Effective:
1 January 2025
Version 016

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company Limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 1
Introduction and Member Obligations

Commenced 1 July 2015

Australian Payments Network Limited
Telephone: (02) 9216 4888

Code Set for
ISSUERS AND ACQUIRERS COMMUNITY
FRAMEWORK

Volume 1
Introduction and Member Obligations

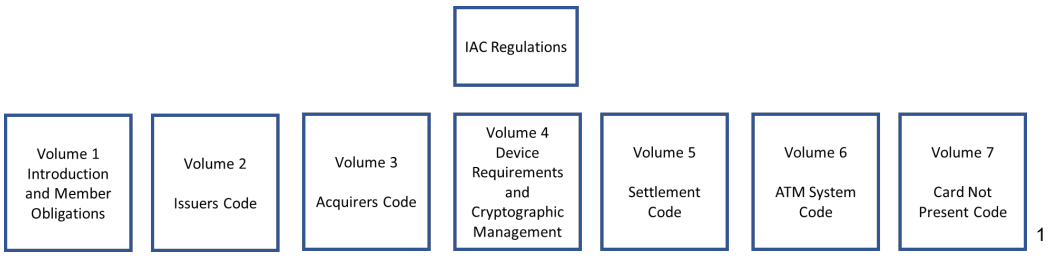
INDEX

PART 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1 Purpose of this Code

The IAC has been established to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. These include minimum security standards, interoperability standards and value added services that support how payment cards are used throughout Australia.

These standards and requirements are contained within the IAC Code Set which is structured as follows:



[1]

Volume 1, this volume, provides an introduction to the IAC standards and services. In addition, it identifies those obligations that IAC participation imposes on its members, referred to as Framework Participants. [2]

Volume 2 is intended for Issuers and contains those aspects of PIN and device security that are considered mandatory for all Issuers participating within the IAC. In addition, this volume contains guidance and recommendations into non-mandatory aspects of Issuer PIN management.[3]

Volume 3 is intended for Acquirers and contains those aspects of ATM and EFTPOS Transaction security that are considered mandatory for all Acquirers participating within the IAC. In addition, this volume contains device management requirements applying to all acquiring members participating in the IAC.[4]

Volume 4 addresses Device approvals. It is an IAC requirement that all Devices, Solutions and Non-Standard Technology hold a current AusPayNet approval prior to and during use within the IAC. This volume also specifies the minimum cryptographic algorithms, key lengths and processes that apply to all PINs and ATM and EFTPOS Transactions exchanged under the IAC.[5]

Volume 5 provides the operational practices and processes involved in IAC settlement.

[1] Amended effective 1/7/19, version 009 r&p 001.19
[2] Last amended effective 1/7/19, version 009 r&p 001.19
[3] Amended effective 1/1/19, version 008 r&p 002.18
[4] Amended effective 1/1/19, version 008 r&p 002.18
[5] Last amended effective 16/12/21, version 013 r&p 001.21

Volume 6 provides both the technical and operational aspects of ATM support under the IAC.

Volume 7 contains the requirements for Issuers and Acquirers in dealing with Card Not Present Transactions, to mitigate the fraud associated with such Transactions. [6]

Other supplementary documents supporting the IAC include the AusPayNet Specification for a Security Control Module Function Set and the KIF Audit Guidelines.

1.2 IAC requirements

1.2.1 *Application of these requirements*

The IAC Code Set applies to all Card Payments except Closed Loop Cards and On-us Transactions. [7]

1.2.2 *Relationship with other standards or guidelines*

This IAC Code Set cross-refers to a number of existing standards and guidelines published by bodies other than AusPayNet that apply to Framework Participants, in their various capacities, in consumer electronic transactions and which may apply to Framework Participants either independently of or by virtue of their incorporation by reference in this IAC Code Set. The requirements of these separate schemes, standards or guidelines have not been duplicated in this IAC Code Set and Framework Participants are expected to have familiarised themselves with and adhere to their responsibilities under all such applicable requirements, as a separate matter from the specific standards and requirements which are detailed in this IAC Code Set. These existing schemes, requirements and guidelines include:[8]

Standard or Guideline	**Application**	**Monitor**
Card Schemes	All Issuers and Acquirers party to particular schemes	Various
ePayments Code	All Framework Participants	Australian Securities and Investments Commission
AS 2805	All Framework Participants	Standards Australia
ISO 9564, 13491 & 11568	All Framework Participants	International Standards Organization
RBA Card Payments Regulation	All Framework Participants	Reserve Bank

[6] Inserted effective 1/7/19, version 009 r&p 001.19
[7] Last amended effective 1/1/20, version 010 r&p 002.19
[8] Last amended effective 1/1/24, version 015 r&p 003.23

1.2.3 *Standards development*

In support of the IAC membership, and to further develop relevant IAC standards, AusPayNet will maintain an active involvement in relevant standards development bodies, including but not limited to:

(a) Standards Australia – relevant working groups and committees;

(b) International Standards Organization – relevant working groups and committees;

(c) PCI Security Standards Council;

(d) EMV Co – relevant working groups.

1.2.4 *Inconsistencies*

(a) If a provision of the Regulations or this IAC Code Set is inconsistent with a provision of the Constitution, the provision of the Constitution prevails.

(b) If a provision of this IAC Code Set is inconsistent with a provision of the Regulations, the provision of the Regulations prevails.

1.2.5 *Governing Law*

This IAC Code Set is to be interpreted in accordance with the same laws which govern the interpretation of the Constitution.

1.3 Interpretation

Interpretations are located in a separate document entitled ‘Interpretations & Definitions’.

1.4 Definitions

Definitions are located in a separate document entitled ‘Interpretations & Definitions’.

The next page is Part 2

PART 2 FRAMEWORK PARTICIPANT OBLIGATIONS

2.1 Adherence to standards[9]

2.1.1 *Issuers*

Subject to clause 4.1 of the Regulations, Issuers must ensure that they and their Third Party Providers ensure:

(a) PIN security and card verification numbers comply with the requirements specified in IAC Code Set Volume 2 (Issuers Code);[10]

(b) Any Devices used in Interchange are approved for use by the Company; [11]

(c) Settlement procedures comply with the requirements and processes given in IAC Code Set Volume 5 (Settlement Code); and

(d) Compliance with the obligations and reporting requirements in relation to Card Not Present Transactions in IAC Code Set Volume 7 (Card Not Present Code).[12]

2.1.2 *Acquirers*

Subject to clause 4.1 of the Regulations, Acquirers must ensure that they and their Third Party Providers ensure:

(a) PIN security complies with all relevant requirements given in the IAC Code Set Volume 3 (Acquirers Code);

(b) ATM requirements and procedures comply with all aspects of IAC Code Set Volume 6 (ATM System Code);

(c) any Devices, Solutions and Non-Standard Technology used in Interchange are approved for use by the Company;[13]

(d) settlement procedures comply with the requirements and processes given in IAC Code Set Volume 5 (Settlement Code);[14]

(e) all Key Injection Devices and services comply with the relevant requirements specified in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management); [15]

(f) all parties to the Interchange, including Merchants and any intermediate network entities maintain procedures and practices for preventing the unauthorised disclosure of Cardholder Data and ensure that unencrypted

[9] Amended effective 1/1/19, version 008 r&p 002.18
[10] Amended effective 1/7/20, version 011 r&p 001.20
[11] Last amended effective 16/12/21, version 013 r&p 001.21
[12] Last amended effective 1/1/20, version 010 r&p 002.19
[13] Last amended effective 16/12/21, version 013 r&p 001.21
[14] Amended effective 1/1/20, version 010 r&p 002.19
[15] Amended effective 1/1/19, version 008 r&p 002.18

authentication is not stored outside of an SCD (see IAC Code Set Volume 3 (Acquirers Code));

(g) that they are aware of the Reserve Bank notification requirements to Merchants regarding merchant pricing requirements. Annexure F (Notice of Standard – Merchant Pricing for Credit, Debit and Prepaid Card Transactions) is an optional guide prepared by AusPayNet which may be used by Acquirers and their Third Party Providers to assist them to comply with their notification requirements; and[16]

(h) compliance with the obligations and reporting requirements in relation to Card Not Present Transactions in Volume 7 (Card Not Present Code). [17]

2.2 Third Party Providers[18]

(a) A Framework Participant may contractually engage one or more Third Party Providers to provide outsourced services and functions, which may include services procured to satisfy the Framework Participant's obligation to perform specific functions and requirements necessary to meet the obligations of the IAC Code Set.

(b) It is the responsibility of the Framework Participant to verify the capacity of its Third Party Provider to provide the outsourced services and functions.

(c) It is the responsibility of the Framework Participant to manage, direct and control the provision of outsourced services and functions by its Third Party Providers, and to ensure such Third Party Providers and any sub-contractor engaged by the Third Party Provider are contractually obliged to comply with all applicable IAC standards and requirements.

2.3 Compromised Terminals

Clauses 2.3.1 to 2.3.2 are Confidential

2.3.1 *Acquirer Actions*

[16] Inserted effective 1/6/17, version 005 r&p 001.17
[17] Inserted effective 1/7/19, version 009 r&p 001.19
[18] Amended effective 1/1/15, version 001 r&p 001.15

2.3.2 *Issuer Actions*

2.4 Change Management

(a) Any proposal to modify or upgrade an existing Interchange that also involves changes by the other party to the Interchange, must be advised by the applicant to the Framework Participant affected no less than 180 days (unless otherwise bilaterally agreed) prior to the date upon which the proposal is to be implemented ("**Implementation Date**").

(b) Each Framework Participant must use reasonable endeavours to make such changes to its own Interchanges by the Implementation Date, or a date otherwise bilaterally agreed, as may be necessary to give effect to a proposal notified to it under this clause.

2.5 Provision of statistics

2.5.1 *Terminal statistics*

(a) Acquirers must report to the Company the number of ATM and EFTPOS Terminals they deploy on a state by state basis for the periods ending on

December, March, June and September. The report must separately identify those Terminals which the Acquirer directly owns and any other Terminals for which it provides acquiring services (e.g., "white label" Terminals owned by a third party).

