Payments Crisis Coordination Framework

November 2026

RESERVE BANK
OF AUSTRALIA

Australian Government
National Office of Cyber Security

Disclaimer

The Payments Crisis Coordination Framework (PCC Framework) is **for information purposes only**. The PCC Framework does not amend, supplement, confer, limit or otherwise affect any power, function, right, obligation or responsibility of or on any entity, including under any arrangement referred to in this framework.

The PCC Framework has been co-authored by the Reserve Bank of Australia and the National Office of Cyber Security of the Department of Home Affairs, with contribution and input from Australian government agencies and participants of the Australian payments industry.[1]

The authors of and contributors to the PCC Framework accept no responsibility for the accuracy, completeness or currency of the PCC Framework (including any information on or about any arrangement referred to in the framework). The accuracy or completeness of the PCC Framework may be affected by events or developments which occur after its publication.

Users of the PCC Framework assume the entire risk related to their use of the framework. Users remain responsible for understanding and complying with their legal and regulatory obligations.

The PCC Framework does not constitute legal, regulatory, risk or other professional advice. If and to the extent users require professional advice, they should seek advice from their own professional advisers.

© Commonwealth of Australia (Department of Home Affairs) and Reserve Bank of Australia 2026

For the full copyright provisions that apply to this publication, see sections 1 to 3 of https://www.rba.gov.au/copyright. The publication may include Excluded Material (such as Third Party Material), each as defined on that page.

ISBN: 978-1-7645772-6-7

[1] Contributors to the development of the PCC Framework included representatives from Australian Federal Police, Australian Payments Network, Australian Payments Plus, Australian Prudential Regulation Authority, Australian Securities and Investments Commission, Australian Securities Exchange, Australian Signals Directorate's Australian Cyber Security Centre, Commonwealth Treasury and National Emergency Management Agency.

Contents

Purpose 4

PCC Framework Guide 4

List of Acronyms 5

Coordination Arrangements Map 6

Coordination Arrangements Map – An Example Scenario 7

Stage 1: Notification 9

Incident Reporting to Government Decision Tree 14

Stage 2: Response 15

Stage 3: Recovery 21

Response Group and Entity Summaries 23

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) 24

National Office of Cyber Security (NOCS) 25

National Coordination Mechanism (NCM) 26

CFR Cyber Assessment and Response Team (CART) 27

AusPayNet Systemic Crisis Group (SCG) 28

AP+ Incident Response Group (IRG) 29

Appendix A: Key Plans and Playbooks 30

Purpose

The Payments Crisis Coordination Framework (PCC Framework) is a 'reference guide' for Australian government entities and payments industry participants. It **consolidates information about the roles and responsibilities of key government and industry groups and entities involved in coordinating a response to a payments crisis** (a system-wide incident affecting the payments sector). While the focus of the PCC Framework is a cyber security crisis affecting the **Australian payments sector**, many arrangements described in this framework may also be relevant during other incidents affecting the payments system.

The PCC Framework is not in itself a coordination mechanism, but a **summary** of key existing arrangements – each of these have their own triggers, procedures and definitions of a crisis.

While the PCC Framework focuses on payments crises, entities are encouraged to engage with government cyber security agencies (e.g. ASD's ACSC and NOCS) for any cyber security incident, regardless of severity. Early engagement can support incident containment and help minimise potential impacts.

PCC Framework Guide

The PCC Framework covers three broad categories of response arrangements during a payments crisis:

- **Whole-of-government response arrangements, focusing on a cyber security payments crisis**
- **CFR response arrangements**
- **Payments industry's coordinated response arrangements.**

Depending on the nature of the crisis and the impacted entity, an entity may have mandatory reporting obligations to, and receive assistance or instruction from, organisations or crisis response groups within each of the three broad categories mentioned above.

The **Coordination Arrangements Map** provides an overview of the organisations and crisis response groups in each category, and the expected interaction between groups or organisations and categories.

The **Notification, Response and Recovery summary tables** provide further details of the roles of organisations or crisis response groups at different stages of a crisis.

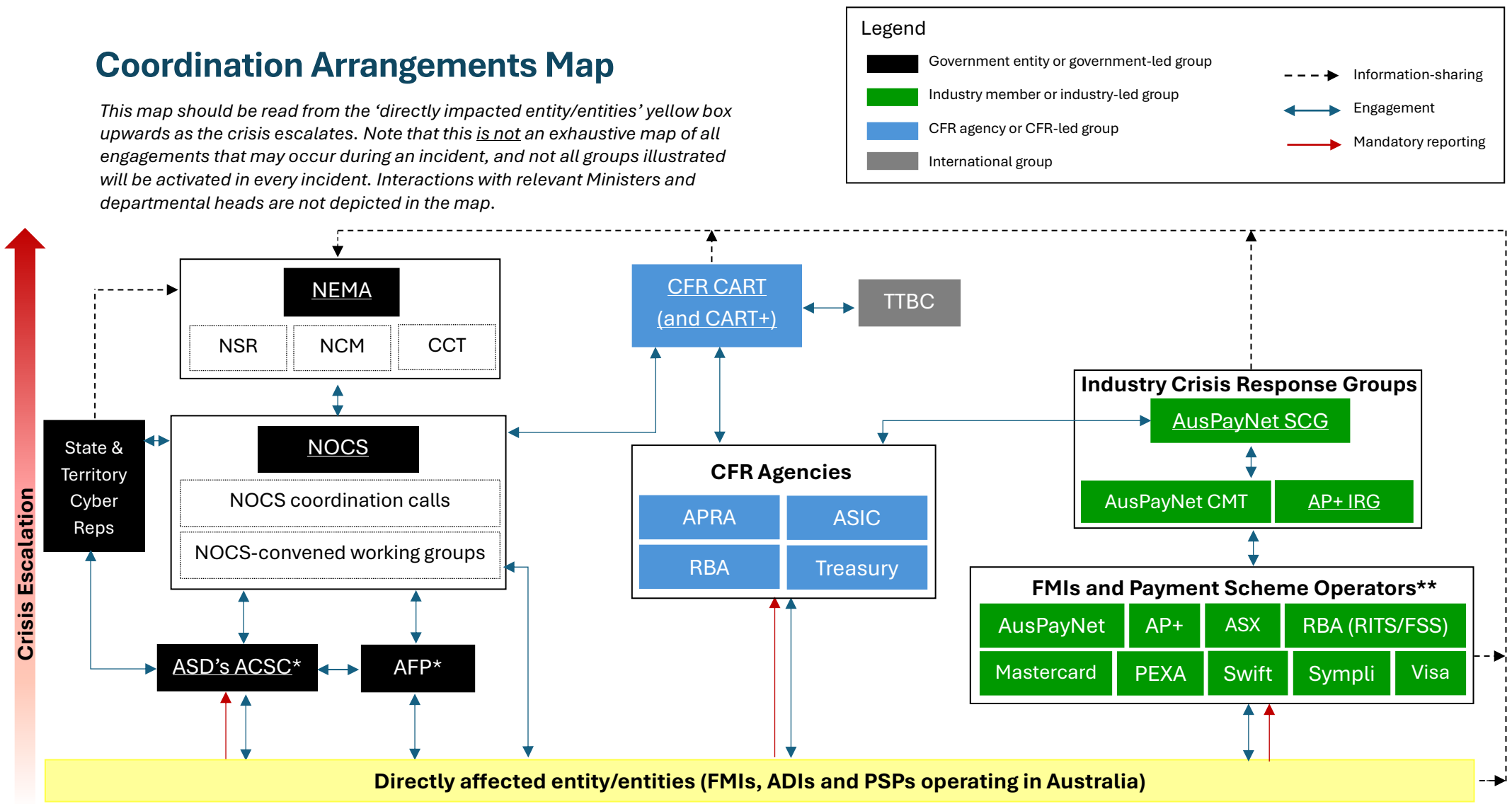
The **Response Group and Entity Summaries** provide a more detailed description of key crisis response groups.

