RESERVE BANK INFORMATION AND TRANSFER SYSTEM

Electronic RITS Self-Certification Statements

User Guide

October 2023

R I T S

1. INTRODUCTION

This User Guide describes roles and responsibilities and the process for Members to submit electronic RITS Self-Certification Statements using the DocuSign® platform (**e-signing platform**).

RITS Members do not need their own DocuSign® account in order to complete and submit the electronic RITS Self Certification Statement. For information about DocuSign®, visit docusign.com.au.

The Self-Certification Statement is an attestation to the Reserve Bank regarding a Member's compliance with the *Business Continuity and Security Standards for RITS Members* (the Standards). Applicable RITS Members are required to submit a Self-Certification Statement at least annually. Further information on the Standards can be found on the RITS Information Facility. The Reserve Bank expects all Members to use the e-signing platform for submitting Self-Certification Statements. If there are specific circumstances that prevent Members from using the platform, please contact the RITS Helpdesk to discuss the matter in more detail. Where the issue cannot be resolved, the Reserve Bank may consider granting approval for temporary use of an alternative method of submission.

2. ROLES AND RESPONSIBILITIES

There are four key roles in the process for completing and submitting a Self-Certification Statement via the e-signing platform, comprising one Compliance contact and three Statement signatories. These roles are defined as follows:

Role	Contact Details Required	Responsibilities
Compliance contact	To be provided to the Reserve Bank: - Corporate email address	- Complete the Self-Certification Statement electronic form. - Enter the contact details of the three Statement signatories.
Signatory 1 – The senior official responsible for RITS Payment Operations	To be provided to the Compliance contact: - Corporate email address - Mobile phone number[(a)]	- Review and sign-off the Self-Certification Statement.
Signatory 2 – The Chief Information Security Officer (CISO) or an equivalent senior official responsible for cybersecurity in relation to RITS Payment Operations		
Signatory 3 – A suitable external firm or an independent senior official from the risk management, compliance or internal audit function)		

(a) Required for the purpose of multi-factor authentication.

A corporate email address is required for each of the roles above. **Personal or group email addresses will not be accepted.** The links emailed to each contact via the e-signing platform are unique and cannot be used by other staff to access the form, even if the link is forwarded.

If the wrong email address has been assigned to any of the four contacts, or if a contact leaves the organisation during the process, please contact the RITS Help Desk on 1800 659 360 or rits@rba.gov.au to amend the address.

3. INSTRUCTIONS

This section sets out instructions for completing and signing the Self-Certification Statement using the e-signing platform.

3.1 Stage 1 – Completing the form

1. **Receipt of the e-signing platform Envelope.** The nominated Compliance contact will receive a link to their e-signing platform envelope via email from dse@aumail.docusign.net. This envelope will contain the Self-Certification Statement. They should follow the instructions within the email to open the Statement. If email is not received, the Compliance contact should check their spam folder and whether the email has been blocked by their organisation's email system.

2. **Acceptance of the Terms.** The Compliance contact will be prompted to review and accept the Bank's e-Signing terms and Privacy Notice before being able to access the Self-Certification Statement in the e-signing platform.

3. **Form Preparation.** Only the nominated Compliance contact will be able to access and complete the fields of the Self-Certification Statement in the e-signing platform. The Compliance contact can save their progress and exit the form by navigating to the menu and selecting 'Finish Later'. The information completed to date will be saved to the e-signing platform. To return to the form, use the link in the initial email from the e-signing platform (referred to in step 1 above).

   Note: To assist the Compliance contact with collating and preparing the responses within their organisation, a blank version of the Self-Certification Statement will be available on the RITS Information Facility in due course or by contacting the RITS Help Desk. Note this version is intended to be used as a working draft within a Members organisation. It cannot be submitted to the Reserve Bank in this format. Responses must be submitted using the Self-Certification Statement provided via the e-signing platform.

4. **Form Completion: Section A.** Complete section A by selecting the Member's Compliance Level. Definitions of Compliance Level 1 and 2 are available in the form.