(b) Consolidated figures will be provided to all IA Participants and also made available from the IAC ATM and EFTPOS Terminal Statistics Database facility found on AusPayNet's Extranet.[20]

2.5.2 *Card fraud data*

(a) Issuers must report card fraud data to the Company on a monthly basis. Information in the report must comply with the requirements set out by the Company and made available from time to time on AusPayNet's extranet.

(b) Consolidated figures will be provided to all IA Participants and also made available from the IAC Card Fraud Database facility found on AusPayNet's Extranet.

2.6 Notification of a Disruptive Event

(a) A IA Participant that experiences a Disruptive Event must notify the Company and all IA Participants that will or are likely to be affected by the Disruptive Event as soon as possible. Notification of a Disruptive Event must be given to the operational contacts listed on AusPayNet's Extranet and subsequently by a IAC Operational Broadcast (see clause 2.7).

(b) Upon notice of a Disruptive Event, 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 committee of management. The Member Incident Plan provides a framework for committee of management communication and consultation during applicable contingency events. If the Chief Executive Officer invokes the Member Incident Plan, the committee of management must comply with its requirements.

2.7 IAC Operational Broadcast

(a) IA Participants may provide operational advice to other IA Participants by issuing an IAC Operational Broadcast (set out in Annexure D).

(b) The IAC Operational Broadcast form may be used to notify other IA Participants about:

(i) unscheduled network outages;

(ii) scheduled network outages;

[20] Amended effective 1/1/19, version 008 r&p 002.18

(iii) to facilitate the exchange of general operational information relevant to network operations;

(iv) Disruptive Events; or

(v) any technical inability to comply with a notification given by the Secretary under clause 2.8 (BIN and AIN Change Management).

2.7.1 *How to Send an IAC Operational Broadcast*

(a) The IAC Operational Broadcast form is an online form which can be accessed, completed and sent by IA Participants using AusPayNet's extranet that is available and processed 24/7.

(b) An IAC Operational Broadcast about a Disruptive Event must include the following information:

(i) the time when the Disruptive Event commenced or is expected to commence;

(ii) the time when normal processing is expected to resume or resumed; and

(iii) the current status of the Disruptive Event.

2.8 BIN and AIN Change Management

This clause 2.8 applies to those BINs and AINs involved in domestic interchange.

Note: Clause 2.8 is also optional, but desirable, for BINs issued domestically where all Transactions are routed via an international card scheme and settled with the international card scheme. The Institutional Identifier Change fee referred to in clause 2.8.1(b) does not apply to those BINs as they are outside domestic Interchange.[21]

2.8.1 *BIN and AIN Change Database*

(a) Other than in the context of a new direct clearing and settlement arrangement, the introduction of a new BIN or AIN, or deletion of or change in the routing of an existing BIN or AIN must occur on an Institutional Identifier Change Date.

(b) An IA Participant wishing to introduce a new BIN or AIN, or change the routing of an existing BIN or AIN, must give the Secretary no less than 10 weeks' notice in advance of the relevant Institutional Identifier Change Date on which such change is to occur and must pay to the Company at the time of giving the notice $6,700 (indexed annually in accordance with Regulation 10.5 and to be rounded to the nearest $100 ($50 being rounded up)). No further fee applies where there is more than one new identifier

[21] Inserted effective 21/11/17, version 006 r&p 002.17

and/or routing change notified to take effect on the same Institutional Identifier Change Date. [22]

(c) An IA Participant wishing to delete an existing BIN or AIN must give the Secretary no less than 10 weeks' notice in advance of the relevant Institutional Identifier Change Date on which such change is to occur.

(d) The Secretary must promptly notify all IA Participants of the new BIN or AIN or the deletion of or change in the routing of an existing BIN or AIN and the Institutional Identifier Change Date on which such change is to occur.

(e) IA Participants must recognise the new BIN or AIN or deletion of or change in the routing of an existing BIN or AIN on and from the relevant Institutional Identifier Change Date notified by the Secretary in accordance with this clause 2.8.1.

Note: "recognise" for the purposes of this clause 2.8.1(e) means making such host system and Terminal changes as are reasonably necessary to ensure that Cards issued on the changed BIN and / or AIN are accepted at Terminals and that Transactions are processed and authorized accordingly.

2.8.2 *Production of test cards*

Issuers that give notice of the introduction of a new BIN or a change to the routing of an existing BIN pursuant to clause 2.8 must, on request by an affected IA Participant, ensure production of any necessary test Cards in sufficient time to allow testing to occur before the applicable Institutional Identifier Change Date.

2.9 Capacity Planning[23]

The IAC committee of management will undertake the facilitation of communication between IA Participants engaged in Interchange to:

(a) consider the capacity and performance requirements for periods of peak demand;

(b) enable IA Participants engaged in Interchange to plan for capacity and performance to maintain services during peak periods of demand;

(c) share information (such as changes in switch arrangements or major product launches) relevant to capacity and performance to maintain the efficiency of Card Payments at all times; and

(d) report and discuss any issues from a capacity requirement and performance perspective.

Next page is Part 3

[22] Amended effective 1/1/16, version 002 r&p 002.15
[23] Amended effective 1/1/20, version 010 r&p 002.19

PART 3 CERTIFICATION

3.1 Introduction

This Part 3 sets out the certification requirements to be met by applicants, and the annual compliance requirements for all IA Participants.

By completing the relevant checklists, an applicant or IA Participant confirms, for the benefit of all IA Participants and the Company, that when it operates in the IAC with other IA Participants it meets the applicable requirements in force at that time, including that:

(a) it conforms with IAC Code Set Volume 3 (Acquirers Code);

(b) it conforms with IAC Code Set Volume 2 (Issuers Code);

(c) all Devices, Solutions and Non-Standard Technology employed in Interchange have been approved for use within the IAC;[24]

(d) its settlement procedures conform with IAC Code Set Volume 5 (Settlement Code);

(e) it conforms with IAC Code Set Volume 6 (ATM System Code); and

(f) any services provided on its behalf by Third Party Providers are provided in conformance with the relevant standards and requirements specified in this Code.[25]

3.2 Annual Security Audits

The Annual Security Audits (Annexure A of this Volume 1) is designed to ensure that uniform security audit procedures are applied among all Framework Participants. To be effective, all entities involved in either the processing of Interchange PINs and/or Transactions from entry at the Terminal up to and including delivery to the Issuer's authorisation processor, or involved in the management and security of PINs must adhere to an agreed set of procedures and adopt a common audit process to ensure adherence to those security procedures.[26]

3.2.1 *Submission of Annual Security Audit*

(a) All IA Participants must complete an Annual Security Audit (see Annexure A) once every calendar year. IA Participants must give the Company prior written notice of the date by which they will complete their Annual Security Audit. It must be signed by the IA Participant and countersigned by either an internal or external auditor and submitted to the Company within six

[24] Last amended effective 1/1/25, version 016 r&p 001.24
[25] Amended effective 1/1/15, version 001 r&p 001.15
[26] Amended effective 20/8/18, version 007 r&p 001.18

months of the end of the calendar year in which the annual audit was completed.[27]

(b) Acquirers who have had a PCI PIN audit completed by a Qualified PIN Assessor (QPA) may meet the requirements in clause 3.2.1 by completing Annexure A.1 and submitting a duly signed copy of the PCI PIN AoC(s). The PCI PIN audit must have been completed in the same calendar year as the part 1 audit (Annexure A.1).[28]

3.2.2 *Third Party Providers*[29]

(a) Where services and functions are provided by a Third Party Provider, its compliance with IAC standards and requirements must be demonstrated by the IA Participant by either submission of:

(i) a separate Annual Security Audit checklist for the Third Party Provider; or

(ii) by inclusion of the Third Party Provider within the IA Participant's own Annual Security Audit checklist.

(b) IA Participants' compliance with the obligation to manage service provision by Third Party Providers as set out in this clause 3.2.2 will be assessed as part of the annual security audit.

3.2.3 *Auditor Signoff*

(a) Auditors co-signing Annual Security Audit must be engaged to perform an independent review of the compliance checklists completed by the IA Participant, and to form an opinion on their completeness and accuracy.

(b) The following is a suggested audit process that could be used by an auditor:

(i) Obtain the completed relevant checklist from the IA Participant.

(ii) Select a representative sample of questions from the checklist, including:

(A) all questions which indicate non-compliance with the IAC Code Set; and

(B) a sample of questions which indicate compliance with the IAC Code Set.

[27] Amended effective 1/7/19, version 009 r&p 001.19
[28] Amended effective 1/1/24, version 015 r&p 003.23
[29] Amended effective 1/1/15, version 001 r&p 001.15

(iii) Perform a walk-through of each of the selected questions with the relevant staff, focusing on how they have assured themselves that the responses to the checklist are complete and accurate.

(iv) Where non-compliance is noted on a checklist, ensure that the IA Participant have an adequate and timely action plan in place, including:

(A) remedial actions which will ensure future compliance to the IAC Code Set;

(B) realistic and appropriate resolution time frames; and

(C) accountability is allocated to the relevant staff within the IA Participant.

(v) Raise all concerns with the IA Participant and achieve satisfactory resolution/agreement.

(vi) The auditor should continually be asking the relevant staff as to:

(A) how they ensure compliance with the IAC Code Set; and

(B) to provide evidence which demonstrates that their compliance control/monitoring procedures are operating effectively.

3.3 Exemption Requests

(a) All IA Participants must at all times comply with the requirements specified in the IAC Code Set unless specifically exempted by the Company.

(b) An IA Participant requiring an exemption from certain requirements must make an application to the Company. The application must include the following information:

(i) the name of the IA Participant requiring the exemption;

(ii) date of the request;

(iii) date the out-of-compliance situation occurred;

(iv) a description of the risk and a risk rating;

(v) the section(s) of the IAC Code Set with which the IA Participant is not in compliance;

(vi) description of the requirement with which the IA Participant is not in compliance;

(vii) a statement on the reason for non-compliance;

(viii) a full description of any compensating controls that are offered as justification for the authorisation of the request; and

(ix) exact details of the IA Participant's action plan to comply with the requirements and an indication as to the likely date of achieving compliance.