List of Acronyms

ABA	Australian Banking Association
ACCC	Australian Competition and Consumer Commission
ADI	Authorised Deposit-taking Institution
AFP	Australian Federal Police
AGCMF	Australian Government Crisis Management Framework
AP+	Australian Payments Plus
AP+ IRG	Australian Payments Plus Incident Response Group
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASD's ACSC	ASD's Australian Cyber Security Centre
ASIC	Australian Securities and Investments Commission
ASX	Australian Securities Exchange
ATO	Australian Taxation Office
AUSCYBERPLAN	Australian Cyber Response Plan
AusPayNet	Australian Payments Network
AusPayNet CMT	Crisis Management Team defined under the AusPayNet Crisis Communications Plan
AusPayNet SCG	AusPayNet Systemic Crisis Group
CCT	The Australian Government Joint Crisis Coordination Team
CFR	Council of Financial Regulators
CFR CART	CFR Cyber Assessment and Response Team
COBA	Customer Owned Banking Association
CTIS	ASD's Cyber Threat Intelligence Sharing
FMA	Financial Markets Authority (New Zealand)
FMI	Financial Market Infrastructure
FSS	Fast Settlement Service
Home Affairs	Department of Home Affairs
NCM	National Coordination Mechanism
NEMA	National Emergency Management Agency
NOCS	National Office of Cyber Security
NPP	New Payments Platform
NSR	National Situation Room
OAIC	Office of the Australian Information Commissioner
PEXA	Property Exchange Australia Limited
PSP	Payment Service Provider
RBA	Reserve Bank of Australia
RBNZ	Reserve Bank of New Zealand
RITS	Reserve Bank Information and Transfer System
SOCI Act	*Security of Critical Infrastructure Act 2018*
TISN	Trusted Information Sharing Network
Treasury	The Commonwealth Treasury
TTBC	Trans-Tasman Council on Banking Supervision

Coordination Arrangements Map

This map should be read from the 'directly impacted entity/entities' yellow box upwards as the crisis escalates. Note that this is not an exhaustive map of all engagements that may occur during an incident, and not all groups illustrated will be activated in every incident. Interactions with relevant Ministers and departmental heads are not depicted in the map.



Threat Intelligence Sharing***

CTIS	TISN

* With the affected entity's consent, ASD's ACSC/AFP will provide incident reporting information to NOCS to support consequence management and whole-of-government coordination.
** FMIs and payment system or scheme operators may communicate updates to their members independent of formal industry crisis response groups.
*** CTIS is a government-led threat sharing group that is free to join. Other private or public threat sharing groups may be used. TISN is a government-led and free-to-join information sharing network. TISN may be used to share lessons learnt from incidents and build operational responses and contingencies to incidents.

Coordination Arrangements Map – An Example Scenario

This table sets out an example crisis scenario, responses and connection points to assist with interpreting the Coordination Arrangements Map.

Example Scenario	A bank operating in Australia experiences a major incident, resulting in a prolonged disruption to their payment operations and system-wide impacts.
Whole-of-government Cyber Security Response	The following arrangements are applicable during a **cyber security** or **cyber** incident, as defined under the SOCI Act and the AGCMF respectively, affecting the payments system: • Under the SOCI Act, if a cyber security incident has a relevant impact on a critical infrastructure asset, responsible entities of critical infrastructure assets are obligated to report critical and other cyber security incidents to ASD's ACSC. For more information and examples on how to comply with this obligation, see Notification of Cyber Security Incident reporting guidance. • Regardless of regulatory requirements, the entity is recommended to engage with NOCS for coordination of the whole-of-government response and engage with ASD's ACSC for technical assistance and AFP for cybercrime investigation purposes. As required, NOCS (together with the entity) will arrange coordination calls and working groups to respond to the incident, involving relevant government and industry entities. • With NEMA agreement, the NCM may be activated at the request of Australian Government agencies, states, territories, industry or the not-for-profit sector. If the incident requires whole-of-government coordination in response and consequence management, NOCS may convene and co-chair the NCM with NEMA. If the incident has extreme to catastrophic impacts, NEMA will lead coordination the incident response and consequence management.
CFR Response	• The entity is required to notify the relevant CFR agency/agencies. • The lead CFR agency may invoke a CFR CART meeting once the incident is triaged. CFR agencies will engage with other relevant government agencies, impacted entities and payments industry crisis response groups as required, and coordinate the response consistent with the CFR's crisis management role, recognising the respective statutory responsibilities of each CFR member agency.
Payments Industry Response	• The entity is required to report to relevant payment system or scheme operators where there are mandatory requirements to do so (e.g. certain RITS Members are required to report to the RBA's RITS Help Desk). • The relevant payment system or scheme operator may invoke an industry crisis response group(s) to manage the industry's collective response to an incident (e.g. invoke business continuity arrangements for processing payments). If the incident reaches the AusPayNet Systemic Crisis Group's threshold, AusPayNet will initiate and coordinate the payments industry's response to the crisis.

