Effective:
23 September 2024
Version 044

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

PROCEDURES

for

HIGH VALUE CLEARING SYSTEM FRAMEWORK: VOLUME 1

(CS4)

Commenced August 1997

Australian Payments Network Limited
Telephone: (02) 9216 4888

PROCEDURES

FOR

HIGH VALUE CLEARING SYSTEM FRAMEWORK
MT CLOSED USER GROUP

(CS4)

INDEX

PART 1 PRELIMINARY

1.1 Definitions

The following words have these meanings in these Procedures unless the contrary intention appears.

"ACK" means Acknowledgment.

"Acknowledgment" ("ACK") means a SWIFT advice, issued by SWIFT in response to the receipt of a message in the SWIFT PDS, advising that the message has been received by SWIFT and passed all necessary validation requirements.

"Advance Information Standards Release Guide" means the document referred to as such in Clause 5.23(a) or such other replacement document as may be published by SWIFT from time to time.

"AEDT" means Australian Eastern Daylight Time.[1]

"AEST" means Australian Eastern Standard Time.[2]

"Affected Participant" means a Framework Participant that is experiencing a Disabling Event which prevents that Framework Participant from sending HVCS payments in the normal way. [3]

"AIF" means Automated Information Facility.

"Applicant" means a person who has lodged an application for membership of the HVCS as a Framework Participant or who proposes to lodge such an application.

"Assisted Transaction" means a transaction entered into RITS by the Reserve Bank of Australia on behalf of the Framework Participant, subject to the appropriate authorisation and in accordance with the RITS Regulations.[4]

"AusPayNet" means Australian Payments Network Limited.[5]

"AusPayNet PDS" means:

(a) the SWIFT PDS, and

(b) any other payment delivery system implemented by the Company from time to time,

for sending and receiving domestic high value payments in the HVCS between Framework Participants.

[1] Inserted effective1/1/18, version 037 r&p 001.17
[2] Inserted effective1/1/18, version 037 r&p 001.17
[3] Inserted effective 19/7/21, version 039 r&p 001.21
[4] Inserted effective 19/7/21, version 039 r&p 001.21
[5] Inserted effective1/1/18, version 037 r&p 001.17

"Automated Information Facility" (**"AIF"**) means the service provided within RITS for the initiation and monitoring of SWIFT message based Commands, Enquiries and Unsolicited Advices.[6]

"Back-up Computer Site" means, in relation to each Framework Participant using the SWIFT PDS, all system configuration components necessary to ensure connection to the SWIFT PDS as an alternate to the Primary Computer Site, particularly when the Primary Computer Site is not available. For the avoidance of doubt, the system components which together comprise a "Back-up Computer Site" need not be situated at the same physical location provided that, taken as a whole, those components satisfy the operational and security requirements of clauses 7.11 to 7. 24 inclusive.[7]

"Back-up Tier" means either of the two tiers of back-up referred to in Clause 7.8(a), and in relation to a Framework Participant, the tier of back-up applicable to that member from time to time as determined in accordance with Clauses 7.8(a) to 7.9(a) inclusive. A Framework Participant's Back-up Tier is determinative of the back-up requirements with which that member must comply.[8]

"Board" means the board of directors of the Company.

"Business Officer" means a person who has the authority to instruct SWIFT to change the FIN-Copy Service Mode.[9]

"BSB Number" means, in relation to a Framework Participant, its BSB Number assigned to it by the Company.

"Business Day" means a day on which RITS is operating to process payments.[10]

"Bypass Mode" [Deleted][11]

"CAP" means Customer Access Point.

"Cash Settlement Rate" [Renamed "ESR"].[12]

"CBT" [Deleted][13]

"Central SWIFT Interface" (**"CSI"**) means the RITS interface to the SWIFT FIN Copy Service. [14]

"Certification Test Plan" means the test plan, incorporating test scripts, produced by the Company for the purpose of obtaining System Certification in accordance with Clauses 7.27(a) to (j) inclusive, to ensure that a Framework Participant's SCI

[6] Last amended effective 1/1/18, version 037 r&p 001.17
[7] Last amended effective 23/4/98, version 001
[8] Amended effective 1/1/14, version 034 r&p 001.14
[9] Inserted effective 19/7/21, version 039 r&p 001.21
[10] Last amended effective 1/1/18, version 037 r&p 001.17
[11] Deleted effective 20/8/04, version 014 r&p 001.04
[12] Last amended effective 13/6/01, version 002 r&p 004.01
[13] Deleted effective 14/11/22, version 041 r&p 001.22
[14] Last amended effective 1/1/18, version 037 r&p 001.17

has the correct PDS configuration loaded and can successfully interact with SWIFT FIN-Copy.

"CEST" means Central European Summer Time.[15]

"CET" means Central European Time.[16]

"Chief Executive Officer" means the person appointed as a chief executive officer of the Company under Article 7.13 and a reference in these Procedures to the Chief Executive Officer includes a reference to a person nominated by the chief executive officer to be responsible for the matter referred to in that reference.

"CLS Payments" means payments exchanged between a Framework Participant and CLS Bank through the SWIFT PDS, normally for the purposes of settling the Australian Dollar leg of foreign exchange transactions. CLS Payments are excluded from the Fallback Solutions provided for in the HVCS Contingency Instructions. [17]

"Collator" [Deleted][18]

"Company" means Australian Payments Network Limited (A.C.N. 055 136 519).

"Core Business Hours" means the minimum period during each Business Day that a Framework Participant's SCI must be logged on to the SWIFT PDS as specified in Clause 4.4(a).[19]

"Core PPS" means the specific hardware and software that is normally used by participants to generate or process the bulk of their RITS SWIFT messages, by value, for high value payments. This would include, for example, systems required for sending correspondent banking and financial markets transactions.[20]

"Crisis Meeting" has the meaning given to it in the AusPayNet Crisis Communications Plan. [21]

"Crisis Management Team" has the meaning given to it in the AusPayNet Crisis Communications Plan. [22]

"CSI" means Central SWIFT Interface.

"Customer" means the customer of the Receiver into whose account payments are credited.

[15] Inserted effective 01/7/02, version 006 r&p 002.02
[16] Inserted effective 01/7/02, version 006 r&p 002.02
[17] Inserted effective 19/7/21, version 039 r&p 001.21
[18] Deleted effective 23/4/13, version 033 r&p 001.13
[19] Amended effective 14/11/22, version 041 r&p 001.22
[20] Last amended effective 1/1/18, version 037 r&p 001.17
[21] Inserted effective 19/7/21, version 039 r&p 001.21
[22] Inserted effective 19/7/21, version 039 r&p 001.21

"Customer Access Point" (**"CAP"**) means a dedicated SWIFT access point that is located within a Framework Participant's premises and is used to access the SWIFT FIN Copy Service.

"Cyber Fraud Event" means any actual or suspected unauthorised or fraudulent payment that:[23]

(a) arises as a result of a cyber security breach in the Framework Participant's own control environment; and

(b) is known or suspected to have been dispatched to another Framework Participant through the SWIFT PDS CUG.

"Daily Settlement Session" has the meaning given to that term in the RITS Regulations (see Clauses 4.1(c) and 4.3).

"Digital Certificate 1" means the PKI digital certificate used to authenticate each SWIFT PDS payment passing between a particular Sender and the Framework Participant to which that payment is addressed. [24]

"Digital Certificate 2" means the PKI digital certificate used to authenticate each payment passing, via the SWIFT FIN-Copy Service, between a particular Sender and the CSI or between the CSI and a particular Framework Participant to which the payment is addressed. **[25]**

"Disabling Event" means**:[26]**

(a) processing, communications or other failure of a technical nature;

(b) inaccessibility (total or partial) to facilities by means of which payments are sent and received; or

(c) manifestation of industrial action,

which affects, or may affect, the ability of any Framework Participant to participate to the normal and usual extent in sending and receiving payments.

"Eligible Payment" means a Payment where both the Sender and Receiver have agreed to operate in the Evening Settlement Session.[27]

"Error of Magnitude" means an error (or a series of errors on the one exchange) of or exceeding $2 million or such other amount as may be determined from time to time by the Management Committee.[28]

"ESA" means Exchange Settlement Account.

---

[23] Inserted effective 14/11/22, version 041 r&p 001.22
[24] Inserted effective 31/10/07, version 024 r&p 004.07
[25] Inserted effective 31/10/07, version 024 r&p 004.07
[26] Last amended effective 1/1/18, version 037 r&p 001.17
[27] Inserted effective 1/7/02, version 006 r&p 002.02
[28] Last amended effective 16/1/09, version 027 r&p 005.08

"ESCA" [Deleted][29]

"ESCA plus NIBO Limit" [Deleted][30]

"ESR" means the interest rate payable by the Reserve Bank of Australia on overnight credit balances of Exchange Settlement Accounts. [31]

"Evening Settlement Session" has the meaning given to that term in Clause 4.1(c).[32]

"Exchange Settlement Account" (**"ESA"**) means an exchange settlement account, or similar account, maintained by a Framework Participant with the Reserve Bank of Australia.

"Exchange Settlement Cash Account" ("ESCA") [Deleted][33]

"Exchange Settlement Funds" has the meaning given in the RITS Regulations.

"Exchange Summary Form" means a summary document substantially in the form of Appendix Gin the format prescribed by the Reserve Bank of Australia. [34]

"Exchange Summary Data File Transfer Facility" [Deleted][35]

"Failure To Match Rules" means the rules set out in clause 9.32.[36]

"Fallback Period" means either a HVCS Fallback Period and/or a Participant Fallback Period, as applicable, declared by the Chief Executive Officer as set out in the Contingency Instructions.[37]

"Fallback Settlement" means, in relation to a Fallback Period, the deferred net settlement of HVCS obligations exchanged during the Fallback Period that is effected in accordance with the Contingency Instructions.[38]

"Fallback Solution" means either the HVCS Fallback Solution and/or the Participant Fallback Solution, as applicable. [39]

"Framework Participant" means a body corporate which in accordance with the Regulations is a participant in the HVCS and which is permitted, in accordance with the Regulations and these Procedures, to use the SWIFT PDS.[40]

---

[29] Deleted effective 20/11/06, version 021 r&p 003.06
[30] Deleted effective 20/11/06, version 021 r&p 003.06
[31] Last amended effective 13/6/01, version 002 r&p 004.01
[32] Inserted effective 01/7/02, version 006 r&p 002.02
[33] Deleted effective 20/11/06, version 021 r&p 003.06
[34] Last amended effective 19/7/21, version 039 r&p 001.21
[35] Deleted effective 23/4/13, version 033 r&p 001.13
[36] Last amended effective 13/11/13, version 034 r&p 001.14
[37] Last amended effective 19/7/21, version 039 r&p 001.21
[38] Amended effective 19/7/21, version 039 r&p 001.21
[39] Inserted effective 19/7/21, version 039 r&p 001.21
[40] Inserted effective 1/7/14, version 034 r&p 001.14

"Future Dated Payment" means any payment entered into the SWIFT PDS in advance of the value date for the payment.

"High Value Clearing System" ("CS4") means the framework of systems and procedures contained in the Regulations for the purpose of co-ordinating, facilitating and protecting the conduct and exchange of AusPayNet PDS payments among Framework Participants and all aspects of the related clearing cycle.

"HSM" means Hardware Security Module: A hardened, tamper-resistant device used for safe storage, generation and management of digital keys.[41]

"HVCS" means High Value Clearing System (CS4).

"HVCS Bilateral Clearing Form" in relation to a Participant Fallback Period, means a form in the format prescribed by the Company that an Affected Participant uses to send HVCS payments to another Framework Participant.[42]

"HVCS Contingency Instructions" means the HVCS contingency instructions set out in Appendix J.[43]

"HVCS Exchange Figures Advice" in relation to a HVCS Fallback Period, means a summary document (provisional or final), issued by and in a format prescribed by the Reserve Bank of Australia, showing the net obligations between a Framework Participant and the other Framework Participants, as calculated by the Reserve Bank of Australia using data received from Framework Participants in the HVCS Exchange Summary Form. [44]

"HVCS Fallback Period" means a period declared by the Chief Executive Officer to be a HVCS Fallback Period under Clause 9.28(a) to authorise the use of the HVCS Fallback Solution as the method for clearing and settlement of HVCS payments during a RITS Outage.[45]

"HVCS Fallback Solution" means the method used for clearing and settlement of HVCS payments during a HVCS Fallback Period that is outlined in Section 3.1 of the HVCS Contingency Instructions.[46]

"In-Flight" in relation to a HVCS Fallback Period, means payments that are stored in the SWIFT FIN Y Copy Service pending a settlement response from RITS when a RITS Outage occurs.[47]

"Interim Session" has the meaning given to that term in Clause 4.1(c).[48]

[41] Amended effective 26/11/18, version 038 r&p 001.18
[42] Inserted effective 19/7/21, version 039 r&p 001.21
[43] Inserted effective 19/7/21, version 039 r&p 001.21
[44] Inserted effective 19/7/21, version 039 r&p 001.21
[45] Inserted effective 19/7/21, version 039 r&p 001.21
[46] Inserted effective 19/7/21, version 039 r&p 001.21
[47] Inserted effective 19/7/21, version 039 r&p 001.21
[48] Last amended effective 1/1/18, version 037 r&p 001.17

"Inter-organisation Compensation Rules" means the document (as amended or replaced) known as the Inter-organisation Compensation Rules, Publication No. 6.1 of the Company.[49]

"MAC" [Deleted][50]
"Management Committee" means the committee constituted pursuant to Part 7 of the Regulations.

"Message Authentication Code" ("MAC") [Deleted][51]

"Morning Settlement Session" has the meaning given to that term in the RITS Regulations (see Clauses 4.1(c) and 4.3).

"NAK" means Negative Acknowledgment.

"Negative Acknowledgment" (**"NAK"**) means a SWIFT advice, issued by SWIFT in response to the receipt of a message, advising that the message has been received by SWIFT and rejected on the basis that it has not met the necessary validation requirements.

"Net Clearing System Obligations Advice" in relation to a HVCS Fallback Period, means a summary document, issued by and in a format prescribed by the Reserve Bank of Australia that shows a Framework Participant's net obligation in the multilateral contingency batch for settlement in RITS, including clearing system interest.[52]

"Net Interbank Obligation" ("**NIBO**") [Deleted][53]

"**NIBO**" [Deleted][54]

"9.00am Settlement" means settlement of certain multilaterally netted payment obligations by debiting and crediting Exchange Settlement Accounts at or about 9.00am or at such other time as may be prescribed by the Reserve Bank of Australia.[55]

"9.00am Settlement Session" has the meaning given to that term in Clause 4.1(c).

"Non Eligible Payment" means a Payment where either the Sender or Receiver or both have not agreed to operate in the Evening Settlement Session.[56]

"PAC" [Deleted][57]

[49] Inserted effective 13/6/01, version 002 r&p 004.01
[50] Deleted effective 31/10/07, version 024 r&p 004.07
[51] Deleted effective 31/10/07, version 024 r&p 004.07
[52] Inserted effective 19/7/21, version 039 r&p 001.21
[53] Deleted effective 20/11/06, version 021 r&p 003.06
[54] Deleted effective 20/11/06, version 021 r&p 003.06
[55] Amended effective 23/4/13, version 033 r&p 001.13
[56] Inserted effective 01/7/02, version 006 r&p 002.02
[57] Deleted effective 31/10/07, version 024 r&p 004.07

"Participant Fallback Period" means a period declared by the Chief Executive Officer to be a Participant Fallback Period under Clause 9.28 to authorise the use of the Participant Fallback Solution as the method for clearing and settlement of HVCS payments during a Participant Outage.[58]

"Participant Fallback Solution" means the method for clearing and settlement of HVCS payments during a Participant Fallback Period that is outlined in Section 3.1 of the Contingency Instructions.[59]

"Participant Outage" means a period during which a Framework Participant experiences a Disabling Event which prevents that Framework Participant from sending HVCS payments in the normal way.[60]

"Participant Start Date" means, in relation to a Framework Participant, the date on and from which that member is entitled to use the SWIFT PDS to send and receive payments, being a date specified as such for that member by the Management Committee in accordance with the Regulations.

"Participating Member" [Deleted][61]

"Payment" means, in relation to an AusPayNet PDS, a payment submitted via that AusPayNet PDS for settlement in RITS. [62]

"Payments Operations" [Deleted][63]

"PPS" means the Payments Processor System which is hardware and software used to generate or process RITS SWIFT messages.[64]

"Primary Computer Site" means, in relation to each Framework Participant using the SWIFT PDS, all system configuration components necessary to ensure connection to the SWIFT PDS on a daily basis. For the avoidance of doubt, the system components which together comprise a "Primary Computer Site" need not be situated at the same physical location provided that, taken as a whole, those components satisfy the operational and security requirements of clauses 7.2 to 7.7 inclusive.[65]

"Proprietary Authentication Code" ("**PAC**") [Deleted][66]

"Real Time Gross Settlement" means, in respect of settlement of payment obligations in any particular settlement system, the processing and settlement of those payment obligations in that system in real time and on a gross (not net) basis.

[58] Inserted effective 19/7/21, version 039 r&p 001.21
[59] Inserted effective 19/7/21, version 039 r&p 001.21
[60] Inserted effective 19/7/21, version 039 r&p 001.21
[61] Deleted effective 1/7/14, version 034 r&p 001.14
[62] Last amended effective 1/1/18, version 037 r&p 001.17
[63] Deleted effective 14/11/22, version 041 r&p 001.22
[64] Last amended effective 1/1/18, version 037 r&p 001.17
[65] Last amended effective 23/4/98, version 001
[66] Deleted effective 31/10/07, version 024 r&p 004.07

"Receiver" means a Constitutional Corporation that receives Payments from another Framework Participant in accordance with the HVCS Regulations and Procedures once admitted into the HVCS. [67]

"Regulations" means the regulations for the HVCS as prescribed by the Company.

"Repair Routing Code BSB" means a BSB number, assigned in accordance with Clause 8.4 (See also Clause 4.9(a)).

"Reports Session" has the meaning given to that term in clause 4.1(a).[68]

"RITS" means the settlement system established and operated by the Reserve Bank of Australia for Real Time Gross Settlement and includes the Central SWIFT Interface. For the avoidance of doubt, references to RITS include that system when operating to effect settlement of Payments on a Real Time Gross Settlement basis and when otherwise operating to effect settlement of payments on a deferred net settlement basis.[69]

"RITS Cash Transfer" or **"Cash Transfer"** means the transfer of funds between Exchange Settlement Accounts undertaken using functionality provided by the Reserve Bank of Australia in the RITS User Interface and in accordance with the RITS Regulations.[70]

"RITS Outage" means a period during which the central site (RITS or CSI) is experiencing a Disabling Event that prevents RITS or CSI, as applicable, from effecting settlement of HVCS payments in the normal way.[71]

"RITS Regulations" means the regulations for RITS published from time to time by the Reserve Bank of Australia.[72]

"RITS User Handbook" means the user guides issued by the Reserve Bank of Australia in connection with the RITS Regulations.

"RITS User Interface" or **"RITS UI"** means the interface made available by the Reserve Bank of Australia through which RITS Members or the Reserve Bank of Australia may input, view and manage transactions; perform administration activities; view and download reports; and perform other ancillary actions within RITS, in accordance with the RITS Regulations.[73]

"SCI" means SWIFT Customer Interface, which means the systems and software supporting the messaging interface to the SWIFT Messaging Service.[74]

[67] Last amended effective 20/11/06, version 021 r&p 003.06
[68] Inserted effective 1/1/18, version 037 r&p 001.17
[69] Last amended effective 1/1/18, version 037 r&p 001.17
[70] Inserted effective 19/7/21, version 039 r&p 001.21
[71] Inserted effective 19/7/21, version 039 r&p 001.21
[72] Last amended effective 1/1/18, version 037 r&p 001.17
[73] Inserted effective 19/7/21, version 039 r&p 001.21
[74] Inserted effective 14/11/22, version 041 r&p 001.22

"Sender" means a Constitutional Corporation that sends Payments to another Framework Participant in accordance with the HVCS Regulations and Procedures once admitted into the HVCS.[75]

"Settlement Close Session" has the meaning given to that term in the RITS Regulations (see Clauses 4.1(a) and 4.3).

"Settlement Day" means a day on which Payments are processed in RITS as specified in, or in accordance with, the RITS Regulations.[76]

"Settlement Session" has the same meaning as in the RITS Regulations.

"SWIFT" means Society For Worldwide Interbank Financial Telecommunication s.c., having its registered address at Avenue Adéle, 1 B-1310 La Hulpe, Belgium.

"SWIFT Customer Security Controls Framework" means SWIFT's set of mandatory and advisory security controls for SWIFT Users as published by SWIFT from time to time.[77]

"SWIFT Customer Security Mandatory Controls Non-Compliance Form" means the form set out at the end of the Yearly Audit Compliance Certificate (Annexure A.2).[78]

"SWIFT FIN Service" means SWIFT's core message transport and processing service described in the SWIFT User Handbook.

"SWIFT FIN-Copy Service" means the service provided by SWIFT to Framework Participants pursuant to the SWIFT Service Agreement.

"SWIFT Network" means the proprietary telecommunication network and associated software owned and utilised by SWIFT to provide communications services to its users.

"SWIFT PDS" means the SWIFT FIN-Copy Service, operating, under normal circumstances, in Y-Mode, configured with Framework Participants' SCIs to meet the processing requirements of the HVCS, together with any ancillary SWIFT services provided in connection with the SWIFT FIN-Copy Service.[79]

"SWIFT PDS CUG" is the group of Framework Participants admitted to use the SWIFT PDS to send and receive payments.

"SWIFT PDS Log" means the record to be maintained by Framework Participants in accordance with Clause 7.24(e) of all system outages, changes to the SWIFT PDS configuration and system test details, which forms part of the Yearly Audit Compliance Certificate.

[75] Last amended effective 20/11/06, version 021 r&p 003.06
[76] Last amended effective 1/1/18, version 037 r&p 001.17
[77] Inserted effective 1/1/18, version 037 r&p 001.17
[78] Inserted effective 1/1/18, version 037 r&p 001.17
[79] Amended effective 14/11/22, version 041 r&p 001.22

"SWIFT PDS Operations Manager" means the person designated as such from time to time by the Chief Executive Officer.

"SWIFT PDS System" means, in relation to a Framework Participant using the SWIFT PDS, that member's own SCI, related software and ancillary equipment used to access the SWIFT PDS and process the sending and receipt of payment instructions.[80]

"SWIFT Secure Channel" means an online application provided by SWIFT, through which a Business Officer can instruct SWIFT to change to the FIN-Copy Service Mode.[81]

"SWIFT Service Agreement" means the agreement effective 16 December 1996 entitled Agreement between the Company and SWIFT for FIN-Copy Service Administration, pursuant to which SWIFT provides its FIN Copy Service to Framework Participants.

"SWIFT T-Copy" or **"T-Copy"** means one of the message copy modes in the SWIFT FIN-Copy Service under which a partial-copy of a payment message is copied to the CSI then forwarded directly to the Receiver without awaiting a settlement response from RITS.[82]

"SWIFT User" means a body corporate that has been granted the right to connect to the SWIFT Network in accordance with the terms and conditions set out in the by-laws of SWIFT and in the SWIFT User Handbook.

"SWIFT User Handbook" means the set of rules and procedures published from time to time by SWIFT (in whatever medium) as the "SWIFT User Handbook" governing use of SWIFT's services.

"System Administrator" means the person appointed by the Reserve Bank of Australia to supervise operation of RITS.[83]

"System Certification" means, in relation to an AusPayNet PDS, the initial certification by the Management Committee in accordance with Part 7 of these Procedures prior to that person being permitted to send and receive payments using that AusPayNet PDS.

"System Certification Checklist" means a checklist in the form of Annexure A.1 of these Procedures, to be used by Framework Participants in accordance with Part 7 of these Procedures to obtain System Certification.

"System Compliance Certificate" means a certificate issued pursuant to Clause 7.27(g) by the Management Committee to a Framework Participant which has successfully completed the process for System Certification.

[80] Amended effective 14/11/22, version 041 r&p 001.22
[81] Inserted effective 19/7/21, version 039 r&p 001.21
[82] Inserted effective 19/7/21, version 039 r&p 001.21
[83] Last amended effective 1/1/18, version 037 r&p 001.17

"System Queue" means the RITS Queue in which each Payment (other than a Warehoused Payment) is held pending processing in RITS prior to settlement.[84]

"Total National Transaction Value" means, in respect of an AusPayNet PDS, the aggregate value of all payments sent and received by all Framework Participants using that AusPayNet PDS. This aggregate value is determined using the statistical data collected for the purposes of and in accordance with Clause 7.9(a).[85]

"Transitional Member" [Deleted][86]

"Transitional Period" [Deleted][87]

"Uninterruptable Power Supply" ("**UPS**") means equipment or facilities which provide for the supply of a continuous source of electricity to the SCI, whether through the use of batteries, generators or any other suitable means, in the event of the loss of mains power.[88]

"UPS" means Uninterruptable Power Supply.

"Warehoused Payments" means Future Dated Payments received by RITS and held pending the due date when the payments are placed back in the System Queue for normal processing.[89]

"Yearly Audit Compliance Certificate" means a certificate in the form of that in Annexure A.2.

"Year" means a calendar year.

1.2 Interpretation

(a) In these Procedures:

(i) the word person includes a firm, a body corporate, an unincorporated association or an authority;

(ii) the singular includes the plural and vice versa;

(iii) a reference to a statute, code or the Corporations Law (or to a provision of a statute, code or the Corporations Law) means the statute, the code, the Corporations Law or the provision as modified or amended and in operation for the time being, or any statute, code or provision enacted in lieu thereof and includes any regulation or rule for the time being in force under the statute, the code, the Corporations Law or the provision; and a reference to a specific time means that time in Sydney unless the context requires otherwise.

[84] Last amended effective 1/1/18, version 037 r&p 001.17
[85] Last amended effective 23/4/98, version 001
[86] Deleted effective 20/11/06, version 021 r&p 003.06
[87] Deleted effective 20/11/06, version 021 r&p 003.06
[88] Amended effective 14/11/22, version 041 r&p 001.22
[89] Last amended effective 1/1/18, version 037 r&p 001.17

(b) Words defined in the Corporations Law have, unless the contrary intention appears, the same meaning in these Procedures.

(c) Words defined in the Regulations have, unless the contrary intention appears, the same meaning in these Procedures.

(d) These Procedures have been determined by the Management Committee and take effect on the date specified by the Chief Executive Officer pursuant to Regulation 1.2.

(e) Headings are inserted for convenience and do not affect the interpretation of these Procedures, Inconsistency with Articles or Regulations

(f) If a provision of the Regulations or these Procedures is inconsistent with a provision of the Articles, the provision of the Articles prevails.

(g) If a provision of these Procedures is inconsistent with a provision of the Regulations, the provision of the Regulations prevails.

1.3 Governing Law

These Procedures are to be interpreted in accordance with the same laws which govern the interpretation of the Articles.

1.4 Copyright

The next page is Part 2

PART 2 EFFECT

(a) These Procedures have the effect set out in Part 2 of the Regulations.

(b) The provisions of these Procedures apply to the Framework known or referred to as the domestic high value clearing system but only with respect to payment instructions sent and received electronically using the SWIFT PDS.