(c) An exemption request form is provided in Annexure C.

3.3.1 *Exemption Process*

The Company will review the exemption request and accompanying documentation and determine if the proposed remedial action/compensating controls with respect to areas of non-compliance are satisfactory to the Company, having regard to the integrity and efficiency of IAC. The Company will advise the IA Participant of the acceptance or rejection of the exemption request.

3.3.2 *Exemption Duration*

Exemptions will only be granted for a defined period of time. The Company may grant duration different to the one requested by the IA Participant. All exemptions granted for non-compliance, regardless of when they expire, must be reviewed and renewed annually.

3.3.3 *Introduction of New or Modified Devices or New Processes*

In cases where a significant change will cause the IA Participant to be out of compliance with the IAC requirements, the IA Participant may not proceed unless appropriate exemptions have been duly granted. Examples include:

(a) deployment of any new SCD (not currently on the Approved Devices List);

(b) continued deployment of an SCD which has reached its approval sunset date; or

(c) implementing changes to PIN or cryptographic key handling or management processing.

3.4 Certification of Prospective IA Participant

(a) Each applicant must arrange for Certification as part of their membership application.

(b) Certification checklists must be used for Certification. An applicant seeking Certification must complete the relevant New IA Participant Checklist (see Annexure B) and the relevant Annual Security Audit (see Annexure A). Any further evidence of compliance which is reasonably requested by the Secretary or the committee of management must be promptly produced to the Secretary following the request.

(c) All applicants must ensure that Third Party Providers meet the obligations set out in clause 2.2 and clause 3.2.2 of this Volume.[30]

[30] Inserted effective 1/1/15, version 001 r&p 001.15

3.4.1 Guidance for External Auditors

(a) When Certification is sought by an applicant who does not have, or does not wish to use, an internal auditor, the Certification checklist must be accompanied by a report of an agreed upon procedures engagement (refer Accounting Standard AUS 904) from an external auditor.

(b) The external auditor engaged by an applicant must be acceptable to the Company. The Company maintains a set of Guidance Procedures for applicants wishing to use an external auditor, which contain a proposed set of acceptable audit procedures. Once an acceptable external auditor has been selected by the applicant the external auditor may obtain the Guidance Procedures from the Company.

3.4.2 Review of Certification documentation

The Company will review the Certification checklists referred to in clause 3.4 above and accompanying documentation and provide a report of its review to the applicant. Details of the application will be provided to the committee of management for its consideration under Regulation 4.3 as to whether:

(a) all requirements appear to have been met, or

(b) any proposed remedial action/compensating controls with respect to areas of non-compliance are satisfactory to the Company having regard to the desirability to maintain the integrity and efficiency of IAC.

Next page is Annexure A

ANNEXURE A ANNUAL SECURITY AUDITS

Note: Annexure A.1 Acquirer Annual Security Audit (Part 1) must be completed annually by all Acquirer Framework Participants in combination with either Annexure A.2 Acquirer Annual Security Audit (Part 2) or a duly signed copy of a PCI PIN Attestation of Compliance[31]

Note: Annexure A.3 Issuer Annual Security Audit must be completed annually by all Issuer Framework Participants.

A.1 ACQUIRER ANNUAL SECURITY AUDIT (PART 1)

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of sensitive data, including PINs and Cardholder Data, and the associated cryptographic practices.[32]

The following documents are referenced in this checklist;

ISO 9564.1-2011	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems[33]
AS 2805.6.1-2002/Amdt 3/2007	Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles
ISO 13491.2-2017	Financial services - Secure cryptographic devices (retail) Part 2: Security compliance checklists for devices used in financial transactions[34]
PCI PIN AoC	Payment Card Industry (PCI) PIN Security Requirements Attestation of Compliance for Onsite Assessments[35]

A.1.1 General Security Controls

(a) Please provide the details for all EFTPOS Terminals, SCRs and EPPs that you currently have deployed. Please use a separate sheet if necessary. All EFTPOS Terminals without PED deployed after 2019 shall be Approved Devices.[36]

Reference IAC Code Set Volume 1, clause 3.1(c).

EFTPOS PIN Entry Devices / Unattended Payment Terminals[37]

Manufacturer	Model No.	Approval Number	Approx Quantity

[31] Amended effective 1/1/24, version 015 r&p 003.23
[32] Last amended effective 1/1/25, version 016 r&p 001.24
[33] Amended effective 21/11/16, version 004 r&p 002.16
[34] Amended effective 1/1/24, version 015 r&p 003.23
[35] Inserted effective 1/1/24, version 015 r&p 003.23
[36] Last mended effective 1/1/25, version 016 r&p 001.24
[37] Inserted effective 1/1/25, version 16 r&p 001.24

Encrypting PIN Pads[38]

Manufacturer	Model No.	Approval Number	Approx Quantity

EFTPOS Terminals without PED (including SCR)[39]

Manufacturer	Model No.	Approval Number	Approx Quantity	Deployed prior to 2019
				Y/N
				Y/N
				Y/N
				Y/N
				Y/N

(b) Please provide the details for all Solutions that you currently have deployed including:[40]

(i) Solutions outside of the approved baseline.

(ii) Solution attestation failures.

Please use a separate sheet if necessary.[41]

Solution Name**	Vendor	Payment App	OS	Outside of Baseline	Attestation Failures	SCRP*	
						Model	Quantity

[38] Inserted effective 1/1/25, version 16 r&p 001.24
[39] Inserted effective 1/1/25, version 16 r&p 001.24
[40] Amended effective 16/12/21, version 013 r&p 001.21
[41] Amended effective 1/1/24, version 015 r&p 003.23

* SCRP is a physical card reader that has been approved by PCI PTS and is a component of a PCI Solution.

** A Solution is a Solution that has been approved against:

- Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC)™
- Payment Card Industry (PCI) Contactless Payments on COTS (CPoC™)
- Payment Card Industry (PCI) Mobile Payments on COTS (MPoC™)[42]

(c) Please provide details for all production SCM devices currently deployed or provided by cloud HSM service provider. Please use a separate sheet if necessary.[43]

Reference IAC Code Set Volume 1, clause 3.1(c).

Manufacturer	Model No.	Quantity

(d) Please provide the details for all Non-Standard Technologies that you currently have deployed. Please use a separate sheet if necessary.[44]

Reference IAC Code Set Volume 1, clause 3.1(c).

Manufacturer	Model No.	Quantity	Additional Information

(e) Third Party Providers[45]

Please provide details of all Third Party Providers used in providing acquiring services. Third party providers include terminal management providers, payment processors, cloud HSM services, and others. Please use a separate sheet if necessary.

Reference IAC Code Set Volume 1, clause 3.1(f).

[42] Inserted effective 1/1/24, version 015 r&p 003.23
[43] Last amended effective 1/1/25, version 016 r&p 001.24
[44] Amended effective 1/1/24, version 015 r&p 003.23
[45] Last amended effective 1/1/25, version 016 r&p 001.24

Third Party Provider Name	Type of service provided	Completion of IAC Security and/or PCI PIN Audit [46]

(f) All parties to the Interchange, including merchants, Acquirers, Third Party Providers and any intermediate network entities maintain procedures and practices to prevent the unauthorised disclosure of Cardholder Data, which includes but is not limited to the Primary Account Number, Cardholder Name, Service Code and Expiration Date.[47]

Reference IAC Code Set Volume 3, clause 2.5.

Yes	No	N/A

If N/A response: Reason

(g) Sensitive authentication data, including but not limited to, full magnetic stripe (or equivalent), CVC2/CVV2/CID, PIN/PIN Block is not stored in any form, outside of an SCD, subsequent to Authorisation.[48]

Reference IAC Code Set Volume 3, clause 2.6.

Yes	No	N/A

If N/A response: Reason

(h) Message Authentication applies to all IAC Interchange Links. The MAC must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1. All interchange PIN and MAC cryptographic functions are performed within an SCM that is an Approved Device.[49]

Reference AS 2805.4.1; IAC Code Set Volume 3, clause 2.4.2.

[46] Any negative findings from the audit of the third party must be reproduced in the relevant section in this audit checklist such that they can be recorded and managed through the exemption process.
[47] Amended effective 1/1/24, version 015 r&p 003.23
[48] Amended effective 1/1/25, version 016 r&p 001.24
[49] Last amended effective 1/1/25, version 016 r&p 001.24

Yes	No	N/A

If N/A response: Reason

(i) Message Authentication applies to all Terminal to Acquirer Links for all financial and key management messages.[50]

Reference AS 2805.4.1, IAC Code Set Volume 3, clause 2.4.3.

Yes	No	N/A

If N/A response: Reason

(j) IAC Interchange Lines comply with the whole-of message encryption practices of IAC Code Set Volume 4, clauses 4.7 and 4.7.1, as applicable.[51]

Reference AS 2805.5.4, IAC Code Set Volume 4, clauses 4.7 and 4.7.1., Threshold Requirement #12.

Yes	No	N/A

If N/A response: Reason

(k) IAC Interchange Links comply with the key management practices of IAC Code Set Volume 4, clause 4.5.2.[52]

Reference Threshold Requirement #10.

Yes	No	N/A

If N/A response: Reason

---

[50] Amended effective 1/1/24, version 015 r&p 003.23
[51] Last amended effective 1/1/25, version 016 r&p 001.24
[52] Last amended effective 1/1/25, version 016 r&p 001.24

(l) IAC Interchange Lines comply with the key management practices of IAC Code Set Volume 4, clause 4.7.2 (if applicable).[53]

Reference Threshold Requirement #12.

Yes	No	N/A

If N/A response: Reason

(m) Terminal key management practices comply with the requirements of IAC Code Set Volume 4, clause 4.8.2.[54]

Reference Threshold Requirement #13.