Example Scenario	A bank operating in Australia experiences a major incident, resulting in a prolonged disruption to their payment operations and system-wide impacts.
Connection Points	Organisations involved in each of the three response categories may come together as part of certain response groups, e.g.: • NOCS Coordination Calls (all categories possible) • CFR CART (regulators) or CFR CART+ (regulators and relevant government agencies) • AusPayNet SCG (industry members and relevant regulators) • NCM (all categories possible) • Threat intelligence sharing groups (all categories possible), e.g. ASD's CTIS is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity at machine speed.

Stage 1: Notification

This table describes the key reporting requirements, roles and responsibilities of entities or crisis response groups that may be involved in the Stage 1 notification phase of a payments crisis. For each stage, response groups and entities are listed in the following order: whole-of-government cyber security response arrangements (excluding CFR), CFR response, payments industry-level response.

Response Group/Entity	Roles and Responsibilities	How to Contact	Reporting Requirements
ASD's ACSC	• **Operational and technical support**: Works with all relevant entities involved in a cyber security incident, providing advice and assistance to impacted entities requesting assistance. • **Information gathering**: Collects details and technical artefacts related to the incident (actual or potential) to enable technical advice and assistance. • **Direct engagement**: Works with the affected entity to understand technical impacts and any network connectivity with other entities. • **Information handling**: Applies Limited Use provisions under the *Intelligence Services Act 2001*, ensuring information voluntarily provided is used and disclosed as required by legislation. • **Facilitates the reporting function:** Hosts ReportCyber and 'Report a cyber security incident' to facilitate	Report via 'Report a cyber security incident'. Entities may also email assist@asd.gov.au or call 1300CYBER1 (1300 292 371).	• **Early engagement with ASD's ACSC is highly recommended** for all impacted entities, regardless of incident severity and reporting requirements, to ensure appropriate technical advice and support can be provided. • **Mandatory** notification of cyber security incident to **ASD's ACSC** (via the 'Report a cyber security incident' page hosted by ASD's ACSC) for responsible entities for certain critical infrastructure assets: ○ within 12 hours of becoming aware of the incident, if the incident is having a significant impact on the availability of the asset; or ○ within 72 hours of becoming aware of the incident, if the incident is having an impact on the availability, integrity or reliability of the asset, or on the confidentiality of information about, or held by, the asset. *Note: The reporting form includes an option for responsible entities to consent to ASD's ACSC sharing the report with NOCS to support consequence management and whole-of-*

Response Group/Entity	Roles and Responsibilities	How to Contact	Reporting Requirements
	reporting to Home Affairs, NOCS and law enforcement. Certain cyber security mandatory reporting information is directly provided to Home Affairs when the entity elects to provide that information to Home Affairs.		*government coordination for nationally significant cyber security incidents.*
NOCS	• **Initial engagement**: Conducts an initial meeting with the impacted entity to understand the nature of the incident and perform an initial impact assessment for internal triaging and to inform assessment of potential consequences. • **Information handling:** Applies Limited Use provisions under the *Cyber Security Act 2024* to incident information voluntarily shared about the incident, ensuring it is used as required by legislation.	Report via 'Report a cyber security incident'.	• NOCS is not a regulator and reporting to NOCS is voluntary. • **Early notifications are strongly recommended** to allow for timely support and advice to be provided for impacted entities. Entities can request for the information to be shared with NOCS via 'Report a cyber security incident'. If NOCS becomes aware of the incident through open source information, NOCS may reach out to offer their assistance.
AFP	• **Cybercrime assessment and investigation**: Assesses the information in submitted cybercrime reports for investigation and intelligence purposes.	Report via ReportCyber.	• **Early engagement** with law enforcement is recommended to support evidence preservation, investigative opportunities and potential disruption activities. Entities can request for the information to be shared with AFP via ReportCyber.

Response Group/Entity	Roles and Responsibilities	How to Contact	Reporting Requirements
Home Affairs	• **Policy and regulatory oversight**: Responsible for policy and regulatory oversight of relevant obligations under the SOCI Act and the *Cyber Security Act 2024*, including monitoring and supporting compliance with cyber security incident reporting obligations for critical infrastructure entities. • **Ransomware and cyber extortion payment reporting:** Under the *Cyber Security Act 2024*, businesses affected by ransomware must report incident details, operational impacts, technical indicators, and any ransom demands, payments, and communications with the threat actor.	Report via Ransomware payment and cyber extortion payment reporting.	• For SOCI Act mandatory cyber security incident reporting, reports submitted to ASD's ACSC may be shared with Home Affairs, as the regulator, where the reporting entity provides consent. See reporting requirements under ASD's ACSC above for details. • **Mandatory reporting** to **Home Affairs** (via the 'Ransomware payment and cyber extortion payment reporting' page hosted by ASD's ACSC) for ransomware payment and cyber extortion payments for reporting business entities within 72 hours of the payment (or from the time the entity becomes aware a payment has been made on their behalf).
OAIC	• **Regulatory oversight:** Oversees compliance with the *Privacy Act 1988* and the Notifiable Data Breaches scheme. Receives notifications of eligible data breaches and may provide guidance, investigate incidents or take regulatory action where appropriate.	Report via Notifiable Data Breach form.	• **Mandatory reporting**: Under the Notifiable Data Breaches scheme, an affected entity must notify affected individuals and the **OAIC** of eligible data breaches. A breach is eligible where there is unauthorised access to, unauthorised disclosure of, or loss of personal information and this is likely to result in serious harm to an individual(s). See the OAIC's Quick reference guide for responding to data breaches for more information.

