G7 Cyber Expert Group: Reconnection Framework Best Practice

With the rise in significant cyber incidents in recent years, organisations are increasingly facing the challenge of addressing the "reconnection question" – whether and when to reconnect with another organisation that has been quarantined following an incident impacting their integrity.

Reconnection is the process of restoring technical access and integration to an organisation that has been technically quarantined after suffering a material cyber incident. This includes a phased resumption of business operations, beginning with the technical reconnection of stakeholders and entities to the organisation. Within this context, it is important that the financial sector has a consistent approach to reconnection.

This G7 Cyber Experts Group (CEG) paper outlines reconnection best practice to support jurisdictions and institutions.[1]

The primary focus is to provide sector-level guidance that may support jurisdictions and their institutions therein in developing their own reconnection frameworks, while promoting high-level alignment across jurisdictions and reducing the risk that inconsistencies in the contents and approach of differing reconnection frameworks could unintentionally exacerbate impacts on the sector. This paper is in turn expected to provide guidance to firms on the wider incident management processes surrounding reconnection. In this paper, 'compromised organisation' refers to the organisation technically quarantined by a cyber incident and 'client organisation' refers to the organisation affected by the compromised organisation, who is deciding whether to reconnect.

The sections below provide guidance and structural themes that a jurisdiction or organisation should consider when forming a reconnection framework. Find more detail in subsequent sections.

Element 1: Purpose

Element 2: Principles

Element 3: Phased activity

Element 4: Governance & Communication

[1] The term 'institutions' encompasses firms, authorities and third parties, and may be used interchangeably with 'organisation'. Though the guidance is focused on the sector, it can be levered by third parties.

Element 1: Purpose

Set out reconnection guidance purpose and how it should be used.

Applicability: This guidance can be used at an institution-level, sector-level, or both. A firm's reconnection policy, which will incorporate risk appetite and business-specific considerations, may differ from one adopted at a sectoral, market, or national level. Its use will vary based on the size, resources, and maturity of the institutions or sectors applying it, offering flexibility to enhance its relevance and applicability.

For those with existing reconnection frameworks, this paper can offer supplementary guidance. Additionally, for resource-constrained institutions seeking to develop a reconnection framework, it can provide high-level support in developing that approach. While not intended as a step-by-step manual, this guidance offers a high-level overview of key considerations to assist in the framework development process.

Scope: This paper is intended as guidance rather than a prescriptive approach to developing a reconnection framework. The guidance can be adaptable to support institutions and sectors of varying complexities and maturities including those that are developing or enhancing existing frameworks. Framing it broadly allows for flexibility in applying the approach to a diverse range of reconnection scenarios and ensuring it can be tailored to the specific needs of different institutions, markets, and jurisdictions.

Value: The purpose of existing reconnection frameworks is to provide advice on best practice to aid the process of safely reconnecting.[2] By utilising the best practice provided in this guidance, jurisdictions and institutions will be supported in developing their own approach to reconnection, one that suits their own individual needs and requirements. The implementation of a reconnection framework and its supporting processes, prior to an incident necessitating reconnection, will enable future reconnection engagements to be better streamlined, while also providing jurisdictions with a coherent conceptual approach and terminology to minimise the risk that divergences could contribute to impacts at a sector-level.

[2] Frameworks such as SIFMA and CMORG (both private sector entities). The UK's Cross Market Operational Resilience Group (CMORG) developed the System Integrity Reconnection Framework and the US's Securities Industry and Financial Markets Association (SIFMA) developed a reconnection framework for Remediating Cyber Events Impacting the Financial Ecosystem.

Structure: A reconnection framework should provide compromised organisations guidance on how to address the steps required leading up to a reconnection decision by key stakeholders, including client organisations. Element 3: 'Phased Activity' provides a structure representative of existing best practice. These steps should outline expectations for how the compromised organisation will assess the impacts of the incident, how remediation activities can be implemented, and how to provide assurance to the market. These steps will support the decision of client organisations to reconnect to the compromised organisation, ultimately helping advance the wider incident management process and eventual business resumption.

Outcome: A reconnection framework should clearly define what the compromised organisation wants to achieve and/or inform, including whether the framework is focused on the technical/cyber risk elements of the reconnection process in isolation, or if it also encompasses business risk and resumption activities. The existing guidance that was reviewed in support of this paper focused on the technical/cyber risks of the reconnection decision process, enabling client organisations to reach a technical recommendation on reconnection that can then inform wider business and operational considerations.

Engagement and Response: The purpose should provide a high-level overview of where and how the framework could possibly support sector response collaboration and information sharing. Engagement and response collaboration are important components of the reconnection process, both between the compromised organisation and its key stakeholders, as well as those impacted more widely across the sector. While bilateral engagement remains an important part of reconnection, collaborative sector response is crucial in supporting assurance and attestation with minimal delay.