(c) The HVCS Procedures consist of two volumes:[90]

(i) This Volume 1, which applies to participation in the HVCS MT CUG; and

(ii) Volume 2, which applies to participation in the HVCS ISO 20022 CUG for the processing of MX messages.[91]

(d) Participation in the HVCS requires participation in both CUGs, and therefore adherence to both volumes of the Procedures. Neither volume can be relied upon in isolation. There is no hierarchy or precedence between the two volumes. Volume 1 applies to the processing of MT format messages. Volume 2 applies to the processing of MX messages. Both Volumes contain a Part 9 relating to contingency processing and associated contingency instructions in an annexure to each volume. Both sets of procedures and instructions must be considered together.[92]

(e) Whilst Volume 1 describes the full use of MT messages, MT messages may only be used in the HVCS MT CUG in one situation: by an intermediary to on-send the domestic leg of an inward cross border MT payment. Any other use of MT messages in the HVCS MT CUG is strictly prohibited and will be deemed a breach of the Procedures and dealt with accordingly. This constraint takes precedence over any other described usage in both volumes of the HVCS Procedures.[93]

The next page is Part 3

[90] Inserted effective 14/11/22, version 041 r&p 001.22
[91] Amended effective 23/9/24, version 044 r&p 001.24
[92] Amended effective 23/9/24, version 044 r&p 001.24
[93] Inserted effective 23/9/24, version 044 r&p 001.24

PART 3 PROCEDURES AND AMENDMENT

3.1 Conduct of Clearings

Pursuant to Regulation 11.1 and in addition to and subject to the Regulations, the sending and receipt of payment instructions by Framework Participants must comply with the applicable practices, procedures, standards and specifications contained in these Procedures.

3.2 Amendments

(a) These Procedures may be varied by the Management Committee in accordance with Regulation 11.3 and Clause 3.2(b) of these Procedures. Any variation to these Procedures must contain an editorial note setting out the effective date of such variation.

(b) Each Framework Participant must notify the Company of any changes to its contact points as specified in Annexure C.1, C.2 and C.3. The Chief Executive Officer may vary Annexure C.1, C.2 and C.3 in accordance with such notification without the need to obtain the approval of the Management Committee or any other person. A variation made by the Chief Executive Officer pursuant to this Clause 3.2(b) will, upon publication by the Company, be binding on that Framework Participant and each other Framework Participant.

3.3 Inconsistency With Other Applicable Rules and Regulations

(a) Some of the provisions of these Procedures refer to or reflect the requirements of SWIFT in relation to the SWIFT PDS or the requirements of the Reserve Bank of Australia in relation to RITS. Those requirements of SWIFT or the Reserve Bank of Australia might change from time to time.[94]

(b) Subject to this Clause 3.3(b), if any provision of these Procedures is inconsistent with any mandatory provision of the SWIFT User Handbook, the provision in the SWIFT User Handbook prevails to the extent of that inconsistency. However, any provision of these Procedures which:

(i) deals with the same subject as any provision of the SWIFT User Handbook, and

(ii) imposes on any Framework Participant more rigorous obligations in relation to that subject than does that provision of the SWIFT User Handbook, or removes or limits any discretion that may have been available under or in accordance with that provision of the SWIFT User Handbook in relation to that subject, or imposes additional obligations to those imposed by that provision of the SWIFT User Handbook in relation to that subject, and

[94] Last amended effective 1/1/18, version 037 r&p 001.17

(iii) can be performed without breaching that other provision of the SWIFT User Handbook, is not to be construed as inconsistent with, and accordingly prevails over, that other provision of the SWIFT User Handbook.

(c) Any provision of these Procedures which restates terms or conditions applicable to, or which otherwise covers, operation of RITS is included for information purposes only and is not, by virtue of these Procedures only, binding under these Procedures. Framework Participants should refer to the RITS Regulations for the terms and conditions of operation of RITS.[95]

(d) Framework Participants should, therefore, be conversant with the relevant provisions of both the SWIFT User Handbook and RITS Regulations.

The next page is Part 4

[95] Last amended effective 1/1/18, version 037 r&p 001.17

PART 4 GENERAL OPERATIONAL REQUIREMENTS

4.1 RITS Operating Day[96]

(a) The RITS operating day is made up of four distinct operating sessions plus three closed sessions to enable completion of 9.00am Settlement, preparation for the Evening Settlement Session and overnight processing. The usual times for the sessions are specified below, but the Reserve Bank may advise other times on any given day.[97]

(b) Future Dated Payments (see Warehoused Payments, Clause 5.12) received by RITS at any time during the operating day will, subject to appropriate checks, be processed and stored by RITS as Warehoused Payments. Future Dated Payments entered outside of RITS operating day will be held on the SWIFT PDS queue and forwarded to RITS on the next Business Day. *NB: See Clause 5.12, Future Dated Payments may only be entered in limited circumstances.*[98]

(c) Framework Participant processing arrangements for same day value payments during each of the operating sessions varies and details are set out below.[99]

(i) Morning Settlement Session – 7.30am to 8.45am Monday to Friday.[100]

(A) Framework Participants may use the Morning Settlement Session to fund their 9.00am Settlement position and prepare for the Daily Settlement Session. SWIFT PDS payments are not available during this period. Any SWIFT PDS payments initiated during this period for same day value will be verified, to ensure they meet all appropriate checks, and held on the System Queue until commencement of the Daily Settlement Session at which time they will be considered for settlement in the normal course.

(ii) 9.00am Settlement Session 8.45am to 9.15am Monday to Friday.

(A) Only RITS processing associated with the 9.00am Settlement will be undertaken during the 9.00am Settlement Session.[101]

(iii) Daily Settlement Session 9.15am to 4.30pm Monday to Friday.[102]

Framework Participants may initiate SWIFT PDS payments for same day value up until the close of the SWIFT PDS operating day in

[96] Last amended effective 1/1/18, version 037 r&p 001.17
[97] Last amended effective 1/1/18, version 037 r&p 001.17
[98] Last amended effective 1/1/18, version 037 r&p 001.17
[99] Last amended effective 23/4/98, version 001
[100] Last amended effective 3/6/99, version 005 r&p 055.99
[101] Last amended effective 1/1/18, version 037 r&p 001.17
[102] Last amended effective 13/7/01, version 003 r&p 005.01

accordance with Clause 4.2(a). However, RITS will continue to be available for RITS "bank to bank" transactions until the end of the Settlement Close Session.[103]

(iv) Settlement Close Session 4.30pm to 5.15pm Monday to Friday.[104]

(A) Framework Participants may continue to test and settle already queued SWIFT PDS payments, and may initiate new Eligible Payments, but no other new payments may be initiated.[105]

(B) It is expected that Framework Participants use reasonable endeavours to ensure that Non Eligible Payments remaining on the System Queue following closure of the Daily Settlement Session are settled. This will assist all Framework Participants in managing their end of day liquidity requirements.

(C) At the end of the Settlement Close Session, on completion of transaction testing, RITS will reject all unsettled Non Eligible Payments remaining on the System Queue using an Abort Notification (see Clause 5.16), including payments with a status of "Deferred".[106]

(v) Interim Session approximately 5.15pm to 5.25pm Monday to Friday.[107]

(A) No transaction processing occurs during the Interim Session. This session is designed to allow those Framework Participants, who have not agreed to participate in the Evening Settlement Session, to obtain end of day reports and finalise their day's work.108

(vi) Evening Settlement Session closure of the Interim Session (approximately 5.25pm) to 10.00pm or such later time as the Reserve Bank may prescribe from time to time Monday to Friday.[109]

(A) Input of SWIFT payments will cut-off prior to the end of the Evening Settlement Session, at 6.05pm / 7.05pm / 8.05pm *(refer clause 4.4(a)(i)). Eligible Payments remaining on the System Queue at 6.30pm / 7.30pm / 8.30pm will be rejected.[110]

[103] Last amended effective 1/1/18, version 037 r&p 001.17
[104] Last amended effective 13/7/01, version 003 r&p 005.01
[105] Inserted effective 1/1/18, version 037 r&p 001.17
[106] Last amended effective 1/1/18, version 037 r&p 001.17
[107] Last amended effective 1/1/18, version 037 r&p 001.17
[108] Inserted effective 1/7/02, version 006 r&p 002.02
[109] Last amended effective 1/1/18, version 037 r&p 001.17
[110] Last amended effective 11/11/13, version 034 r&p 001.14

(B) Those members that have agreed with the Reserve Bank of Australia to participate in the Evening Settlement Session must have sufficient front and back office staff available for efficient inter-bank dealings during the Evening Settlement Session. Framework Participants will be able to alter this agreement with the Reserve Bank of Australia in accordance with arrangements prescribed from time to time by the Reserve Bank of Australia.[111]

(vii) Reports Session 10.00pm to 10.30pm or such later time as the Reserve Bank may prescribe from time to time* (refer clause 4.4(a)(i)A) Monday to Friday.[112]

(A) No transaction processing occurs during the Reports Session. This session is designed to allow Framework Participants who have been operating in the Evening Settlement Session to obtain end of day reports and finalise their day's work. [113]

(B) RITS will issue "Time Period" advices throughout the day to those Framework Participants which have elected to receive them, advising those Framework Participants of the move to each new operational session, with the exception of the commencement of the 9.00am Settlement Session for which no advice will be issued.[114]

4.2 SWIFT PDS Operating Day

(a) SWIFT PDS operating hours for the sending of payments are:[115]

(i) 9.15am to 4.30pm Monday to Friday for the exchange of all applicable message types; and[116]

(ii) until 6.05pm / 7.05pm / 8.05pm* (refer clause 4.4(a)) for the exchange of MT202 and associated messages for those Framework Participants that have agreed to participate in the Evening Settlement Session.[117]

(iii) Framework Participants may initiate payments, for same day value, at any time during the SWIFT PDS operating hours specified in this Clause 4.2.

(iv) Following closure of the SWIFT PDS for the day, RITS will continue to accept same day value payments provided:[118]

[111] Inserted effective 1/7/02, version 006 r&p 002.02
[112] Last amended effective 1/1/18, version 037 r&p 001.17
[113] Last amended effective 1/1/18, version 037 r&p 001.17
[114] Last amended effective 1/1/18, version 037 r&p 001.17
[115] Last amended effective 23/4/98, version 001
[116] Last amended effective 1/07/02, version 006 r&p 002.02
[117] Last amended effective 20/6/05, version 017 r&p 003.05
[118] Last amended effective 1/1/18, version 037 r&p 001.17

(A) SWIFT has sent an Acknowledgment for that MT103 payment prior to 4.30pm;[119]

(B) SWIFT has sent an Acknowledgment for that MT202 payment prior to 4.30pm for Non Eligible Payments or prior to 6.05pm / 7.05pm / 8.05pm*(refer clause 4.4(a)) for Eligible Payments; and[120]

(C) the payment is received at RITS Queue prior to 4.30pm for Non Eligible Payments and prior to 6.05pm /7.05pm/ 8.05pm* (refer clause 4.4(a)) for Eligible Payments.[121]

(b) Framework Participants will need to consider RITS cut off arrangements in evaluating an appropriate internal cut-off time for sending SWIFT PDS payments.[122]

(c) All payments on RITS Queue during the Settlement Close Session, will be tested and either settled or queued depending upon the status of the payment and funds availability. Non Eligible Payments remaining on the System Queue once the Settlement Close Session has closed will be rejected.[123]

(d) Eligible Payments remaining on the System Queue at 6.30pm / 7.30pm / 8.30pm* (refer clause 4.4(a) will be rejected.[124]

(e) Future Dated Payments initiated on any particular Business Day after closure of the SWIFT PDS will be held on the SWIFT PDS queue pending despatch to RITS on the next Business Day.[125]

4.3 Extension of Normal Operating Hours

RITS operating hours may be extended or varied by the System Administrator for SWIFT PDS payments where normal operations have been adversely affected by extraordinary circumstances. The System Administrator will notify all Framework Participants of such extensions or varied operating hours. [126]

4.4 Core Business Hours

(a) For assessment of Framework Participants' SCI availability requirements, in accordance with Clause 7.24, RITS Core Business Hours are 9.15am to 5.15pm, Monday to Friday for those Framework Participants that are not participating in the Evening Settlement Session, and 9.15am to 6.30pm / 7.30pm / 8.30pm*(refer clause 4.4(a)(i)) for those Framework Participants that are participating in the Evening Settlement Session, for any day on

[119] Last amended effective 12/12/03, version 011 r&p 003.03
[120] Last amended effective 20/06/05, version 017 r&p 003.05
[121] Last amended effective 6/6/23, version 042 r&p 001.23
[122] Last amended effective 1/1/18, version 037 r&p 001.17
[123] Last amended effective 1/1/18, version 037 r&p 001.17
[124] Inserted effective 11/11/13, version 034 r&p 001.14
[125] Last amended effective 1/1/18, version 037 r&p 001.17
[126] Last amended effective 1/1/18, version 037 r&p 001.17

which RITS is operational.[127]

**NOTE in relation to processing times:*[128]

(i) Evening Settlement Session closure times and Reports Session start and closure times are determined with reference to Central European Time and Central European Summer Time and therefore will vary throughout the year.[129]

(ii) As a guide Central European Summer Time commences at the end of March and concludes at the end of October. Australian Eastern Summer Time usually commences at the beginning of October and concludes at the end of March. However, the relevant commencement and conclusion dates do not always coincide.[130]

(iii) The following table may assist Framework Participants in aligning processing times for summer time and normal time across the two time zones.[131]

(A) 10.00am CET = 8.00pm AEDT[132]

(B) 10.00am CEST = 6.00pm AEST[133]

(C) 10.00am CEST = 7.00pm AEDT[134]

(D) 10.00am CET = 7.00pm AEST[135]

(b) The closure times for the Evening Settlement Session may be varied by the Reserve Bank of Australia in consultation with AusPayNet. Any variation to the closure times for the Evening Settlement Session will result in variations to the start and closure times for the Reports Session.[136]

(c) The Reserve Bank of Australia will, where practicable, notify HVCS Framework Participants of any such variations in advance of the day(s) that those variations apply to.[137]

4.5 SCI Start Up Requirement[138]

(a) Framework Participants must be logged on to SWIFT PDS prior to 9.15am on each day that the SWIFT PDS is open for business and remain logged

[127] Last amended effective 14/11/22, version 041 r&p 001.22
[128] Inserted effective 1/7/02, version 006 r&p 002.02
[129] Last amended effective 1/1/18, version 037 r&p 001.17
[130] Last amended effective 1/1/18, version 037 r&p 001.17
[131] Inserted effective 1/7/02, version 006 r&p 002.02
[132] Last amended effective 1/1/18, version 037 r&p 001.17
[133] Last amended effective 1/1/18, version 037 r&p 001.17
[134] Last amended effective 1/1/18, version 037 r&p 001.17
[135] Last amended effective 1/1/18, version 037 r&p 001.17
[136] Last amended effective 1/1/18, version 037 r&p 001.17
[137] Inserted effective 18/11/02, version 009 r&p 006.02
[138] Amended effective 14/11/22, version 041 r&p 001.22

on for the entire operating day.

(b) If a Framework Participant:

(i) is unable to log its SCI on to SWIFT PDS for commencement of the Daily Settlement Session;[139]

(ii) experiences any technical or operational problem with its SCI during the then current Business Day; or[140]

(iii) experiences any technical problems with its Core PPS during the then current Business Day,[141]

(c) which prevents it from processing payments, the Framework Participant must advise details of the outage to the System Administrator (see Annexure C.1) as soon as possible, but no later than 30 minutes after that Framework Participant first became aware of the problem.

(d) Where it is considered the outage will be protracted the System Administrator will advise Framework Participants in accordance with Clause 9.7.

(e) Where a Framework Participant has advised details of a system outage in accordance with Clause 4.5(b) and the problem has subsequently been corrected, that Framework Participant must advise the System Administrator that the problem has been rectified and that the Framework Participant can resume normal processing. After receiving advice from a Framework Participant under this Clause 4.5(e), the System Administrator will immediately advise Framework Participants of the changed circumstances.

(f) Full details of all system outages, including the date/time, cause and duration of the problem must be recorded in the SWIFT PDS Log.

(g) Framework Participants experiencing difficulties with their Core PPS, rather than their SCI, must ensure that the SCI remains logged on to SWIFT for the entire Business Day to allow for the receipt of inward payments.[142]

(h) Full details of Contingency Procedures requirements are set out in PART 9 of these Procedures.

4.6 SCI Close Down[143]

Framework Participants must remain logged on to the SWIFT PDS on each Business Day on which RITS is operating until payments processing for the day has been completed. Once payment processing has been completed at the central site, those Framework Participants who have elected to receive Time

[139] Amended effective 14/11/22, version 041 r&p 001.22
[140] Amended effective 14/11/22, version 041 r&p 001.22
[141] Last amended effective 14/8/08, version 026 r&p 004.08
[142] Last amended effective 14/11/22, version 041 r&p 001.22
[143] Amended effective 14/11/22, version 041 r&p 001.22

Period Advices will receive a Time Period Advice from RITS, advising a change in operational state "RTGS System Queue Processing Complete".[144]

4.7 Holiday Arrangements

(a) The SWIFT PDS will be open for normal operations on any day on which RITS is operating. [145]

(b) An annual listing of days on which RITS will not be operating may be obtained from RITS using the AIF (see generally PART 6). Framework Participants wishing to utilise this service should refer to the RITS Regulations.[146]

(c) Framework Participants based in a location not experiencing a public holiday on a day on which RITS is closed will be unable to process payments for value that day. It will be a decision for individual Framework Participants as to whether they offer SWIFT PDS payment facilities on that day. Any payments to be sent on such a day will need to be entered as Future Dated Payments.[147]

4.8 SWIFT PDS BIC/BSB Data

(a) BIC/BSB particulars for Framework Participants will be recorded in the Company's "HVCS BIC/BSB Directory". The paper based version of the BIC/BSB Directory will list all SWIFT PDS BIC/BSB links both numerically, by BSB number, and alphabetically in Framework Participant order. Framework Participants' Repair Routing Code BSBs will be recorded alphabetically in Framework Participant order in a separate section of the Directory. File and Record Formats for the HVCS BIC/BSB Directory are set out in Annexure H.[148]

(b) A monthly BIC/BSB Update Report, listing all changes made to the BIC/BSB links since the last report, will also be available in electronic or paper form. File and Record Formats for the BIC/BSB Update Report are set out in Annexure H.

(c) If a Framework Participant operates multiple SWIFT PDS BICs, that member must advise the Company of details of each BSB linked to each BIC. If the volume of data is significant, details may be provided on computer diskette in the format set out in Annexure H.

(d) Each Framework Participant must advise the Company of any new BIC/BSB links or changes to its existing BIC/BSB details. New and amended BIC/BSB data will be activated for use within the SWIFT PDS from the effective date of the monthly amendment advice containing the changes in accordance with this Clause 4.8(b).

[144] Last amended effective 1/1/18, version 037 r&p 001.17
[145] Last amended effective 1/1/18, version 037 r&p 001.17
[146] Last amended effective 1/1/18, version 037 r&p 001.17
[147] Last amended effective 1/1/18, version 037 r&p 001.17
[148] Last amended effective 23/4/98, version 001

(e) The Company will provide Framework Participants with a monthly copy of the Directory or the Update Report in either electronic or paper form. To allow Framework Participants sufficient time to amend their own files AusPayNet will provide the Directory/Update Report to Framework Participants 14 days in advance of the effective date for the new version.

4.9 Repair Routing Code BSB Processing

(a) If a Framework Participant wants to send a payment and details of the intended Receiver are known but insufficient details are available to precisely identify the beneficiary's branch, that member may send the payment to that Receiver using that Receiver's Repair Routing Code BSB (see Clause 8.4). Use of the Repair Routing Code BSB informs the Receiver that the particulars of the payment are incomplete and that manual intervention is required.

(b) The Sender may only forward the payment to the intended Receiver using that Receiver's Repair Routing Code BSB, after it has reasonably decided that it is impracticable to contact the originator of the payment to clarify beneficiary details.

(c) Where the Receiver is unable to apply any payment sent to it in accordance with this Clause 4.9, the Receiver must return the payment to the Sender in accordance with Clause 4.15.

(d) Any apparent abuse of the Repair Routing Code BSB facility should immediately be brought to the attention of the Framework Participant in question, so that corrective action can be implemented.

(e) Continual abuse of the repair facility should be reported to the Management Committee which may take such action as it considers necessary to prevent that abuse continuing so as to protect the efficiency of the HVCS.

4.10 SWIFT PDS Log

(a) Framework Participants must maintain a SWIFT PDS Log in which they will record details of all:[149]

(i) system outages and the time required to re-establish live operations (Clause 4.5(b));

(ii) alterations to their Primary and Backup Computer Site system configurations (Clause 7.2(a), 7.12(a) and 7.13(a));

(iii) the date, time, duration and results of Backup Computer Site testing (Clause 7.19); and

[149] Last amended effective 23/4/98, version 001

(iv) the date, time, duration, and percentages of all reportable instances of degraded SCI performance (Clause 7.25), and the cause and remedy (if known).[150]

(b) Data from the SWIFT PDS Log will form the basis of Framework Participants' responses to selected segments of the Yearly Audit Compliance Certificate (see Annexure A.2).

4.11 Central Site Automated Information Facility Destination Code

(a) The RITS Central Site SWIFT destination code for Automated Information Facility messages (Commands, Enquires and Unsolicited messages) is RSBKAUSR. Framework Participants utilising the service must ensure that Automated Information Facility messages forwarded to RITS record the above mentioned destination code.[151]

(b) Full details regarding RITS Automated Information Facility are contained in the RITS Regulations.[152]

4.12 Rules Governing Compensation Claims

(a) Any claims among Framework Participants for compensation for which provision is made in this PART 4 in respect of payments in the HVCS, must be made in accordance with the Inter-organisation Compensation Rules, to the extent applicable, unless the Framework Participants which are parties to a particular compensation claim agree (on a case by case basis) to alternative compensation arrangements in respect of that particular claim.[153]

(b) Each Framework Participant must nominate, in writing, to the Company a compensation contact point for the purposes of the Inter-organisation Compensation Rules. Full details of any compensation claim made in accordance with the Inter-organisation Compensation Rules must be provided to the relevant Framework Participant's nominated compensation contact point as set out in Annexure C.3. Framework Participants must promptly notify the Company in writing of any changes in the contact details of their compensation contact points not less than 5 business days prior to such changes taking effect, clearly identifying the effective date in their advice.[154]

4.13 Disputes Relating to Compensation Claims

If the Framework Participants concerned are unable to agree upon any matter arising in connection with a claim for compensation in respect of a payment in the HVCS, the provisions of Part 13 of the Regulations will apply to resolution of that disagreement.[155]

---

[150] Inserted effective 1/1/22, version 040 r&p 003.21
[151] Last amended effective 1/1/18, version 037 r&p 001.17
[152] Last amended effective 1/1/18, version 037 r&p 001.17
[153] Last amended effective 13/06/01, version 002 r&p 004.01
[154] Amended effective 1/1/12, version 032 r&p 001.12
[155] Last amended effective 13/6/01, version 002 r&p 004.01

4.14 Request for Return of a Settled Payment Sent in Error

(a) Where a Framework Participant decides (for whatever reason) that a previously settled Payment was sent in error, it may request return of that Payment from the Receiver using a SWIFT Request For Cancellation message (MT192 or MT292).

(b) Payments settled across RITS are irrevocable and accordingly any decision to return a Payment in response to a request to do so under this Clause 4.14(a) rests with the Receiver. The Receiver is under no obligation under these Procedures to return a settled Payment.[156]

(c) Where the Receiver agrees in accordance with Clause 4.14(a) to return any payment or otherwise returns the payment in accordance with Clause 4.16, it must return the funds to the Sender using the same message type as the original payment order. In general, the contents of block 4 (message text) of the original payment order should be returned unaltered. However, due to the processing requirements of RITS and the need to identify these payments as returned payments, some fields will need to be changed. These are:[157]

(i) Field 20, this field should contain a new transaction reference number which is unique to the Framework Participant returning the payment.

(ii) Field 32A, if the payment is returned on a day other than the day on which it was received, this field must be changed to show the value date as the date o return, otherwise the payment will be rejected by RITS.[158]

(iii) Field 72, the original contents of this field must be deleted and replaced with the appropriate SWIFT codeword, as set out in the SWIFT User Handbook, plus reason codes and the transaction reference number of the original returned payment order.

(d) Refer Annexure D Message Content for additional information regarding field usage for returned payments.

(e) Where funds are returned in accordance with Clause 4.14(c), on any day after the value date of the original payment, the Sender may request compensation from the Receiver, for the Receiver's use of the funds.

(f) On receipt of a claim in accordance with this Clause 4.14(e), the Receiver is obliged to pay compensation in accordance with Clause 4.12(a), subject to refusal justifiable on legally sustainable grounds.

[156] Last amended effective 1/1/18, version 037 r&p 001.17
[157] Last amended effective 1/1/18, version 037 r&p 001.17
[158] Last amended effective 1/1/18, version 037 r&p 001.17

4.15 Receiver Unable to Apply Payment

(a) The procedures in Clauses 4.15(a) to 4.15(g) inclusive apply where the Receiver is unable to apply an inward payment due to incorrect or incomplete beneficiary information.[159]

(b) In such cases the payment must be returned:

(i) within four hours of receipt of the original payment message; or

(ii) if the Receiver is unable to return the payment within that four hour period because of end of day closure of RITS, within four hours after the commencement of the next Business Day's Daily Settlement Session (see also Clause 4.15(e)).[160]

(c) If the Receiver must return any payment to the Sender under Clause 4.15(a), the Receiver must use the same message type as used for the original payment order. In general, the contents of block 4 (message text) of the original payment order should be returned unaltered. However, due to the processing requirements of RITS and the need to identify these payments as returned payments, some fields will need to be changed. These are:[161]

(i) Field 20, this field should contain a new transaction reference number which is unique to the Framework Participant returning the payment.

(ii) Field 32A, if the payment is returned on a day other than the day on which it was received, this field must be changed to show the value date as the date of return, otherwise the payment will be rejected by RITS.[162]

(iii) Field 72, the original contents of this field must be deleted and replaced with the appropriate SWIFT codeword, as set out in the SWIFT User Handbook, plus reason codes and the transaction reference number of the original returned payment order.

(d) Refer Annexure D Message Content for additional information regarding field usage for rejected payments.

(e) Where the Receiver is unable under Clause 4.15(a) to return a payment on the day of receipt of it, the Sender is entitled to compensation in accordance with Clause 4.12(a) for the Receiver's use of the funds.[163]

(f) On receipt of a claim in accordance with this Clause 4.15(e), the Receiver is required to pay the relevant compensation, subject to refusal justifiable on legally sustainable grounds.

(g) Any apparent breach of Clause 4.15(a), should immediately be brought to

[159] Last amended effective 13/6/01, version 002 r&p 004.01
[160] Last amended effective 1/1/18, version 037 r&p 001.17
[161] Last amended effective 1/1/18, version 037 r&p 001.17
[162] Last amended effective 1/1/18, version 037 r&p 001.17
[163] Last amended effective 13/6/01, version 002 r&p 004.01

the attention of the Framework Participant concerned, so that corrective action can be taken by that member.[164]

(h) Continual breaches of Clause 4.15(a) by the same Framework Participant should be reported to the Management Committee.

(Note: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) imposes pre-conditions which must be satisfied before financial institutions may initiate, pass on or take any other action to carry out electronic funds transfers instructions. Please refer to Part 5 of the Act for details.)[165]

4.16 Incorrectly Applied Items

(a) Where it is ascertained by either the Sender or the Receiver that a payment has been misapplied, including where it has been applied to an account other than that of the intended beneficiary because the Sender transmitted incorrect account number details on which the Receiver relied (see Clause 4.17(a), the Receiver must on becoming aware of the error endeavour to promptly reverse that payment from the account to which it has been applied and apply the funds to the intended account, if known, or if not known, return the funds to the Sender in accordance with Clause 4.14(c).[166]

Note: It is up to the Receiver to determine whether and how Customers are to be notified or prior authorisation obtained in relation to the reversals of incorrectly applied items.