Response Group/Entity	Roles and Responsibilities	How to Contact	Reporting Requirements
CFR Agencies	• **Lead agency determination**: Assess the impact of the incident and liaise with relevant regulators to determine which CFR agency will lead the response based on regulatory remit. Triage the incident based on its materiality to the financial system. • **Government coordination**: Determine which other government agencies should be engaged for broader coordination. • **Communication strategy**: Decide on the approach for communicating with the impacted entity.	Clearing and settlement facilities supervised by the **RBA** and **ASIC** report via phone/email as agreed with these agencies. **APRA** regulated entities should report via this form: Report to APRA. Australian financial services (AFS) licensees and Australian credit licensees (credit licensees) report to **ASIC** via the prescribed form available in the ASIC Regulatory Portal.	• **Mandatory reporting**: A holder of an Australian Clearing and Settlement Facility Licence under Part 7.3 of *the Corporations Act 2001* who is subject to the Financial Stability Standards for Central Counterparties and/or Securities Settlement Facilities, each as determined under section 827D(1) of the *Corporations Act 2001*, have regulatory reporting requirements to the **RBA**. This includes informing the RBA in a timely manner of any events or changes to that entity's operations or circumstances that may materially impact its management of risks or ability to continue operations. • **Mandatory reporting** by APRA-regulated entities to **APRA** of relevant information security and operational risk incidents, in accordance with the notification requirements and timeframes in Prudential Standard CPS 234 and CPS 230 respectively. • **Mandatory reporting** by AFS licensees and credit licensees to **ASIC** for reportable situations. Regulatory Guide 78 *Breach reporting by AFS licensees and credit licensees* (RG 78) provides further guidance as to when (and what) licensees must report to ASIC. Entities may also have reporting obligations under ASIC's Market Integrity Rules.

Response Group/Entity	Roles and Responsibilities	How to Contact	Reporting Requirements
RITS Help Desk (RBA)	• **Operational support**: Provides continuous operational assistance to RITS Members, ensuring system availability and resolving issues promptly.	Contact via phone: 1800 659 360 or +61 2 9551 8930 or email: rits@rba.gov.au *Calls to and from the RITS Help Desk numbers are recorded.*	• **Mandatory reporting**: RITS Members must immediately report to the **RBA's RITS Help Desk** any operational problem that may impact the efficiency of their settlements across RITS. The RITS Member Incident Reporting Arrangements detail the requirements for notification and reporting to the RITS Help Desk.
FMIs and Payment Scheme Operators	• **Impact assessment**: Assess the impact of the incident on the system, scheme or facility to determine severity and potential consequences. • **Industry response activation**: Decide whether to invoke industry incident response plans and groups to ensure coordinated action.	Report as agreed in rulebook or participation agreement.	• Various contractual-based notification requirements per scheme may apply.

Incident Reporting to Government Decision Tree

Financial Institutions and Market Infrastructures

Mandatory

Cyber Security Incidents

- **ASD's ACSC and OAIC –** where there is a breach of Consumer Data Right information (see single reporting portal* for details)
- **ASD's ACSC and Home Affairs –** entities responsible for critical infrastructure assets under the SOCI Act with a cyber security incident notification obligation.**
- **Home Affairs –** reporting business entity who has made a ransomware payment (or is aware another entity has provided a ransomware entity on their behalf).
- **OAIC –** for eligible data breaches (see single reporting portal** and Quick reference guide for responding to data breaches)

Cyber Security or Operational Incidents

- **APRA** – APRA regulated entities.
- **ASIC** – ASIC regulated entities.
- **RBA** – Holders of an Australian Clearing and Settlement Facility Licence under Part 7.3 of the *Corporations Act 2001* and RITS Members.

Recommended

Cyber Incidents

- **ASD's ACSC** – recommended except in the mandatory cases mentioned on this page and in the single reporting portal.
- **NOCS.**
- **AFP** – submit a Report of Crime if a police investigation is required.

* An online list of Commonwealth legislative reporting requirements that could be triggered by a cyber security incident.

** Mandatory for responsible entities for certain critical infrastructure assets under the SOCI Act. See Notification of Cyber Security Incidents Guidance.

Stage 2: Response

This table describes the key roles and responsibilities and triggers for involvement of entities or crisis response groups that may be involved in the Stage 2 response phase to a payments crisis.

Response Group/Entity	Roles and Responsibilities	Triggers	Further Information
ASD's ACSC	• **Operational and technical support**: Works with all relevant entities involved in a cyber security incident, providing advice and assistance to impacted entities requesting assistance. ASD provides Incident Response support for the agency/organisation leading the investigation. • **Threat intelligence sharing**: Collates and disseminates cyber threat information with government and industry, such as impacts and mitigation strategies, including through ASD's CTIS. Ensures the broader sector is aware of potential threats as a result of the incident. • **Public communication support**: Assists in developing and distributing communications to inform public messaging across jurisdictions and focuses on ensuring public statements do not compromise ongoing investigations. • **National and international liaison**: Coordinates with the Australian Intelligence Community, Australian states and territories, federal law enforcement and overseas jurisdictions to support national response efforts.	• ASD's ACSC will determine the level of assistance provided depending on each incident where required or requested by the impacted entity.	• Cyber incident management arrangements for Australian governments (CIMA) • ASD's Cyber Threat Intelligence Sharing (CTIS)
NOCS	• **Coordination calls:** Engages with the impacted entity, ASD, AFP, state and territory government cyber representatives (where jurisdictional impact exists) and other relevant Australian government departments. • **Situation overview:** Coordination calls provide an overview of the incident, the current operational situation, emerging or	• NOCS is the Australian Government Coordinating Agency responsible for coordinating responses to Tier 2 and 3 cyber security incidents,	• NOCS Financial Sector Playbook • Australian Cyber Response Plan (AUSCYBERPLAN)

Response Group/Entity	Roles and Responsibilities	Triggers	Further Information
[redacted]	potential impacts, and the extent of coordinated consequence management activities required. • **Impact and consequence tracking:** Maintains a consolidated view of actual and emerging impacts across service delivery, jurisdictions, industry and community to support whole-of-government coordination and escalation decisions. • **Working groups:** Establishes coordinated response working groups where specific lines of effort are required to address impacts. These groups operate in parallel with coordination calls, with updates provided during wider coordination meetings. Further details are outlined in the NOCS Financial Sector Playbook. • **Public communications:** Supports communication to the public about the impacts of a cyber security incident, including impacts to government services and where to access assistance. Communications are developed in consultation with the impacted entity. The National Cyber Security Coordinator may make public announcements via official NOCS channels, with the entity's consent. • **Government advice and escalations:** Provides regular updates and advice to support decision-making by the National Cyber Security Coordinator and relevant senior officials. In partnership with NEMA, NOCS may convene the NCM for nationally significant incidents of severe impact/complexity.	consistent with the 4-tier model or crisis coordination under the AGCMF. As the Australian Government Coordination Agency, for Tier 1 incidents NOCS will determine its level of involvement and support depending on the severity of the incident (e.g. data breach of sensitive information, impacts to other critical infrastructure sectors, or major operational system outages).	• Australian Government Crisis Management Framework (AGCMF)
AFP	• **Evidence gathering:** Works with government, industry and international partners to collect, analyse and share evidence that supports the investigation, attribution, disruption and prosecution of cybercriminals.	• AFP involvement may be triggered where cybercrime offences impact a	• Cyber incident management arrangements for