Element 2: Principles

Provide foundational principles that support consistency and clarity throughout the reconnection process.

Cultural considerations around reconnection: Cyber security is a common and shared concern for all stakeholders and should be approached as a cooperative rather than competitive endeavour. It is important to foster a culture of non-judgment, especially as no organisation is immune to cyber-attacks or incidents. The decision to reconnect should

ideally be collaborative between the compromised organisation and client firm(s) (See Element 4: 'Governance & Communication', which highlights the importance of the process being a two-way dialogue).

Trust, transparency and open communication: The effectiveness of a principles-based approach in reconnection processes hinges on fostering trust, open communication, and transparency among stakeholders. These interrelated elements create an environment conducive to effective collaboration, leading to more efficient engagement and decision-making in support of recovery. To establish and maintain trust, stakeholders should consistently demonstrate reliability and stability throughout the reconnection process, building upon existing relationships. Transparency, although sometimes challenging during cyber incidents due to legal constraints, is crucial for defining accountabilities, developing shared situational awareness, and informing mitigation activities. It builds confidence and enables informed decision-making, thereby enhancing the overall reconnection process. Open communication, particularly from client organisations about their specific assurance needs from the outset of an incident, further strengthens this foundation. By prioritising these principles, stakeholders can create a dynamic that supports a trusted, open, and efficient reconnection process, ultimately leading to more effective outcomes in challenging situations.

Structured and consistent processes: Utilising a consistent approach and supporting processes ensures that stakeholders on all sides have a shared high-level understanding of how the situation is being managed. By adhering to a consistent approach, the sector can apply the reconnection framework in a wide range of incidents where cyber integrity impacts have led to an organisation becoming technically quarantined in part or full.

Reputable assurance: It is recommended that the compromised organisation engages with a reputable and independent third-party provider (usually a cyber response company or vendor) that has the technical background and experience to support their assurance efforts. By working with trusted experts, the compromised organisation can provide credible assurance to stakeholders while restoring confidence and contributing to the process of a smooth resumption of business.

Beyond the third-party provider, it is also helpful to understand a client organisation's criteria for what 'good' assurance encompasses. This may include, among other things, demonstrating that the necessary technical and procedural controls are in place, that the

root cause of the incident has been effectively addressed, and that appropriate measures have been taken to prevent future incidents. This can aid clear communication and quicken the assurance process.

Record keeping: Actions performed throughout an investigation during the incident and while reconnecting should be recorded, and the integrity and provenance of the records must be preserved. This ensures that evidence remains forensically sound and reliable for analysis and legal purposes, and generally allows for less opportunity for misunderstanding. Incident data should also be collected, as this is critical to understanding what occurred during the incident and for conducting effective recovery activities.

Overall cyber and operational resilience can be strengthened from the lessons learned following an incident and reconnection process. Records of communications and decision making are effective foundations to learn and improve future reconnection processes. It is important to maintain awareness of potential legal constraints related to the use and sharing of such information and to work within legal and regulatory frameworks to maximise learning and improvement while respecting necessary confidentiality.

Element 3: Phased Activity

Break the reconnection process into phases of activity to establish clear steps to incident assessment, remediation, assurance, reconnection, and recovery.

Phased approach: A phased approach provides organisations and the sector more widely with a structured, consistent, and incremental model for progressing through a reconnection process. These phases also help to facilitate efficient and effective communications between the compromised organisation and firms that have disconnected, both at an industry level and in bilateral engagements, to potentially reduce time to recover. The details captured in these phases are not intended to be comprehensive and may not be applicable in all situations – stakeholders should use them as a baseline to develop a more technical and detailed approach based on the specifics of the scenario.

Manageable components: Existing frameworks, like those developed through CMORG and SIFMA/FSSCC, use phased activity to break the broader reconnection process into more discrete and manageable components, each with their own specific (and scalable)

thresholds around assurance. These can be used to structure bilateral engagements with the compromised organisation, as well as through a 'many-to-one' sector response information sharing process.

Sequential phases: This paper divides the activity involved in the reconnection process into four core phases and one subsequent phase: (i) Assess, (ii) Remediate, (iii) Assure, (iv) Reconnect, and (v) Recover (See 'Figure 1' for a visual representation of the sequential phases).