Any notification of, or other arrangements with Customers, regarding the reversal of a misapplied payment beyond any obligation otherwise imposed on the Receiver by statute, common law or these Procedures, is a proprietary matter for the Receiver.[167]

(b) If the Sender requests the Receiver to endeavour to reverse a payment in accordance with Clause 4.16 and the payment is reversed, but it is subsequently ascertained that the original payment was not misapplied and ought not have been reversed, then as between the Sender and Receiver the Sender bears responsibility and must indemnify the Receiver in respect of any damage or claim the Receiver may suffer arising because of the reversal of that payment.[168]

4.17 Processing by Account Number Only[169]

(a) If funds have been applied by the Receiver in accordance with the account number details provided by the Sender but the funds have been applied to the wrong account, then as between the Sender and Receiver, the Receiver is not liable to compensate the Sender, any person on whose behalf the Sender sends a payment, the intended beneficiary or any other person for

[164] Last amended effective 13/6/01, version 002 r&p 004.01
[165] Inserted effective 30/4/07, version 022 r&p 001.17
[166] Last amended effective 19/9/02, version 007 r&p 004.02
[167] Inserted effective 13/6/01, version 002 r&p 004.01
[168] Last amended effective 19/9/02, version 007 r&p 004.02
[169] Inserted effective 30/11/01, version 004 r&p 006.01

loss of such payment. In these circumstances, liability, if any, for compensating any person for temporary or permanent loss of such payment and for any other loss or damage which a person may suffer directly or indirectly in connection with the payment is the responsibility of the Sender. Receivers are entitled to rely solely on account number details in all circumstances, regardless whether any beneficiary name details are transmitted with the account number details or are otherwise known to the Receiver. Receivers are not obliged (including under any duty to the Sender which may but for this Clause 4.17(a) arise at law or in equity) to check whether account number details are correct. If a Receiver suffers loss or damage, or receives any claim for loss or damage, arising because the Receiver has relied solely on account number details provided by the Sender when processing a payment, the Sender must fully indemnify the Receiver in relation to such loss or damage or claim. [170]

(Notes:

1. *For the purpose of this Clause 4.17(a), account number details means the BSB number and account number or, in the case of a Receiver which has a unique account numbers system, the account number only.*[171]

2. *The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires that certain information must be included in electronic funds transfer instructions. Please refer to Part 5 of the Act for details.*[172]

3. *Beneficiary Details contained in Sequence B of the MT202COV variant are for information only and do not constitute payment instructions to the receiving Framework Participant.)*[173]

4.18 Requests for Back Valuation and Forward Valuation of Payments

(a) Where a payment is received after its due date because the Sender despatched it late, the Sender may request the Receiver to back value the payment. On receipt of a request under this Clause 4.18(a)to back value a payment, the Receiver must back value that payment, subject to refusal justifiable on legally sustainable grounds.[174]

(b) Where a payment is back valued under Clause 4.18(a), the Receiver is entitled to compensation from the Sender. [175]

(c) Where a payment is received before its due date because the Sender despatched it early, the Sender may request the Receiver to forward value the payment. On receipt of a request under this Clause 4.18(c) to forward value a payment, the Receiver must forward value that payment, subject to refusal justifiable on legally sustainable grounds.

[170] Inserted effective 30/11/01, version 004 r&p 006.01
[171] Last amended effective 21/11/09, version 029 r&p 003.09
[172] Last amended effective 21/11/09, version 029 r&p 003.09
[173] Inserted effective 21/11/09, version 029 r&p 003.09
[174] Last amended effective 13/6/01, version 002 r&p 004.01
[175] Last amended effective 13/6/01, version 002 r&p 004.01

(d) Where a payment is forward valued under Clause 4.18(c), the Sender is entitled to compensation from the Receiver.[176]

(e) Subject to Clause 4.12(a), a Framework Participant may claim compensation from another Framework Participant in any circumstance, additional to those set out in this PART 4, that is applicable to HVCS payments and is contemplated by the Inter-organisation Compensation Rules.[177]

The next page is Part 5

[176] Last amended effective 13/6/01, version 002 r&p 004.01
[177] Last amended effective 13/6/01, version 002 r&p 004.01

PART 5 SWIFT PDS CLOSED USER GROUP

5.1 Overview

(a) The SWIFT PDS CUG uses the facilities of the SWIFT FIN-Copy Service, designed to meet the needs of high value clearing systems internationally. The SWIFT FIN-Copy Service allows each country to configure its closed user group to meet its own specific requirements. AusPayNet has worked with SWIFT to configure the SWIFT PDS to meet the Australian domestic high value clearing needs of its members. For the SWIFT PDS CUG AusPayNet's SWIFT PDS configuration allows some variation from normal SWIFT messaging, to cater for RITS requirements. Details of SWIFT PDS CUG requirements are set out in this PART 5 and in Annexure D.[178]

(b) To use the SWIFT PDS to send and receive payments a Framework Participant must be a SWIFT User and must meet the mandatory security control objectives in the SWIFT Customer Security Controls Framework. [179]

5.2 SWIFT Membership

Each Applicant proposing to use the SWIFT PDS which is not a SWIFT User, should approach the SWIFT Regional Account Manager regarding SWIFT requirements to becoming a SWIFT User. The size and international nature of the SWIFT network requires that the connection of new SWIFT Users be carried out on set dates (March, June, September and December) each year. Because of this requirement and internal systems development by the Applicant, SWIFT advises that Applicants proposing to use the SWIFT PDS should allow at least 6 months to complete the SWIFT membership process.

5.3 SWIFT PDS Closed User Group Management

(a) The SWIFT PDS CUG will be administered by the Company. The Company will be responsible for certification pursuant to Clauses 7.27(a) to (j) inclusive, the daily operation of the SWIFT PDS CUG and the maintenance and implementation of the HVCS Regulations and Procedures applicable to the SWIFT PDS CUG.

(b) Applicants should contact the SWIFT PDS Operations Manager concerning requirements for HVCS membership and the requirements in relation to use of the SWIFT PDS. Copies of applicable SWIFT forms can be obtained from the Company by contacting the SWIFT PDS Operations Manager.[180]

5.4 SWIFT PDS CUG Membership Application - General

(a) Applicants proposing to use the SWIFT PDS will be required to complete the applicable SWIFT forms for SWIFT PDS CUG membership for test and

[178] Last amended effective 1/1/18, version 037 r&p 001.17
[179] Last amended effective 1/1/18, version 037 r&p 001.17
[180] Last amended effective 20/6/05, version 017 r&p 003.05

training and/or SWIFT PDS CUG membership for live operations (as the case may be).[181]

(b) Completed forms should be returned to the SWIFT PDS Operations Manager as the Company may be required to countersign the completed forms before on-sending them to SWIFT if the Applicant is to be admitted to the SWIFT PDS CUG.[182]

5.5 SWIFT PDS CUG Membership Application for Test and Training

(a) As part of their overall SWIFT PDS System development, Applicants should ensure that they apply for membership of the SWIFT PDS CUG for test and training purposes in sufficient time to ensure their system will be available for proprietary testing. A minimum of 21 days should be allowed for processing the application and inclusion of the Applicant's details in the SWIFT PDS CUG records.

(b) As specified in Clause 5.4(a) Applicants must complete the applicable SWIFT forms for SWIFT PDS CUG membership for test and training and forward them to the Company's SWIFT PDS Operations Manager. If the Applicant is to be admitted to the SWIFT PDS CUG for test and training purposes, the Company will countersign the completed forms and forward them to SWIFT. SWIFT will then update the SWIFT PDS CUG test and training records using the Applicants' details on those forms. [183]

(c) After receipt of advice from SWIFT, the Company will inform the Applicant when SWIFT PDS CUG records have been updated and the date from which the Applicant can commence test and training in the SWIFT PDS CUG.

5.6 SWIFT PDS CUG Membership Application for Live Operations

(a) As part of the System Certification process set out in Clause 7.27(a), each Applicant must complete the applicable SWIFT forms for SWIFT PDS CUG membership for live operations, and attach the completed form to the System Certification Checklist which is to be forwarded to the Company in accordance with Clause 7.27(d).[184]

(b) Where the Applicant's application for System Certification is successful the Company will, following Management Committee's approval in accordance with Regulation 5.5, forward the completed forms to SWIFT. SWIFT will then update the SWIFT PDS CUG live operations records using the Applicants' details on that form. [185]

(c) The Secretary will, in accordance with Regulation 5.7, advise the Applicant of the date on which the Applicant may commence participation in SWIFT PDS.

[181] Last amended effective 20/6/05, version 017 r&p 003.05
[182] Last amended effective 20/6/05, version 017 r&p 003.05
[183] Last amended effective 20/6/05, version 017 r&p 003.05
[184] Last amended effective 20/6/05, version 017 r&p 003.05
[185] Last amended effective 20/6/05, version 017 r&p 003.05

5.7 Amendment of Framework Participant SWIFT PDS CUG Details

(a) Any Framework Participant wishing to amend its SWIFT PDS CUG details must complete the applicable SWIFT form and forward the form to the Company's SWIFT PDS Operations Manager. If the Company approves that amendment it will countersign the form and then forward it to SWIFT.[186]

(b) The Company will advise the Framework Participant concerned when that amendment has been carried out.

5.8 HVCS Suspension/Withdrawal of a Framework Participant[187]

(a) Where a Framework Participant's membership of HVCS is terminated pursuant to Regulation 5.17 or is suspended pursuant to Regulation 5.10, this will result in termination of the Framework Participant's membership to the SWIFT PDS CUG and require reapplication to the SWIFT PDS CUG. The Company will immediately advise SWIFT of the change to the SWIFT PDS CUG membership.[188]

(b) SWIFT will confirm receipt of the request, with a further advice confirming removal of applicant data from the SWIFT PDS CUG.[189]

5.9 HVCS Framework Participant Re-entry[190]

(a) Where the Company revokes a Framework Participant's suspension in terms of Regulation 5.16, it must immediately advise SWIFT of the reinstatement of the member.[191]

(b) SWIFT will confirm receipt of the request, with a further advice confirming successful implementation of applicant data and such Framework Participant may reapply to the SWIFT PDS CUG.[192]

5.10 Bank Identifier Code (BIC)

(a) Framework Participants must have a current SWIFT BIC. Framework Participants can define multiple BICs for use within the SWIFT PDS.

(b) Where a Framework Participant chooses to implement multiple BICs it must advise the Company of full details of the BSBs attached to each BIC in accordance with Clause 4.8(c).

[186] Last amended effective 20/6/05, version 017 r&p 003.05
[187] Amended effective 14/11/22, version 041 r&p 001.22
[188] Last amended effective 14/11/22, version 041 r&p 001.22
[189] Last amended effective 14/11/22, version 041 r&p 001.22
[190] Amended effective 14/11/22, version 041 r&p 001.22
[191] Last amended effective 14/11/22, version 041 r&p 001.22
[192] Last amended effective 14/11/22, version 041 r&p 001.22

5.11 Valid SWIFT PDS Payment Messages[193]

(a) Two kinds of payment messages have been authorised for use in the SWIFT PDS CUG:[194]

(i) MT103 Single Customer Credit Transfer; and[195]

(ii) MT202 General Financial Institution Transfer.

(b) Framework Participants must ensure that all SWIFT PDS CUG payment messages contain the FIN-Copy Service Identifier "PDS" in Field 103, in accordance with Clause 8.6(a).

(c) The MT103+ variation of the MT103 Single Customer Credit Transfer will be an allowable message type within the SWIFT PDS CUG. The MT103+ is distinguished from the MT103 by the use of the code "STP" in the validation flag field (message tag 119) within the user header block (block 3).[196]

(d) The MT202COV variation of the MT202 General Financial Transfer will be an allowable message type within the SWIFT PDS CUG. The MT202COV is distinguished from the MT202 by the use of the code "COV" in the validation flag field (message tag 119) within the user header block (block 3). Beneficiary details contained in sequence B of the MT202COV are for information only and do not constitute payment instructions to the receiving Framework Participant.[197]

(e) Each Framework Participant is responsible for ensuring that payment messages, including usage and content of fields in those messages, conform to the specifications set out in Annexure D.

(Note: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires that certain information must be included in electronic funds transfer instructions. Please Refer to Part 5 of the Act for details.)[198]

5.12 Warehoused Payments

(a) Framework Participants may enter any payment (as a Future Dated Payment) into the SWIFT PDS System provided the value date for that payment is the next Business Day. RITS determines the value date from the "Value Date" contained within Field 32A of the payment message.[199]

(b) Future Dated Payments will be held in the SWIFT PDS queue and forwarded to RITS on the next Business Day.[200]

---

[193] Last amended effective 12/12/03, version 011 r&p 003.03
[194] Last amended effective 19/11/01, version 004 r&p 006.01
[195] Inserted effective 19/11/01, version 004 r&p 006.01
[196] Inserted effective 19/11/01, version 004 r&p 006.01
[197] Last amended effective 21/11/09, version 029 r&p 003.09
[198] Inserted effective 30/4/07, version 022 r&p 001.17
[199] Last amended effective 1/1/18, version 037 r&p 001.17
[200] Last amended effective 1/1/18, version 037 r&p 001.17

(c) To assist Framework Participants assess liquidity requirements for the day participants may use RITS to view their own Warehoused Payments, both inward and outward (excluding inward SWIFT PDS Payments with a status of deferred) due for settlement that day, from 7.00am on. With commencement of the Daily Settlement Session (9.15am) the Payments will be placed on the System Queue and processed in the normal manner.[201]

(d) Framework Participants can recall Warehoused Payments utilising a Recall Request, full details of which are available in the RITS Regulations.

5.13 Recall Request

Where a SWIFT PDS payment is held on the RITS Queue or is a Warehoused Payment the Sender may seek return of the payment by issuing a Recall Request. Full details of the Recall Request (Message Based Command) procedure are available in the RITS Regulations.[202]

5.14 Out of Hours Payments

(a) Payments sent "for value today" but despatched to RITS after normal RITS operating hours, on any particular Business Day, will be acknowledged (ACKed) by the SWIFT Fin-Copy Service and held in the SWIFT FIN-Copy queue pending opening of RITS on the next Business Day. As the value date will no longer be valid the payment will be rejected by RITS and the SWIFT FIN-Copy Service will advise details of the rejection to the Sender.[203]

(b) Payments sent "for value today" but despatched to RITS, on any particular Business Day, before RITS operating hours will be acknowledged (ACKed) by the SWIFT FIN-Copy Service and held in the SWIFT FIN-Copy queue pending opening of RITS on that Business day.[204]

5.15 Sender Notification (MT012)

On the successful settlement of a Payment, RITS will send settlement details to SWIFT FIN-Copy which will forward a Sender Notification (MT012) to the Sender advising full details of the settlement, including the Sender's ESA balance following settlement of the Payment.[205]

5.16 Abort Notification (MT019)

(a) When RITS is unable to process a payment it will send details of rejection of that payment to SWIFT FIN-Copy, which will forward an Abort Notification (MT019) to the Sender advising the reason for the rejection.[206]

(b) On closure of the Settlement Close Session, RITS will automatically reject each payment remaining on the System Queue and send details of that

[201] Last amended effective 1/1/18, version 037 r&p 001.17
[202] Last amended effective 1/1/18, version 037 r&p 001.17
[203] Last amended effective 1/1/18, version 037 r&p 001.17
[204] Last amended effective 1/1/18, version 037 r&p 001.17
[205] Last amended effective 1/1/18, version 037 r&p 001.17
[206] Last amended effective 1/1/18, version 037 r&p 001.17

rejection to SWIFT FIN-Copy, which will forward an Abort Notification (MT019) to the Sender advising the reason for the rejection.[207]

5.17 Receiver Payment Order (MT103/MT202 and variants)[208]

(a) On advice from RITS, of the successful settlement of a Payment, SWIFT FIN-Copy will identify the original payment message, add the settlement information (time of settlement and the ESA balance following settlement of the Payment) in Field 115, and forward the original Payment with the additional settlement particulars to the Receiver (using MT103, MT202 or their respective variants as appropriate).[209]

(b) A more detailed description of the SWIFT FIN-Copy message process is contained in Annexure D.[210]

5.18 Undelivered Message Reports

(a) The following standard SWIFT reports are issued in response to a Framework Participant's request for information concerning undelivered SWIFT FIN and SWIFT FIN-Copy messages.

(i) Solicited Undelivered Message Report (MT066) issued in response to a MT046;

(ii) Undelivered Message Report at a Fixed Hour (MT082) issued in response to a MT044; and

(iii) Undelivered Message Report at Cut-off Time (MT083) issued in response to a MT044.

(b) Where the report is dealing with FIN-Copy messages, details of fields 431 (Message Status) and 103 (Service Code) will be present in the report. Full details regarding the above reports are available from the FIN System Messages module of the SWIFT User Handbook.

5.19 Delivery Notifications

Although not part of the standard SWIFT PDS service, the Sender can specify on an individual payment basis, whether they require advice of delivery ("Delivery Notification") or a non-delivery warning ("Non-Delivery Warning"). These advices relate to the delivery or non-delivery of the payment to the Receiver and will be delivered via the SWIFT FIN Service. Normal SWIFT fees will apply for the provision of Non-Delivery Warning (MT010) and Delivery Notification (MT011) messages.

5.20 Conditional Payments

Normal SWIFT procedures as set out in the SWIFT User Handbook will apply in

[207] Last amended effective 1/1/18, version 037 r&p 001.17
[208] Last amended effective 1/1/18, version 037 r&p 001.17
[209] Last amended effective 21/11/09, version 029 r&p 003.09
[210] Last amended effective 21/11/09, version 029 r&p 003.09

relation to payments containing approved SWIFT codes in Field 72, such as "/HOLD/" for a payment requiring identification before completion.

5.21 SWIFT CUG Fees

(a) The SWIFT fee for payments processed across the CUG, has three components:

(i) a Domestic FIN Message Charge;

(ii) a Sender Notification Charge; and

(iii) a FIN-Copy Supplement Charge.

(b) The actual SWIFT charges will vary from time to time and Framework Participants will be advised, by SWIFT, of any changes to the CUG fee structure.

(c) SWIFT CUG fees will be invoiced as part of the normal SWIFT fee cycle.

5.22 SWIFT Archival Arrangements

SWIFT archives all sent and received messages and their associated input and delivery history for the past 123 days. Framework Participants can obtain copies of the data by instituting either a Retrieval Request (Text and History - MT020) or a Retrieval Request (History - MT022). Both messages include the Message Status (Field 431), recording the status of the original message which is being retrieved.

5.23 SWIFT Approval Standards Amendments

(a) SWIFT operates under strict change control procedures. Amendments to the SWIFT applications normally are introduced once a year, usually in November. SWIFT publishes throughout each year several versions of its "Advance Information Standards Release Guide" advising full details of the forthcoming changes to the SWIFT FIN Service standards. The first version of the Advance Information Standards Release Guide is normally issued in or around January each year. That guide also specifies the date on which the amended standards are to be introduced, although, particularly in the early stages, it is subject to change.

(b) If the yearly changes to SWIFT standards directly affect the SWIFT PDS, the Management Committee will advise Framework Participants of these changes and details of action required by Framework Participants.

(c) Each Framework Participant must implement changes to that member's SWIFT PDS System in accordance with the Advance Standards Release Guide. Such changes will be reviewed when the Company reviews that member's Yearly Audit Compliance Certificate (see Clause 7.28(a)).

5.24 Requests by Framework Participants for SWIFT PDS Amendments

(a) If a Framework Participant wishes to propose an amendment to the existing SWIFT PDS configuration, that member should submit details of the proposal to the Company using a Change Request Form (see Annexure F), and forward the completed form to the Secretary. The details may be submitted by e-mail, using an electronic version of Annexure F (saved as a rich text format attachment).[211]

(b) The Secretary will acknowledge receipt of the completed Change Request Form and arrange for details to be provided to the Management Committee, which must consider the proposal as soon as reasonably practicable.

(c) The Secretary will advise details of the Management Committee's decision to the Framework Participant which submitted the relevant Change Request Form.

5.25 SWIFT Customer Support Centre

Normal SWIFT Customer Support Centre facilities will be available should Framework Participants experience difficulties with the SWIFT system, in accordance with the SWIFT User Handbook.

The next page is Part 6

[211] Last amended effective 30/09/02, version 008 r&p 005.02

PART 6 AUTOMATED INFORMATION FACILITY

6.1 AIF Availability

(a) RITS allows Framework Participants the scope to implement a variety of Credit and Liquidity Management mechanisms and has provided a number of Command and Enquiry options to assist Framework Participants in this regard. A full range of Commands and Enquiries is available on RITS. However, for those Framework Participants which wish to automate their payments processing, a sub-set of Commands and Enquiries is available via the SWIFT FIN service utilising RITS Automated Information Facility (AIF).[212]

(b) The availability of separate Credit (Credit Status) and Liquidity (ESA Status) controls, allows Framework Participant's payment areas to release payments to the System Queue independently of any decision by that member's Credit and Liquidity areas. Each Framework Participant must decide whether it will utilise the AIF and, if so, where within its organisation these facilities would be best administered.

(c) A range of RITS AIF Unsolicited Messages and Reports are also available to Framework Participants via the SWIFT FIN service.[213]

(d) Framework Participants requiring further information on the AIF should refer to the RITS Regulations and RITS User Handbook.

The next page is Part 7

[212] Last amended effective 1/1/18, version 037 r&p 001.17
[213] Last amended effective 1/1/18, version 037 r&p 001.17

PART 7 FRAMEWORK PARTICIPANT TECHNICAL REQUIREMENTS

7.1 Environmental Requirements

To safeguard the SWIFT PDS and Framework Participants' interests with respect to their participation in the HVCS, it is necessary to impose certain minimum operational and security requirements on each Framework Participant's SWIFT PDS System environment. Each Framework Participant using the SWIFT PDS is required to meet specified standards in the following key areas in accordance with this PART 7. [214]

7.2 Primary Computer Site Overview[215]

(a) Every component of the Primary Computer Site configuration must be appropriately protected against fire, flood and water damage.

(b) The SCI hardware, and any related hardware included in each Framework Participant's Primary Computer Site configuration which is essential to the continuous operation and availability of that member's SWIFT PDS System, must have an Uninterruptable Power Supply.[216]

(c) All alterations to each Framework Participant's Primary Computer Site configuration since the date of its last Yearly Audit Compliance Certificate, or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist, are to be recorded in its SWIFT PDS Log.[217]

7.3 Primary Hardware and Software Requirements [Deleted][218]

7.4 Primary Computer Site Security Requirements[219]

(a) Each Primary Computer Site must have a minimum of one HSM (Hardware Security Module) to enable Secure Login, Select (SLS) functions using PKI (Public Key Infrastructure).[220]

(b) A second HSM is required to provide system redundancy.[221]

[214] Last amended effective 14/11/22, version 041 r&p 001.22
[215] Amended effective 14/11/22, version 041 r&p 001.22
[216] Amended effective 14/11/22, version 041 r&p 001.22
[217] Last amended effective 18/4/05, version 015 r&p 001.15
[218] Deleted effective 14/11/22, version 041 r&p 001.22
[219] Last amended effective 14/11/22, version 041 r&p 001.22
[220] Last amended effective 31/10/07, version 024 r&p 004.07
[221] Last amended effective 31/10/07, version 024 r&p 004.07

(c) The second HSM must be tested a minimum of once every six months including Active-Active configurations to ensure adequate redundancy by demonstrating that each single site configuration can continue to operate if the primary HSM is removed from operation and the second HSM takes over.[222]

7.5 Primary Operating System Security [Deleted][223]

7.6 Primary Site Communication Requirements [Deleted][224]

7.7 SWIFTNet IP Network[225]

(a) Each Framework Participant must have two differently routed communication lines, each to a separate SWIFT Point of Presence (POP), ie. a primary line and a secondary line.[226]

(b) If the adopted configuration makes use of two of the same communications options, to negate the possibility of a single point of failure they must either:

(i) Be sourced from a separate service provider for each facility; or

(ii) If the same service provider is used then connectivity must be through diverse connection points.

(c) Secondary communication lines to the Primary Computer Site must be tested at least four times a year at intervals of no less than two months.

7.8 Back-up Computer Requirements

(a) Each Framework Participant must have a Back-up Computer Site configuration which includes the hardware, software and ancillary equipment required to recover that member's SWIFT PDS System operations if its Primary Computer Site fails.[227]

(b) The level of back-up computer support that a Framework Participant must have is dependent upon the value of SWIFT PDS payments sent and received using the SWIFT PDS. Each Framework Participant will fall within one of the following two Backup Tiers, for the purposes of the back-up requirements of these Procedures, based on the transaction values that each processes and subject to Clause 7.9(a). The two Back-up Tiers are:[228]

(i) Tier 1 Back-up: 2.00% or more of Total National Transaction Value;

[222] Last amended effective 14/11/22, version 041 r&p 001.22
[223] Deleted effective 14/11/22, version 041 r&p 001.22
[224] Deleted effective 18/04/05, version 015 r&p 001.05
[225] Inserted effective 13/10/03, version 010 r&p 002.03
[226] Last amended effective 26/11/18, version 038 r&p 001.18
[227] Last amended effective 23/4/98, version 001
[228] Amended effective 1/1/14, version 034 r&p 001.14

(ii) Tier 2 Back-up: up to but not including 2.00% of Total National Transaction Value.[229]

(c) Each Framework Participant must comply with the requirements for back-up specified in these Procedures for the Back-up Tier applicable to that member, as determined in accordance with this Clause 7.8.

(d) Any Framework Participant may implement more robust back-up arrangements than those required to comply with these Procedures if that member believes it to be necessary or desirable in its particular circumstances.

(e) The Company will advise each Framework Participant of the Back-up Tier applicable to that member annually along with the publication of the yearly audit compliance reminder issued in Q4 of each calendar year, or upon notification of a success HVCS membership application.[230]

7.9 Transaction Data Back-up Tier Allocation[231]

(a) The Company will allocate Back-up Tiers based on each Framework Participant's percentage of Total National Transaction Value. The data used will be for the calendar Q3 period. Where a new Framework Participant joins the HVCS during the statistical collection period, its percentage share of Total National Transaction Value will be calculated on a pro-rata basis by reference to the actual period of membership of that Framework Participant.[232]

(b) If any Framework Participant reasonably believes that it should be allocated a different Back-up Tier, then that member may in writing provide justification and a request that the Company consider applying a different Back-up Tier. The Company will notify the Participant of the outcome of its consideration and make any change as it deems appropriate.[233]

(c) An Applicant for HVCS membership must provide to the Company in connection with its HVCS membership application a reasonable estimate in writing of its likely SWIFT PDS traffic. The Secretary will be entitled to rely on that member's estimate when notifying it, pursuant to Clause 7.8(e), of the Back-up Tier which will apply to it for that period.[234]

7.10 Review of Member's Back-up Arrangements [Deleted][235]

7.11 Back-up Computer Site Overview

(a) Each Framework Participant must maintain a Back-up Computer Site suitably configured to meet the minimum back-up requirements applicable

[229] Amended effective 1/1/14, version 034 r&p 001.14
[230] Amended effective 14/11/22, version 041 r&p 001.22
[231] Amended effective 1/7/14, version 034 r&p 001.14
[232] Last amended effective 14/11/22, version 041 r&p 001.22
[233] Amended effective 14/11/22, version 041 r&p 001.22
[234] Amended effective 1/7/14, version 034 r&p 001.14
[235] Deleted effective 14/11/22, version 041 r&p 001.22

to that member under these Procedures. [236]

7.12 Tier 1 Back-up - Geographically Remote Back-up Computer Site Requirements

(a) Each Framework Participant allocated tier 1 Back-up Tier must maintain, as a minimum requirement, a Back-up Computer Site which is geographically remote from its Primary Computer Site, in terms of Clause 7.11, and which otherwise meets the requirements specified in this Clause 7.12.[237]

(b) A tier 1 Back-up Framework Participant must be able to: [238]

(i) begin sending and receiving payments within two (2) hours in the event of a systems failure within the Primary Computer Site; or[239]

(ii) switch to its Back-up Computer Site and begin sending and receiving payments within four (4) hours in the event of a site failure at the Primary Computer Site.[240]

(c) The Framework Participant must ensure that its Back-up Computer Site is secure from unauthorised entry and that access to the area is controlled to protect against insider and external threats.[241]

(d) The Back-up Computer Site must be appropriately protected against fire, flood and water damage.