Yes	No	N/A

If N/A response: Reason

(n) Host systems which support Terminals using the TCP/IP protocol for communications meet the requirements of IAC Code Set Volume 3, clause 3.5.

Yes	No	N/A

If N/A response: Reason

(o) Privacy of communication complies with AS 2805.9 for all Terminal to Acquirer links, or any other privacy of communication standard approved by the committee of management (EFTPOS Terminals only).[55]

Reference IAC Code Set Volume 3, clause 2.4.5.

[53] Last amended effective 1/1/25, version 016 r&p 001.24
[54] Amended effective 1/1/25, version 16 r&p 001.24
[55] Amended effective 1/1/24, version 015 r&p 003.23

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to ensure all PINs are encrypted using DEA 3 or AES when transmitted outside a Secure Cryptographic Device. If a transaction is logged, the PIN block must be permanently masked or deleted from the record before it is logged.[56]

Reference IAC Code Set Volume 4, clause 4.4.2.

Yes	No	N/A

If N/A response: Reason

(q) Each type of Device, Solution and Non-Standard Technology used in Interchange has been approved for use within the IAC.[57]

Reference IAC Code Set Volume 1, clause 3.1(c); Threshold Requirement #1.

Yes	No	N/A

If N/A response: Reason

(r) Clear text PINs and clear-text keys exist only in an SCD designed for use in its operational environment.[58]

Reference IAC Code Set Volume 3, clause 2.2(d); ISO 9564-1 4.2.

Yes	No	N/A

If N/A response: Reason

---

[56] Last amended effective 1/1/25, version 016 r&p 001.24
[57] Last amended effective 1/1/25, version 016 r&p 001.24
[58] Amended effective 1/1/24, version 015 r&p 003.23

(s) All deployed ATM payment applications have been reviewed by the Acquirer or a trusted third party on behalf of the Acquirer and have been shown to contain no known security vulnerabilities or other security weakness.[59]

Reference IAC Code Set Volume 3, clause 2.2(f).

Yes	No	N/A

If N/A response: Reason

(t) Terminals using the TCP/IP protocol for communications with the host over public network meet the requirements of IAC Code Set Volume 3, clause 3.2.4(b), (c) and (i). [60]

Yes	No	N/A

If N/A response: Reason

A.1.2 Device Management

(a) Documented procedures exist, and are followed, to ensure that the deployed PIN entry device is managed in accordance with the privacy shielding requirements in clause 3.2.3 of IAC Code Set Volume 3 (Acquirers Code).[61]

Yes	No	N/A

If N/A response: Reason

(b) For Terminals running applications, documented, auditable, key management procedures exist and are followed for the secure management of any key used in the authentication processes associated with Terminal software authentication. The Acquirer shall hold and follow these procedures where it owns these keys, and shall assure themselves that the relevant party has and follows these procedures where a party

[59] Last amended effective 1/1/25, version 016 r&p 001.24
[60] Inserted effective 1/1/25, version 016 r&p 001.24
[61] Amended effective 1/1/24, version 015 r&p 003.23

other than the Acquirer (e.g. Terminal vendor or third party developer) owns these keys.[62]

Reference IAC Code Set Volume 3, clause 3.2.5(c),(e).

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist, and are followed, to ensure that any Remote Management Solution for an SCM is managed in accordance with the requirements of clause 3.3.4 of IAC Code Set Volume 3 (Acquirers Code).

Yes	No	N/A

If N/A response: Reason

(d) All symmetric encryption functionality weaker than DES-3 has been disabled within every deployed SCM.[63]

Reference IAC Code Set Volume 3, clause 3.3.2; Threshold Requirement #8.

Yes	No	N/A

If N/A response: Reason

(e) Acquirers shall maintain a register of all authorised payment and non-payment applications per device.[64]

Reference IAC Code Set Volume 3, clause 3.2.5(e).

[62] Last amended effective 1/1/24, version 015 r&p 003.23
[63] Last amended effective 1/1/25, version 016 r&p 001.24
[64] Amended effective 1/1/23, version -014 r&p 002.22

Yes	No	N/A

If N/A response: Reason

A.1.3 General Key Management[65]

(a) If for archival purposes, reconstruction of a given key is required at a later date, procedures exist and are followed to ensure the key is retained in a form such as to preclude it being intentionally used again as active keying material.[66]

Reference ISO 11568, clause 4.16.

Yes	No	N/A

If N/A response: Reason

A.1.4 Supplementary Questions for Acquirers who are submitting PCI PIN AoC/s[67]

Note: The following requirements are only to be completed by Acquirers submitting a duly signed copy of a PCI PIN Attestation of Compliance to accompany this A.1 Acquirer Annual Security Audit (Part 1) submission (as described in clause 3.2.1).[68]

(a) Compliance with the requirements of the PCI PIN Security Requirements has been confirmed.[69]

Yes	No	N/A

If N/A response: Reason

---

[65] Amended effective 1/1/25, version 016 r&p 001.24
[66] Amended effective 1/1/24, version 015 r&p 003.23
[67] Amended effective 1/1/24, version 015 r&p 003.23
[68] Amended effective 1/1/24, version 015 r&p 003.23
[69] Amended effective 1/1/24, version 015 r&p 003.23

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Acquirer Annual Security Audit (Part 1) the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Annual Security Audit (Part 1) the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

A.2 ACQUIRER ANNUAL SECURITY AUDIT (PART 2)

Annexure A.2 Acquirer Annual Security Audit (Part 2) must be completed unless submitting a duly signed copy of a PCI PIN Attestation of Compliance, completed within the same calendar year as the A.1 Annual Security Audit (Part 1).[70]

Reference Code Set Volume 1, Clause 3.2.1 (b).

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805 and ISO 9564.[71]

A.2.1 General Security Controls[72]

(a) Any clear-text PIN block format combined with a PIN encryption process has the characteristics that, for different accounts, encryption of the same PIN value under a given encryption key does not predictably produce the same encrypted results. (Note the format 0, format 3 and format 4 PIN blocks specified in ISO 9564.1 meet this requirement.)[73]

Reference ISO 9564.1, clauses 9.3 and 9.4; PCI PIN SR 3-1.

Yes	No	N/A

If N/A response: Reason

(b) No procedure requires or permits the Cardholder to disclose the PIN (verbally or in writing).[74]

Reference ISO 9564.1, clause 6.1.3; PCI PIN SR 2-1

Yes	No	N/A

If N/A response: Reason

A.2.2 Device Management

(a) Any SCD capable of encrypting a key and producing a cryptogram of that key is protected against unauthorised use to encrypt known keys or known

[70] Amended effective 1/1/24, version 015 r&p 003.23
[71] Amended effective 21/11/16, version 004 r&p 002.16
[72] Last amended effective 1/7/20, version 011 r&p 001.20
[73] Amended effective 1/1/24, version 015 r&p 003.23
[74] Last amended effective 1/1/24, version 015 r&p 003.23

key components. This protection takes the form of either or both of the following:

(i) Dual controls are required to enable the key encrypting functions; and/or[75]

(ii) Physical protection of the equipment (e.g., locked access, dual locks from the SCD) under dual control.[76]

Reference ISO 13491-2, clauses E12 and E13; PCI PIN SR 32-1. [77]

Yes	No	N/A

If N/A response: Reason

(b) Document procedures exist, and are followed, to determine that an SCD has not been subjected to unauthorised modification or substitution prior to loading cryptographic keys. This assurance takes the form of one or more of the following procedures:[78]

(i) Physical inspection and/or testing of the equipment immediately prior to key loading; and/or[79]

(ii) Physical protection of the equipment (e.g., locked access, dual locks from the SCD) under dual control.[80]

Reference ISO 13491-2, clauses A42 and A43; PCI PIN SR 33-1.

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist, and are followed, to ensure that the SCD is physically protected or otherwise controlled to prevent the SCD being stolen, modified in an unauthorised way, and then returned without detection.[81]

[75] Amended effective 1/1/25, version 016 r&p 001.24
[76] Amended effective 1/1/25, version 016 r&p 001.24
[77] Amended effective 1/1/25, version 016 r&p 001.24
[78] Amended effective 1/1/25, version 016 r&p 001.24
[79] Inserted effective 1/1/25, version 016 r&p 001.24
[80] Inserted effective 1/1/25, version 016 r&p 001.24
[81] Amended effective 1/1/24, version 015 r&p 003.23

Reference ISO 13491-2, clauses A41, A46 and A48; PCI PIN SR 30-1.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist to ensure that keys are not installed in any SCD where suspicious alteration of an SCD has been detected until the SCD has been inspected and a reasonable degree of assurance has been reached that the SCD has not been subject to any unauthorised physical or logical modifications.[82]

Reference ISO 13491-2, requirement A48; PCI PIN SR 29.

Yes	No	N/A

If N/A response: Reason

(e) Documented, auditable, key management procedures exist and are followed for the secure management of any Acquirer controlled key used in the authentication processes associated with Terminal software authentication.[83]

Reference Code Set Vol 3, clause 3.2.5(a); PCI PIN SR 29.

Yes	No	N/A

If N/A response: Reason

(f) If the SCD can translate a PIN from one PIN block format to another or if the SCD verifies PINs, then procedures exist, and are followed, to prevent or detect, repeated unauthorised calls resulting in the exhaustive determination of PINs.[84]

[82] Amended effective 1/1/24, version 015 r&p 003.23
[83] Last amended effective 1/1/24, version 015 r&p 003.23
[84] Amended effective 1/1/24, version 015 r&p 003.23

Reference ISO 13491-2, requirement C5.

Yes	No		N/A

If N/A response: Reason

A.2.3 General Key Management

(a) Documented procedures exist, and are followed to control keys so that they exist in only one or more of the permissible forms:[85]

(i) In a SCD;

(ii) Encrypted under a DEA 2, AES or DEA 3 key;

(iii) Managed as two or more full length components using the principles of dual control and split knowledge; or

(iv) Managed as m of n key shares under a Secret Sharing Scheme.

