact details of critical RBA staff, RITS Members and other external contacts are maintained in this facility to allow for ready communication. A teleconference facility can be used to enable communications between the RBA and external stakeholders.

External Suppliers

The RBA relies on a range of external third-party suppliers to assist with the support of RITS. In general, and where relevant, service contracts are maintained that outline the agreed level of services provided such as availability and uptime, and support response times. These contracts are reviewed regularly by the RBA.

Member Resilience and Connectivity

In recognition that the efficient operation of RITS is also dependent on the operational reliability and resilience of RITS Members, the RBA requires Members to comply with the *Business Continuity and Security Standards for RITS Members* with respect to their RITS payment operations. The standards cover such things as business continuity planning, operational resilience, recovery timeframes, security protection and monitoring, incident management, testing and training. Members are required to complete an annual self-certification statement of compliance.

Member access to the RITS user interface is via a private network (ASX Net/ANNI) and/or via the internet. Members may employ redundant network connectivity to RITS to provide additional resilience. Members with only internet connectivity are encouraged to have resilient internet arrangements. Users logging in via the RITS launch page are automatically routed to the active site, and so do not need to be aware of which site is the active site.

RITS Assessments

RITS is a systemically important payment system and, as such, has been assessed by the International Monetary Fund as part of its Financial Sector Assessment Program for Australia. The RBA conducts an annual assessment of RITS against the Principles for Financial Market Infrastructures, which are international standards set by the Bank for International Settlements and the International Organization of Securities Commissions. These assessments are published on the RBA's website: http://www.rba.gov.au/payments-and-infrastructure/rits/assessments.html.

If you have any questions, please contact the RITS Help Desk on 1800 659 360 or rits@rba.gov.au.

Payments Settlements Department

10 October 2022