(e) The Back-up Computer Site, including SCI hardware and any related hardware essential to the continuous operation and availability of the system, must have an Uninterruptable Power Supply.[242]

(f) All alterations to the Framework Participant's Back-up Computer Site configuration since the date of its last Yearly Audit Compliance Certificate, or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist, are to be recorded in its SWIFT PDS Log. [243]

7.13 Tier 2 Back-up - Single Building Back-up Computer Site Requirements [244]

(a) Each Framework Participant allocated tier 2 Back-up Tier must maintain, as a minimum requirement, a Back-up Computer Site which meets the requirements specified in this Clause 7.13(a). Each Framework Participant to which this Clause 7.13(a) applies may maintain a Back-up Computer Site in the same building as that member's Primary Computer Site, instead of a geographically remote site as is required for the tier 1 Back-up Tier. Each

[236] Last amended effective 14/11/22, version 041 r&p 001.22
[237] Amended effective 14/11/22, version 041 r&p 001.22
[238] Last amended effective 1/1/14, version 034 r&p 001.14
[239] Amended effective 1/1/14, version 034 r&p 001.14
[240] Inserted effective 1/1/14, version 034 r&p 001.14
[241] Amended effective 26/11/18, version 038 r&p 001.18
[242] Amended effective 14/11/22, version 041 r&p 001.22
[243] Last amended effective 18/4/05, version 015 r&p 001.15
[244] Amended effective 1/1/14, version 034 r&p 001.14

Framework Participant maintaining its Back-up Computer Site in the same building as its Primary Computer Site is not required to meet the redundancy requirements set out in Clauses 7.13(a) and 7.18.[245]

(b) The Framework Participant must ensure that its Back-up Computer Site is secure from unauthorised entry and that access to the area is controlled to protect against insider and external threats.[246]

(c) The Back-up Computer Site must be appropriately protected against fire, and flood and water damage.

(d) The Back-up Computer Site, including SCI hardware and any related hardware essential to the continuous operation and availability of the system, must have an Uninterruptable Power Supply.[247]

(e) All alterations to the Framework Participant's Back-up Computer Site configuration since the date of its last Yearly Audit Compliance Certificate, or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist, are to be recorded in its SWIFT PDS Log.[248]

(f) A tier 2 Back-up Framework Participant must be able to:[249]

(i) begin sending and receiving payments within four (4) hours in the event of a systems failure within the Primary Computer Site; or [250]

(ii) switch to its Back-up Computer Site and begin sending and receiving payments within six (6) hours in the event of a site failure at the Primary Computer Site.[251]

(g) Although geographical remoteness of the Back-up Computer Site from the Primary Computer Site is not a mandatory requirement for those Framework Participants subject to tier 2 back-up requirements in accordance with Clause 7.8(a), those Framework Participants are encouraged to consider the merits of geographically remote back-up which is strongly recommended.[252]

7.14 Back-up Hardware and Software Requirements[253]

[245] Last amended effective 14/11/22, version 041 r&p 001.22
[246] Amended effective 26/11/18, version 038 r&p 001.18
[247] Amended effective 14/11/22, version 041 r&p 001.22
[248] Last amended effective 18/4/05, version 015 r&p 001.15
[249] Amended effective 1/1/14, version 034 r&p 001.14
[250] Last amended effective 1/1/14, version 034 r&p 001.14
[251] Last amended effective 1/1/14, version 034 r&p 001.14
[252] Amended effective 1/1/14, version 034 r&p 001.14
[253] Amended effective 14/11/22, version 041 r&p 001.22

7.15 Back-up Security Requirements

Subject to Clause 7.13(a) (same building Back-up Computer Site) the Back-up Computer Site must contain at least one HSM.[254]

7.16 Back-up Operating System Security

Each Framework Participant must ensure that the operating system security under which its Back-up Computer Site SCI runs provides as a minimum the same level of operating system security as required by the SWIFT Customer Security Controls Framework. [255]

7.17 Back-up Communication Requirements [Deleted][256]

7.18 SWIFT IP network[257]

Subject to Clause 7.13(a) (same building Back-up Computer Site) each Framework Participant must maintain at least one communication line to a SWIFT POP from that member's Back-up Computer Site. This must be a separate communication line than those used at the Primary Computer Site and must be routed through a different exchange. It may connect to the same SWIFT POP(s) used by the Primary Computer Site.[258]

7.19 Testing of Back-up Configuration

(a) Each Framework Participant must test its Back-up Computer Site system configuration including Active-Active configurations to ensure adequate redundancy by demonstrating that one site configuration can continue to operate if the other site is completely removed from operation at least twice a year at intervals of no less than four months. It is recommended that the tests involve live traffic, but if Framework Participants are unable to achieve this then the test may be carried out using "test mode" traffic.[259]

(b) Full details of all Back-up Computer Site system tests required to be carried out under this Clause 7.19, including the dates that those tests were carried out and the results achieved, must be recorded by each Framework Participant concerned in that member's SWIFT PDS Log.

7.20 Payments Operations Overview [Deleted][260]

7.21 Payments Operations Security Requirements [Deleted][261]

7.22 Maintenance Requirements [Deleted][262]

---

[254] Last amended effective 31/10/07, version 024 r&p 004.07
[255] Last amended effective 14/11/22, version 041 r&p 001.22
[256] Deleted effective 18/4/05, version 015 r&p 001.15
[257] Inserted effective 13/10/03, version 010 r&p 002.03
[258] Last amended effective 26/11/18, version 038 r&p 001.18
[259] Last amended effective 14/11/22, version 041 r&p 001.22
[260] Deleted effective 14/11/22, version 041 r&p 001.22
[261] Deleted effective 14/11/22, version 041 r&p 001.22
[262] Deleted effective 18/4/05, version 015 r&p 001.15

7.23 SWIFTNET IP network [Deleted][263]

7.24 System Availability

(a) Each Framework Participant must be logged on to the SWIFT PDS during the Core Business Hours (see Clause 4.4(a)).

(b) Each Framework Participant must maintain high reliability and achieve prompt resumption of payments processing following any disruption to its high value payments systems. This is to ensure efficient operation of the Australian payments system and maintain market liquidity. The following requirements apply to tier 1 Back-up and tier 2 Back-up respectively:[264]

(i) Each tier 1 Back-up Framework Participant's system (which includes the SCI and the Core PPS) must meet a minimum of 99.7% up-time during the Core Business Hours on an annual basis. [265]

(A) Following any disruption of processing during Core Business Hours, a tier 1 Back-up Framework Participant must substantially resume payments processing in accordance with clause 7.12(b)(i) or 7.12(b)(ii) as applicable. [266]

(B) Failure to resume payments processing within the timeframes prescribed in clause 7.12(b)(i) or 7.12(b)(ii) as applicable will result in formal reporting by the Member at the next Management Committee meeting. [267]

(C) No single outage of any tier 1 Back-up Framework Participant's SCI and/or Core PPS may exceed four (4) hours duration and the aggregate duration of all such outages of a SCI and/or Core PPS during the Year may not exceed six (6) hours for those Framework Participants that do not participate in the Evening Settlement Session and eight (8) hours for those Framework Participants that participate in the Evening Settlement Session. [268]

(c) Each tier 2 Back-up Framework Participant's system (which includes the SCI and the Core PPS) must meet a minimum of 99.5% up-time during the Core Business Hours on an annual basis. [269]

(ii) Following any disruption of processing during Core Business Hours, a tier 2 Back-up Framework Participant must substantially resume payments processing in accordance with clause 7.13(f)(i) or 7.13(f)(ii) as applicable. [270]

---

[263] Deleted effective 14/11/22, version 041 r&p 001.22
[264] Last amended effective 1/1/14, version 034 r&p 001.14
[265] Last amended effective 14/11/22, version 041 r&p 001.22
[266] Last amended effective 1/1/14, version 034 r&p 001.14
[267] Amended effective 1/1/14, version 034 r&p 001.14
[268] Last amended effective 14/11/22, version 041 r&p 001.22
[269] Amended effective 14/11/22, version 041 r&p 001.22
[270] Inserted effective 1/1/14, version 034 r&p 001.14

(iii) Failure to resume payments processing within the timeframes prescribed in clause 7.13(f)(i) or 7.13(f)(ii) as applicable will result in formal reporting by the Member at the next Management Committee meeting.[271]

(iv) No single outage of any tier 2 Back-up Framework Participant's SCI and/or Core PPS may exceed six (6) hours duration and the aggregate duration of all such outages of a SCI and/or Core PPS during the Year may not exceed ten (10) hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen (13) hours for those Framework Participants that participate in the Evening Settlement Session.[272]

(d) The Provisions of this Clause 7.24 apply equally to each Framework Participant's Primary Computer Site and Back-up Computer Site configurations.

(e) Each Framework Participant must maintain a SWIFT PDS Log containing details of all its SWIFT PDS System outages, the nature of the problem causing each outage, the time taken to correct that problem and whether processing of payments was switched to that member's Back-up Computer Site must be maintained. The SWIFT PDS Log forms part of that Framework Participant's Yearly Audit Compliance Certificate (see Clause 7.28(a)).

(f) In addition to formal incident reporting to the Management Committee, Framework Participants must report any single outage of two (2) hours or more to the Company. Annexure A.3 may be used for this purpose. The Company will notify the Management Committee of such outages, whether or not the outage also forms the basis of a Framework Participant's formal incident report.[273]

7.25 Minimum System Throughput Requirements[274]

(a) Each Framework Participant's SCI must be capable of processing a minimum of 50% of its average daily SWIFT PDS transaction volume in any one hour (Average Hourly Transaction Volume ('AHTV'), including both inward and outward traffic and associated Acknowledgments.[275]

(i) In respect of the System Certification, each Applicant must estimate its daily SWIFT PDS transaction volume, and specify that estimate in its System Certification Checklist.

(ii) The provisions of this Clause 7.25 apply equally in respect of both the Primary Computer Site and Back-up Computer Site.

(b) *Impaired Performance Monitoring and Reporting:* Each Framework Participant shall calculate the Required Hourly Transaction Volume (RHTV)

[271] Inserted effective 1/1/14, version 034 r&p 001.14
[272] Inserted effective 1/1/14, version 034 r&p 001.14
[273] Amended effective 1/1/14, version 034 r&p 001.14
[274] Amended effective 1/7/14, version 034 r&p 001.14
[275] Last amended effective 14/11/22, version 041 r&p 001.22

required to satisfy the Clause 7.25(a) requirement as 400% of the Average Daily Transaction Volume (ADTV) used in the current year's Yearly Audit Compliance Certificate, reduced to an hourly figure.[276]

$$RHTV = \frac{ADTV * 4}{\text{Core Business Hours}}$$

(c) During periods where the system throughput is degraded, records shall be maintained of the actual Transaction throughput achieved on an hourly basis. If the hourly throughput is below 51% of AHTV then a record shall be made of the event and logged in the Swift PDS log, recording the percentage of RHTV, date, time, duration and when known, cause and remedial action.

(d) Any such periods shall be reported in the Yearly Audit Compliance Certificate in accordance with Table 1.

Percentage of AHTV	Performance Period
50%	Report if period is 6 hours or greater
35%	Report if period is 5 hours or greater
25%	Report if period is 4 hours or greater
12%	Report if period is 3 hours or greater

Table 1 Performance Reporting Requirements

7.26 Framework Participant Archival Requirements

Each Framework Participant must maintain archival records of all Payments and associated messages sent and received using the SWIFT PDS for each Business Day and must retain those records for a minimum of seven (7) years.

7.27 Initial Certification of Framework Participant's SWIFT PDS System

(a) Each Applicant must arrange for certification of its SWIFT PDS System in accordance with Clauses 7.27(a) to (j) inclusive by completing and submitting a System Certification Checklist. The System Certification Checklist must be in the form appearing in Appendix A1 and is to be completed and signed by a duly authorised officer of the Applicant.

(b) Copies of the System Certification Checklist and Certification Test Plan can be obtained from the Company by contacting the SWIFT PDS Operations Manager.

[276] Inserted effective 1/1/22, version 040 r&p 003.21

(c) Each Applicant must demonstrate, by completing the test scripts contained within the Certification Test Plan, that its SCI is configured correctly and capable of processing SWIFT PDS messages in accordance with the HVCS Regulations and Procedures. The Company does not require Framework Participants to provide test results, except as set out in Clause 7.27(d), but a copy should be produced and retained for internal audit purposes. AusPayNet may, as part of the verification process, request a Framework Participant to provide test results to assist in evaluation of the Certification results. In the event that a Framework Participant is unable to produce the requested results the Framework Participant will need to re-run the test in question. Full details of the certification test requirements are set out in the Certification Test Plan.[277]

(d) The completed System Certification Checklist and the test result forms required in terms of the Certification Test Plan are to be provided to the SWIFT PDS Operations Manager. Where actual test results differ from the expected result and the Framework Participant believes that it has successfully completed the test, supporting evidence should be provided so that AusPayNet can ensure that no misunderstanding of the test requirements has occurred.[278]

(e) The completed System Certification Checklist must be signed by a duly authorised officer of the Applicant. Any evidence of that authorisation which is reasonably requested by the Secretary must be promptly produced to the Secretary following the request.[279]

(f) The Company will evaluate the test result forms, as set out in the Certification Test Plan, any test data provided in terms of Clause 7.27(d) and the related System Certification Checklist, within fourteen days of receipt of the completed System Certification Checklist, and provide a detailed report of its evaluation to the Applicant. If all requirements have been met, details of the successful System Certification will be provided to the Management Committee.

(g) On acceptance of the System Certification Checklist by the Management Committee, the Secretary will promptly notify all Framework Participants of the successful System Certification and, if the relevant successful Applicant is already a Framework Participant, the date from which that successful Applicant will be entitled to send and receive payments using the SWIFT PDS.

(h) The Management Committee will provide to the successful Applicant a System Compliance Certificate confirming and evidencing successful System Certification with respect to the SWIFT PDS.

(i) If the certification process fails in part, the Company will provide the applicant with details of the deficiency as part of its report as specified in Clause 7.27(f), and request either a partial or complete re-run of the certification

[277] Last amended effective 14/11/22, version 041 r&p 001.22
[278] Amended effective 14/11/22, version 041 r&p 001.22
[279] Amended effective 14/11/22, version 041 r&p 001.22

process, depending upon the nature of the problem. The applicant will be required to rectify all deficiencies and submit supporting evidence as required by the Company.

(j) Upon receipt of the additional certification documentation the Company will carry out a review of the material in terms of Clause 7.27(f).

7.28 Yearly Audit Compliance

(a) Each Framework Participant must submit to the Company annually a Yearly Audit Compliance Certificate, in the form of Annexure A.2, by the end of January each year, such certificate to cover the prior calendar year and confirm that all SWIFT upgrades required since the last Yearly Audit Compliance Certificate have been implemented.[280]

(b) The Yearly Audit Compliance Certificate is to be signed by a duly authorised officer of the Framework Participant. Any evidence of that authorisation which is reasonably requested by the Secretary must be promptly produced to the Secretary following that request.[281]

(c) See also Annexure A.2 for further instructions on the procedural requirements in relation to Yearly Audit Compliance Certificates.

7.29 Failure to Meet Technical Requirements

(a) If the Yearly Audit Compliance Certificate given by a Framework Participant in accordance with Clause 7.28(a) reveals that a Framework Participant has failed to meet any of the technical requirements specified in this Part 7, the Company will, subject to Clause 7.29(c), notify the Framework Participant of the deficiency, in writing, requesting rectification of the deficiency within 30 days of the date of that notice.

(b) If any deficiency specified in any notice issued by the Company in accordance with Clause 7.29(a) is not rectified within the permitted 30 day period, the Company will advise details of the deficiency and action taken to date to the Management Committee for consideration as to what action will be taken, which could include (without limitation) suspension of the Framework Participant under Regulation 5.10.

(c) If, in the opinion of the Chief Executive Officer, the deficiency notified in accordance with Clause 7.29(b) is such that it poses a risk to the efficiency or security of the HVCS, the deficiency will be reported directly to the Management Committee. The Management Committee may then take such remedial action which it considers necessary or desirable under the Regulations and these Procedures, including (without limitation) suspension of the Framework Participant under Regulation 5.10.

[280] Last amended effective 16/1/09, version 027 r&p 005.08
[281] Amended effective 14/11/22, version 041 r&p 001.22

7.30 SCI Modifications and Upgrades[282]

(a) Any Framework Participant implementing any new SCI must successfully complete the normal initial certification process, in accordance with Clauses 7.27(a) to 7.27(f) inclusive, prior to implementing the new configuration.

(b) Any Framework Participant implementing any upgrade or modification of its existing SCI, or any part of that system, must, prior to sending and receiving payments using the upgraded or modified system, ensure that the upgraded or modified system complies with minimum technical standards and specifications required under the Regulations and these Procedures.

(c) If a Framework Participant upgrades or modifies, or proposes to upgrade or modify, its SCI, then the Management Committee may require that Framework Participant to provide to it particulars of that, or that proposed, upgrade or modification within 14 days of receipt of the Management Committee's request.

(d) The Management Committee may then review the particulars of that, or that proposed, upgrade or modification provided to it under this Clause 7.30(c) and may issue such instructions as it considers necessary to ensure that the upgraded or modified SCI complies or will, after implementation of the proposed upgrade or modification, comply with the minimum technical standards and specifications required under the Regulations and these Procedures.

The next page is Part 8

[282] Amended effective 14/11/22, version 041 r&p 001.22

PART 8 SWIFT PDS MESSAGE CONTENT SPECIFICATIONS

8.1 Overview

To provide for maximum automation of processing of Framework Participants inward payments, it is essential that SWIFT PDS payments input by the Sender conform to the message content specifications set out in this Part 8 and Appendix D. Close attention by Framework Participants to the completion of SWIFT PDS message details in accordance with these Procedures, will ensure the smooth and efficient operation of each Framework Participant's own SWIFT PDS System and the SWIFT PDS as a whole.

(Note: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requires that certain information must be included in electronic funds transfer instructions and that certain information must be obtained in respect of those instructions before financial institutions may initiate, pass on or take any other action to carry out the electronic funds transfer instructions. Please refer to Part 5 of the Act for details.)[283]

8.2 Message Preparation Guidelines

Message preparation guidelines, designed to assist in the straight through processing of SWIFT PDS payments, are set out in Annexure I. The guidelines are not mandatory, as they exceed normal SWIFT requirements, but are strongly recommended as a means of maximising the level of automation available within Framework Participants' own systems.

8.3 BSB Number

(a) To use the SWIFT PDS each Framework Participant must have a BSB Number which will represent the ultimate destination for delivery of payments to that Framework Participant.

(b) If an Applicant has not already been allocated a BSB Number by the Company because of its participation in another Framework (which BSB Number is also valid for the HVCS upon notification to AusPayNet to activate that BSB Number for the HVCS), that Applicant must request allocation of a BSB Number from the Company when applying to join the HVCS.

8.4 Repair Routing Code BSB

All Framework Participants must assign one BSB Number, to be known as the Repair Routing Code BSB, to which Framework Participants may direct payments if details of the intended recipient Framework Participant are known but there is insufficient information available to precisely identify the beneficiary's branch. Each Framework Participant must advise the Company of its Repair Routing Code BSB, which can be an existing BSB Number, by completing a "BSB and BIC Amendment Advice" available from the Company.

[283] Inserted effective 30/4/07, version 022 r&p 001.17

8.5 BIC/BSB Relationship

All authorised HVCS BSB Numbers must be linked to Framework Participant's BIC or BICs, where multiple BICs have been defined, and will be recorded in the Company's publication "HVCS BIC/BSB Directory". Each Framework Participant must ensure that the BIC and BSB Numbers included in SWIFT PDS payments sent by it conform to the approved arrangements as set out in the "HVCS BIC/BSB Directory".

8.6 FIN-Copy Service Code Identifier

(a) SWIFT use an identification code called the FIN-Copy Service Code Identifier to uniquely identify the various FIN-Copy services operating within the SWIFT Network internationally.

(b) The characters "PDS" will be the FIN Copy Service Code Identifier for the SWIFT PDS. Framework Participants must ensure that their SWIFT PDS Systems are configured to set Field 103 in the User Header Block 3 to "PDS" for all SWIFT PDS (MT103, MT202 and their variants).[284]

8.7 Character Set

Normal SWIFT Character Set requirements, as set out in the SWIFT User Handbook, will apply for all SWIFT PDS payments.

8.8 Transaction Reference Number (TRN)

(a) Framework Participants are responsible for ensuring that all SWIFT PDS payments contain a unique Transaction Reference Number ("TRN") (Field 20), and that the TRN is unique within any given fourteen (14) day period. Where a Framework Participant uses multiple Logical Terminals (LT) it must ensure the uniqueness of its TRNs across all LTs.

(b) All TRNs are a maximum of 16 alpha-numeric characters in length.

(c) To ensure the uniqueness of TRNs across individual high value systems (HVCS, RITS, Austraclear System), it has been agreed with the operators of these other high value systems that all RITS and Austraclear System TRNs will commence with a four character alpha identifier. The RITS TRN alpha identifier will be "RITS" while the Austraclear System identifier will be "ACLR".[285]

(d) SWIFT PDS messages will not require a TRN alpha identifier but Framework Participants must ensure that they exclude the use of "RITS" and "ACLR" alpha characters from the first four digits of their SWIFT PDS TRN generation routine.

[284] Last amended effective 21/11/09, version 029 r&p 003.09
[285] Last amended effective 18/4/05, version 015 r&p 001.15

(e) Where a message is to be re-sent as the result of the original message being rejected by RITS, the Sender of the message to be re-sent must assign a new TRN to the re-sent message.[286]

8.9 Value Date

(a) Framework Participants may input payments for same day value or otherwise in accordance with Clause 5.12(a). RITS will ascertain the payment value date from the value date contained within the Amount Field (Field 32A) in the payment message.[287]

(b) Where a Framework Participant inputs a payment with a value date more than 5 Settlement Days in advance of the input date, RITS will reject the payment and SWIFT FIN-Copy will return an Abort Notification (MT019) to the Sender advising the reason for that rejection. Framework Participants should note that payments may only be entered as Future Dated Payments strictly in accordance with Clause 5.12(a).[288]

8.10 Currency

Framework Participants may only send payments denominated in Australian dollars.

The next page is Part 9

[286] Last amended effective 1/1/18, version 037 r&p 001.17
[287] Last amended effective 1/1/18, version 037 r&p 001.17
[288] Last amended effective 1/1/18, version 037 r&p 001.17

PART 9 CONTINGENCY PROCEDURES

9.1 Application of Part 9

(a) The provisions of this PART 9 are designed to enable orderly operation of the SWIFT PDS during a Contingency.[289]

(b) Contingency means:[290]

(i) a Disabling Event occurring at the:

(A) Framework Participant level;

(B) central site (RITS and CSI) level; or

(C) SWIFT network level; or

(c) Any event or other event or circumstance specified by the Management Committee for the purposes of this PART 9.

9.2 Application of Appendix J (HVCS Contingency Instructions)[291]

(a) Where a Disabling Event occurring at the Framework Participant level prevents the Framework Participant from sending payments in the normal way (**Participant Outage**); or where a Disabling Event occurring at the central site level (RITS or CSI) prevents RITS from effecting settlement of payments in the normal way (**RITS Outage**), then the Contingency Instructions may also apply.

(b) During any period in which any provisions of this PART 9 apply, to the extent of any inconsistency, the Contingency Instructions will prevail over these provisions in Part 9 and over any other provisions of these Procedures.

9.3 Responsibilities

(a) Framework Participants have a responsibility to each other, and to the system as a whole, to co-operate in resolving any processing difficulties.

(b) To the extent that such co-operation does not adversely affect its own processing environment, a Framework Participant receiving a request for assistance from any other Framework Participant, the Company or the System Administrator may not unreasonably withhold such assistance.

[289] Amended effective 19/7/21, version 039 r&p 001.21
[290] Inserted effective 19/7/21, version 039 r&p 001.21
[291] Inserted effective 19/7/21, version 039 r&p 001.21

9.4 Nature of Contingency

(a) Abnormal processing conditions which may occur, within the overall high value system, and need to be provided for include:[292]

(i) A Disabling Event occurring at the Framework Participant level. Note that if the Disabling Event is a Participant Outage, the Contingency Instructions may also apply.

(ii) A Disabling Event occurring at the central site (RITS or CSI) level. Note if the Disabling Event is a RITS Outage, the Contingency Instructions may also apply.

(iii) A Disabling Event occurring at the SWIFT communication service (SWIFT FIN Service or SWIFT FIN-Copy Service) level. Note the Contingency Instructions do not apply to this type of Contingency.

(iv) Any other event or circumstance specified by the Management Committee and designated a Contingency for the purpose of this Part 9.

9.5 Framework Participant System Failure Overview[293]

(a) The appropriate response to a Disabling Event at the Framework Participant level depends very much upon the nature of the problem, the time of day that the problem occurs and the level of redundancy that the Framework Participant concerned has available at its Primary Computer Site. While each Framework Participant has responsibilities regarding timely fallback to back-up arrangements, in accordance with Clauses 7.11 to 7.13(a), usually only that Framework Participant will be in the position to properly evaluate the problem and decide on the appropriate course of action for the particular circumstances applying at the time.

(b) The Procedures set out in this PART 9 (and where applicable the Contingency Instructions) are designed to provide a framework within which each Framework Participant can consider its response to a particular Disabling Event, but it is recognised that outside factors, for example nature of the Disabling Event and the time of day that the problem occurs, might affect that Framework Participant's course of action, and where applicable, ability to comply with any contingency procedures in this PART 9 such as fallback to the Back-up Computer Site. In accordance with Clause 9.6(a), a Framework Participant must immediately notify the System Administrator of any Disabling Event and in doing so must indicate:

(i) If the circumstances are such that the Framework Participant is unable to comply with any contingency procedures in this PART 9 or if any applicable provisions of this PART 9 would in the circumstances be inappropriate.

[292] Amended effective 19/7/21, version 039 r&p 001.21
[293] Amended effective 19/7/21, version 039 r&p 001.21

(ii) If the Disabling Event has or may cause a Participant Outage, the Framework Participant must:

(A) immediately notify the System Administrator in accordance with Clause 9.6(a) and refer to the Contingency Instructions;

(B) immediately consider and discuss with the System Administrator that the Framework Participant's potential response may be to request the declaration of the Participant Fallback Period, during which the Framework Participant is permitted to send payments using the Participant Fallback Solution provided for in the Contingency Instructions;

(C) use the Participant Outage runsheet in the Contingency Instructions as a guide for the time of day that any such decision to request or declare a Participant Fallback Period should be taken.

(c) Each Framework Participant experiencing a Disabling Event affecting its ability to receive inward payments will continue to have inward settled Payments delivered to the SWIFT PDS queue pending re-establishment of its SWIFT PDS System operations. It is important that each Framework Participant resolve its inward payments processing problems as soon as possible, either by correcting the problem with its Primary Computer Site or initiating fallback to its Back-up Computer Site.

(d) In all cases, a Framework Participant experiencing a Disabling Event must continue to manage its ESA liquidity position in RITS throughout the Disabling Event. [294]

(e) Details of all SCI system or Core PPS problems that adversely affect the ability of any Framework Participant to send and receive payments must be recorded in that member's SWIFT PDS Log in accordance with Clause 4.5(f).[295]

(f) Redundancy and back-up arrangements for proprietary payment processors linked to CBTs (see also Clause 9.6(a)) are not part of these procedures, but Framework Participants are expected to comply with normal industry best practice in these areas.

9.6 All Disabling Events to be Advised to System Administrator[296]

(a) Any Framework Participant experiencing a Disabling Event which adversely affects its ability to send or receive payments in a normal way must immediately advise the System Administrator in accordance with Clause 4.5(b). That Framework Participant must provide to the System Administrator brief details of the problem being experienced and, if

[294] Last amended effective 14/11/22, version 041 r&p 001.22
[295] Last amended effective 14/11/22, version 041 r&p 001.22
[296] Amended effective 19/7/21, version 039 r&p 001.21

applicable, give some indication as to when its SWIFT PDS System is likely to be operating as normal. This will assist the System Administrator in deciding whether or not to advise all Framework Participants of the issue.