Reference ISO 11568, clauses 4.1.3; PCI PIN SR 8-1.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure a person entrusted with a key component reasonably protects that component such that no person (not similarly entrusted with that component) can observe or otherwise obtain that component.[86]

Reference ISO 11568, clauses 4.1.2; PCI PIN SR 8-2.

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist and are followed to ensure keys and key components are generated using a random or pseudo-random process

[85] Amended effective 1/1/24, version 015 r&p 003.23
[86] Amended effective 1/1/24, version 015 r&p 003.23

such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys.[87]

Reference ISO 11568, clauses 4.6.1.1; PCI PIN SR 5-1.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist to ensure each of the following:[88]

(i) A key is changed if its compromise is known or suspected;

(ii) Keys encrypted under or derived from a compromised key are changed;

(iii) Key is not changed to a variant or a transformation of the compromised key; and

(iv) The amount of time in which the compromised key remains active is consistent with the risk to all affected parties.

Reference ISO 11568, clauses 4.17; PCI PIN SR 22-1.

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure a key is used for only a single designated purpose.[89]

Reference ISO 11568, clause 4.1.7; PCI PIN SR 19.

Yes	No	N/A

If N/A response: Reason

---

[87] Amended effective 1/1/24, version 015 r&p 003.23
[88] Amended effective 1/1/24, version 015 r&p 003.23
[89] Amended effective 1/1/24, version 015 r&p 003.23

(f) Documented procedures exist and are followed to ensure that when a key is installed under dual control using key components that these key components are only combined within a SCD.[90]

Reference ISO 11568, clause 4.10.2; PCI PIN SR 12-4.

Yes	No	N/A

If N/A response: Reason

(g) Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. Key components are combined using one of the following functions:[91]

Key shares are combined to form a key by a process such that no active bit of the key could be determined without knowledge of m of n key shares.

Reference ISO 11568, clause 4.1.2; PCI PIN SR 12-4.

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure when in secure transit, cleartext key components are protected from compromise in one of the following manners:[92]

(i) Key components are transported in separate tamper-evident packaging; and/or

(ii) Key components are transported in an Approved Device.

Reference ISO 11568, clause 4.1.2; PCI PIN SR 12-4.

Yes	No	N/A

If N/A response: Reason

---

[90] Amended effective 1/1/24, version 015 r&p 003.23
[91] Amended effective 1/1/24, version 015 r&p 003.23
[92] Last amended effective 1/1/24, version 015 r&p 003.23

(i) Documented procedures exist and are followed to ensure a cleartext key component is:[93]

(i) Under the supervision of a person authorised by management with access to this component; or

(ii) Locked in a security container in such a way that can be obtained only by a person with authorized access; or

(iii) In secure transit; or

(iv) In an Approved Device.

Reference ISO 11568, clause 4.10.2, Annex B; PCI PIN SR 13-5.

Yes	No	N/A

If N/A response: Reason

(j) Documented procedures exist and are followed to protect the transfer of a key, key component or key share into SCDs so as to prevent the disclosure of the key, key components or key shares. Examples of procedures include physical inspection of the SCD equipment to detect evidence of monitoring and dual custody of the loading process.[94]

Reference ISO 11568, clause 4.10.2, Annex B; PCI PIN SR 14.

Yes	No	N/A

If N/A response: Reason

(k) Documented procedures exist and are followed to ensure that a key exists at only the minimal number of locations consistent with the operation of the system (e.g., including disaster recovery purposes, dual processing sites).[95]

[93] Last amended effective 1/1/24, version 015 r&p 003.23
[94] Last amended effective 1/1/25, version 016 r&p 001.24
[95] Amended effective 1/1/24, version 015 r&p 003.23

Reference ISO 11568, clauses 4.1.6 and 4.11.2.

Yes	No	N/A

If N/A response: Reason

(l) Documented procedures exist and are followed, to prohibit, except by chance, the entry or use of the same key in more than one PIN entry device.[96]

Reference ISO 11568, 4.11.1; PCI PIN SR 20-1.

Yes	No	N/A

If N/A response: Reason

(m) Documented procedures exist and are followed to ensure a key shared between communicating parties is not shared, except by chance, between any other communicating parties.[97]

Reference ISO 11568, 4.11.1; PCI PIN SR 17-1.

Yes	No	N/A

If N/A response: Reason

(n) Procedures exist and are followed to ensure a key or key component that has been used for a cryptographic purpose is erased or destroyed when it is no longer required using approved destruction procedures.[98]

Reference ISO 11568, 4.14; PCI PIN SR 24, 31.

Yes	No	N/A

If N/A response: Reason

---

[96] Amended effective 1/1/24, version 015 r&p 003.23
[97] Amended effective 1/1/24, version 015 r&p 003.23
[98] Amended effective 1/1/24, version 015 r&p 003.23

(o) Documented procedures exist and are followed to ensure that when a key transport key (KTK) is changed because its compromise is known or suspected, an organisation which has previously shared the key is informed of the compromise even if the KTK is no longer in use.[99]

Reference ISO 11568, 4.17; PCI PIN SR 22-1.4.

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to monitor cryptographic synchronisation errors and to investigate multiple synchronisation errors to ensure the SCD is not being misused to determine keys or PINs.[100]

Reference PCI PIN SR 18-1.

Yes	No	N/A

If N/A response: Reason

(q) Documented procedures exist and are followed to ensure if two or more of a key's components or shares are stored within the same security container (which is under dual control), then each component and share is secured in separate tamper evident packaging to preclude any component or share holder from gaining access to sufficient components or shares to reconstruct the key.[101]

Reference ISO 11568, 4.12.1; PCI PIN SR 21-3.1.

Yes	No	N/A

If N/A response: Reason

---

[99] Amended effective 1/1/24, version 015 r&p 003.23
[100] Amended effective 1/1/24, version 015 r&p 003.23
[101] Last amended effective 1/1/25, version 016 r&p 001.24

(r) Documented procedures exist and are followed to ensure a key loading device does not retain a clear-text copy of any key it has successfully transferred.[102]

Reference ISO 13491-2 F8; PCI PIN SR 6-4, 13-4.4.

Yes	No	N/A

If N/A response: Reason

(s) If personal computers are used to load encryption keys into a PIN entry device, procedures exist and are followed to ensure, at a minimum the following controls:[103]

(i) The software loads the encryption key without recording the value in non-volatile storage;

(ii) Hardware used for the key loading function is maintained under dual control;

(iii) Hardware use is monitored and logs of key loading activity are maintained;

(iv) Cable attachments and hardware are examined before each use to ensure that the equipment is free from tampering;

(v) That the computer is started from power off position for each site's key loading activity; and

(vi) An SCD is used in conjunction with the personal computer to complete all cryptographic processing and for the storage of all encryption keys.

Reference PCI PIN SR 13-9.

Yes	No	N/A

If N/A response: Reason

(t) Documented procedures exist and are followed to maintain a record of every instance when a container securing cryptographic materials is

[102] Amended effective 1/1/24, version 015 r&p 003.23
[103] Amended effective 1/1/24, version 015 r&p 003.23

opened to record date, time, person(s) involved and the purpose of the access.[104]

Reference ISO 11568 4.1.4; PCI PIN SR 26-1.

Yes	No	N/A

If N/A response: Reason

(u) Documented procedures exist and are followed to ensure if keys are loaded or transported using an electronic key loading device then:[105]

(i) The key loading device is a device approved by an Approved Standard Entity with an Accepted Standard;

Reference IAC Code Set Volume 3, clause 2.3.1(a).

(ii) The key loading device is under the supervision of a person authorised by management, or is stored in a secure manner (e.g. in a safe) such that no unauthorised person may have access to it; and

Reference IAC Code Set Volume 3, clause 3.4(b) and ISO 13491.2, clause F.3.

(iii) The key loading device is designed or controlled so that only authorised personnel under dual control can utilise and enable it to output a key into another SCD. Such personnel ensure that the transfer is not being monitored, e.g., that there is no key recording device inserted between the SCDs.

Reference IAC Code Set Volume 3, clause 3.4(b); ISO 13491.2, clause F.3.

Yes	No	N/A

If N/A response: Reason

---

[104] Amended effective 1/1/24, version 015 r&p 003.23
[105] Inserted effective 1/1/25, version 016 r&p 001.24

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Acquirer Annual Security Audit (Part 2) the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Annual Security Audit (Part 2) the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

A.3 ISSUER ANNUAL SECURITY AUDIT

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805 and IAC Code Set Volume 4.[106]

The following documents are referenced in this checklist;[107]

AS 2805.6.1-2002/Amdt 3/2007	Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles
ISO 9564.1-2017	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems.[108]
ISO 9564.2-2014	Financial services – Personal Identification Number (PIN) management and security – Part 2: Approved algorithms for PIN encipherment.[109]
ISO 13491.1-2016	Financial Services – Secure cryptographic device (retail) – Part 1: Concepts, requirements and evaluation methods.[110]
ISO.13491.2-2017	Financial Services – Secure cryptographic devices (retail) – Part 2: Security compliance checklists for devices sued in financial transactions.[111]
Shamir, Adi (1979)	"How to share a secret", Communications of the ACM, 22 (11): 612-613, doi:10.1145/359168.359176.[112]

A.3.1 General Security Controls

These controls apply to all issuing services including issuing obligations in Interchange. Section 3.3 will address specific requirements and concerns where Issuers allow the transmission of cardholder PINs over open Networks in compliance with Part 3 of IAC Code Set Volume 2.[113]

[106] Amended effective 1/1/19, version 008 r&p 002.18
[107] Amended effective 1/1/24, version 015 r&p 003.23
[108] Inserted effective 1/1/19, version 008 r&p 002.18
[109] Inserted effective 1/1/19, version 008 r&p 002.18
[110] Inserted effective 1/1/19, version 008 r&p 002.18
[111] Inserted effective 1/1/19, version 008 r&p 002.18
[112] Inserted effective 1/1/19, version 008 r&p 002.18
[113] Inserted effective 1/1/19, version 008 r&p 002.18

(a) Please provide the details for all production SCM devices currently deployed or provided by cloud HSM service provider. Please use a separate sheet if necessary.[114]

Reference IAC Code Set Volume 1, clause 3.1(c); IAC Code Set Volume 2, clause 2.2.