The phases should typically be sequential to provide a logical step-through process, i.e. Phase 1 'Assess' is a necessary activity before Phase 2 'Remediate' can begin. However, depending on the scenario it may be appropriate for some activities to happen in parallel, where a subsequent phase can be initiated before the previous is fully closed out – this is particularly true in existing reconnection frameworks of the Assure and Reconnect phases, which are initiated in a feedback loop. Moreover, certain prerequisites must be met before the reconnection phase can begin. It should be noted that the execution of Phase 1 'Assess' is based on the premise of prior preparation.

Gateway outcomes: It is best practice in existing frameworks for each phase to have a gateway 'outcome', set at a principles-based level, that needs to be achieved before it can be deemed to be completed. This ensures stakeholders on all sides are working towards a common high-level position. Client stakeholders can use the guidance in the framework to stipulate what specific assurance they would need to see before the next phase can be progressed to.

Existing best practice: As noted above, existing frameworks commonly feature the following 'Core phases': (i) Assess, (ii) Remediate, (iii) Assure and (iv) Reconnect. The 'Subsequent phase', (v) Recover, is also included in these frameworks and is captured below for visibility. However, the recovery phase is out of the scope in the context of reconnection as a technical process and is more focused on broader business resumption. Existing frameworks also commonly feature outcome statements to be achieved between each phase.

Core phases: Effective frameworks usually include some variation of the following phases.

(i) Assess: The compromised organisation will assess the overall impact from the incident. This may include financial, reputational, and operational (including data loss and third-party risk) exposures. Root cause analysis is also part of effective incident and problem management. This process ensures that corrective actions are targeted and effective, which is crucial for providing reliable assurance to stakeholders. Identifying the tactic, technique and procedures (TTP) of initial infection provides regulators and sector partners confidence about potential future impacts and assurance regarding containment.

- Outcome: The compromised organisation has identified the type and extent of the attack and implemented its incident response playbooks. They have sufficient understanding of (i) root cause of the attack, to limit further impacts and (ii) impacts to operations, technology, markets, customers, and supply chain to facilitate remediation.

(ii) Remediate: The compromised firm will need to remediate the impacts uncovered in the 'Assess' phase to minimise further damage, limit any further contagion, repair systems and prepare for business resumption. Remediation also minimises the potential for reoccurrence of the initial intrusion and informs any 'lessons learned' activity and post-incident reporting. Once the impacts of the incident are remediated, the compromised organisation can assure clients it is safe to reconnect.

- Outcome: The compromised organisation has restored affected systems to a known and trusted state that is appropriately protected and can evidence or demonstrate the integrity of remediated systems, libraries, reference data, hardware and other components as required.

(iii) Assure: Though not always required, client firms can require an attestation from the individual accountable for security and/or operations at the compromised firm, including an investigation from a trusted third-party cyber security firm, as assurance before they consider a reconnection decision. For many larger firms with extensive compliance and regulatory requirements, there may be a requirement that the attestation is provided by a reputable cyber security vendor to ensure quality of investigation and assurance.

The attestation should include comprehensive information demonstrating that industry-accepted remediation steps have been taken. This could encompass a) a detailed root cause; b) evidence of successful containment measures; c) confirmation of eradication of the threat; d) proof of recovery of key systems and datastores to pre-infection resilience;

e) detailed description of updated backup and recovery plans and capabilities; f) documented testing results verifying the effectiveness of above measures; g) outline of lessons learned and improvements made to prevent similar incidents in the future; and h) assurance of ongoing monitoring and incident response readiness. These steps may need to be progressed in parallel during forthcoming recovery phases and may not be completed before an attestation is provided; institutions may need to consider reconnection decisions before these activities are fully closed out.

Before agreeing to reconnect with a compromised organisation, its clients or partners may outline their own organisational-specific security or assurance requirements. This could include specific information about the incident, proof of certain security measures being implemented, or other forms of verification that it is safe to resume normal interactions. During the attestation process, it would be beneficial for firms to assess and note the sustainability of their contingency plans. The existence of robust, longer term contingency measures or viable arrangements for customers may alleviate the pressure to hastily connect or rush due diligence, allowing for a more thorough and measured approach to the reconnection process, particularly in cases of protracted events.

Overall, a formal attestation should be considered good practice where feasible and subject to the specifics of the scenario.

- Outcome: The compromised organisation has provided sufficient assurance that it is ready to be reconnected to and to resume normal operations. Typically, though not always, this will be reached through the provision of an attestation to client stakeholders, ideally signed by an individual accountable for security and responsible for reconnection within the compromised organisation.

(iv) Reconnect: Reconnection occurs when firms are sufficiently assured of the safety of systems and networks, and they decide to reconnect to the compromised organisation. Varying forms of assurance may be required through the reconnection process (see the 'feedback loop' between 'Assure' and 'Reconnect' in 'Figure 1'). Enhanced monitoring will occur as reconnection is attempted.