(b) In accordance with Clause 9.6(a), if the Framework Participant's Disabling Event has or may cause a Participant Outage, the Affected Participant must notify the System Administrator and discuss the potential for a Participant Fallback Period to be declared.

9.7 Advice of HVCS Framework Participants Experiencing a Disabling Event[297]

If the System Administrator considers that a Framework Participant's Disabling Event is likely to be protracted, the System Administrator is responsible for immediately advising details of the Framework Participant experiencing those problems to all HVCS Framework Participants by issuing a RITS broadcast message.

9.7.1 Advice of a Participant Fallback Period[298]

If the Disabling Event has caused a Participant Outage, and a Participant Fallback Period has or could be declared, the System Administrator will advise all Framework Participants of this in accordance with the Contingency Instructions.

9.7.2 End-to-end test of Fallback Solutions[299]

Each Framework Participant must participate in an end-to-end test of Fallback Solutions provided for in the Contingency Instructions, occurring annually or as otherwise advised, on the dates specified by the Management Committee from time to time.

9.8 HVCS Processing Difficulties Contact Points

Framework Participants must, before using the SWIFT PDS to send or receive payments, nominate and advise the Company and the System Administrator of a contact point(s) to whom information or enquiries must be directed in the event of processing difficulties. A list of contact points is shown in Annexure C.1.

9.9 HVCS Payments to Framework Participants Experiencing a Disabling Event[300]

Framework Participants with payments to be sent to any Framework Participant experiencing a Disabling Event that affects its ability to receive inward payments will need to consider the liquidity implications of continuing to forward payments to that Framework Participant via the SWIFT PDS. Framework Participants should also consider the urgency or special requirements of any payments to be sent to a Framework Participant experiencing a Disabling Event, as payments may be

[297] Amended effective 19/7/21, version 039 r&p 001.21
[298] Inserted effective 19/7/21, version 039 r&p 001.21
[299] Amended effective 19/7/21, version 039 r&p 001.21
[300] Amended effective 19/7/21, version 039 r&p 001.21

delayed in the SWIFT queue for some considerable time.

9.10 HVCS Payments to a Framework Participant During a Participant Fallback Period[301]

(a) If a Framework Participant's Disabling Event causes a Participant Fallback Period to be declared, then Framework Participants with payments to be sent to the Affected Participant must continue to use SWIFT PDS, having regards to the liquidity implications and potential delays outlined above. The Participant Fallback Solution provides a means for the Affected Participant to send payments. It cannot be used as a means for the Affected Participant to receive payments outside of the SWIFT PDS.

(b) Framework Participants must, to the best of their ability, pause sending payments to an Affected Participant if requested to do so by the Affected Participant.

9.11 Simultaneous Failure of Framework Participant's Primary and Back-up Configurations[302]

If a Framework Participant's Disabling Event causes both its Primary Computer Site and Back-up Computer Site to fail, such that it cannot fallback to the Back-up Computer Site and is prevented from sending or receiving payments in the usual way, then that Framework Participant will need to consider alternative arrangements for sending and receiving domestic high value payments.

9.12 Sending Payments[303]

If the Disabling Event is preventing a Framework Participant from sending payments in the usual way (Participant Outage), the Contingency Instructions may apply and a Participant Fallback Period could be declared. During this time the alternative arrangements for the Affected Participant to send payments in the HVCS will be the Participant Fallback Solution provided for in the Contingency Instructions. In accordance with Clause 9.46a), the Affected Participant must notify the System Administrator of the Disabling Event and obtain approval to use the Participant Fallback Solution by means of a Participant Fallback Period being declared.

9.13 Receiving Payments[304]

If the Disabling Event is preventing a Framework Participant from receiving payments in the usual way then that Framework Participant must be aware that in accordance with Clause 9.10, their inbound payments will, subject to appropriate testing by RITS, continue to be settled and will be queued on that Framework Participant's SWIFT queue pending re-establishment of its connection. For the avoidance of doubt, and in accordance with Clause 9.10(a), the Participant Fallback Solution cannot be used as a means for that Framework

[301] Inserted effective 19/7/21, version 039 r&p 001.21
[302] Amended effective 19/7/21, version 039 r&p 001.21
[303] Inserted effective 19/7/21, version 039 r&p 001.21
[304] Inserted effective 19/7/21, version 039 r&p 001.21

Participant to receive payments outside of the SWIFT PDS. Further, that Framework Participant must continue to manage its ESA position in RITS throughout the Disabling Event and may in some circumstances consider requesting that other Framework Participants limit or pause the dispatch of further payments until the Disabling Event is resolved.

9.14 Need for Framework Participants to Re-establish SCI Connection in the Shortest Possible Time[305]

Payments forwarded to a Framework Participant experiencing a Disabling Event affective its inward payments processing will, subject to appropriate testing by RITS, be settled and queued on that Participant's SWIFT queue pending re-establishment of its connection. It is therefore imperative that the Framework Participant endeavour to re-establish its SCI connection either from the Primary Computer Site or Back-up Computer Site without delay.[306]

9.15 Advise System Administrator When Disabling Event is resolved[307]

(a) Where any Framework Participant's Disabling Event is resolved, and if applicable, its SWIFT PDS System is operating again in the normal way, that Framework Participant must immediately advise:

(i) the System Administrator; and

(ii) if the System Administrator has issued a RITS broadcast message to all HVCS Framework Participants in respect of the problem, the Company;

of the change of status.

(b) If a Participant Fallback Period is in operation at the time that the Disabling Event is resolved, the Affected Participant must comply with the Contingency Instructions with respect to the continued use of the Participant Fallback Solution and reversion to the SWIFT PDS for sending payments.

9.16 RITS or CSI (Central Site) Disabling Event[308]

(a) Both RITS and the CSI have two processors and each can withstand the failure of one of its two processors. However, if both processors should fail the system will revert to its back-up site. Until the move to processing using that back-up site is complete all RITS processing will cease. Framework Participants forwarding SWIFT PDS payments to RITS during this period will have those payments queued in the SWIFT PDS pending recovery of RITS. [309]

[305] Last amended effective 14/11/22, version 041 r&p 001.22
[306] Amended effective 14/11/22, version 041 r&p 001.22
[307] Amended effective 19/7/21, version 039 r&p 001.21
[308] Last amended effective 21/7/21, version 039 r&p 001.21
[309] Last amended effective 1/1/18, version 037 r&p 001.17

(b) Technically it is possible for the CSI to fail separately from RITS. In these circumstances other payment delivery feeder systems to RITS, such as RITS, might continue to use RITS to settle payments on a Real Time Gross Settlement basis, because those payment delivery systems are unaffected by failure of the CSI. [310]

9.17 Advice of RITS Central Site Failure[311]

The System Administrator is responsible for advising all Framework Participants, of any Disabling Event occurring at the RITS or the CSI level, and any action initiated to correct the situation including the likely time until the system will be operating as normal. Advice by the System Administrator in accordance with this Clause 9.17 will be given either by issuing a RITS broadcast message if possible or otherwise by the most expeditious means reasonably available using Framework Participant's contact points in Annexure C.1.[312]

9.18 Resynchronisation of RITS Data Base[313]

(a) The Reserve Bank of Australia has advised that if RITS fails and the RITS data base is corrupted, that data base including Framework Participants' ESA balances, will be recreated from separately maintained "redo logs". However, because there may be a period of several minutes after compilation of the last redo log and the actual system failure, there is a possibility that some data on previously settled Payments may be lost. In this case the Reserve Bank of Australia will contact each Framework Participant to verify the ESA balance and associated transactions. Where a difference exists between the balance quoted by the Reserve Bank of Australia and a Framework Participant's position, the figure quoted by the Reserve Bank of Australia will be final.[314]

(b) A difference in the ESA balance figure indicates that one or more previously "settled payments" have been lost and the Senders and Receivers of the payments in question will need to adjust their own figures accordingly and the Sender must re-send those payments. Framework Participants requiring further details should refer to the RITS Regulations and RITS User Handbook.

9.19 Central Communications Failure (SWIFT FIN Service)[315]

9.19.1 Partial Communications Failure (SWIFT FIN-Copy)

(a) Standard SWIFT procedures set out in the SWIFT User Handbook will apply where the SWIFT Network or part of the SWIFT Network is experiencing difficulties.

---

[310] Last amended effective 1/1/18, version 037 r&p 001.17
[311] Last amended effective 1/1/18, version 037 r&p 001.17
[312] Last amended effective 19/7/21, version 039 r&p 001.21
[313] Last amended effective 1/1/18, version 037 r&p 001.17
[314] Last amended effective 1/1/18, version 037 r&p 001.17
[315] Inserted effective 20/08/04, version 014 r&p 001.04

(b) If normal SWIFT fallback arrangements fail to resolve the problem and the difficulties become protracted, the System Administrator in conjunction with the Chief Executive Officer, will notify Framework Participants of the likely extent of the problem, using the contact details set out in Annexure C.1, and action proposed. If a notice in accordance with this Clause 9.19.1(b) is issued it will be necessary for Framework Participants to consider alternative arrangements for the despatch of payments.

9.20 Failure of Both RITS and/or CSI Primary & Back-up Configurations[316]

(a) If a Disabling Event causes both RITS main site and back-up site to fail, or the main CSI and back-up to fail, the System Administrator will need to consider alternative means of processing payments. If the Disabling Event causes a RITS Outage the System Administrator:[317]

(i) could recommend to the Company that a HVCS Fallback Period be declared during which time the HVCS Fallback Solution provided for in the Contingency Instructions will apply;

(ii) must notify all Framework Participants if a HVCS Fallback Period has or could be declared; and

(iii) will have regard to the timings in the RITS Outage runsheet timings in the Contingency Instructions and use this as a guide for the time of day that any such decision to declare a HVCS Fallback Period may need to be taken.

(b) The System Administrator has responsibility for advising full details of the failure and intended alternative processing arrangements to Framework Participants using a RITS broadcast message if possible or otherwise by the most expeditious means reasonably available using Framework Participant's contact points in Annexure C.1.[318]

(c) In the event that the System Administrator issues a RITS broadcast message under either clause 9.7, clause 9.17 or clause 9.19.1(b), or otherwise notifies HVCS Framework Participants of any other Contingency under Part 9 of these Procedures, then the Chief Executive Officer may, if he considers it appropriate to do so, invoke the Member Incident Plan, which is available on the Company's Extranet, either by written notice to, or verbally notifying, the Management Committee. The Member Incident Plan provides a framework for Management Committee communication and consultation during applicable contingency events. If the Chief Executive Officer invokes the Member Incident Plan, the Management Committee will comply with its requirements.[319]

Note: Clause 9.7 relates to a Framework Participant Disabling event, clause 9.17 relates to a central site (RITS or CSI) Disabling Event, and clause 9.19 relates

[316] Last amended effective 1/1/18, version 037 r&p 001.17
[317] Last amended effective 19/7/21, version 039 r&p 001.21
[318] Last amended effective 1/1/18, version 037 r&p 001.17
[319] Last amended effective 19/7/21, version 039 r&p 001.21

to a SWIFT Network Disabling Event.[320]

9.21 FIN-Copy Operating in Bypass Mode [Deleted][321]

9.22 Decision to Abandon Y-Copy Processing [Deleted][322]

9.23 SWIFT PDS Payment Instructions Processed in Bypass Mode [Deleted][323]

9.24 CLS Payments [Deleted][324]

9.25 Future Dated Payments in Bypass Mode [Deleted][325]

9.26 Deferred Status Payments in Bypass Mode [Deleted][326]

9.27 Possible Duplicated Settlement Amounts [Deleted][327]

9.28 Fallback Period[328]

(a) The Chief Executive Officer may, in consultation with the System Administrator, declare that a specified period is to be a Fallback Period. Any such declaration must be notified to Framework Participants by the System Administrator by the most expeditious means reasonably available using the Framework Participants' contact points in Annexure C.1. [329]

(b) Any HVCS Fallback Period owing to a RITS Outage and Participant Fallback Period owing to a Participant Outage will be undertaken in accordance with the Contingency Instructions, unless otherwise agreed by the Company and advised by the System Administrator. [330]

(c) During a Fallback Period, every HVCS payment sent and received pursuant to the Fallback Solutions provided for in the Contingency Instructions is irrevocable at the time of receipt of that payment by the Receiver. For the avoidance of doubt, in relation to the Participant Fallback Solution, the reference to "receipt of that payment" in this Clause 9.28(c) means actual receipt by the Receiver of the hard copy or electronic form of the relevant payment instruction.[331]

Note 1: During a Fallback Period, Framework Participants should not send HVCS payments by means of instruments that fall within other clearing systems

[320] Last amended effective 19/7/21, version 039 r&p 001.21
[321] Deleted effective 20/8/04, version 014 r&p 001.04
[322] Deleted effective 20/8/04, version 014 r&p 001.04
[323] Deleted effective 20/8/04, version 014 r&p 001.04
[324] Deleted effective 20/8/04, version 014 r&p 001.04
[325] Deleted effective 20/8/04, version 014 r&p 001.04
[326] Deleted effective 20/8/04, version 014 r&p 001.04
[327] Deleted effective 20/8/04, version 014 r&p 001.04
[328] Inserted effective 20/8/04, version 014 r&p 001.04
[329] Last amended effective 19/7/21, version 039 r&p 001.21
[330] Amended effective 19/7/21, version 039 r&p 001.21
[331] Last amended effective19/7/21, version 039 r&p 001.21

(eg. direct entry credits).[332]

9.29 Possible Duplicate Payments [Deleted][333]

9.30 Deferred Net Settlement[334]

Subject to Clause 9.34, where RITS cannot be used to effect settlement of HVCS payments on a Real Time Gross Settlement basis, settlement must be conducted in accordance with Clauses 9.31(a) to 9.33(a).[335]

9.31 Method of Settlement

(a) Settlement under Clause 9.30, between Framework Participants in respect of each HVCS payment (other than payments addressed to, or sent by, CLS Bank International) must be effected:[336]

(i) across Exchange Settlement Accounts using Fallback Settlement; and[337]

(ii) either for the multilateral net amount owing between each Framework Participant and all other Framework Participants or for the bilateral net amount owing between one Framework Participant and another Framework Participant.[338]

(b) Payments settled by RITS, prior to the decision to move to deferred net settlement in accordance with Clause 9.28(a), are not affected by Clauses 9.31(a) to 9.33(a) inclusive as they have already been irrevocably settled. Normal RITS reports will be available to Framework Participants, using the AIF, as soon as RITS is operational.[339]

(c) For Settlement under clause 9.30, each Framework Participant is responsible for separately identifying the amounts which are payable and receivable in respect of all payments sent and received by it, and where applicable, for directly notifying the relevant settlement figures to the Reserve Bank of Australia. Where this is undertaken during a HVCS Fallback Period or a Participant Fallback Period, it must be done in accordance with the Contingency Instructions. [340]

Note: Payments addressed to, or sent by, CLS Bank International, should not be included in the relevant settlement figures, because such payments must not be processed on a deferred settlement basis.[341]

[332] Last amended effective 1/1/18, version 037 r&p 001.17
[333] Deleted effective 19/7/21, version 039 r&p 001.21
[334] Amended effective 13/11/13, version 034 r&p 001.14
[335] Last amended effective 1/1/18, version 037 r&p 001.17
[336] Last amended effective 23/04/13, version 014 r&p 001.13
[337] Last amended 13/11/13, version 034 r&p 001.14
[338] Last amended effective 19/7/21, version 039 r&p 001.21
[339] Last amended effective 19/7/21, version 039 r&p 001.21
[340] Last amended effective 19/7/21, version 039 r&p 001.21
[341] Last amended effective 20/8/04, version 014 r&p 001.04

9.32 Failure To Match Rules[342]

(a) For Settlement under clause 9.30, the Failure to Match Rules are as follows:[343]

(i) if the amount that one Framework Participant claims is owed to it by another Framework Participant is larger than the amount admitted by that other Framework Participant, the lesser amount will be accepted as the final settlement figure;[344]

(ii) in particular, if one Framework Participant does not admit that any amount is owing, or fails to provide settlement figures by the latest time allowed, the final settlement figure in that case will be zero;[345]

(iii) similarly, if each of two Framework Participants claims that the balance between them is in its favour, or if each of two Framework Participants claims that the balance between them is in favour of the other, the final settlement figure in that instance will be zero.[346]

9.32.2 ESA Entries[347]

The Reserve Bank of Australia will apply entries to the Exchange Settlement Accounts of Framework Participants in accordance with the final settlement figures calculated in accordance with this PART 9.[348]

9.33 Interest Adjustment Where Settlement Delayed

(a) Where settlement in respect of any exchange of any payment is (for whatever reason) effected on a day other than the day on which that payment was exchanged for value, an adjustment of interest will be made between the creditor and debtor Framework Participants in respect of that payment calculated at the ESR. [349]

(b) The Reserve Bank of Australia will record the net balance owing to or by each Framework Participant for each day on which it despatched settlement figures and calculate the interest on the net balance owing for the number of days elapsed until the day of settlement using the ESR applicable to each of those days during that period.[350]

[342] Amended effective 13/11/13, version 034 r&p 001.14
[343] Amended effective 19/7/21, version 039 r&p 001.21
[344] Inserted effective 13/11/13, version 034 r&p 001.14
[345] Inserted effective 13/11/13, version 034 r&p 001.14
[346] Inserted effective 13/11/13, version 034 r&p 001.14
[347] Inserted effective 13/11/13, version 034 r&p 001.14
[348] Amended effective 18/1/16, version 036 r&p 002.15
[349] Last amended effective 23/04/13, version 014 r&p 001.13
[350] Inserted effective 13/11/13, version 034 r&p 001.14

(c) The Reserve Bank of Australia will notify each Framework Participant of the net amount due to or by it on account of such interest and include such interest each day in the Fallback Settlement amount of each Framework Participant.[351]

9.34 Failure To Settle

The provisions of Part 12 of the Regulations apply if any Framework Participant is unable to meet its HVCS payment obligations due to be discharged at any particular Fallback Settlement.[352]

9.35 Settlement Contact Points

The primary and fallback contact details and numbers to be used to contact the Reserve Bank of Australia and the settlement contact points for each Framework Participant are specified in Annexure C.2. Each Framework Participant must notify the Reserve Bank of Australia in writing of any change to its settlement contact point (including any temporary change) at least five business days prior to the change, clearly identifying the effective date in their advice. Each Framework Participant is solely responsible for the consequences of any failure by it to notify the Reserve Bank of Australia of any change to its settlement contact point in accordance with this Clause 9.35.[353]

9.36 Errors and Adjustments to Totals of Exchanges

(a) All adjustments to totals caused by any error must be accounted for in the manner set out in this Clause 9.36:[354]

(i) For each error which is an Error of Magnitude, the Receiver or the Sender, whichever first locates the error must notify the other immediately the details of the error are known. Once the error is agreed by both those Framework Participants, an adjustment (including interest calculated in accordance with Clause 9.30) must be effected as follows:[355]

9.36.1 Errors of Magnitude

(a) if the error is agreed before 7.00am Sydney time on any day, then either:

(i) where RITS is not, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, the necessary adjustment must be made in the next Fallback Settlement, or[356]

(ii) where RITS is, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, the necessary adjustment must be made by sending a Payment for same day value

[351] Inserted effective 13/11/13, version 034 r&p 001.14
[352] Last amended effective 13/11/13, version 034 r&p 001.14
[353] Last amended effective 13/11/13, version 034 r&p 001.14
[354] Last amended effective 20/8/04, version 014 r&p 001.04
[355] Last amended effective 20/8/04, version 014 r&p 001.04
[356] Last amended effective 1/1/18, version 037 r&p 001.17

on that day, or[357]

(b) if the error is agreed after 7.00am Sydney time on any day, the necessary adjustment must be made in a manner and at a time agreeable to both Framework Participants concerned, provided that if not effected earlier it must be effected either:

(i) where RITS is not, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, in the next Fallback Settlement after that day, or[358]

(ii) where RITS is, at the time of that agreement, functioning to effect settlements on a Real Time Gross Settlement basis, by sending a Payment for same day value no later than on the next Business Day, and[359]

9.36.2 Errors which are not Errors of Magnitude

(a) For each error which is not an Error of Magnitude, an adjustment must be effected as follows:

(i) if the error is found on the day of receipt of the erroneous payment or within 3 Business Days after the day on which that erroneous payment was sent, then either:

(A) where RITS is not, at the time at which the error is found, functioning to effect settlements on a Real Time Gross Settlement basis the necessary adjustment must be made in a Fallback Settlement on any of those days, or[360]

(B) where RITS is, at the time at which the error is found, functioning to effect settlements on a Real Time Gross Settlement basis the necessary adjustment must be made by sending a Payment for same day value on any of those days, or [361]

(ii) if the error is not found on the day of receipt of the erroneous payment or within 3 Business Days after the day on which the erroneous payment was sent necessary adjustment must be made in a manner and at a time to be agreed between the Framework Participants concerned.

[357] Last amended effective 1/1/18, version 037 r&p 001.17
[358] Last amended effective 1/1/18, version 037 r&p 001.17
[359] Last amended effective 1/1/18, version 037 r&p 001.17
[360] Last amended effective 1/1/18, version 037 r&p 001.17
[361] Last amended effective 1/1/18, version 037 r&p 001.17

9.37 Interest Adjustments For Errors

(a) The interest payable pursuant to Clause 9.36(a) will be calculated as follows:[362]

(i) in respect of the first day - interest will be calculated at the ESR; and[363]

(ii) in respect of subsequent days - interest will be calculated at the ESR; however if, because of a rate of interest actually obtained by, lost to, or paid by either or both of those Framework Participants concerned upon the amount involved or upon an amount equivalent thereto, it would be equitable for some other rate to be applied, then such other rate will be applied.[364]

9.38 Further Provisions Relating to Interest

If the Receiver and Sender concerned are unable to agree upon any question arising under Clause 9.36, the provisions of Regulations Part 13 will apply.[365]

9.39 Losses

The provisions of Part 13 of the Regulations apply in all cases where a loss has to be met by reason of a conflict of opinion as to which Framework Participant was responsible for the loss. [366]

9.40 SWIFT PDS and RITS/RTGS System Failure [Deleted][367]

9.41 Exchange Summary Data File Transfer Facility [Deleted][368]

The next page is Part 10

[362] Last amended effective 20/8/04, version 014 r&p 001.04
[363] Last amended effective 13/6/01, version 002 r&p 004.01
[364] Last amended effective 13/6/01, version 002 r&p 004.01
[365] Last amended effective 20/8/04, version 014 r&p 001.04
[366] Last amended effective 20/8/04, version 014 r&p 001.04
[367] Deleted effective 20/8/04, version 014 r&p 001.04
[368] Deleted effective 23/4/13, version 014 r&p 001.13

PART 10 TRANSITIONAL ARRANGEMENTS [DELETED][369]

[Deleted]

The next page is Part 11

[369] Deleted effective 20/11/06, version 021 r&p 003.06

PART 11 CYBER FRAUD EVENT[370]

11.1 Application of Appendix K (Cyber Fraud Instructions)

Where a Cyber Fraud Event occurs, then the Cyber Fraud Instructions will apply.

11.2 Fraud and Cyber Contact Point(s)

The Company will maintain a list of contact point(s) in Annexure L: Cyber Fraud contacts.

The next page is Annexure A

[370] Inserted effective 14/11/22, version 041 r&p 001.22

ANNEXURE A CERTIFICATION CHECKLIST

A.1 SYSTEM CERTIFICATION CHECKLIST FOR MEMBERSHIP OF THE HIGH VALUE CLEARING SYSTEM ("HVCS")[371]

(Clause 7.27)

It is a requirement of the HVCS that Framework Participants satisfy certain system and environmental requirements specified in the HVCS Regulations and Procedures prior to sending or receiving payments. Copies of the System Certification Checklist are available from the Company and can be obtained from the SWIFT PDS Operations Manager.

The System Certification Checklist has been designed to assist applicants and particularly audit personnel to ensure that all requirements have been met. The System Certification Checklist is divided into a number of self-contained sections, each detailing a range of requirements cross-referenced to the relevant Clause of the HVCS Procedures. Each item in the System Certification Checklist requires a simple positive (tick) or negative (cross) response. Should a particular item require clarification or the provision of additional data, comment or information can be included at the foot of each section or a separate advice provided and attached to the System Certification Checklist.

If any clarification or additional information is required, regarding the certification process, applicants should contact the SWIFT PDS Operations Manager.

The System Certification Checklist must be completed and signed by a duly authorised officer for and on behalf of the Applicant.

The actual commencement date for a new Framework Participant is designated by the Management Committee at the time the membership application is approved. However, where the applicant has a preferred launch date, the completed System Certification Checklist and the related test results will need to be provided to the Company no less than four weeks prior to that date.

A.1.1 Certification Testing

It is strongly recommended that Framework Participants perform certification testing on both their primary and backup configurations but it is recognised that this may cause difficulties for some members where an existing production environment is being utilised. If this is the case a Framework Participant may complete its certification on a similar configuration such as a test system. Where this occurs it is expected that the test configuration will closely replicate the live environment, details of which will be provided to AusPayNet as part of the Certification Test Factsheet. A hardcopy of the test results are not required except in those cases where the actual test result differs from the expected result in which case the requirements of Clause 7.27(d) apply.

[371] Last amended effective 20/11/06, version 021 r&p 003.06

SYSTEM CERTIFICATION CHECKLIST[372]

TO: THE HVCS MANAGEMENT COMMITTEE SECRETARYAUSTRALIAN PAYMENTS NETWORK LIMITED
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
SYDNEY NSW 2000

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM NAME OF APPLICANT ("Applicant") _____

PLACE OF INCORPORATION _____

AUSTRALIAN COMPANY NUMBER
AUSTRALIAN REGISTERED BODY NUMBER _____

REGISTERED OFFICE ADDRESS _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

EMAIL ADDRESS _____

Environment - Primary Computer Site

- A primary and backup HSM are available (Clauses 7.4(a) and 7.4(b)) (including Active-Active configurations). ☐
- Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available (Clause 7.7(a)). ☐
- Uninterruptable Power Supply (UPS) is available and supplied to the SCI hardware configuration (Clause 7.2(a)). ☐
- The area is fitted with adequate protection against fire, flood and water damage (Clause 7.2(a)). ☐

Environment - Backup Computer Site

- **Tier 1 Back-up Applicants Only -** Backup computer site is geographically separate from the primary site (Clause 7.12(a)). ☐
- **Tier 2 Back-up Applicants Only -** Backup computer site configuration meets requirements (Clause 7.13(a)). ☐

[372] Last amended effective 1/1/24, version 043 r&p 002.23

- **Tier 1 Back-up Framework Participant Only -** At least one SWIFT communication line is available, which is physically different from the two located at the primary site. The line must be encrypted (Clause 7.18). ☐

- UPS is available and supplied to the SCI hardware configuration (Clauses 7.12(e) and 7.13(d)). ☐

- The area is fitted with adequate protection against fire, flood and water damage (Clauses 7.12(d) and 7.13(c)). ☐

- The Backup configuration is capable of moving to live operations within the approved timeframe (Clauses 7.12(a) and 7.13(a)). ☐

Security[373]

- Self-attestation to the SWIFT Customer Security Controls Framework has been completed and submitted to SWIFT for each 8-character BIC operating in the PDS as per the SWIFT Customer Security Controls Policy (Clause 5.1(b)). ☐

- All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[374] (Clause 5.1(b)) ☐

System Availability[375]

- **Tier 1 Back-up Applicants only** - the system (which includes the SCI and the Core PPS) must be available at least 99.7% of the Core Business Hours (Clause 7.24(a)(i)). The level of system redundancy is designed to ensure: ☐

  (i) No single outage will exceed four (4) hours (Clause 7.24(a)(i)). ☐

  (ii) Yearly downtime will not exceed six (6) hours for those Framework Participants that do not participate in the Evening Settlement Session and eight (8) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.24(a)(i)). ☐

- **Tier 2 Back-up Applicants only** - the system (which includes the SCI and the Core PPS) must be available at least 99.5% of the Core Business Hours (Clause 7.24(c)). The level of system redundancy is designed to ensure: ☐

  (i) No single outage will exceed six (6) hours (Clause 7.13(f)). ☐

  (ii) Yearly downtime will not exceed ten (10) hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen (13) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.24(c)). ☐

System Performance[376]

[373] Last amended effective 1/1/18, version 037 r&p 001.17
[374] Note – if all mandatory controls have not been satisfied please complete the SWIFT Customer Security Mandatory Controls Non-compliance form.
[375] Last amended effective 1/1/14, version 034 r&p 001.14
[376] Amended effective 1/1/22, version 040 r&p 003.21

- Primary SCI is capable of processing 50% of daily transaction volume in 1 hour (Clause 7.25(a)). ☐
- Backup SCI is capable of processing 50% of daily transaction volume in 1 hour (Clause 7.25(a)). ☐
- Periods of system throughput degradation will be logged and reported if they reach the levels specified in the table below (Clause 7.25(c)) ☐

Percentage of AHTV*	Impaired Performance Period
50%	6 hours or greater
35%	5 hours or greater
25%	4 hours or greater
12%	3 hours or greater

* AHTV is average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgments

Operations[377]

- SWIFT PDS messages are stored on a suitable medium for a minimum of 7 years (Clause 7.26). ☐
- A SWIFT PDS Log is maintained that details dates, times and durations of backup tests, outages and their cause, periods of degraded SCI performance, changes to either the primary or backup environments etc (Clauses 4.5(f), 7.2(c), 7.12(f), 7.13(e), 7.19(b), 7.25(a), 7.25(c) and 9.5(e)). ☐

Certification Test Plan Results[378]

The following Certification Test Plan forms have been completed and are attached:

- Certification Test Factsheet; ☐
- Specific Conditions Test Checklist; and ☐
- Community Test Checklist. ☐

Full details of test script results required in terms of Clause 7.27(d) are attached.