Response Group/Entity	Roles and Responsibilities	Triggers	Further Information
[redacted]	• **Jurisdiction coordination:** Coordinates with state and territory law enforcement agencies to determine investigative ownership, establish lead agency arrangements and ensure a coordinated law enforcement response. • **Law enforcement response:** Leads and coordinates national law enforcement efforts, including through the JPC3 and Operation Aquila, to identify, investigate and disrupt cybercriminal actors and syndicates, minimise harm, and support the prosecution of offenders.	Commonwealth government entity, critical infrastructure, systems of national significance, or have the potential to cause significant harm to the Australian economy, national security, or the Australian community.	Australian governments (CIMA)
NEMA	**NEMA** • **Coordination and consequence management**: Runs the NSR and leads coordination and consequence management for Tier 4 incidents through the NCM and the CCT (see below). NEMA may also lead Tier 3 coordination at the request of NOCS, if the response requirements are beyond the coordination capacity or capability of NOCS. • **Decision support:** Provides situational reporting and advice to support senior government decision-making, including escalation, activation of national arrangements, and cross-sector coordination as required. **CCT** • **Australian government response coordination:** Supports coordination of Australian Government actions, in line with the strategic intent set by the NCM. It may bring together representatives from Australian Government agencies, as well as other key stakeholders. **NSR** • **Incident monitoring:** Conducts 24/7 monitoring of all hazards via the NSR Operations Section, to provide ongoing	• The NCM may be activated for any incident tier under the AGCMF, at the request of a relevant government agency or industry entity and with NEMA agreement where incidents have significant sectoral or multi-jurisdictional impacts requiring enhanced Commonwealth coordination, but do not warrant whole-of-government crisis activation.	• Australian Government Crisis Management Framework (AGCMF) • Australian Government Joint Crisis Coordination Team (CCT) • National Situation Room (NSR) • National Coordination Mechanism (NCM)

Response Group/Entity	Roles and Responsibilities	Triggers	Further Information
[redacted]	situational awareness of incidents including current and potential impacts. Stakeholders use information provided for decision support before, during and after crises. **NCM** • **Crisis stabilisation:** Facilitates national coordination and decision-making by sharing information, defining problems and finding solutions to stabilise crises quickly. • **Collaborative forum:** Enables stakeholders to coordinate, communicate and collaborate in response to the consequences of the crisis. • **Invitee determination:** Determines invitees based on the nature of each crisis. Organisations with equity in the crisis may be invited, including stakeholders from Australian, state, territory and local governments, as well as industry and not-for-profit members of impacted sectors.		
CFR CART	• **Supervisory and emergency activities**: Decides on the need and scope of additional supervisory engagement and emergency response (e.g. resolution, liquidity support). • **Public communication**: Coordinates financial stability messaging, cross-government communication and triggers other emergency response mechanisms. Public communications are coordinated by NOCS during a Tier 2 or Tier 3 cyber security crisis, or by NEMA during a Tier 4 crisis under the AGCMF. • **Government coordination**: Coordinates with relevant government agencies via the CFR CART+ if required. • **Cross-border coordination**: Coordinates with the TTBC agencies when incidents may impact regulated entities with branches in New Zealand.	• The CFR CART may be used to share information among CFR agencies about cyber security and operational incidents at a financial institution or FMI where there is a potential impact to financial stability. • CFR CART's response is determined by factors such as the impacts to the entity, financial system and public.	• Memorandum of Understanding on Crisis Management between the members of the CFR

Response Group/Entity	Roles and Responsibilities	Triggers	Further Information
RBA (operational and liquidity response including RITS Help Desk)	• **Central point of response:** Acts as the central point of contact and response for incidents that disrupt the normal settlement operation of RITS Members' payment obligations across RITS or the FSS. • **Decisions regarding settlement continuity:** Decides whether to invoke fallback arrangements (together with other payment system or scheme operators as required) and vary RITS session times. • **Support system liquidity:** Engages in domestic market operations as required. • **Manage communication with RITS Members and relevant operators:** Notifies contacts of an incident, provides status updates as required and notification that the issue has been rectified. - • **Operational support:** Provides operational support to RITS Members requiring assistance in their response to the incident.	• An incident that disrupts the efficient settlement of RITS Members' obligations across RITS and/or the FSS.	
AusPayNet SCG	• **Industry-wide coordination**: Coordinates the payments industry's response including facilitating the coordinated invocation of resilience solutions and aligning actions across stakeholders. • **Centralised information management:** Provides centralised information and communications through briefings to SCG and industry members and key stakeholders. • **Dynamic scope adjustment**: Monitors and adjusts the coordination scope as crisis severity changes (e.g. more entities or payment rails impacted).	• A large proportion of customers impacted across one or more major institutions. • No access to critical and non-substitutable payment systems (e.g. NPP, cards, direct entry). • The recovery timeframe is extended or unknown (multi-day disruption).	

Response Group/Entity	Roles and Responsibilities	Triggers	Further Information
AP+ IRG	• **Incident declaration and instructions**: Declares incidents and issues instructions or directions to service providers and member participants to implement emergency operational activities. • **Coordination of communications**: Coordinates communications and activities with members and service providers to ensure alignment and timely response. • **Collaboration with AP+ crisis management team**: Works closely with the AP+ internal crisis management team, which liaises with external stakeholders including government bodies, regulators, and the general public.	• Each scheme (i.e. NPP, BPAY, eftpos) has its own criteria set out in the relevant incident management framework, based on the incident scenario and severity level.	• AP+ Scheme Rules (section 15)

Stage 3: Recovery

This table describes the key roles and responsibilities, including post-crisis activities, of entities or crisis response groups that may be involved in the Stage 3 recovery phase of a payments crisis. As not all groups may be activated in a crisis, not all listed activities may take place.