Manufacturer	Model No.	Quantity

(b) Third Party Provider Name[115]

Reference IAC Code Set Volume 1, clause 3.1(f).

Please provide details of all Third Party Providers associated with the management of PINs and the associated cryptographic practices used in providing issuing services. Card manufacturers handling PINs for card personalisation may provide PCI Card Production AOC as an alternative to the annual security audit checklist. Please use a separate sheet if necessary.[116]

Third Party Provider Name	Type of service provided	Completion of IAC Security or PCI Card Production Audit[117]

[114] Last amended effective 1/1/25, version 016 r&p 001.24
[115] Amended effective 1/1/24, version 015 r&p 003.23
[116] Last amended effective 1/1/25, version 016 r&p 001.24
[117] Amended effective 1/1/25, version 016 r&p 001.24. Any negative findings from the audit of the third party must be reproduced in the relevant section in this audit checklist such that they can be recorded and managed through the exemption process.

(c) Any clear-text PIN block format combined with a PIN encryption process has the characteristics that, for different accounts, encryption of the same PIN value under a given encryption key does not predictably produce the same encrypted results. (Note the format 0, format 3 and format 4 PIN blocks specified in ISO 9564.1 meet this requirement.)[118]

Reference ISO 9564.1, clauses 9.3 and 9.4; PCI PIN SR 3-1.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist and are followed to ensure all PINs are encrypted using DEA 3 or AES when transmitted outside a Secure Cryptographic Device, except where Part 3 of IAC Code Set Volume 2 applies. If a transaction is logged, the PIN block must be permanently masked or deleted from the record before it is logged.[119]

Reference ISO 9564.1 clause 4.2;ISO 9564.2.

Yes	No	N/A

If N/A response: Reason

(e) No procedure requires or permits the Cardholder to disclose the PIN verbally or in writing.[120]

Reference ISO 9564.1 clause 6.1.3; PCI PIN SR 2-1.

Yes	No	N/A

If N/A response: Reason

(f) Message Authentication applies to all IAC Interchange Links. The MAC must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1. All interchange PIN and

[118] Last amended effective 1/1/24, version 015 r&p 003.23
[119] Last amended effective 1/1/25, version 016 r&p 001.24
[120] Last amended effective 1/1/25, version 016 r&p 001.24

MAC cryptographic functions are performed within an SCM that is an Approved Device.[121]

Reference IAC Code Set Volume 4, clause 4.5.1.

Yes	No	N/A

If N/A response: Reason

(g) IAC Interchange Lines comply with the whole-of message encryption practices of IAC Code Set Volume 4, clauses 4.7 and 4.7.1, as applicable[122]

Reference AS 2805.5.4; IAC Code Set Volume 4, clauses 4.7 and 4.7.1; Threshold Requirement #12.

Yes	No	N/A

If N/A response: Reason

(h) IAC Interchange Links comply with the key management practices of IAC Code Set Volume 4, clause 4.5.2.[123]

Reference Threshold Requirement #10.

Yes	No	N/A

If N/A response: Reason

---

[121] Last amended effective 1/1/24, version 015 r&p 003.23
[122] Last amended effective 1/1/25, version 016 r&p 001.24
[123] Last amended effective 1/1/25, version 016 r&p 001.24

(i) IAC Interchange Lines comply with the key management practices of IAC Code Set Volume 4, clause 4.7.2 (if applicable).[124]

Reference Threshold Requirement #12.

Yes	No	N/A

If N/A response: Reason

A.3.2 Device Management

(a) Each type of SCM used in Interchange or for the handling or management of plaintext PINs and/or related keys, and those devices providing a Remote Management Solution for Security Control Modules have been approved for use within the IAC.[125]

Reference IAC Code Set Volume 2, clauses 2.2 and 4.2; ISO 13491.1, ISO 13491.2; Threshold Requirement #1.[126]

Yes	No	N/A

If N/A response: Reason

(b) Document procedures exist, and are followed, to ensure that any Remote Management Solution for an SCM is managed in accordance with the requirements of IAC Code Set Volume 2, clause 4.5.

Yes	No	N/A

If N/A response: Reason

---

[124] Last amended effective 1/1/25, version 016 r&p 001.24
[125] Last amended effective 1/1/25, version 016 r&p 001.24
[126] Last amended effective 1/1/25, version 016 r&p 001.24

A.3.3 Key Management

(a) Documented procedures exist, and are followed to control keys so that they exist in only one or more of the permissible forms:[127]

(i) In a SCD;

(ii) Encrypted under a DEA 2, DEA 3 or AES key;

(iii) Managed as two or more full length components using the principles of dual control and split knowledge; and/or

(iv) Managed as m of n key shares under a Secret Sharing Scheme.

Reference ISO 11568, clauses 4.1.3; PCI PIN SR 8-1.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure a person entrusted with a key component or a key share, reasonably protects that component or share such that no person (not similarly entrusted with that component or share) can observe or otherwise obtain that component or share.[128]

Reference ISO 11568, clauses 4.1.2; PCI PIN SR 8-2[129]

Yes	No	N/A

If N/A response: Reason

---

[127] Last amended effective 1/1/24, version 015 r&p 003.23
[128] Last amended effective 1/1/25, version 016 r&p 001.24
[129] Last amended effective 1/1/25, version 016 r&p 001.24

(c) Documented procedures exist and are followed to ensure keys, key components and key shares are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys.[130]

Reference ISO 11568, clause 4.6.1.1; PCI PIN SR 5-1.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist to ensure each of the following:[131]

(i) A key is changed if its compromise is known or suspected;

(ii) Keys encrypted under or derived from a compromised key are changed;

(iii) A key is not changed to a variant or a transformation of the compromised key; and

(iv) The amount of time in which the compromised key remains active is consistent with the risk to all affected parties.

Reference ISO 11568, clause 4.17; PCI PIN SR 22-1.[132]

Yes	No	N/A

If N/A response: Reason

---

[130] Last amended effective 1/1/25, version 016 r&p 001.24
[131] Amended effective 1/1/24, version 015 r&p 003.23
[132] Amended effective 1/1/25, version 016 r&p 001.24

(e) Documented procedures exist and are followed to ensure a key is used for only a single designated purpose.[133]

Reference ISO 11568, clause 4.1.7; PCI PIN SR 19.[134]

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure that when a key is installed under dual control using key components that these key components or key shares are only combined within a SCD.[135]

Reference ISO 11568, clause 4.10.2; *PCI PIN SR 12-4.*[136]

Yes	No	N/A

If N/A response: Reason

(g) Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. Key components are combined using one of the following functions:[137]

(i) XOR and/or

(ii) Encryption

[133] Last amended effective 1/1/25, version 016 r&p 001.24
[134] Last amended effective 1/1/25, version 016 r&p 001.24
[135] Last amended effective 1/1/25, version 016 r&p 001.24
[136] Last amended effective 1/1/25, version 016 r&p 001.24
[137] Last amended effective 1/1/24, version 015 r&p 003.23

Key share are combined to form a key by a process such that no active bit of the key could be determined without knowledge of m of n key shares.

Reference ISO 11568, clause 4.1.2; PCI PIN SR 12-4.[138]

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure when in secure transit, cleartext key components are protected from compromise in one of the following manners:[139]

(i) Key components are transported in separate tamper-evident packaging; or

(ii) Key components are transported in a device meeting the requirements of a Secure Cryptographic Devic.

Reference ISO 11568, clause 4.1.2; PCI PIN SR 12-4.[140]

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure a cleartext key component is:[141]

(i) Under the supervision of a person authorised by management with access to this component; or

(ii) Locked in a security container in such a way that can be obtained only by a person with authorized access; or

(iii) In secure transit; or

(iv) In a Secure Cryptographic Device.

[138] Amended effective 1/1/25, version 016 r&p 001.24
[139] Last amended effective 1/1/24, version 015 r&p 003.23
[140] Amended effective 1/1/25, version 016 r&p 001.24
[141] Last amended effective 1/1/24, version 015 r&p 003.23

Reference ISO 11568, clause 4.10.2, Annex B; PCI PIN SR 13-5.

Yes	No	N/A

If N/A response: Reason

(j) Documented procedures exist and are followed to ensure if keys are loaded or transported using an electronic key loading device then:[142]

(i) The key loading device is a device approved by an Approved Standard Entity with an Accepted Standard;[143]

(ii) The key loading device is under the supervision of a person authorised by management, or is stored in a secure manner (e.g., in a safe) such that no unauthorised person may have access to it; and

(iii) The key loading device is designed or controlled so that only authorised personnel under dual control can utilise and enable it to output a key into another SCD. Such personnel ensure that the transfer is not being monitored, e.g., that there is no key recording device inserted between the SCDs.

Reference IAC Code Set Vol 1, Clause 3.1(c); ISO 13491.2, clause F.3.

Yes	No	N/A

If N/A response: Reason

(k) Documented procedures exist and are followed to protect the transfer of a key, key component or key share into SCMs so as to prevent the disclosure of the key, key components or key shares. Examples of procedures include physical inspection of the SCD equipment to detect evidence of monitoring and dual custody of the loading process.[144]

[142] Last amended effective 1/1/25, version 015 r&p 003.23
[143] Amended effective 1/1/25, version 016 r&p 001.24
[144] Last amended effective 1/1/24, version 015 r&p 003.23

Reference ISO 11568, clause 4.10.2, Annex B; PCI PIN SR 14.

Yes	No	N/A

If N/A response: Reason

(l) Documented procedures exist and are followed to ensure that a key exists at only the minimal number of locations consistent with the operation of the system (e.g., including disaster recovery purposes, dual processing sites).[145]

Reference ISO 11568, clauses 4.1.6 and 4.11.2.