REPRESENTATIONS AND UNDERTAKINGS

By executing this System Certification Checklist the Applicant:

(a) acknowledges that for the Applicant to qualify as a Framework Participant of HVCS to use the SWIFT PDS to send and receive payments under the HVCS Regulations and Procedures the Applicant must have obtained System Certification in accordance with the HVCS Regulations and Procedures and that this System Certification Checklist is required to obtain that System Certification;

[377] Amended effective 1/1/22, version 040 r&p 003.21
[378] Last amended effective 14/8/08, version 026 r&p 004.08

(b) warrants and represents that the information contained in this completed System Certification Checklist (including without limitation the attached test results) is correct and accurately reflects the results of system testing using the appropriate test script supplied by the Company for the purpose of that testing;

(c) acknowledges that the Company and each other Framework Participant of the HVCS relies and will continue to rely on the accuracy of the information and the Applicant's representations, acknowledgments, warranties and undertakings contained in this Certification checklist; and

(d) agrees that if the Applicant is accepted as a Framework Participant and/or if the Applicant is permitted to use the SWIFT PDS to send and receive payments, then, in consideration of such acceptance as a Framework Participant and/or permission to use the SWIFT PDS, the Applicant will:

(i) immediately notify the Company if it becomes, or has become, aware that any information contained in this System Certification Checklist (including without limitation the attached test results) is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and

(ii) provide to the Company with that notification full particulars of that wrong or misleading information.

Terms used in this Checklist in a defined sense have the same meanings as in the HVCS Procedures unless the context requires otherwise.

SIGNED FOR AND ON BEHALF
OF [NAME OF APPLICANT]:

_____

SIGNATURE OF AUTHORISED PERSON
By signing this System Certification Checklist the signatory states that the signatory is duly authorised to sign this System Certification Checklist for and on behalf of [NAME OF APPLICANT]

_____

NAME OF AUTHORISED PERSON (BLOCK LETTERS)

_____

OFFICE HELD

DATE:

The next page is Annexure A.2

A.2 YEARLY AUDIT COMPLIANCE CERTIFICATE FOR CONTINUING MEMBERSHIP OF THE HIGH VALUE CLEARING SYSTEM ("HVCS)[379]

(Clause 7.28(a))

It is a requirement of the HVCS that Framework Participants using the SWIFT PDS continue to meet at all times the SWIFT PDS and related environmental requirements, specified in the HVCS Regulations and Procedures. To assist with ensuring system-wide compliance, Framework Participants are required to carry out a yearly compliance audit in accordance with Clause 7.28(a) of the HVCS Procedures. Copies of the Yearly Audit Compliance Certificate to be given by each Framework Participant are available from the Company and can be obtained from the SWIFT PDS Operations Manager.

The Yearly Audit Compliance Certificate contains a standard checklist designed to assist Framework Participants and particularly audit personnel to ensure that all requirements have been met. The checklist is divided into a number of self-contained sections, each detailing a range of requirements cross-referenced to the relevant Clause of the HVCS Procedures. Each item in the checklist requires a simple positive (tick) or negative (cross) response. Should a particular item require clarification or the provision of additional information, comments can be included at the foot of each section or in a separate advice provided and annexed to the Yearly Audit Compliance Certificate.

Each Framework Participant is required to maintain a SWIFT PDS Log (see Clause 4.10(a)) containing details of:

(a) the date, time and nature of all its system outages, and the time required to re-establish live operations;

(b) alterations to its Primary Computer Site or Backup Computer Site system configuration since the date of its last Yearly Audit Compliance Certificate or if it has not previously given a Yearly Audit Compliance Certificate, the date of its System Certification Checklist;

(c) the date, time, duration and results of all its backup tests; and

(d) the date, time, duration, and percentages of all reportable instances of degraded SCI performance (Clause 7.25), and the cause and remedy (if known).[380]

The SWIFT PDS Log will form the basis of a number of the certification checks and should be perused to ensure that complete and adequate details are recorded.

If any additional information or clarification is required the Framework Participant should contact the SWIFT PDS Operations Manager.

The Yearly Audit Compliance Certificate (including the checklist) must be completed and signed by a duly authorised officer for and on behalf of the Framework Participant.

[379] Last amended effective 26/11/18, version 038 r&p 001.18

[380] Inserted effective 1/1/22, version 040 r&p 003.21

The Yearly Audit Compliance Certificate must be completed and returned to the Company by the end of January each year, such certificate to cover the prior calendar year and confirm that all SWIFT upgrades required since the last Yearly Audit Compliance Certificate have been implemented.[381]

[381] Last amended effective 16/1/09, version 027 r&p 005.08

YEARLY AUDIT COMPLIANCE CERTIFICATE[382]

TO: COMPLIANCE MANAGERAUSTRALIAN PAYMENTSNETWORK LIMITED
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
SYDNEY NSW 2000

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM: NAME OF FRAMEWORK PARTICIPANT ("Member") _____

PLACE OF INCORPORATION _____

AUSTRALIAN COMPANY NUMBER
AUSTRALIAN REGISTERED BODY NUMBER _____

REGISTERED OFFICE ADDRESS _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

EMAIL ADDRESS _____

Environment - Primary Computer Site

- A primary and backup HSM is available (Clauses 7.4(a) and 7.4(b)) (including Active-Active configurations). ☐
- Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available (Clause 7.7(a)). ☐
- Uninterruptable Power Supply (UPS) is available and supplied to the SCI hardware configuration (Clause 7.2(a)). ☐
- The area is fitted with adequate protection against fire, flood and water damage (Clause 7.2(a)). ☐
- The backup HSM was tested twice during the year (Clause 7.4(b)). ☐
- The secondary SWIFT communication line was tested on a minimum of four times during the year (Clause 7.7(a)). ☐

Environment - Backup Computer Site

- **Tier 1 Back-up Framework Participants Only -** Backup computer site is geographically separate from the primary site (Clause 7.12(a)). ☐

[382] Last amended effective 1/1/24, version 043 r&p 002.23

- **Tier 2 Back-up Framework Participants Only -** Backup computer site configuration meets requirements (Clause 7.13(a)). ☐

- **Tier 1 Back-up Framework Participant Only -** At least one SWIFT communication line is available, which is physically different from the two located at the primary site. The line must be encrypted (Clause 7.18). ☐

- UPS is available and supplied to the SCI hardware configuration (Clauses 7.12(e) and 7.13(d)). ☐

- The area is fitted with adequate protection against fire, flood and water damage (Clauses 7.12(d) and 7.13(c)). ☐

- **Tier 1 Back-up Framework Participant Only** - The Backup configuration's ability to move to live operations, with the required timeframes (as per clause 7.24(b)), was successfully tested at least twice during the year (Clause 7.19(a)) (including Active-Active configurations). ☐

- **Tier 2 Back-up Framework Participants Only** - The Backup configuration's ability to move to live operations, with the required timeframe (as per clause 7.13(f)), was successfully tested at least twice during the year (Clause 7.19(a)). ☐

Security

- Operating system security which runs on the SCI hardware functionally conforms to the SWIFT Customer Security Controls Framework (Clause 5.1(b) and 7.16). ☐

System Availability[383]

- **Tier 1 Back-up Framework Participants Only:**

  (i) The system (which includes the SCI and the Core PPS) was available at least 99.7% of the Core Business Hours during the last year (Clause 7.24(b)()); ☐

  (ii) No single outage exceeded four (4) hours (Clause 7.24(b)(C); and ☐

  (iii) Yearly downtime did not exceed six (6) hours for those Framework Participants that do not participate in the Evening Settlement Session and eight (8) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.24(b)(C). ☐

- **Tier 2 Back-up Framework Participants Only:**

  (The system (which includes the SCI and the Core PPS) was available at least 99.5% of the Core Business Hours during the last year (Clause 7.24(c)); ☐

  (iv) No single outage exceeded six (6) hours (Clause 7.24(c)); and ☐

  (v) Yearly downtime did not exceed ten (10) hours for those Framework Participants that do not participate in the Evening Settlement Session and thirteen (13) hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.24(c)). ☐

[383] Last amended effective 1/1/14, version 034 r&p 001.14

System Performance[384]

- Backup SCI is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.25(a)). ☐
- During the last year the system throughput was degraded to the level and for the periods detailed below (clause 7.25(b)). ☐

Percentage of AHTV*	Impaired Performance Period	Provide details of date, time, duration, cause and remedy if applicable. Otherwise insert N/A
50%	6 hours or greater	
35%	5 hours or greater	
25%	4 hours or greater	
12%	3 hours or greater	

* AHTV is average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgments.

Operations

- SWIFT PDS messages are stored on a suitable medium for a minimum of 7 years (Clause 7.26). ☐

SWIFT PDS Log

- A SWIFT PDS Log has been maintained and all appropriate details recorded as required in terms of these Procedures (Clause 4.10(a)). ☐

SWIFT Approved Standards Amendments

- Yearly SWIFT standards amendments as set out in the final version of the Advance Information Standards release guide for the relevant year and which are applicable to the SWIFT PDS, have been successfully implemented as required (Clause 5.23).[385] ☐

SWIFT Customer Security Controls Framework[386]

- Self-attestation to the SWIFT Customer Security Controls Framework has been completed and submitted to SWIFT for each 8-character BIC operating in the PDS as per the SWIFT Customer Security Controls Policy for the period corresponding to this annual compliance certificate (Clause 5.1(a)). ☐

- All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[387] (Clause 5.1(a)). ☐

Fallback Mode Processes and Testing[388]

- Documented procedures exist and staff are appropriately trained in fallback mode processes that meet the requirements of PART 9 of the Procedures.[389] ☐

[384] Amended effective 1/1/22, version 040 r&p 003.21
[385] Amended effective 30/11/01, version 004 r&p 006.01
[386] Inserted effective 1/1/18, version 037 r&p 001.17
[387] Note – if all mandatory controls have not been satisfied please complete the SWIFT Customer Security Mandatory Controls Non-compliance form.
[388] Inserted effective 18/1/16, version 036 r&p 002.15
[389] Inserted effective 18/1/16, version 036 r&p 002.15

- The most recent end-to-end test of fallback mode as required under Clause 9.7.2 of the Procedures was undertaken.[390] ☐

REPRESENTATIONS AND UNDERTAKINGS

By executing this Certificate the Member:

(a) acknowledges that under the HVCS Procedures the Member is required to submit this Yearly Audit Compliance Certificate to the Company in accordance with those Procedures;

(b) warrants and represents that the information contained in this Yearly Audit Compliance Certificate is correct and accurately reflects both the information recorded in the SWIFT PDS Log maintained by the Member under the HVCS Procedures and the operational status generally of the Member's systems used for HVCS exchanges;

(c) acknowledges that the Company and each other Framework Participant of the HVCS relies and will continue to rely on the accuracy of the information and the Member's representations, acknowledgments, warranties and undertakings contained in this Yearly Audit Compliance Certificate; and

(d) undertakes to immediately notify the Company if it becomes aware that any information contained in this Yearly Audit Compliance Certificate is wrong or misleading (including without limitation because of any omission to provide relevant additional information) and to provide to the Company with that notification full particulars of that wrong or misleading information.

SIGNED FOR AND ON BEHALF
OF *[NAME OF MEMBER]*:

_____

SIGNATURE OF AUTHORISED PERSON
By signing this Certificate the signatory states that the signatory is duly authorised to sign this Certificate for and on behalf of [NAME OF MEMBER]

_____

NAME OF AUTHORISED PERSON (BLOCK LETTERS)

_____

OFFICE HELD

DATE:

[390] Inserted effective 18/1/16, version 036 r&p 002.15

SWIFT Customer Security Mandatory Controls Non-Compliance[391]

This form maybe used by an HVCS Framework Participant to report non-compliance of the SWIFT Customer Security Mandatory Controls. Alternatively, participants may submit to AusPayNet the information contained in their SWIFT Customer Security Control Policy self-attestation.

This form will need to be populated separately for each instance of non-compliance.

TO: RISK AND COMPLIANCE
AUSTRALIAN PAYMENTS NETWORK
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
SYDNEY NSW 2000

or:

compliance@auspaynet.com.au

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM: NAME OF FRAMEWORK PARTICIPANT ("Member") _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

EMAIL ADDRESS _____

Control Item Not Satisfied	
Explanation of Non-Compliance	
Plan to Become Compliant	
Target Compliance Date	

Please copy the table above as necessary to report multiple instances of non-compliance

The next page is A.3

[391] Inserted effective 1/1/18, version 037 r&p 001.17

A.3 Incident Report

INCIDENT REPORT[392]

This form may be used by an HVCS Framework Participant to report a breach of Clause 7.24(f) *as part of that Framework Participant's Yearly Audit Compliance Certificate (see Clause 7.28(a)) or for the purposes of advising AusPayNet of any such breach prior to completion of the Yearly Audit Compliance Certificate.*

TO: RISK AND COMPLIANCE
AUSTRALIAN PAYMENTS NETWORK
SUITE 2, LEVEL 17,
GROSVENOR PLACE, 225 GEORGE STREET,
SYDNEY NSW 2000

or:

compliance@auspaynet.com.au

RE: THE HIGH VALUE CLEARING SYSTEM FRAMEWORK (CS4)

FROM: NAME OF FRAMEWORK PARTICIPANT ("Member") _____

NAME OF CONTACT PERSON _____

TELEPHONE NUMBER _____

EMAIL ADDRESS _____

Date of the outage	
Time outage began	
Time outage ended	
Description of event	

[392] Last amended effective 26/11/18, version 038 r&p 001.18

Impact	
Type of system failure (e.g. hardware, software, network etc.)	
Steps taken to resolve and/or work around the problem (including time frames for problem determination and decisions taken and details of any contingency measures invoked, including use of Back-up system).	
Analysis of what caused the outage	
Steps taken to mitigate risk of problem occurring again (e.g. improved monitoring, quicker response times, more controls and checks, new procedures/technology, etc).	
Author of incident report & contact details	

The next page is A.4

A.4 Guidelines for Certification when using Third Party Service Providers [393]

The purpose of these guidelines is to provide information to High Value Clearing System (HVCS) Framework Participants or Applicants (FP/A) who intend to use Third Party Providers (TPP) to supply the infrastructure to meet the technical requirements set out in Annexure A1 System Certification Checklist and Annexure A.2 Yearly Audit Compliance Certificate. This includes services commissioned as Infrastructure as a Service (IaaS) in the cloud.

Use of Third Party Providers for provision of a complete service (provision of primary and backup site and application software) is only available to Tier 2 Framework Participants (see clauses 7.8(a) and 7.19).

This document contains information on what requirements must be met by the Third Party Provider, by the Framework Participant or Applicant, or by both.

It is incumbent on the Framework Participant /Applicant to receive the appropriate signoff of these requirements from their TPP.

Environment - Primary Computer Site

	TPP	FP/A
• A primary and backup HSM are available (Clauses 7.4(a) and 7.4(b)).	☑	
• Two SWIFT communication lines, a primary and a secondary line for redundancy purposes, are available and both are encrypted (Clause 7.7(a)).	☑	☑
• Uninterruptable Power Supply (UPS) is available and supplied to the SCI hardware configuration (Clause 7.2(b)).	☑	
• The area is fitted with adequate protection against fire, flood and water damage (Clause 7.2(a)).	☑	
• The backup HSM was tested twice during the year (Clause 7.4(c)). (A2 Requirement only)	☑	
• The secondary SWIFT communication line was tested on a minimum of four times during the year (Clause 7.7(c)). (A2 Requirement only)	☑	☑

Environment - Backup Computer Site

• **Tier 2 Framework Participants -** Backup computer site configuration meets requirements (Clause 7.13(a)).	☑
• UPS is available and supplied to the SCI hardware configuration (Clauses 7.12(a) and 7.13(a)).	☑
• The area is fitted with adequate protection against fire, flood and water damage (Clauses 7.12(d) and 7.13(c)).	☑

[393] Last amended effective 14/11/22, version 041 r&p 001.22

Security

- Operating system security which runs on the SCI hardware functionally conforms to the SWIFT Customer Security Controls Framework (Clause 5.1(a) and 7.16). ☑

System Availability[394]

- The system (which includes the SCI and the Core PPS) was available at least 99.7% of the core RITS hours during the last year (Clause 7.24(b)). ☑
- No single outage exceeded 2 hours (Clause 7.24(b)). ☑ ☑
- Yearly downtime did not exceed 5 hours for those Framework Participants that do not participate in the Evening Settlement Session and 8 hours for those Framework Participants that do participate in the Evening Settlement Session (Clause 7.24(b)). ☑ ☑

System Performance[395]

TPP **FP/A**

- Primary SCI is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.25(a)). ☑
- Backup SCI is capable of processing 50% of the daily transaction volume in 1 hour (Clause 7.25(a)). ☑
- During the last year the system throughput was degraded to the level and for the periods detailed below (clause 7.25(b)). ☐

Percentage of AHTV*	Impaired Performance Period	Provide details of date, time, duration, cause and remedy if applicable. Otherwise insert N/A
50%	6 hours or greater	
35%	5 hours or greater	
25%	4 hours or greater	
12%	3 hours or greater	

* AHTV is average daily SWIFT PDS transaction volume in any one hour, including both inward and outward traffic and associated Acknowledgments.

Operations

- SWIFT PDS messages are stored on a suitable medium for a minimum of 7 years (Clause 7.26). ☑

SWIFT PDS Log

- A SWIFT PDS Log has been maintained and all appropriate details recorded as required in terms of these Procedures (Clause 4.10(a)). ☑ ☑

SWIFT Approved Standards Amendments

- Yearly SWIFT standards amendments as set out in the final version of the Advance Information Standards release guide for the relevant year and which are applicable to ☑

[394] Last amended effective 1/1/18, version 037 r&p 001.17
[395] Amended effective 1/1/22, version 040 r&p 003.21

the SWIFT PDS, have been successfully implemented as required (Clause 5.23(a)). (A2 Requirement only)

SWIFT Customer Security Controls Framework[396]

- Self-attestation to the SWIFT Customer Security Controls Framework has been completed and submitted to SWIFT for each 8-character BIC operating in the PDS as per the SWIFT Customer Security Controls Policy for the period corresponding to this annual compliance certificate (Clause 5.1). ☑
- All mandatory security control objectives as defined in the SWIFT Customer Security Controls Framework have been met.[397] (Clause 5.1). ☑ ☑

The next page is Annexure B

[396] Inserted effective 1/1/18, version 037 r&p 001.17

[1] Note – if all mandatory controls have not been satisfied please complete the SWIFT Customer Security Mandatory Controls Non-compliance form.

ANNEXURE B DELETED

B.1 FIN Copy of Entry Form [Deleted][398]

B.2 FIN Copy Service Form [Deleted][399]

B.3 FIN Copy withdrawal form [Deleted][400]

B.4 FIN Copy re-entry form [Deleted][401]

The next page is Annexure C

[398] Deleted effective 20/6/05, version 017 r&p 003.05
[399] Deleted effective 20/6/05, version 017 r&p 003.05
[400] Deleted effective 20/6/05, version 017 r&p 003.05
[401] Deleted effective 20/6/05, version 017 r&p 003.05

ANNEXURE C PROCESSING DIFFICULTIES, SETTLEMENT AND COMPENSATION CONTACT POINTS

Annexure C is issued as a separate document.

The next page is Annexure D

Annexure D is confidential

ANNEXURE D MESSAGE CONTENT[402]

(Clause 8.1)

Confidential

The next page is Annexure E

Annexure E is Confidential

[458] Last amended effective 1/1/18, version 037 r&p 001.17

ANNEXURE E SWIFT PDS CBT SECURITY REQUIREMENTS [DELETED][459]

[DELETED]

The next page is Annexure F

[459] Deleted effective 26/11/18, version 038 r&p 001.18

ANNEXURE F CHANGE REQUEST FORM

(Clause 5.25)

	AusPayNet documents	***Joint documents***
Change Request Number	**AusPayNet ….**	**AusPayNet/RBA ….**
Short Title		
Priority: *(high, medium or low)*		
Project team member for Contact:		
Contact telephone number:		

(To be Completed by AusPayNet)

Document affected:	
Change requested by:	*Organisation:* *Name:* *Telephone number:*

Description of change:

Reasons for change:

Benefits/disadvantages of changing:
Benefits:
Disadvantages:

Effects of not changing:

CHANGE REQUEST FORM

TO: AUSTRALIAN PAYMENTS NETWORK LIMITED

The Secretary:

e-mail Address:

FROM: **Date sent:**

Name of Financial Institution:

Change Request Number:

AusPayNet documents: **AusPayNet**

Joint documents: **AusPayNet/RBA**

Short Title:

Priority High/Medium/Low

Project team member for Contact:

Contact phone number:

Document affected:

Change requested by: Organisation:

Name:

Telephone number:

Description of change:

Reasons for change:

Benefits/disadvantages of changing:

Benefits:

Disadvantages:

Effects of not changing:

The next page is Annexure G

ANNEXURE G EXCHANGE SUMMARY[460]

Annexure G is displayed on the Company's extranet

The next page is Annexure H

[460] Last amended effective 18/1/16, version 036 r&p 002.15

ANNEXURE H HVCS BIC/BSB DIRECTORY

(Clause 4.8)

The following functional specifications have been prepared to assist Framework Participants to make the necessary modifications to their own proprietary systems.

General Characteristics:

The electronic files will be a fixed length file produced on a 31/2" floppy disk and contain the same fields as the printed reports. There will be a header, a variable number of detail records and a trailer for each file.

Record Descriptions

Header Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field (all zeros)	1	N (Contains "0")
2 - 9	File Effective Date	8	N (CCYYMMDD)
10 - 23	Creation Date & Time Stamp	14	N (CCYYMMDDhhmmss)
24 - 32	File update Number	9	N
33 - 209	Spare	177	AN

Detail Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains "1")
2 - 7	BSB Number	6	N
8 - 9	BSB Usage Indicator (see Note 1 for detail)	2	AN
10 - 44	BSB Name	35	AN

45 - 79	BSB Street Address	35	AN
80 - 99	BSB City/Town/Suburb	20	AN
100 - 102	BSB State	3	AN
103 - 106	BSB Post Code	4	N
107 – 109	Framework Participant	3	AN
110 - 120	BIC	11	AN
121 - 209	Reserved for future use	89	AN

Trailer Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains “9”)
2 - 10	Number of detail records on File	9	N
11 - 209	Spare	199	AN

BIC BSB UPDATE REPORT

Record Descriptions:

Header Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field (all zeros)	1	N (Contains “0”)
2 - 9	File Effective Date	8	N (CCYYMMDD)
10 - 23	Creation Date & Time Stamp	14	N (CCYYMMDDhhmmss)

24 - 32	File update Number	9	N
33 – 209	Spare	177	AN

Detail Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains “1”)
2 - 4	Change Indicator (see Note 2 for detail)	3	AN
5 - 10	BSB Number	6	N
11 - 12	BSB Usage Indicator (see Note 1 for detail)	2	AN
13 - 47	BSB Name	35	AN
48 - 82	BSB Street Address	35	AN
83 - 102	BSB City/Town/Suburb	20	AN
103 - 105	BSB State	3	AN
106 - 109	BSB Post Code	4	N
110 - 112	Framework Participant	3	AN
113 - 123	BIC	11	AN
124 - 209	Reserved for future use	86	AN

Trailer Record

BYTE LOCATIONS	FIELD NAME	FIELD LENGTH	DATA FORMAT
1	Control Field	1	N (Contains “9”)
2 - 10	Number of detail records on File	9	N
11 - 209	Spare	199	AN

Legend:

N Numeric only, left zero fill
AN Alpha/Numeric

Notes on Detail Record:

Note 1:

The BSB Usage indicator has the following values:

00 - BSB
01 - BSB Repair Routing Code

Note 2

The Change Indicator will have the following values:

ADD - if the record has been added
CHG - if the record has been changed
DEL - if the record has been deleted

The next page is Annexure I

Annexure I is Confidential

ANNEXURE I MESSAGE PREPARATION GUIDELINES FOR SWIFT PDS PAYMENTS[461]

Confidential

[461] Last amended effective 21/11/09, version 029 r&p 003.09

The next page is Annexure J

ANNEXURE J CONTINGENCY INSTRUCTIONS FOR THE HIGH VALUES CLEARING SYSTEM (CS4)[462]

1. INTRODUCTION

These Contingency Instructions provide instructions and guidance for High Value Clearing System (HVCS) Framework Participants (Participants) to ensure the continuity of orderly clearing and settlement in the event that either:

- a Participant experiences a Disabling Event that prevents it from sending HVCS payments in the normal way; or
- the Reserve Bank of Australia (RBA) experiences a Disabling Event that prevents the Reserve Bank Information and Transfer System (RITS) from settling HVCS payments in the normal way.
- Participants must comply with the instructions set out in this document.

1.1 Relationship with other documents

Document	Relationship / Purpose	Owner
HVCS Contingency Industry Test Strategy	The high-level strategy for testing HVCS contingency arrangements.	AusPayNet
HVCS Contingency Industry Test Plan	The detailed test plan for industry contingency test exercises. A test plan is produced for each annual test.	AusPayNet
HVCS Exchange Summary Form	A summary document substantially in the form of Appendix G in a format prescribed by the RBA. Used by a Framework Participant to submit its net bilateral obligations with each of its counterparties to the RBA for net settlement the next day.	RBA
HVCS Bilateral Clearing Form	A document in a format prescribed by AusPayNet used by an Affected Participant to send HVCS payments to another Framework Participant.	AusPayNet
RITS Member Contingency Procedures (MCP)	High-level procedures to be followed by RITS Members if a contingency disrupts the efficient operation of RITS or the Fast Settlement Service (FSS) over an extended period.	RBA
AusPayNet Member Incident Plan (MIP)	Framework for industry coordination during an operational incident affecting the HVCS.	AusPayNet
AusPayNet Crisis Communication Plan (CCP)	Framework for industry and media communication during a major disruption to any of the payments systems or infrastructure that fall under the remit of AusPayNet.	AusPayNet

2 SCOPE

These Contingency Instructions provide instructions and guidance for Framework Participants in the event of an extended RITS Outage or an extended Participant Outage. The Contingency Instructions are intended to set a baseline of operational requirements and expectations among Participants to ensure the continuity of HVCS payments during a HVCS Fallback Period or a Participant Fallback Period.