Response Group/Entity	Roles and Responsibilities
ASD's ACSC	• **ASD service**: Provides services that can be engaged to assist entities in understanding requirements and methods to harden their systems, including information from ASD's ACSC technical guidance and information obtained during the investigation of the incident.
NOCS	• **Post-incident evaluation:** The National Cyber Security Coordinator leads post-incident evaluations for Tier 3 or 4 cyber security incidents to strengthen national crisis management plans and preparedness. The outcomes of the evaluation are reported to and distributed across government, to ensure identified lessons are integrated into consequence management processes and continuous improvement.
Home Affairs	• **Post-incident review**: The Cyber Incident Review Board (the Board) may review significant cyber security incidents after response activities have concluded. It identifies lessons learned and provides recommendations to government and industry to help prevent, respond to and minimise the impact of similar incidents and uplift Australia's cyber resilience in the future. The Board may cause a review to be undertaken on written referral by either the Minister for Cyber Security, the National Cyber Security Coordinator, an impacted entity or a member of the Board. Home Affairs supports the Board as its Secretariat and governance function.
CFR CART	• **Post-incident review:** Gathers all participants' feedback to determine what worked well, gaps, areas for improvement and/or further regulatory action required.
RBA (operational and liquidity response including RITS Help Desk)	• **Incident closure confirmation:** Confirms issue is rectified to RITS Members. • **Post-crisis review:** Receives incident report and lessons learnt from relevant entities and issues an incident report where relevant.

Response Group/Entity	Roles and Responsibilities
AusPayNet SCG	• **Recovery oversight**: Coordinates rollback of temporary solutions implemented during the crisis. • **Crisis closure communication**: Confirms and communicates the official 'crisis over' status to stakeholders. • **Recovery taskforce**: Stands up a recovery taskforce to coordinate the 'clean-up' activities post-crisis if required (e.g. reconciliation of impacted payments). • **Post-crisis review**: Conducts reviews to assess the effectiveness of the AusPayNet Systemic Crisis Playbook and identify improvements.
AP+ IRG	• **Remediation planning**: Identifies and communicates effective remediation plans and actions to members. • **Post-incident review**: Conducts post-incident reviews, tracks remediation activities through to completion, and proposes recommendations for amendments to the incident management framework where applicable.

Response Group and Entity Summaries

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)

Purpose during a crisis: ASD's ACSC is the Australian Government's lead on national cyber security operational matters, providing technical advice and assistance to impacted entities.

Chair/Led by: ASD's ACSC.

Types of members: ASD's ACSC works directly with the impacted entity and if required other impacted entities.

Crisis notification: Entities are encouraged to inform ASD's ACSC of a cyber security incident as soon as it is identified regardless of the severity of the incident. Organisations can report an incident via 'Report a cyber security incident' (cyber.gov.au) or email assist@asd.gov.au or call 1300CYBER1 (1300 292 371). See Stage 1 above for details on reporting requirements.

Decisions in a crisis: Provision of operational and technical advice and assistance directly to impacted entities.

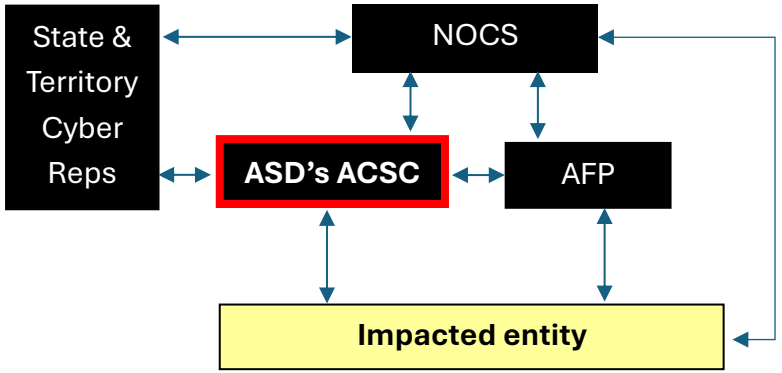
Communications: Facilitates information sharing between entities and sharing technical artefacts and relevant incident information with law enforcement and/or other government agencies, with permission from the impacted entity. Information sharing is conducted in line with the Limited Use provisions established under the *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024*.

The ASD's Cyber Threat Intelligence Sharing (CTIS) is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity at machine speed. ASD's ACSC is not responsible for the distribution of external public communications but supports the development of public messaging in consultation with NOCS.

Roles post crisis: ASD's ACSC offers post-incident services, including programs for critical infrastructure such as CI-UP, which help entities strengthen resilience against future cyber security incidents.

Triggers to invoke: ASD's ACSC triages cyber security incident reports and assesses other incident notifications via threat intelligence sharing from partners and global cyber threat monitoring. ASD'S ACSC will arrange a meeting with the impacted entity when required, or on request.

Mini map (the group or entity that is the focus of this page is outlined in red):



National Office of Cyber Security (NOCS)

Purpose during a crisis: Coordinates consequence management activities across the whole-of-government in response to nationally significant cyber security incidents impacting Australia.

Chair/Led by: National Cyber Security Coordinator.

Types of members: NOCS coordination calls and NOCS-convened working groups may include relevant government agencies and members of the payments industry.

Crisis notification: While there is no mandatory obligation to notify NOCS of an incident, notification is highly encouraged to allow the provision of early support, advice, and general awareness in the case the incident becomes more severe. Notifications can come directly from impacted entities or via 'Report a cyber security incident' when the impacted entity has provided their consent.

Decisions in a crisis: Decision-making in a crisis is always made in consultation with the impacted entity. These may include the convening of coordination calls, NOCS-convened working groups, communications and information sharing.