Yes	No	N/A

If N/A response: Reason

(m) If for archival purposes, reconstruction of a given key is required at a later date, procedures exist and are followed to ensure the key is retained in a manner such as to preclude it being intentionally used again as active keying material.[146]

Reference ISO 11568, 4.16.

Yes	No	N/A

If N/A response: Reason

---

[145] Amended effective 1/1/24, version 015 r&p 003.23
[146] Last amended effective 1/1/24, version 015 r&p 003.23

(n) Documented procedures exist and are followed to ensure a key shared between communicating parties is not shared between any other communicating parties.[147]

Reference ISO 11568, 4.11.1; PCI PIN SR 17-1.[148]

Yes	No	N/A

If N/A response: Reason

(o) Procedures exist and are followed to ensure a key, key component or key share that has been used for a cryptographic purpose is erased or destroyed when it is no longer required using approved destruction procedures.[149]

Reference ISO 11568, 4.14; PCI PIN SR 24, 31.[150]

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to ensure that when a key transport key (KTK) is changed because its compromise is known or suspected, an organisation which has previously shared the key is informed of the compromise even if the KTK is no longer in use.[151]

Reference ISO 11568, 4.17; PCI PIN SR 22-1.4.[152]

Yes	No	N/A

If N/A response: Reason

---

[147] Amended effective 1/1/24, version 015 r&p 003.23
[148] Amended effective 1/1/25, version 016 r&p 001.24
[149] Last amended effective 1/1/24, version 015 r&p 003.23
[150] Last amended effective 1/1/25, version 016 r&p 001.24
[151] Amended effective 1/1/24, version 015 r&p 003.23
[152] Amended effective 1/1/25, version 016 r&p 001.24

(q) Documented procedures exist and are followed to ensure if two or more of a key's components or shares are stored within the same security container (which is under dual control), then each component and share is secured in separate tamper evident packaging to preclude any component or share holder from gaining access to sufficient components or shares to reconstruct the key.[153]

Reference ISO 11568, 4.12.1; PCI PIN SR 21-3.1.

Yes	No	N/A

If N/A response: Reason

(r) Documented procedures exist and are followed to ensure a key loading device does not retain a clear-text copy of any key it has successfully transferred.[154]

Reference ISO 13491-2 F8; PCI PIN SR 6-4, 13-4.4.[155]

Yes	No	N/A

If N/A response: Reason

(s) Documented procedures exist and are followed to maintain a record of every instance when a container securing cryptographic materials is opened to record date, time, person(s) involved and the purpose of the access.[156]

Reference ISO 11568 4.1.4; PCI PIN SR 26-1.[157]

Yes	No	N/A

If N/A response: Reason

---

[153] Last amended effective 1/1/25, version 016 r&p 001.24
[154] Amended effective 1/1/24, version 015 r&p 003.23
[155] Amended effective 1/1/25, version 016 r&p 001.24
[156] Amended effective 1/1/24, version 015 r&p 003.23
[157] Amended effective 1/1/25, version 016 r&p 001.24

A.3.4 General Security Controls for PIN Usage over Open Networks [158]

This section addresses the minimum requirements for PIN usage in Issuer functionality offered over open networks which don't employ secure cryptographic devices for PIN entry. This includes, but is not limited to, PIN change and delivery mechanisms, internet banking registration systems, and other internet product offerings by an Issuer (Part 3 of IAC Code Set Volume 2).

(a) Documented procedures exist and are followed to ensure the Issuer complies with the current version of ISO 9546.1 to the maximum extent possible consistent with the Issuer's security policies and risk management requirements.

Reference IAC Code Set Volume 2, clause 2.1.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure the concurrent existence of clear text PIN and PAN is kept to the absolute minimum possible consistent with the functionality being implemented.[159]

Reference IAC Code Set Volume 2, clause 3.1(a)(i).

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist and are followed to ensure the Identification of the Cardholder uses additional identifying data other than that contained on or in the Card itself.[160]

Reference IAC Code Set Volume 2, clause 3.1(a)(ii).

Yes	No	N/A

If N/A response: Reason

---

[158] Inserted effective 1/1/9, version 008 r&p 002.18
[159] Amended effective 1/1/24, version 015 r&p 003.23
[160] Amended effective 1/1/24, version 015 r&p 003.23

(d) Documented procedures exist and are followed to ensure Issuers provide Cardholders with a means to determine that the dialogue with the Issuer is genuine.[161]

Reference IAC Code Set Volume 2, clause 3.1(a)(iii).

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure the Issuer uses calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and implements additional Cardholder authentication.[162]

Reference IAC Code Set Volume 2, clause 3.1(a)(iv).

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure all systems transporting PIN data or PAN data, or both, over open networks provide mutual assurance to the Issuer and Cardholder that they are both genuine.[163]

Reference IAC Code Set Volume 2, clause 3.1(a)(v).

Yes	No	N/A

If N/A response: Reason

---

[161] Amended effective 1/1/24, version 015 r&p 003.23
[162] Amended effective 1/1/24, version 015 r&p 003.23
[163] Amended effective 1/1/24, version 015 r&p 003.23

(g) Documented procedures exist and are followed to ensure all events involving the transmission of the PIN or PAN, or both, back to the Cardholder are acknowledged using an out-of-band mechanism.[164]

Reference IAC Code Set Volume 2, clause 3.1(a)(vi).

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure Issuers provide Cardholders with the means to confirm the outcome of events involving a PIN or a PAN or both.[165]

Reference IAC Code Set Volume 2, clause 3.1(a)(vii).

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure Issuers consider threats arsing through device convergence resulting from technological change in selecting acceptable out-of-band mechanisms.[166]

Reference IAC Code Set Volume 2, clause 3.1(a)(viii).

Yes	No	N/A

If N/A response: Reason

---

[164] Amended effective 1/1/24, version 015 r&p 003.23
[165] Amended effective 1/1/24, version 015 r&p 003.23
[166] Amended effective 1/1/24, version 015 r&p 003.23

A.3.5 Transaction Verification[167]

This section addresses the requirements to ensure that all forms of card verification values are generated independently without collision for any given card.

(a) From 1 January 2026, documented procedures exist and are followed to ensure that for all Cards issued from this date, all values for the variants of CSC for a Card are unique and unpredictable. This includes:

(i) the CVV2 (or equivalent CSC) printed on the card itself,

(ii) the CVC1 (or equivalent CSC) encoded in the magnetic stripe discretionary data, and

(iii) the iCVV (or equivalent CSC) encoded in the EMV Track Two Equivalent Data.

Reference IAC Code Set Volume 2, clause 2.10.

Yes	No	N/A

If N/A response: Reason

(b) from 1 January 2026, documented procedures exist and are followed to ensure that for all Transactions the CVC1 and iCVV (or equivalent CSC) is verified as correct.

Reference IAC Code Set Volume 2, clause 2.10.

Yes	No	N/A

If N/A response: Reason

---

[167] Inserted effective 1/7/20, version 011 r&p 001.20

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Issuer Annual Security Audit the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Issuer Annual Security Audit the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

Next page is Annexure B

ANNEXURE B NEW FRAMEWORK PARTICIPANT CERTIFICATION

Note: Annexure B.1 Acquirer Certification Checklist is ONLY to be completed by a new Framework Participant.

B.1 ACQUIRER CERTIFICATION CHECKLIST

To: The Secretary
Australian Payments Network Limited
Suite 2, Level 17, Grosvenor Place[168]
225 George Street,
Sydney NSW 2000

Re: Issuers and Acquirers Community

From: Name of Applicant ("**Applicant**"): _____

Place of Incorporation: _____

ACN / ABN / ARBN: _____

Registered Office Address _____

_____

Name of Contact Person:: _____

Telephone Number: ( ) _____

Email Address: _____

CERTIFICATION OBJECTIVES

The objective of Certification is to ensure that each IAC Applicant that becomes an Acquirer confirms for the benefit of each other Framework Participant and the Company that it meets the technical, operational and security requirements applicable to Acquirers which are set out in IAC Code Set Volume 3 (Acquirers Code), IAC Code Set Volume 5 (Settlement Code) and IAC Code Set Volume 6 (ATM System Code) as applicable.

REPRESENTATIONS AND UNDERTAKINGS

By signing this Acquirer Certification Checklist, the Applicant:

(a) acknowledges that membership of IAC is conditional on the Applicant having obtained Certification in accordance with the IAC Regulations and Manual and that this Acquirer Certification Checklist is required to obtain that Certification;

[168] Amended effective 1/1/24, version 015 r&p 003.23

(b) warrants that it satisfies the requirements applicable generally to Acquirers as set out in IAC Code Set Volume 3 (Acquirers Code), IAC Code Set Volume 5 (Settlement Code) (save where and only to the extent that the Applicant provides for settlement in accordance with the settlement rules and practices of eftpos Payments Australia Ltd) and IAC Code Set Volume 6 (ATM System Code) as at the date of this Acquirer Certification Checklist, and that the information contained in this completed Acquirer Certification Checklist is correct and accurately reflects current IAC requirements;

(c) if the Applicant is granted Certification, agrees to:

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

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

Terms used in this Acquirer Certification Checklist have the same meanings as in the IAC Code Set unless otherwise defined.

SIGNED for and behalf of **THE APPLICANT**

By signing this Acquirer Certification Checklist the signatory states that the signatory is duly authorised to sign this Acquirer Certification Checklist for and on behalf of the Applicant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Certification Checklist the signatory states that the signatory is duly authorised to sign this Acquirer Certification Checklist as auditor for and on behalf of the Applicant and that the signatory is satisfied with the accuracy of the responses contained within the certification checklist.

Name of Auditor	Signature of Auditor
Date	

Note: This Annexure B.2 Issuer Certification Checklist is ONLY to be completed by a new Framework Participant.