[462] Inserted effective 19/7/21, version 039 r&p 001.21

2.1 Applicable Scenarios

2.1.1 RITS Outage

This is a period during which the RBA is experiencing a Disabling Event that prevents RITS from effecting settlement of HVCS payments in the normal way. The scenario would be such that the RBA has ruled out the possibility to resolve the Disabling Event in time to complete settlement of HVCS payments in the normal way on that day. Where this occurs, AusPayNet, after consultation with the RBA, can declare a HVCS Fallback Period during which the HVCS Fallback Solution will be used to enable same-day clearing to occur, with settlement deferred to the next business day. The HVCS Fallback Solution comprises:

Fallback Clearing	Same-day clearing through the SWIFT PDS in T-Copy Mode.
Fallback Settlement	Deferred (next-day) multilateral net settlement using data submitted to the RBA from Participants in HVCS Exchange Summary Form spreadsheets.

2.1.2 Participant Outage

This is a period during which a Participant is experiencing a Disabling Event that prevents that Participant from sending HVCS payments in the normal way. The scenario would be such that the Affected Participant, in consultation with AusPayNet and the RBA, is not confident that the Disabling Event can be resolved in time to send any payments deemed urgent by the Affected Participant before the RITS cut-off times. Where this occurs, AusPayNet can declare a Participant Fallback Period during which the Participant Fallback Solution can be used to enable same-day clearing of the Affected Participants outbound HVCS payments to continue, with settlement of the net bilateral obligations occurring on the same day via RITS Cash Transfers. The Participant Fallback Solution comprises:

Fallback Clearing	Outbound payments: Clearing information sent from the Affected Participant to each Receiver using the HVCS Bilateral Clearing Form. Note that inbound payments will continue to be sent to the Affected Participant through the SWIFT PDS in the normal way.
Fallback Settlement	Outbound payments: Deferred (same-day) bilateral net settlement using RITS Cash Transfers. Note that the settlement of inbound payments received by RITS through the SWIFT PDS feeder will be effected in the normal way (RTGS).

2.1.3 Out of Scope

Arrangements for the following Contingency scenarios are outside the scope of these Contingency Instructions:

- Disabling Events occurring at the Participant, RITS or CSI level that can be resolved on the same day, within the checkpoint times outlined in the RITS Outage Runsheet and Participant Outage Runsheet contained in these Contingency Instructions.

- Contingency arrangements for a Disabling Event at the SWIFT Network level.

- Contingency arrangements for HVCS payments to or from CLS Bank. During a RITS Outage, Participants must not send payments to CLS Bank using the HVCS Fallback Solution. A CLS AUD holiday could be declared in such circumstances, in accordance with the CLS Bank's own contingency procedures.

- **2.2 Document Structure**

- The Contingency Instructions for each of the two outage scenarios are divided into the following sections:

Section	Description
Runsheets	Checkpoint times and sequence of events for declaring a Fallback Period and using the Fallback Solution
Instructions	*Operational Readiness*: Pre-requisites and preparation for a Fallback Period. *Participation:* Who participates during a Fallback Period. *Entering Fallback*: Declaring a Fallback Period and invoking the Fallback Solution. *During Fallback*: Using the Fallback Solution. *Exiting Fallback*: Decision and processes to exit a Fallback Period. *Operational Capacity*: Payment volumes when using the Fallback Solution. *Applying Funds*: Applying funds received through the Fallback Solution to Customer accounts.

2.3 Classification of Instructions

These Contingency instructions can be applied under PART 9 of these Procedures which is designed to enable orderly operation of the HVCS during a Contingency. In accordance with Clause 9.3(a) of these Procedures, Participants have a responsibility to each other, and to the system as a whole, to cooperate in resolving any processing difficulties. To the extent that such co-operation does not adversely affect its own processing environment, a Participant should provide such co-operation.

There are three classifications of instructions:

Rating	Definition
Must	Participants are required to implement all 'Must' items. These *requirements*: • define a minimum level of functionality in order for a Fallback Solution to be viable and meet its objectives; • enable Participants to meet their clearing obligations and minimise disruption to Customers.
Should	Participants are expected to implement 'Should' items. These *expectations:* • provide instructions and guidance on aspects of the Fallback Solution that may vary based on the specifics of a Participants systems or operations.
Could	Participants are encouraged to consider 'Could' items but are not required to implement them. These *considerations*: • provide indications of recommended best practice.

2.4 Classification of Framework Participants

These Contingency Instructions classify Participants in accordance with Clause 7.9(a) of these Procedures regarding the Back-up Computer Site a Participant must maintain in order to resume SWIFT PDS operations during a disruption to their Primary Computer Site. Back-up Computer Site tiers are based on the Participants payment values:

- Tier 1 Back-up: 2.00% or more of Total National Transaction Value.
- Tier 2 Back-up: up to but not including 2.00% of Total National Transaction Value.
- The Total National Payment Value means the aggregate value of all payments sent and received by all Framework Participants participating in the SWIFT PDS. This aggregate value is determined using statistical data collected over a period of three consecutive calendar months, in accordance with Clause 7.9(a) of these Procedures.

3 RITS Outage Runsheet

This runsheet outlines the checkpoint times and sequence of events for a HVCS Fallback Period. It is based on the following assumptions:

1) The priority is recovering RITS in order to resume normal operations. As such, a decision to declare a HVCS Fallback Period is unlikely to be taken ahead of the checkpoint times outlined. However, where a recovery of RITS has been ruled out ahead of the checkpoint times, then ensuring ongoing clearing of HVCS payments becomes a priority and a HVCS Fallback Period may be declared earlier. Once active, T-Copy mode will remain in place for the duration of the PDS Operating Day.

2) HVCS Fallback operations for the day, up to and including the submission of HVCS Exchange Summary Forms to the RBA (Step 6), should be complete by 21:00.

3) To achieve this, the decision to declare a HVCS Fallback Period should be taken by 16:00. Where it is necessary to delay this decision, the 21:00 completion time may also be delayed and the time available to Participants for clearing payments using the HVCS Fallback Solution (Step 4) may be reduced.

4) If a Disabling Event occurs after 15:00, the assumption is that a HVCS Fallback Period would not normally be required; however the RBA would assess the conditions and potential systemic impact on the day of the event.

5) In all cases, a decision to declare a HVCS Fallback Period will not be taken within one hour of a Disabling Event occurring in order to allow for sufficient investigation by the RBA. Participants should begin preparing for a potential HVCS Fallback Period when a Disabling Event occurs, but will be given a minimum of 30 minutes from when the HVCS Fallback Period is declared to the implementation of the HVCS Fallback Solution.

Step / Checkpoint		Time	Description	Who
Before	RITS Disabling Event occurs and incident coordination begins.	Before 15:00	A Disabling Event prevents RITS from effecting settlement in the normal way. An incident is raised and managed in accordance with the AusPayNet Member Incident Plan and if applicable, the Crisis Communication Plan. The RBA works to resolve the issue and recover RITS. Participants are aware of the potential for a HVCS Fallback Period and begin to prepare.	RBA, AusPayNet and Participants

	Decision taken to invoke HVCS Fallback Period.	By 16:00	The RBA determines RITS cannot be recovered in time to complete settlement and AusPayNet declare a HVCS Fallback Period.	RBA and AusPayNet
Checkpoint	**HVCS Fallback decision point.**	**16:00**	**Decision to declare HVCS Fallback Period to be made by this time.**	
Step 1	SWIFT instructed to change FIN-Copy Service mode.	15 min	A Business Officer instructs SWIFT via the SWIFT Secure Channel. The Business Officer will request that SWIFT close the service and effect the change no earlier than 30 minutes from the time that the HVCS Fallback Period was declared to Participants.	AusPayNet or RBA
Step 2	SWIFT undertake FIN-Copy Service mode change.	45 min	SWIFT enact the service mode change. SWIFT require a maximum of 45 minutes to do this (i.e. from the point of being instructed to the point that the service reopens in T-Copy mode).	SWIFT
Checkpoint	**T-Copy start time.**	**17:00**	**PDS to be operating in T-Copy mode by this time.**	
Step 3	RBA confirms change of mode to Participants.	5 min	The RBA notify Participants upon receiving confirmation from SWIFT that the mode has changed.	RBA
Step 4	Clearing continues in T-Copy.	2 hrs	Participants exchange HVCS payments. This could include clearing up to a full day's volume of payments, including any additional steps Participants must perform when operating in T-Copy. The RBA will notify Participants of the approaching T-Copy Cut-off Time 30 minutes before the Cut-off Time.	Participants
Checkpoint	**T-Copy Cut-off time.**	**19:00**	**No further T-Copy clearing to occur after this time.**	
Step 5	SWIFT instructed to change FIN-Copy Service mode.	5 min	A Business Officer instructs SWIFT via the SWIFT Secure Channel to change the FIN-Copy Service from T-Copy to Y-Copy mode.	AusPayNet or RBA
Step 6	Participants compile and submit provisional HVCS Exchange Summary Forms to RBA.	2 hrs	Participants record the net bilateral obligations arising from the payments exchanged in Step 4 in the HVCS Exchange Summary Form. Each Participant sends one HVCS Exchange Summary Form to the RBA. The RBA confirms receipt of these via encrypted email. Resolution of discrepancies and failures to match is performed in Step 8.	Participants

Step 7	RBA produces and sends Provisional HVCS Exchange Figures Advice to Participants.	1 hr	The RBA generate a Provisional HVCS Exchange Figures Advice for each Participant based on the HVCS Exchange Summary Forms submitted in Step 6. Any mismatching net bilateral positions between Participants will be displayed in this advice. The advices will be sent to Participants via encrypted email. Participants have until the commencement of the Morning Settlement Session the next day to reconcile any discrepancies with other Participants and submit a revised version of their HVCS Exchange Summary Form to the RBA (see Step 12).	RBA
Step 8	Overrun buffer.	2 hrs	Buffer if Steps 1 to 7 overrun. Participants can use this time to resolve mismatching net bilateral positions advised by the RBA in Step 7.	-
Checkpoint	**Midnight.**	**00:00**	**Hard cut-off time. Step 7 must be complete by this time.**	
Step 9	RITS recovery continues.	6.5 hrs	Where necessary, the RBA continue work to recover RITS ready for the overnight processing required before the next day.	RBA
Step 10	RITS reports and overnight processing occurs.		RBA proceed with normal report production and overnight processing required to prepare RITS for the next day.	
Step 11	RITS connection to SWIFT Feeder restored.		Once RITS is recovered and the system date has rolled forward, the SWIFT Feeder connection is restored. The backlog of settlement requests held in the CSI from T-Copy clearing the previous day will enter RITS and be rejected due to the back-dated value date. Senders can use the RITS UI to view the record of rejected T-Copy settlement requests (see Step 12).	
Checkpoint	**RITS available.**	**06:30**	**RITS to be available by this time to prepare contingency batch.**	
Step 12	Participants perform optional reconciliation of HVCS Exchange Summary Forms to RITS.	30 min	Using the RITS UI, Participants can export a record of payments sent in T-Copy the previous day (Step 4) and rejected by RITS (Step 11). Participants can also obtain a record of payments settled or rejected by RITS prior to the Disabling Event using statements produced in Step 10, or the RITS UI. Participants can elect to use these RITS records to reconcile the net obligations in their Exchange Summary Forms which may help to resolve a failure to match discrepancy identified in Step 7.	Participants

			Where required, Participants can submit a revised HVCS Exchange Summary Form to the RBA at any time between Step 8 and Step 12 (inclusive).	
Checkpoint	**HVCS Exchange Summary Form discrepancies rectified.**	**07:00**	**1. RBA applies Failure To Match (FTM) rules to all remaining discrepancies.**	
Step 13	RBA produces and sends Final Exchange Figures Advice & Net Clearing System Obligations Advice to Participants.	30 min	2. The RBA apply FTM rules in accordance with Clause 9.32(a) of these Procedures to any remaining discrepancies in Participant's HVCS Exchange Summary Form and sends a Final HVCS Exchange Figures Advice to Participants via encrypted email. 3. This will include a Net Clearing System Obligations Advice that shows a Participant's multilateral net position in the contingency batch, including clearing interest	RBA
Checkpoint	**RITS Morning Settlement Session starts.**	**07:30**	**RBA enters the contingency batch in RITS at the commencement of the Morning Settlement Session (MSS).**	
Step 14	Participants pre-fund ESAs.	25 min	Where required, Participants pre-fund their ESA in preparation for settlement of the contingency batch.	Participants
Step 15	Contingency batch entered in RITS and settlement testing begins.	5 min	Batch obligations could settle immediately if all Participants in the batch have sufficient ESA funds.	RBA
Step 16	Contingency batch settlement testing period.	30 min	Participants with a shortfall of ESA funds must finalise funding within this 30 minute window. Settlement testing for the contingency batch times out after 30 minutes.	Participants
Checkpoint	**Contingency batch settled.**	**08:45**	**If the contingency batch has not settled by the end of this period the RBA may extend the MSS as necessary until the batch is settled.**	
After	9.00am batch settlement occurs.	30 min	Only processing associated with the 9.00am batch can be undertaken during this session. The contingency batch cannot settle in this session.	RBA
Checkpoint	**RITS Daily Settlement Session starts.**	**09:15**	**RITS Daily Settlement Session will not begin until the previous day's HVCS obligations have settled.**	
After	Normal operations resume.	-	HVCS payments dispatched on the current day clear in Y-Copy mode.	-

4 Participant Outage Runsheet

This runsheet outlines the checkpoint times and sequence of events for a Participant Fallback Period. It is based on the following assumptions:

1) The priority is recovering the Affected Participant's Disabling Event in order to resume normal operations. As such, a decision to declare a Participant Fallback Period is unlikely to be taken ahead of the checkpoint times outlined. However, if the Affected Participant has urgent payments to send and cannot estimate their recovery time; or is able to rule out a recovery ahead of the checkpoint times, then minimising the delay to payments becomes a priority and a Participant Fallback Period could be declared earlier.

2) Where the Affected Participant has not recovered by 15:00, a Participant Fallback Period could be declared, during which time the Participant Fallback Solution can be used to send payments from the Affected Participant to Receivers. Payments to the Affected Participant must continue to go through the SWIFT PDS and will be queued in the Affected Participant's SWIFT systems until their inward processing is restored. These payments will continue to be tested and settled in RITS as per the normal operation of the SWIFT PDS Feeder.

3) The Participant Fallback Period checkpoints are linked to RITS session times and rules. This allows Receivers to effectively manage their end of day liquidity operations and ensure they have sufficient operational staff available.

4) Outgoing payments from the Affected Participant to Receivers should be complete by the end of the RITS Settlement Close Session at 17:15. The checkpoint times and instructions regarding the frequency of bilateral clearing and settlement should enable the Affected Participant to send and settle at least one batch of payments per Receiver. Where the Affected Participant is Evening Agreed and wishes to send payments to another Evening Agreed Participant after the Settlement Close Session, the Affected Participant must obtain prior agreement from the Receiver. These payments must be complete by the Evening Settlement Cut-off.

5) Where the volume of payments the Affected Participant intends to send a Receiver exceeds the instructions on payment volumes, the Affected Participant must obtain prior agreement from the Receiver.

6) If the Affected Participant's Disabling Event occurs after 14:00, AusPayNet in consultation with the RBA, would normally expect that a Participant Fallback Period would not be required, but would consider the value of outstanding payments in its assessment.

Step / Checkpoint		Time	Description	Who
Before	Disabling Event occurs and incident coordination begins.	Before 14:00	A Disabling Event occurs that prevents the Affected Participant from sending HVCS payments in the normal way. An incident is raised and managed according to the AusPayNet Member Incident Plan. The Affected Participant works to resolve the issue. All Participants are aware of the potential for a Participant Fallback Period and begin to prepare. During this period, the Affected Participant actively manages their ESA balance and where necessary, recycles liquidity via RITS Cash Transfers. Other Participants must be able to pause outbound payments to the Affected Participant if requested to do so by the Affected Participant.	RBA, AusPayNet and Participants
	Decision taken to declare a Participant Fallback Period.	By 15:00	If the Affected Participant has not recovered by this time, AusPayNet, in consultation with the RBA and the Affected Participant, declare a Participant Fallback Period.	AusPayNet, RBA and Affected Participant
Checkpoint	**Participant Fallback decision point.**	**15:00**	**Decision to declare a Participant Fallback to be made by this time.**	
Step 1	Affected Participant sends payments using the HVCS Bilateral Clearing Form and enters corresponding RITS CT.	60 min	The Affected Participant produces and sends a HVCS Bilateral Clearing Form to Receivers; and enters the corresponding bilateral settlement obligations to RITS via Cash Transfer.	Affected Participant
Step 2	Receivers accept the HVCS Bilateral Clearing Form and enter corresponding RITS CT.	30 min	Receivers review the HVCS Bilateral Clearing Form received from the Affected Participant and enter the corresponding bilateral settlement obligation to RITS via Cash Transfer.	Other Participants

Checkpoint	**RITS Daily Settlement Session ends.**	**16:30**	**Cut-off for sending payments.**	
Step 3	RITS CT matched and bilateral obligations settle.	-	Settlement occurs when the Cash Transfers input by the Affected Participant and Receiver are matched in RITS, subject to the Affected Participant having sufficient ESA funds.	-
Step 4	Receivers post payments to Customer accounts.	45 min	The Receiver should aim to apply funds received from the Affected Participant to Customer accounts before the RITS Settlement Close Session ends. Where this is not possible, the Receiver could inform the Affected Participant of the expected completion time.	Other Participants
Checkpoint	**RITS Settlement Close Session ends.**	**17:15**	**Cut-off for settlement of payments.**	
-	Overrun buffer.	45 min to 3 hr 15	The Affected Participant can send additional payments during this period if they and the Receiver are both Evening Agreed and where the Receiver agrees to accept the payments.	Affected Participant
Checkpoint	**RITS Evening Settlement cut-off.**	**18:30** **19:30** **20:30**	**Cut-off for settlement of Evening Agreed Participant payments.**	

5 RITS Outage Instructions

5.1 Operational Readiness

The following instructions cover items that Participants are expected to have in place in preparation for a HVCS Fallback Period.

5.1.1 Operational Readiness

Participants **must** be operationally ready to continue to participate in the HVCS if a HVCS Fallback Period is declared. This includes:

1) being familiar with these Procedures and the Contingency Instructions;

2) being capable of making the internal system and operational changes required to send and receive payments during the HVCS Fallback Period;

3) participating in contingency test exercises coordinated by AusPayNet; and

4) ensuring staff are available and contactable at all times during the HVCS Fallback Period and during planned contingency test exercises.

5) Participants **must** attest to their adherence with these requirements as part of the completion of the Yearly Audit Compliance Certificate (Annexure A.2).

5.1.2 Projected ESA Balance

Participants **must** have reliable and preferably system-based methods for tracking their bilateral net settlement obligations and projected ESA balance during a HVCS Fallback Period.

Note: Depending on the nature of the Disabling Event, it may not be possible for Participants to obtain the most recent record of their ESA balance from RITS. As such, Participants must be ready to use the last-known ESA balance according to their own internal records or obtained from RITS prior to the Disabling Event.

5.1.3 Non-Current Day Payments

Participants **must** have reliable and preferably system-based methods for preventing future-dated and back-dated payments from being sent in SWIFT T-Copy[463] and for identifying fu ture-dated and back-dated payments received in error.

5.1.4 Processing Rules

Participants **should** establish system rules required to smoothly handle differences between SWIFT T-Copy messages compared to SWIFT Y-Copy. Requirements will depend on the configuration of Participants internal systems. For example:

463 SWIFT does not perform date validations on payment messages sent to the FIN-Copy Service and as such, these messages will be delivered straight to the Receiver when T-Copy mode is in operation.

- Senders will not receive MT012 or MT019 responses from RITS for payments sent under T-Copy. Participants that rely on these messages **should** have a system-based method to account for this in their downstream processing.

- Senders will receive a negative acknowledgement (NAK) from SWIFT with error code X09 for payments sent while the SWIFT PDS FIN-Copy Service is closed to change modes. Participants **should** establish system rules to process these NAK's. Payments can be resent once the SWIFT PDS reopens in T-Copy.

- Receivers will not see Field 115 or the Digital Certificate 2 field in messages received under T-Copy. In addition to this, where a payment was dispatched under Y-Copy but subsequently released under T-Copy, Receivers will also see an empty PAC trailer added to block 5 of the message. Participants that use these fields **should** have systems-based means to account for this in their downstream processing.

5.2 Participation

The following instructions describe the extent to which Participants are expected to participate in the HVCS when a HVCS Fallback Period has been declared.

5.2.1 Extent of Participation

When a HVCS Fallback Period has been declared and the SWIFT PDS is operating in T-Copy Mode:

1) All Participants **must** continue to *accept* payments received from another Participant. Instructions for applying incoming funds to Customer accounts are set out in Section 6.7.

2) Tier 1 Participants **must** continue to *send* payments in accordance with the operational capacity instructions in Section 6.6.

3) Tier 2 Participants **should** continue to *send* payments in accordance with the operational capacity instructions in Section 6.6 but can, where it determines in advance that it will not send payments, elect to opt-out, in accordance with 6.2.2.

4) All Participants **must** manage their forecast liquidity position during the HVCS Fallback Period, taking account of the net bilateral obligations due for settlement in the contingency batch the next day.

5.2.2 Participation Opt-Out

Tier 2 Participants that do not intend to continue sending payments during a HVCS Fallback Period **must** have pre-agreed this arrangement with AusPayNet. Where there are extenuating circumstances in which the Tier 2 Participant needs to send payments during a HVCS Fallback Period, the Tier 2 Participant **must** notify and obtain prior agreement from the Receiver.

Note: A list of pre-agreed Tier 2 Participants will be available from the AusPayNet Extranet site such that during a HVCS Fallback Period, it is clear that other Participants should not expect to receive payments from those on the list.

5.2.3 SWIFT Connectivity

Participants **must** remain connected to the SWIFT PDS during the HVCS Fallback Period. That is, a Participant must not disable its connection to the SWIFT network via physical or logical means or deliberately undertake any action that would result in them being unable to send or receive payments via the SWIFT PDS.

5.3 Entering HVCS Fallback

The key checkpoint times for declaring and entering a HVCS Fallback Period are set out in the RITS Outage Runsheet. In summary, where a Disabling Event prevents RITS from settling HVCS payments the priority is recovering RITS in order to resume normal system operations. As such, a decision to declare a HVCS Fallback Period is unlikely to be taken ahead of the checkpoint times outlined. However, if the RBA rule out a recovery of RITS ahead of the checkpoint times, then minimising the delay to payments becomes the priority and a HVCS Fallback Period could be declared earlier. If a Disabling Event occurs after 15:00, the RBA would not normally expect to declare a HVCS Fallback Period, but would assess the conditions and potential systemic impact on the day of the event. In all cases, a decision to declare a HVCS Fallback Period will not be taken within one hour of a Disabling Event occurring in order to allow for sufficient system investigation by the RBA.

The following instructions apply once a HVCS Fallback Period has been declared.

5.3.1 Participant Preparation Time

Participants **should** begin preparing for a potential HVCS Fallback Period when a Disabling Event occurs, but will be given a minimum lead time of 30 minutes from the decision to declare a HVCS Fallback Period to its implementation. AusPayNet or the RBA will instruct SWIFT to close the FIN-Copy Service and effect the change to T-Copy no earlier than 30 minutes from the time that the HVCS Fallback Period was declared to Participants.

Transition to SWIFT T-Copy

AusPayNet or the RBA inform SWIFT of the incident by phone call and foreshadow the impending action to change the SWIFT FIN-Copy Service from Y-Copy to T-Copy mode. The instruction is formally lodged with SWIFT using the SWIFT Secure Channel.[464]

Upon instruction, SWIFT commence the procedure to switch the FIN-Copy Service mode. Switching modes takes up to 45 minutes during which time the FIN-Copy Service will close for up to 15 minutes. The impact on payments during the transition to T-Copy is as follows:

- **Before**: Payments sent before the SWIFT FIN-Copy Service closes, including those that were deferred in RITS or In-Flight when the Disabling Event began, will remain stored in the SWIFT FIN-Copy Service. When the SWIFT FIN-Copy Service closes, SWIFT will immediately forward the stored payments to the Receiver. The messages delivered to the Receiver will contain an empty PAC trailer in block 5 of the message and will not contain a Digital Certificate 2 from RITS. This indicates that the message was sent when the FIN-Copy Service was in Y-Copy mode, and has subsequently bypassed RITS due

464 Information available at https://www.swift.com/myswift/secure-channel

to the mode change. The Sender will not receive MT012 or MT019 responses for these payments.

- **During**: Payments sent while the SWIFT FIN-Copy Service is temporarily in a closed state will receive a NAK from SWIFT with error code X09. The Sender can resend these payments when the SWIFT FIN-Copy Service reopens.
- **After**: Payments sent after the SWIFT FIN-Copy Service reopens in T-Copy mode will immediately be forwarded to the Receiver by SWIFT. The messages delivered to the Receiver will not contain a Digital Certificate 2 from RITS. This indicates that the message was sent in T-Copy mode and has bypassed RITS.[465] The Sender will not receive MT012 or MT019 responses for these payments.

5.3.2 Notifying Participants

The RBA will notify Participants upon receiving confirmation from SWIFT that FIN-Copy Service mode has been changed. Service notifications will be sent to RITS Operational Contacts via email and SMS.[466]

5.3.3 Confirmation of ESA Balance

If possible, the RBA will provide Participants with confirmation of their last known ESA balance prior to entering the HVCS Fallback Period. This may not be possible if the Disabling Event prevents the RBA from accessing this information, in which case, Participants **must** use their own internal records.

5.3.4 Payment Status

Participants **must** use their internal system records to determine the status of payments sent prior to and during the HVCS Fallback Period.

Note: As previously described, receipt of a MT012 or MT019 response from RITS indicates that a payment has been processed by RITS. Once the FIN-Copy Service has reopened in T-Copy mode, the absence of a MT012 or MT019 response from RITS indicates that a payment has bypassed RITS. For the avoidance of doubt, payments sent prior to the Disabling Event for which the Sender has received a MT012 or MT019 have been settled or rejected and their processing can be considered as complete.

5.4 During HVCS Fallback

5.4.1 Message Format

Senders **must** continue to format MT103 and MT202 messages in accordance with the Message Preparation Guidelines set out in these Procedures.

5.4.2 Preventing Non-current Day Payments

Participants **must** ensure that the methods they use for preventing future and back dated

465 MT096 messages will still be created and sent to the CSI as per Y-Copy, but will not be passed to RITS.
466 See RITS Member Contingency Procedures (available on the RITS Information Facility) for details.

payments from being sent in T-Copy and for identifying future and back dated payments received in T-Copy are operating as expected.

5.4.3 Reversing Non-current Day Payments

Senders **must** be responsible for rectifying any future or back dated payments mistakenly sent during the HVCS Fallback Period.

5.4.4 Cash Transfers

Participants **should** send payments that would ordinarily be submitted to RITS through a Cash Transfer as a SWIFT payment, if required.

5.4.5 Projected ESA Balance

Participants **must** use their internal system records to track their bilateral net settlement obligations and projected ESA balance during a HVCS Fallback Period.

5.5 Exiting HVCS Fallback

5.5.1 Approaching T-Copy Cut-Off Time

The RBA will send a notification to Participants thirty minutes prior to the Cut-off Time instructing Participants to begin finalising payments.

5.5.2 T-Copy Cut-Off Time

Participants **must** stop sending payments at the Cut-off Time. It is important that Participants do not continue to send payments after this time in order for each Participant to obtain their final bilateral net positions prior to compilation of the HVCS Exchange Summary Form.