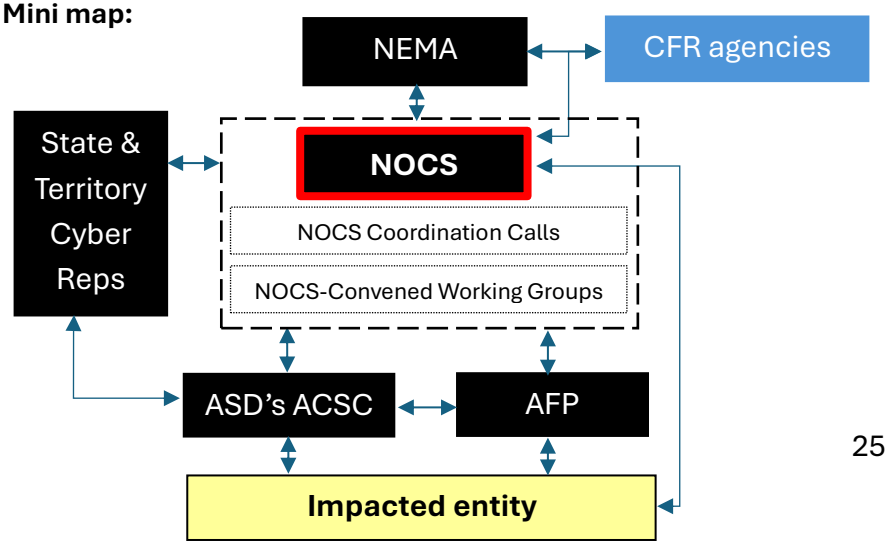
Communications: Engages with the impacted entity directly, information-sharing with other state and territory and Australian government agencies, public announcements via the Coordinator's official social media page (with the consent of the entity). Information-sharing is conducted in line with the Limited Use provisions established under Part 4 of *the Cyber Security Act 2024*. NEMA will lead public communications in a Tier 4 crisis with contributions from NOCS and other agencies.

Roles post crisis: NOCS conducts quarterly post-incident evaluations of the Australian Government's response to cyber security incidents. Within 12 months of Tier 3 crisis coordination no longer being required for cyber security incidents, NOCS as the Australian Government Coordination Agency will conduct a whole-of-Australian-Government evaluation with outcomes shared across the Australian Government and relevant stakeholders as soon as practical. A comprehensive review is essential to assess outcomes, identify improvements and enhance future cyber security response and resilience.

Playbook/ToR: Sector-specific playbooks are available on the NOCS website, for each critical infrastructure sector.

Triggers to invoke: Engagement with NOCS is based on incident impact, such as a sensitive data breach, disruption to other critical infrastructure sectors, or major operational system outages. Detailed thresholds are outlined in the publicly available AUSCYBERPLAN.

Mini map:



National Coordination Mechanism (NCM)

Purpose during a crisis: Facilitates national coordination and supports decision making by sharing information, solving problems and finding solutions to stabilise crises quickly.

Chair/Led by: NEMA. Other relevant Australian Government agencies, such as NOCS may co-chair the NCM.

Types of members: No permanent ongoing membership of the NCM. Invitees are determined on a per-incident basis. This may include relevant stakeholders across government, industry and not-for-profit sectors. An Australian Government Crisis Coordination Team (CCT) can be established by NEMA to support coordination of Australian Government actions, in line with the strategic intent set by the NCM. A specialised NCM, the NCM-AUSGOV, may also be convened which is restricted to Australian Government officials.

Crisis notification: Notifications of cyber security incidents and outages are typically received from NOCS or the National Situation Room 24/7 watch floor.

Decisions in a crisis: The NCM is a platform for collaboration and collective decision-making. This includes actions to coordinate lines of effort to stabilise the crisis quickly and mitigate crisis impacts, as well as managing public messaging.

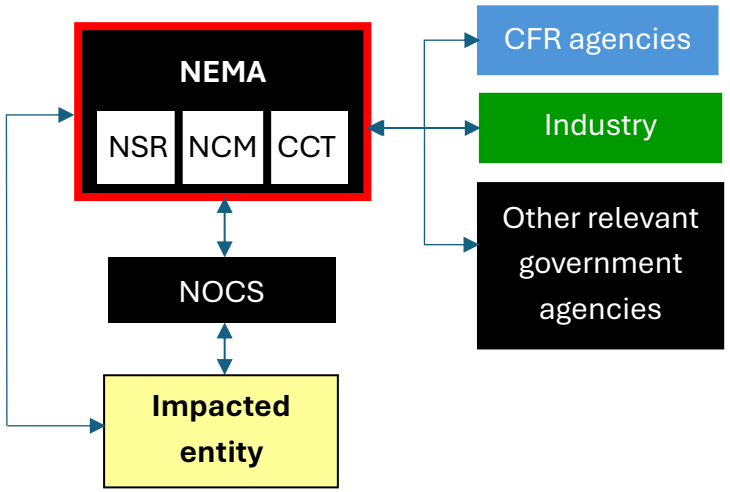
Communications: The information shared in NCMs is dependent on each crisis and may be sent across a wide network of stakeholders to provide decentralised situational awareness. NEMA contributes to communications where it is supporting another agency's response, or will lead public crisis communications for Tier 4 incidents as defined in the AGCMF.

Roles post crisis: Where NEMA is the Australian Government Coordinating Agency of a significant crisis, NEMA is responsible for conducting a whole-of-Australian-Government evaluation within 12 months of Tier 3 or Tier 4 crisis coordination no longer being required.

Playbook/ToR: The AGCMF outlines how the NCM is used by the Australian Government during a crisis. A NOCS-NEMA NCM protocol covers arrangements between the two agencies for coordination during high-tier cyber security incidents.

Triggers to invoke: The NCM can be activated with NEMA agreement for any incident tier under the AGCMF, as requested by an agency. For Tier 4 incidents, the NCM is the peak crisis coordination mechanism. The triggers include circumstances where an incident impacts multiple jurisdictions or sectors, multiple crises are occurring concurrently, or there is community expectation for the Australian Government to play a national leadership role.

Mini map:



CFR Cyber Assessment and Response Team (CART)

Purpose during a crisis: Facilitates collaboration among member agencies and coordinates regulatory responses to cyber security and operational incidents at a financial institution or FMI that could pose systemic risk or an impact to financial stability.

Chair/Led by: Notified CFR agency, or as agreed by CART.

Types of members: CFR agencies (APRA, ASIC, RBA and Treasury)

As needed, CART+ members which includes other Australian government agencies could be involved. CFR CART may also engage with TTBC agencies including RBNZ, FMA and Treasury of New Zealand.

Crisis notification: Notification by affected entity (mandatory, e.g. APRA CPS 234 and CPS 230, or voluntary), supervisory engagements, TTBC, NCM or media notification.