B.2 ISSUER CERTIFICATION CHECKLIST

To: The Secretary
Australian Payments Network Limited
Suite 2, Level 17, Grosvenor Place[169]
225 George Street,
Sydney NSW 2000

Re: Issuers and Acquirers Community

From: Name of Applicant ("**Applicant**"): _____

Place of Incorporation: _____

ACN / ABN / ARBN: _____

Registered Office Address _____

_____

Name of Contact Person: _____

Telephone Number: ( ) _____

Email Address: _____

CERTIFICATION OBJECTIVES

The objective of Certification is to ensure that each IAC Applicant that becomes an Issuer confirms for the benefit of each other Framework Participant and the Company that it meets the technical, operational and security requirements applicable to Issuers which are set out in IAC Code Set Volume 2 (Issuers Code) and IAC Code Set Volume 5 (Settlement Code) as applicable.

REPRESENTATIONS AND UNDERTAKINGS

By signing this Issuer Certification Checklist, the Applicant:

(a) acknowledges that membership of IAC is conditional on the Applicant having obtained Certification in accordance with the IAC Regulations and Manual and that this Issuer Certification Checklist is required to obtain that Certification;

[169] Amended effective 1/1/24, version 015 r&p 003.23

(b) warrants that it satisfies the requirements applicable generally to Issuers as set out in Part 5 of IAC Code Set Volume 2 (Issuers Code) and IAC Code Set Volume 5 (Settlement Code) (save where and only to the extent that the Applicant provides for settlement in accordance with the settlement rules and practices of eftpos Payments Australia Ltd) as applicable, as at the date of this Issuer Certification Checklist, and that the information contained in this completed Issuer Certification Checklist is correct and accurately reflects current IAC requirements;[170]

(c) if the Applicant is granted Certification, agrees to:

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

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

Terms used in this Issuer Certification Checklist have the same meanings as in the IAC Code Set unless otherwise defined.

SIGNED for and behalf of **THE APPLICANT**

By signing this Issuer Certification Checklist the signatory states that the signatory is duly authorised to sign this Issuer Certification Checklist for and on behalf of the Applicant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Issuer Certification Checklist the signatory states that the signatory is duly authorised to sign this Issuer Certification Checklist as auditor for and on behalf of the Applicant and that the signatory is satisfied with the accuracy of the responses contained within the Issuer Certification Checklist.

Name of Auditor	Signature of Auditor
Date	

The next page is Annexure C

[170] Amended effective 1/1/24, version 015 r&p 003.23

ANNEXURE C EXEMPTION REQUEST FORM

Framework Participant: _____ Approval to disclose to eftpos Payments Australia Limited **given** / **not given** (*delete as applicable*):

Authorised by:_____

Date:_____

Date of Request: _____ Date of Original Request: _____ Reference Number:_____

Section & clause number of requirement	Requirement for which Framework Participant is not in compliance	Situation (reason for non-compliance)	Risk	Rank	Compensating Controls	Residual Risk	Action to be taken and timeframe
If exemption is sought in respect of a particular device, insert Manufacturer, model, revision and software version	Type in the actual wording of the Requirement with which the Framework Participant is not complying	Describe the situation, including when and why out-of-compliance occurred.	Describe the risks the out-of-compliance situation poses	High, Medium or Low	List the compensating controls that reduce the risk	High, Medium or Low	List what you are doing to correct the non-compliance **For Extension Request** Indicate the reason why an extension is sought **Promised date of correction** Indicate the date when the situation will be corrected.

Risk Weighting

HIGH	MEDIUM	LOW
• potential loss of integrity of PINs • potential material losses to Framework Participants, Card Acceptors or Cardholders • potential mass fraud • potential loss of public confidence	• potential reduced integrity of PINS • potential changes to financial content of transaction • potential monetary losses to Framework Participants, Card Acceptors or Cardholders could be significant.	• minimal effect on the integrity of PINs • potential monetary losses to Framework Participants would not be significant.

Next page is Annexure D

ANNEXURE D IAC OPERATIONAL BROADCAST FORM

Disclaimer:

This document has been compiled from information provided by third parties. No representation or warranty is made by AusPayNet as to the truth or accuracy of the information and AusPayNet, its officers, employees and agents expressly disclaim all and any liability in respect of the information.

DOCUMENT TITLE *<Framework Participant>* *<Brief Broadcast Title>*	
DOCUMENT NUMBER:	IAC CS3\COB\nnn.yyyy
DETAILS	
Date of Advice:	<DD/MMM/YYYY>
Notifying Framework Participant:	
Framework Participant Experiencing Difficulty:	
CONTACT POINT	
Name:	<Contact Name>
Phone Number:	<Contact Phone>
Fax Number:	<Contact Fax>
Email Address:	<Contact Email>
PAYMENT SYSTEM AFFECTED	IAC – Issuers and Acquirers Framework
PROCESSES AFFECTED List of processes affected which may directly or indirectly impact other Framework Participants: • Unscheduled network outage; • Scheduled network outage; • Exchange of Operational Information; and • Disruptive Event.	
EXPECTED DURATION OF AFFECTED PROCESS	
Date Occurred / Scheduled:	<DD/MMM/YYY>
Start Time of Outage:	<HH:MM> (Approximate)
End Time of Outage:	<HH:MM> (Approximate)

COMMUNICATION PROCESS	
Advise Framework Participants:	<YES / NO>
Advise Non- Members:	<YES / NO>
AusPayNet to provide prepared Statement:	<YES / NO>
(Please attach text of statement in Attachments below)	
Refer media to affected Framework Participant:	<YES / NO>

COMMENTS

ATTACHMENTS
Attach any IAC Operational Broadcast (COB) related documents here.

AusPayNet Comments

Next page is Annexure E

ANNEXURE E PRINCIPLES FOR TECHNOLOGIES AT POINT OF INTERACTION [171]

[Deleted]

Next page is Annexure F

[171] Deleted effective 1/1/20, version 010 r&p 002.19

ANNEXURE F NOTICE OF STANDARD MERCHANT PRICING FOR CREDIT, DEBIT AND PREPAID CARD TRANSACTIONS[172]

[Acquirer Logo] ***[Informative]***

F.1 INTRODUCTION AND PURPOSE

Reforms driven by the Reserve Bank of Australia, and enacted by the Australian Competition and Consumer Commission banning excessive surcharging have come into effect.

Specifically, from 1 September 2016, Large Merchants are required to ensure that their customer surcharges for accepting credit, debit and prepaid card payments do not exceed the cost of acceptance for each of those payment types. The requirement applies to all other merchants from 1 September 2017.

This document summarises the key elements of these reforms. More information is available through the Q&As created by the RBA and the ACCC.

F.2 BENEFITS TO MERCHANTS

The framework emphasises the right of merchants to surcharge to cover their acceptance costs and signal differences in costs to consumers. It also improves the transparency of payment costs to merchants.

F.3 PERMITTED SURCHARGES AND COST OF ACCEPTANCE

Merchants are entitled to levy surcharges for card transactions as long as they do not exceed the cost of acceptance for the Merchant for that scheme at that time.

The cost of acceptance is the average cost for a card scheme for a particular reference period, calculated by expressing the total value of all merchant service fee/s and other applicable fees and premiums paid by you to us or third party payment facilitators as a percentage of the total value of all card transactions for that scheme during that reference period.

F.4 MERCHANT FEE STATEMENTS

Each month and annually from 1 June 2017, we will provide you with a fee statement, indicating the average fees applicable to the card transactions we acquire for you, to help you calculate your costs of acceptance for the following:

(a) **debit card schemes** (which include prepaid card schemes in all cases): eftpos (administered by eftpos Payments Australia Limited), Debit Mastercard, and Visa Debit; and,[173]

[172] Inserted effective 1/6/17, version 005 r&p 001.17
[173] Amended effective 1/1/20, version 010 r&p 002.19

(b) **credit card schemes**: MasterCard Credit, and Visa Credit.

This transparency will help merchants to know how much it costs them to accept card payments and will also enable merchants to make more informed decisions about whether to surcharge different payment methods.

The fee statement will clearly detail:

(a) the reference period to which the fee statement relates;

(b) the fees paid by you to us in relation to the card transactions we acquired for you during the reference period; these will be the aggregate of merchant service fees, Terminal rental fees, gateway or fraud prevention fees, and any other fees for processing transactions (such as international service assessments, switching fees and fraud-related chargeback fees, but not the cost of any actual chargebacks);

(c) the total value of card transactions we acquired for you during the reference period; and

(d) the average cost of acceptance for card transactions by scheme.

The fee statement will typically follow the format set out below:

MERCHANT FEE STATEMENT **FOR THE PERIOD [ ] TO [ ]** **(Statement Period)**						
	eftpos / eftpos Prepaid	**Debit Mastercard/ Mastercard Prepaid**	**Mastercard Credit**	**Visa Debit / Visa Prepaid**	**Visa Credit**	**Other***
TOTAL VALUE OF CARD TRANSACTIONS $AUD ("X")						
TOTAL VALUE OF FEES $AUD ("Y")						
AVERAGE COST OF ACCEPTANCE ("Y/X%")						

* Acquirers are encouraged, but not obliged, to disclose acceptance costs for card payment types not expressly covered by the reforms (e.g. Union Pay, JCB, Diners Club).

Note: Merchants will be able to surcharge any of the cards covered by the RBA's standard up to the average percentage cost of acceptance in their annual statement for that card type. However, some merchants may have other costs of accepting a particular type of card that they would like to include in their surcharge. These may include:

- *gateway fees paid to a payment service provider*

- *the cost of fraud prevention services paid to an external provider*
- *any Terminal costs paid to a provider other than the merchant's acquirer or payments facilitator*
- *the cost of insuring against forward delivery risk. This applies to agents (such as travel agents) who pay an external party to insure against the risk that the agent will be liable to a customer for the failure of a principal supplier (such as an airline or hotel) on payments accepted via cards.*

If those costs meet the requirements for inclusion and can be documented, merchants will be able to add them to the costs charged by their acquirer or payment facilitator over the previous year and, based on their total costs, calculate their average percentage cost for that card system. Merchants may not surcharge above this average cost.

END