5.5.3 SWIFT PDS Reversion

AusPayNet or the RBA will instruct SWIFT to revert the SWIFT PDS FIN-Copy Service to Y-Copy mode. This may be lodged in advance of the Cut-off Time but will instruct SWIFT not to action the change any earlier than the Cut-off Time. The SWIFT timings and process for doing this are the same as for the switch to T-Copy performed earlier in the day.

5.5.4 Submit HVCS Exchange Summary Forms

Participants **must** compile their HVCS Exchange Summary Form and submit it to the RBA via email within two hours of the Cut-off Time.

Note: The RBA will consolidate and compare the HVCS Exchange Summary Form submitted by each Participant to generate a Provisional HVCS Exchange Figures Advice for each Participant. Where applicable, the HVCS Exchange Figures Advice will advise a Participant that the amount of a net bilateral obligation they have submitted fails to match the amount submitted by the other Participant (failure to match).

5.5.5 Agree Provisional HVCS Exchange Figures Advice

Participants **should** provide the RBA with email confirmation that they agree to the Provisional HVCS Exchange Figures Advice provided by the RBA at the earliest possible

opportunity and by no later than 30 minutes before commencement of the Morning Settlement Session (7am) on the day after the HVCS Fallback Period. Where the HVCS Exchange Figures Advice from the RBA has advised a Participant of a failure to match, the Participant must investigate this and if required, submit a revised HVCS Exchange Summary Form to the RBA before 7am on the day after the HVCS Fallback Period.

Note: From 7am on the day after the HVCS Fallback Period, the RBA will generate and send a Final HVCS Exchange Figures Advice and Net Clearing System Obligations Advice showing a Participant's multilateral net position in the contingency batch, including clearing interest. Where a failure to match remains unresolved, the RBA will apply Failure To Match rules and proceed with the contingency batch.

5.5.6 Failure To Match

The RBA will apply Failure To Match rules in accordance with Clause 9.32(a) of these Procedures if two or more Participants cannot agree on the amount owing for a given obligation.

5.5.7 Reconciliation to RITS

Participants **should** reconcile the internal record of payments (used to calculate their net bilateral obligations) to RITS when RITS recovers.

Note: When RITS is recovered and the system date has rolled forward to the day after the HVCS Fallback Period, the SWIFT Feeder connection is restored. The backlog of HVCS settlement requests stored in the CSI will enter RITS and be rejected due to the back-dated value date. Participants can use the RITS UI to view and export the record of rejected T-Copy payments. Participants can also obtain the record of payments settled or rejected by RITS prior to the Disabling Event using MT950 statements or the RITS UI. Participants can use these RITS records to reconcile the internal records used to calculate the net bilateral obligations submitted to the RBA in the HVCS Exchange Summary Form, which could help to resolve failure(s) to match advised by the RBA in the HVCS Exchange Figures Advice.

Where the reconciliation to RITS cannot be completed before 7am on the day after the HVCS Fallback Period, and the RBA has applied Failure To Match rules in order to proceed with the contingency batch, Participants can continue the reconciliation after the batch has settled and if required, bilaterally arrange the return or correction of a mistaken payment in normal way (in accordance with these Procedures).

5.5.8 ESA Funding

Participants **must** fund any ESA balance shortfall that prevents the contingency batch from settling before the Morning Settlement Session ends.

5.6 Operational Capacity

The following instructions describe the volume of payments that Participants are expected to be operationally capable of processing within the HVCS Fallback Period timeframes.

5.6.1 Payment Volumes

Participants **must** be capable of processing the same volume of payments under T-Copy as they would under Y-Copy. That is, payment volumes must not be reduced during the HVCS Fallback Period because of operational capacity limitations.

Note: For the avoidance of doubt, processing means undertaking the end-to-end steps in the RITS Outage Runsheet which includes exchanging clearing messages in T-Copy, applying funds to Customer accounts, submitting net bilateral settlement obligations to the RBA using the HVCS Exchange Summary Form, and resolving any failure to match discrepancies where required. This requires Participants to ensure the processes they use during a HVCS Fallback Period are scalable for business-as-usual payment volumes.

5.6.2 Staffing

Participants **must** have a pre-determined plan to call on sufficient staff to undertake all steps set out in the RITS Outage Runsheet if a HVCS Fallback Period is declared. Where necessary, this will include non-payment operations staff from the credit, treasury or client account functions, or any other function required by a Participant to facilitate payment exchange during the HVCS Fallback Period.

5.6.3 Timings

Participants **must** be capable of completing all steps set out in the RITS Outage Runsheet within the allocated timeframes.

5.7 Applying Funds

A fundamental objective of the HVCS Fallback Solution is to minimise the potential for systemic disruption during a protracted RITS Disabling Event that could, in extremis, cause financial harm and undermine confidence in the payments system. To achieve this, it is important that Participants actively endeavour to make incoming funds available to Customers prior to deferred interbank settlement occurring the next day. This may require Participants to accept a higher degree of credit risk than when RITS is processing HVCS payments on a RTGS basis.

It should be noted that the HVCS Fallback Solution is intended to be used in the event of a technical disruption to RITS during otherwise normal market conditions. The option to invoke the HVCS Fallback Solution would be assessed at the time considering all relevant factors, including prevailing market conditions. AusPayNet and the RBA could elect not to invoke the HVCS Fallback Solution in adverse conditions where deferred net settlement could give rise to undue risk.

The following section provides instructions and guidance on the extent to which Participants are expected to apply funds to Customers during a HVCS Fallback Period. It makes a distinction between two relevant terms:

- *Posting*: a Participant credits the beneficiary Customer's account but does not make the funds available to the Customer until interbank settlement has occurred. Such credits are sometimes referred to as "uncleared funds" and denoted as a visible credit that does not yet form part of the balance of available funds.

- *Availability*: where a Participant enables the beneficiary Customer to make use of funds posted to the Customer's account. This could be in advance of interbank settlement occurring.

5.7.1 Posting

Participants **must** post funds received during a HVCS Fallback Period such that the credit entry is visible to the recipient Customer on the same day. With the exception of funds availability, Participants must treat all other aspects of the posting in the same way as normal. This includes interest accruals, which must accrue from the date of clearing not settlement, and returning payments that cannot be applied in accordance with the timeframes in Clause 4.23 of these Procedures.

5.7.2 Availability

Participants **should** make a sufficient proportion of total incoming funds available to Customers, so that the objective of the HVCS Fallback Solution can be materially achieved. Decisions concerning the availability of funds is a matter for each Participant and could vary depending on risk appetite, however the expectation is that Participants will maximise the value of funds made available to the greatest extent possible, in accordance with their internal risk appetite. As a guide, achieving the objectives of the HVCS Fallback Solution is estimated to require Participants to make at least 80 per cent of the total value of funds received during a HVCS Fallback Period available to its Customers.

5.7.3 Risk Policy

Participants **must** have an internally agreed risk policy that sets out the approach to meeting instruction 6.7.2 on funds availability during a HVCS Fallback Period. The policy must be documented and approved by the relevant senior personnel; and must be readily available in the event of a HVCS Fallback Period.

Note: The specifics of a Participants' risk policy is entirely a matter for the Participant and could depend on a range of factors including credit appetite, counterparty relationships, net exposures arising from incoming and outgoing settlement obligations; and the value of individual payments received. The policy should contemplate circumstances where Customer's outbound payments are contingent on the availability of funds received. Given the potential time constraints during a HVCS Fallback Period, it may be necessary for Participants to prioritise the assessment of inbound payments that will fund outbound payments due to occur on the same day. As noted, the HVCS Fallback Solution is intended to be used in the event of a technical disruption to RITS during otherwise normal market conditions.

5.7.4 Timely Implementation

Participants **must** be capable of implementing their risk policy during a HVCS Fallback Period, including assessment and approval of credit decisions, within the timeframes set out in the RITS Outage Runsheet.

Note: Participants could consider using a value threshold to determine lower value payments that do not require individual credit assessment before the funds are made available to Customers. For most Participants, a lower bound threshold of $1mn would represent around 90 per cent of total inbound payment volume, but only 2 per cent of total value. Such a

threshold could be an operationally efficient approach to prioritising credit decisions for the remaining 10 per cent of payments within the potentially constrained timeframes.

6. Participant Outage Instructions

6.1 Operational Readiness

The following instructions cover items that Participants are expected to have in place in preparation for a Participant Fallback Period.

6.1.1 Operational Readiness

Participants **must** be operationally ready for a Participant Fallback Period. This includes:

1) being familiar with these Procedures and the Contingency Instructions;

2) being capable of making the internal system and operational changes required to send and receive payments during a Participant Fallback Period;

3) participating in contingency test exercises coordinated by AusPayNet; and

4) ensuring staff are available and contactable at all times during the Participant Fallback Period and during planned contingency test exercises.

Participants **must** attest their adherence with these requirements in the Yearly Audit Compliance Certificate (Annexure A.2).

6.2 Participation

The following instructions describe the extent to which Participants are expected participate in the HVCS when a Participant Fallback Period has been declared.

Instructions for Affected Participant

6.2.1 Sending Payments

The Affected Participant **must** use the Participant Fallback Solution provided for in these Contingency Instructions as the alternative method of sending any payments it considers to be urgent during a Participant Fallback Period.

6.2.2 Participation Opt-Out

Tier 2 Participants that do not intend to use the Participant Fallback Solution if they experience a Disabling Event **must** have pre-agreed this arrangement with AusPayNet. Where there are extenuating circumstances in which a pre-agreed opt-out Participant needs to send payments using the Participant Fallback Solution, the Participant **must** obtain prior agreement AusPayNet and from the Receiver(s).

Note: A list of the pre-agreed opt-out Participants will be available from the AusPayNet extranet site, such that during a Disabling Event, it is clear to other Participants that a Participant Fallback Period is unlikely to be declared.

6.2.3 Managing ESA Balance

The RBA Domestic Markets Department will contact the Affected Participant where significant deviations in ESA balances are observed.

Instructions for Other Participants

6.2.4 Receiving Payments

All Tier 1 Participants **must** accept payments from an Affected Participant through the Participant Fallback Solution, in accordance with the operational capacity instructions in Section 7.6.

6.2.5 Receiving Payments

All Tier 2 Participants **should** accept payments received from an Affected Participant through the Participant Fallback Solution, in accordance with the operational capacity instructions in Section 7.6. Refusals, if any, **must** be communicated to AusPayNet.

6.2.6 Sending Payments

Participants **must** continue to use the SWIFT PDS for sending payments to the Affected Participant, whilst having regard to the possible liquidity implications and processing delays described in Clause 9.8 of these Procedures. The Participant Fallback Solution provides a means for the Affected Participant to send payments. It cannot be used as a means for the Affected Participant to receive payments outside of the SWIFT PDS.

6.2.7 Pausing Payments

Participants **must**, to the best of their ability, pause sending payments to an Affected Participant if requested to do so by the Affected Participant.

6.3 Entering Participant Fallback

An Affected Participant cannot use the Participant Fallback Solution without prior authorisation from AusPayNet. Authorisation is granted when AusPayNet, or the RBA acting on behalf of AusPayNet, formally declares a Participant Fallback Period.

The key checkpoint times for declaring and entering a Participant Fallback Period are outlined in the Participant Outage Runsheet. In summary, where the Affected Participant's Disabling Event prevents it from sending HVCS payments the priority is to resolve the issue and resume normal operations. If the Disabling Event is not resolved by 15:00 then minimising the delay to payments becomes the priority and AusPayNet, in consultation with the RBA and the Affected Member, could declare a Participant Fallback Period. A Participant Fallback Period could be declared earlier than 15:00 if the Affected Participant has urgent payments to send and cannot estimate their recovery time; or is able to rule out a recovery ahead of the checkpoint times. Decisions concerning a Participant Fallback Period will be communicated to RITS operational contacts via email and SMS.

If the Affected Participant's Disabling Event occurs after 14:00, AusPayNet in consultation with the RBA, would normally expect that a Participant Fallback Period would not be required, but would consider the value of outstanding payments in its assessment.

A Participant Fallback Period will not be declared if the Disabling Event prevents the Affected Participant from using the Participant Fallback Solution.

The following instructions apply once a Participant Fallback Period has been declared.

6.4 During Participant Fallback

6.4.1 Bilateral Clearing Frequency

The Affected Participant **must** limit the number of HVCS Bilateral Clearing Forms it sends to a Receiver to no more than one every hour, unless agreed with the Receiver.

6.4.2 Payment Volumes

The Affected Participant **must** limit the volume of payments contained in a single HVCS Bilateral Clearing Form to the volumes set out in the operational capacity instructions in section 7.6, unless agreed with the Receiver.

6.4.3 Payment Value Date

The Affected Participant **must** only send value-today payments using Participant Fallback Solution. Future dated payments are not permitted.

6.4.4 Receiver Acknowledgement

The Receiver **must** immediately acknowledge receipt of a HVCS Bilateral Clearing Form from the Affected Participant via encrypted email or phone call to the Affected Participant.

6.4.5 RITS Cash Transfers

The Affected Participant and Receiver **must** each enter a single Cash Transfer for the value of the net bilateral obligation created for each individual HVCS Bilateral Clearing Form exchanged.

Note: If the Affected Participant is unable to access the RITS UI to enter a Cash Transfer, it can contact the RITS Help Desk to request an Assisted Payment.[467]

6.4.6 Settlement Timing

The Affected Participant and Receiver **must** each enter the RITS Cash Transfer and confirm its settlement within 30 minutes of the HVCS Bilateral Clearing Form being sent.

6.4.7 Status Reporting

The Affected Participant **must** update the RBA and AusPayNet at least every 30 minutes, or as requested, on the status of payments sent using the Participant Fallback Solution and the

467 Please see the Assisted Transactions User Guide, available at https://www.rba.gov.au/rits/info/pdf/Assisted_Transactions_User_Guide.pdf

value and volume of payments outstanding.

Note: The Affected Participant **must** also continue update the RBA and AusPayNet on the status of the Disabling Event and expected resolution time, in accordance with the RTGS and Retail Payments Incident Reporting Arrangements for RITS Members.

6.4.8 Potential SWIFT Resumption

Where the Affected Participant is able to resolve the Disabling Event while using the Participant Fallback Solution, and where it can prevent payments already sent through the Participant Fallback Solution from being released to the SWIFT PDS, the Affected Participant **could** revert to SWIFT for sending payments. If it is not possible to prevent the release of payments already sent, the Affected Participant **must** consult with AusPayNet and the RBA on whether to:

1) revert to SWIFT and resolve potential duplicate payments by requesting a Return of Payment from the Receiver; or

2) hold all outward SWIFT payments and continue using the Participant Fallback Solution.

*Note: In accordance with these Procedures, the Affected Participant **must** resume inward payment processing in the shortest possible time. The Affected Participant must consult with the RBA and AusPayNet if holding outward payments will also prevent inward payments processing from resuming.*

6.4.9 Unexpected SWIFT Resumption

Where the Affected Participant resolves the Disabling Event while the Participant Fallback Solution is in use, and unexpectedly begins to release payments to the SWIFT PDS, the Affected Participant **must** pause all further outward payments processing. The Affected Participant must initiate the request for a Return of Payment for any duplicate payments released, and refer to instruction 7.4.8 on consultation with AusPayNet and the RBA before reverting to SWIFT, or otherwise continue using the Participant Fallback Solution for sending further payments.

6.4.10 Return of Payment

The Affected Participant **must** complete all Return of Payment requests in accordance with Part 4 of these Procedures.

6.5 Exiting Participant Fallback

6.5.1 Cut-off Times

The Affected Participant **must** follow RITS session times and rules when using the Participant Fallback Solution. Meaning:

- Outgoing payments from the Affected Participant to Receivers must be sent and settled in RITS by the end of the Settlement Close Session.

- Where the Affected Participant is Evening Agreed and wishes to send payments to another Evening Agreed Participant after the Settlement Close Session, the Affected

Participant must obtain prior agreement from the Receiver and these payments must be sent and settled in RITS by the Evening Settlement Cut-off.

6.5.2 RITS Extension

The Affected Participant **could** request an extension to the RITS session times. The RBA will, in the normal way, consider the value and volume of payments outstanding in its assessment of whether to grant an extension.

6.6 Operational Capacity

The following instructions describe the extent to which Participants are expected to be operationally capable of sending and receiving payments during a Participant Fallback Period.

6.6.1 Staffing

All Participants **must** have a pre-determined plan to call on sufficient staff to undertake all steps set out in the Participant Outage Runsheet if a Participant Fallback Period is declared.

Instructions for Affected Participant

6.6.2 Bilateral Clearing Forms

The Affected Participant **must** be operationally capable of sending the higher of the following two:

- As many HVCS Bilateral Clearing Forms as required to cover at least 80 per cent of its outstanding outgoing transaction value; or
- A total of five HVCS Bilateral Clearing Forms per hour, with each form sent to a different Receiver (i.e. five Receivers).

Note: In all cases, the Affected Participant must limit the number of HVCS Bilateral Clearing Forms sent to a single Receiver to no more than one every hour, unless agreed with the Receiver.

6.6.3 Payment Volumes

The Affected Participant **must** be operationally capable of sending at least fifty payments in each HVCS Bilateral Clearing Form and of entering a single RITS Cash Transfer to effect interbank settlement of the bilateral obligation within 30 minutes of the HVCS Bilateral Clearing Form being sent. Fewer than **fifty** payments can be sent if required.

Note: The Affected Participant can increase the number of payments contained in a single HVCS Bilateral Clearing Form if agreed with the Receiver. This recognises that in some cases it may be preferable to send or receive one larger file rather than multiple smaller files.

6.6.4 Payment Values

The Affected Participant **should** be operationally capable of prioritising higher-value payments for inclusion in the HVCS Bilateral Clearing Form. The Affected Participant can

include lower-value payments in the HVCS Bilateral Clearing Form if required, subject to this being in accordance with instruction 7.6.2 and 7.6.3.

Note: For most Participants, sending payments greater than $10 million in value will constitute 80 per cent or more of the total outgoing daily transaction value.

Instructions for Other Participants

6.6.5 Bilateral Clearing Forms

The Receiver must be operationally capable of receiving a minimum of one HVCS Bilateral Clearing Form containing at least fifty payments every hour and of entering a single RITS Cash Transfer to effect interbank settlement of the bilateral obligation within 30 minutes of the HVCS Bilateral Clearing Form being received.

6.6.6. Applying Funds

The Receiver **must** be operationally capable of applying payments received in each HVCS Bilateral Clearing Form to Customer accounts on the same day. This includes any screening and downstream processing the Receiver needs to perform prior to applying funds to Customer accounts. For the avoidance of doubt, funds **should** be made available to the Customer for use when the payment is applied to their account.

The next page is Annexure K

ANNEXURE K CYBER FRAUD INSTRUCTIONS FOR THE HIGH VALUE CLEARING SYSTEM[468]

1. Introduction and scope

These Cyber Fraud Instructions are applied under PART 11 of the HVCS Procedures and it provides instructions and guidance for High Value Clearing System Framework Participants in the event that a Framework Participant experiences or is affected by a Cyber Fraud Event. It is intended to adopt a principles-based approach rather than a prescriptive approach in respect of Cyber Fraud Events. The intention is to set a baseline of operational requirements and expectations to enhance the framework's ability to deal with suspected and confirmed fraudulent payments.

Under Regulation 4.12 of the HVCS Regulations, Framework Participants ***must*** provide all reasonable assistance to each other Framework Participant and to the Management Committee to investigate any actual or suspected fraudulent activity involving or possibly involving HVCS and identify the source of any fraudulent activity involving HVCS. These Cyber Fraud Instructions are intended to provide guidance on how Framework Participants can provide such assistance to each other.

Framework Participants processing high-value transactions on behalf of a third party ***should*** inform users of their services of the obligation to comply with the Procedures and these Cyber Fraud Instructions.

There are three classifications of instructions:

Rating	Definition
Must	Framework Participants are required to implement all 'must' items. These requirements: • refer to the Regulations and other HVCS or SWIFT requirements; • enable Framework Participants to meet their obligations and minimise risk to other members.
Should	Participants are expected to implement 'should' items. These expectations*:* • provide instructions and guidance on aspects of the Cyber Fraud Event that may vary based on the specifics of a Framework Participant's systems or operations.
Could	Participants are encouraged to consider 'could' items but are not required to implement them. These considerations: • provide indications of recommended best practice.

2. Relationship with other documents

Nothing in these Cyber Fraud Instructions affect a Framework Participant's obligations to comply with the Procedures or the Framework Participant's regulatory and framework requirements.

[468] Inserted effective 14/11/22, version 041 r&p 001.22

If a provision of these Cyber Fraud Instructions is inconsistent with a provision of the Procedures, the provisions of the Procedures prevail.

The following documents interact with these Cyber Fraud Instructions.

Document	Relationship / Purpose	Owner
AusPayNet Member Incident Plan (MIP)	Framework for industry coordination during an operational incident affecting the HVCS.	AusPayNet
AusPayNet Crisis Communication Plan (CCP)	Framework for industry and media communication during a major disruption to any of the payments systems or infrastructure that fall under the remit of AusPayNet.	AusPayNet
RITS Member Incident Reporting Arrangements	Arrangements specified by the RBA for reporting by RITS Members during an incident that affects RITS operations, including successful or partly successful cyber-attacks on RTGS or retail payments systems.	RBA
SWIFT Customer Security Program (CSP)	Programme providing support to SWIFT's users in the fight against cyber-attacks and reinforcing the security of the global financial community. Further information available via the SWIFT Knowledge Centre.	SWIFT
SWIFT Recovery Roadmap (SWIFT bulletin 10047)	A SWIFT bulletin providing general advice to SWIFT members on how to respond to a cyber-security incident. Further information available via the SWIFT Knowledge Centre.	SWIFT

3. Definitions and Interpretation

Words defined in the Procedures have, unless the contrary intention appears, the same meaning in these Cyber Fraud Instructions. Otherwise, in these Cyber Fraud Instructions:

Isolation Event means the affected Framework Participant is undertaking the processes set out in SWIFT Recovery Roadmap, which may include suspending the machine, unplugging from the network, shutting down the required ports on the switch or putting the system in an isolated VLAN with an aim to identifying the weakness(es) that resulted in the Cyber Fraud Event. Any questions relating to the processes set out in the SWIFT Recovery Roadmap ***should*** be directed to SWIFT Customer Support.

In these Cyber Fraud Instructions:

(a) the word person includes a firm, a body corporate, an unincorporated association or an authority;

(b) the word "includes" and "including" is not taken as limiting the meaning of the words

preceding it;

(c) the singular includes the plural and vice versa;

(d) headings are inserted for convenience and do not affect the interpretation of these Cyber Fraud Instructions;

(e) a reference to a statute or code means the statute or the code, or the provision as modified or amended and in operation for the time being, or any statute, code or provision enacted in lieu thereof and includes any regulation or rule for the time being in force under the statute, the code, or the provision; and a reference to a specific time means that time in Sydney unless the context requires otherwise.

4. Cyber Fraud Event

Where a Cyber Fraud Event is detected, the affected Framework Participants ***must*** review these Cyber Fraud Instructions.

These Cyber Fraud Instructions will not apply if a fraud event does not meet the definition of a Cyber Fraud Event.

Where a Cyber Fraud Event also constitutes a Disabling Event, part 9 of the Procedures and the Contingency Instructions may not apply in all cases, as determined by the Company in the circumstances.

5. Fraud and cyber contacts

Each Framework Participant must nominate and advise the Company and the System Administrator of a contact point(s) to whom information or enquiries may be directed if a Cyber Fraud Event arises. The Framework Participant must ensure its nominated contact point(s) remain up to date.

The Company will maintain a list of contact point(s) in Annexure L: Cyber Fraud contacts.

6. Monitoring, testing and maintenance

Pursuant to Regulation 4.9 of the HVCS Regulations, each Framework Participant ***must*** ensure that its own systems and procedures provide appropriate protection against fraudulent activity in connection with HVCS, in accordance with these Regulations and Procedures.[469]

The Management Committee may undertake cyber incident response testing across the HVCS from time to time on reasonable notice. On the Management Committee's request, the Framework Participants ***must*** participate in such testing.

[469] Framework Participants ***could*** consider available market tools that facilitate the case management of fraud payment remediation, which may assist in meeting this obligation and ensuring the timely identification and remediation of payment fraud.

7. Notification and reporting requirements

On becoming aware of a Cyber Fraud Event:

(a) A Sender that causes or may cause the Cyber Fraud Event:

(i) must report the Cyber Fraud Event in accordance with the requirements to report successful and near-miss cyber-attacks specified in the RITS Member Incident Reporting Arrangements (if applicable); and

(ii) ***must*** report the Cyber Fraud Event to the Company in accordance with Regulation 4.10 of the HVCS Regulations (if applicable), and ***must*** comply with the reporting requirements indicated in the CCP or MIP (if applicable); and

(b) A Receiver that is or may be affected by a Cyber Fraud Event (eg Receivers of confirmed or suspected fraudulent payments):

(i) should report the Cyber Fraud Event to the Company in accordance with Regulation 4.10 of the HVCS Regulations (if applicable); and

(ii) ***should*** notify the Sender where the Sender may not already be aware of payments the Receiver has identified as suspicious through its own screening. The Sender can be notified using the applicable contact point(s) maintained in Annexure L or via the Company.

8. Obligations of Receivers

If a Receiver that is affected by or potentially affected by a Cyber Fraud Event (e.g. a Receiver becomes aware that it has received payment arising from a Sender that is the subject of a Cyber Fraud Event), it ***should*** freeze and hold suspected fraudulent payments if requested by the Sender and/or the Management Committee. This does not apply if the Sender requests for Return of a Settled Payment Sent in Error, in accordance with clause 4.14(a) of the Procedures.

9. Obligations of Senders

If a Sender that causes or may cause a Cyber Fraud Event, it (on becoming aware):

(a) must immediately assess steps are appropriate to be undertaken in the circumstances to prevent or reduce the likelihood of other fraudulent or potentially fraudulent payments from being transmitted through the SWIFT PDS and action these steps. For example, it could remove itself from the SWIFT PDS CUG by initiating an Isolation Event or undertake other appropriate action;

(b) must comply with directions received from the System Administrator in relation to the Cyber Fraud Event (if any); and/or

(c) must comply with directions from the Management Committee in relation to the Cyber Fraud Event, including a direction to initiate an Isolation Event.

While the Isolation Event is active, the Sender that is isolating will not be able to send or receive any HVCS payment processing.

10. Existing an Isolation Event

Prior to exiting an Isolation Event, the Sender that that is isolating a Cyber Fraud Event must:

(a) provide assurance to the Management Committee that the cause of the Cyber Fraud Event has been resolved. This may include providing the Management Committee with relevant information about the Cyber Fraud Event and the Isolation Event, including a description of the control failures that enabled the Cyber Fraud Event, what rectification measures have been applied, any independent verifications and controls reviews undertaken, details of penetration testing and any other information as may be appropriate in the circumstances or as otherwise requested by the Management Committee;

(b) ensure the authenticity and integrity of payments queued in the Framework Participants SWIFT systems have been checked prior to reconnection to the SWIFT PDS; and

(c) if requested by the Management Committee, heighten its monitoring and screening of payments for a specified period of time after reconnection.

The Isolation Event will continue until the Management Committee notifies the Framework Participant experiencing the Cyber Fraud Event that it has provided sufficient assurance to Management Committee (acting in its sole discretion) that the cause of the Cyber Fraud Event has been identified and addressed to prevent any further impact to other Framework Participants or risk to the integrity of the HVCS.

11. Powers and Duties of the Management Committee

The Management Committee can exercise its powers as set out in the HVCS Regulations.

12. Framework Participants' Liability in a Cyber Fraud Event

Framework Participants' liability is as set out in Regulation 4.11 of the HVCS Regulations.

The next page is Annexure L

ANNEXURE L CYBER FRAUD CONTACTS[470]

Annexure L is located separately

- END -

[470] Inserted effective 14/11/22, version 041 r&p 001.22