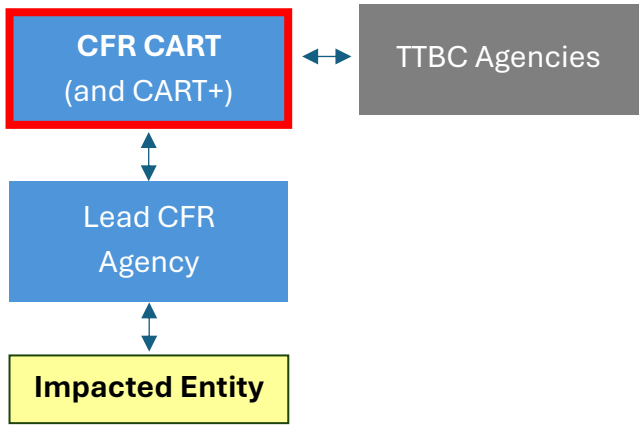
Decisions in a crisis: Decides leading CFR agency; triages crisis severity; coordinates communications with the impacted entity and decides supervisory response; coordinates messaging to other government agencies about response; escalates to whole-of-government response (NOCS, NCM) if multiple entities affected and there is risk to financial stability.

Communications: External public communications to industry participants and general public, if required.

Roles post crisis: Post-incident review if needed as determined by CART – includes all stakeholders involved in the response and aims to identify wins, gaps and areas for improvement.

Triggers to invoke: The CFR CART may be used to share information among CFR agencies about cyber security and operational incidents at a financial institution or FMI where there is a potential impact to financial stability.

Mini map:



AusPayNet Systemic Crisis Group (SCG)

Purpose during a crisis: Coordinate the payments industry's response to a systemic crisis including centralised information management and facilitating the coordinated invocation of resilience solutions across participants.

Chair/Lead by: AusPayNet.

Types of members: Major banks, regulators, FMIs, technology providers and other payment system participants as required.

Crisis notifications: AusPayNet can be notified of a disruption via direct contact from the impacted organisation, other participants in the payments system, regulators or FMIs.

Decisions in a crisis: Activation of the SCG; facilitates discussion and decisions on what resilience solutions to activate and in what sequence; manages the rollback of resilience solutions; and confirms when the crisis is resolved.

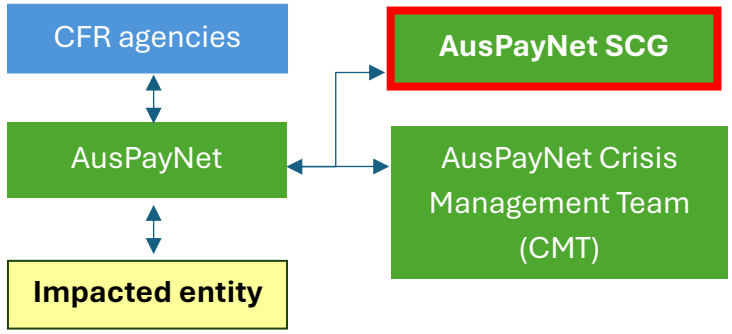
Communications: Issues approved and aligned factual updates to SCG and industry members and key stakeholders to support coordinated industry situational awareness and communications. If required, ABA and COBA will be briefed as SCG observers to support their own communications towards their members.

Roles post crisis: Leading the evaluation of the SCG response effectiveness and identifying improvements.

Triggers to invoke:

- Member Incident Plan: Smaller-scale incident (e.g. impacting a single member), but with potential for contagion, longer recovery horizon and regulatory/media interest.
- Crisis Communications Plan: More serious incident affecting multiple members, with potential for multi-day recovery and requiring industry coordination to prevent a crisis.
- Systemic Crisis Group: A large proportion of customers across one or more major financial institutions are impacted with no access to critical payment systems and extended or unknown recovery timeframes.

Mini map:



AP+ Incident Response Group (IRG)

Purpose during a crisis: Manages incidents, outages and disabling events impacting AP+ schemes (NPP, BPAY and eftpos). The IRG is also responsible for determining and communicating actions and remediation plans to minimise impact of the incident to members.

Chair/Lead by: AP+.

Types of members: Committee members of the individual schemes including financial institutions, retailers, payments service providers, gateways and critical third parties.

Crisis notifications: AP+ conducts internal monitoring for disruptions and may also be notified via service providers or scheme participants via email or phone call.

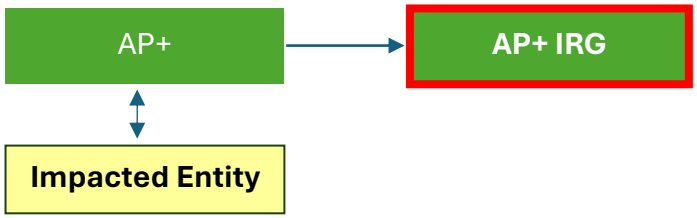
Decisions in a crisis: Declaration of incidents; issues directions to service providers and member participants to implement emergency operational activities.

Communications: Shares information only with its members and the internal AP+ Crisis Management Team. The AP+ Crisis Management Team may notify other parties (Home Affairs, RBA, AusPayNet, regulators and the public) as required.

Roles post crisis: Responsible for undertaking post incident review; reviewing any related response plans to incorporate lessons learnt; tracking remediation activities through to completion; and where applicable to a specific scheme, propose recommendations for amendments to the incident management framework.

Triggers to invoke: Each scheme's IRG applies its own criteria based on the specific incident scenario and severity level set out in each scheme's incident management frameworks.

Mini map:



Appendix A: Key Plans and Playbooks

Australian Government Crisis Management Framework

The AGCMF is the Australian Government's capstone policy framing Australia's national crisis management arrangements.

Available at: Australian Government Crisis Management Framework (AGCMF).

Australian Cyber Response Plan

The AUSCYBERPLAN outlines the Australian Government's cyber security incident response coordination arrangements.

Available at: Australian Cyber Response Plan.

Cyber Incident Management Arrangements

The CIMA for Australian governments provide a basis for an Australian government's cooperation on responses to national cyber security incidents.

Available at: Cyber Incident Management Arrangements.

NOCS Financial Sector Playbook

The Financial Sector Playbook is a high-level guide for how NOCS will coordinate the national response and consequence management activities for a cyber security incident impacting an entity in the financial sector.

Available at: Financial Sector Playbook.