5. **Form Completion: Section B.** Complete section B as follows:

   For each sub-standard, indicate the 'Level of Compliance' with that standard by selecting one of the following options:
   - Fully Compliant
   - Partially or Not Compliant
   - Not Applicable (only relevant for Standards 1.02, 4.03 and 5.08)
   - Not Attesting (only relevant for recommended standards)

   Whenever 'Partially or Not Compliant' is selected, further specify from the drop-down list whether it is 'Partially Compliant' or 'Not Compliant'. In addition, further details must be provided, including a remediation plan and any interim milestone dates. The 'Expected timeframe for remediation' field must also be completed.

Note: Members are also able to include comments when 'Fully Compliant' is selected but this is not mandatory.

6. **Form Completion: Section C.** In accordance with Standard 4.03, if a Member is unable to use the SWIFT KYC-Security Attestation application to provide the Reserve Bank with access to view their SWIFT Customer Security Controls Framework (CSCF) attestation, such as for unpublished Business Identifier Codes (BICS) used in the SWIFT Payment Delivery System, the Member must attach a copy of the attestation lodged with SWIFT to the annual Self-Certification Statement. This document can be attached in Section C.

   Note: For the avoidance of doubt, there is no expectation that Members attach any other documents to the Self-Certification Statement. Should Members wish to include further information relevant to the submission, supporting documents can be attached in Section C. The sensitivity of each document should be considered prior to including it.

7. **Internal Review.** Before finalising the Self-Certification Statement and initiating signing by the Statement signatories, we recommend that the Compliance contact downloads and shares a draft version for internal review and commentary. This can be done by selecting the Download icon:

8. **Completion Checklist: Section D.** Once all necessary data fields of the Self-Certification Statement have been completed, complete the Completion Checklist in Section D by initialling against each of the statements.

9. **Finalising the Statement.** Once the Completion Checklist is complete, the Self-Certification Statement can be finalised by selecting Finish.

   Note: After this point, the Compliance contact will not have access to make any further changes to the document.

10. **Nomination of Signatories.** The Compliance contact will receive an email prompting them to nominate the three Statement signatories. The Compliance contact will need to provide the corporate email address and mobile phone number for each signatory. The Statement signatories must hold the roles described at Section 2 (Roles and Responsibilities).

3.2 Stage 2 – Sign off

11. **Sign-off: Section E.** Each signatory will receive an email from dse@aumail.docusign.net with a link to the completed Statement. If a link is not received, the signatory should check their blocked emails and spam folder. After clicking this link the signatory will receive an access code via SMS to input into the e-signing platform, as multi-factor authentication (MFA) protection will be enabled for the Statement signatories. Once MFA is completed, the signatory will need to accept the Bank's e-Signing terms and Privacy Notice, and then complete their sign-off in Section E of the form as prompted.

The second Statement signatory will receive their link via email after the first Statement signatory has completed their sign-off, and so on.

12. **Correction of data at sign-off.** If an issue with the Self-Certification Statement is identified at the point of signing by any of the three Statement signatories, the signatory will need to 'void' the envelope. It is not possible for a Member to amend information in the Self-Certification Statement after step 9. The Member should contact the RITS Help Desk to reinitiate the sign off process. The Compliance contact will receive a new link to the previous version of the Self-Certification Statement (containing all of the information previously provided). The Compliance contact must amend the information as necessary, and then revert to step 8 above. The Compliance contact will not be required to re-complete step 10.

13. **Document Management.** Once signed, an email will automatically be sent from the e-signing platform to notify the *RITS Help Desk* and all participants involved in the Self-Certification Statement that it has been completed. Each participant will be able to download a copy of the completed and signed Self-Certification Statement at this time by using the link provided in the email from the e-signing platform.

    Documents will be available for download from the e-signing platform for up to 90 days after completion after which time they will be deleted from that platform. If you require a copy after this date, please contact the *RITS Help Desk.*