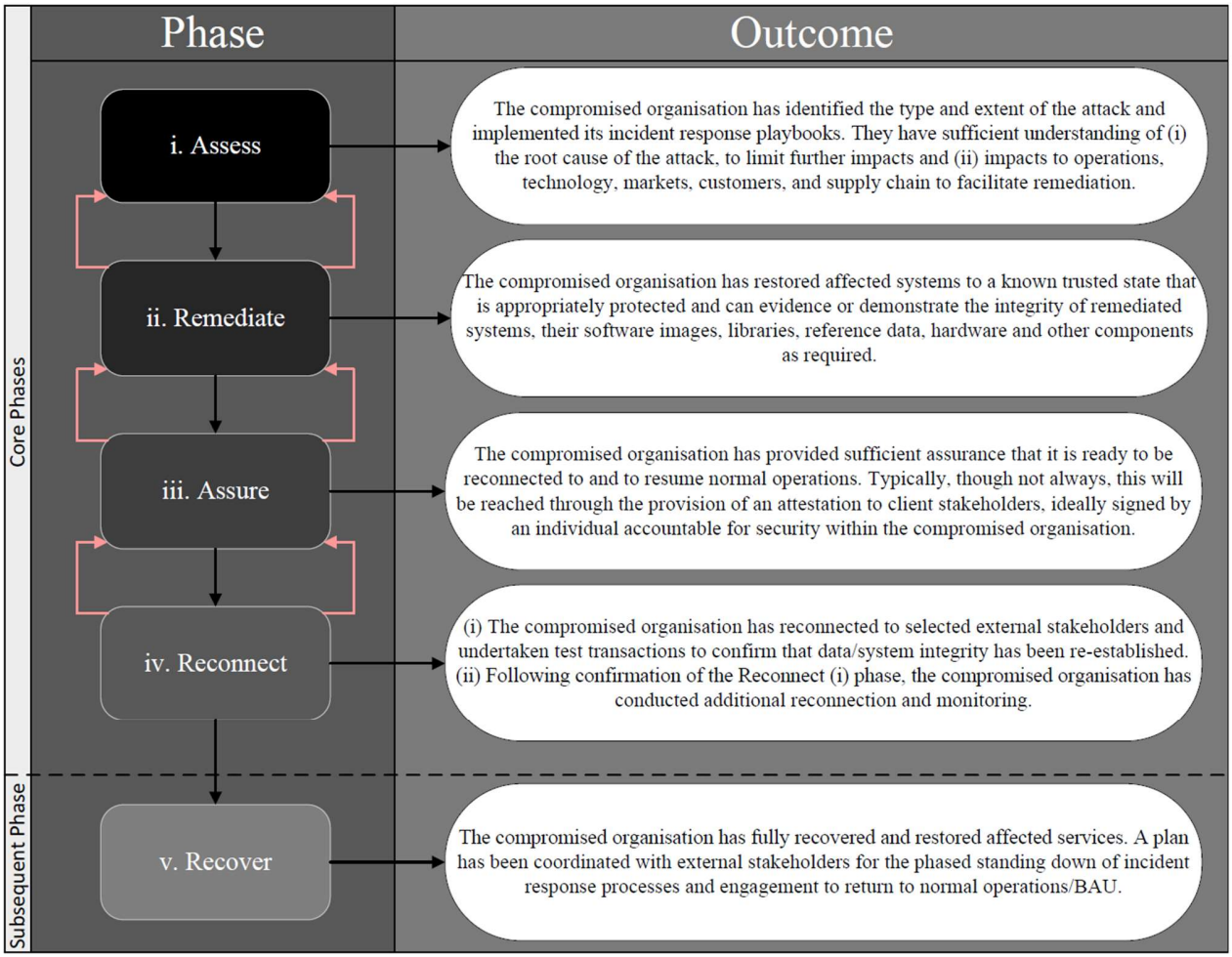
- Outcome: (i) The compromised organisation has reconnected to selected external stakeholders and undertaken test transactions to confirm that data/system integrity has been re-established. (ii) Following confirmation of the Reconnect (i) phase, the compromised organisation has conducted additional reconnection and monitoring.

Subsequent phase: Some frameworks may also want to consider business recovery and resumption; however, this is not necessarily specific to the technical elements of the reconnection process.

(v) Recover: Recovery occurs when client firms have reconnected and resumed services as usual. All previous phases will have occurred before this point.

- Outcome: The compromised organisation has fully recovered and restored affected services. A plan has been coordinated with external stakeholders for the phased standing down of incident response processes and engagement to return to normal operations/business as usual.

Figure 1: Phases commonly used in existing reconnection frameworks [3]



[3] This diagram was developed from the existing CMORG and SIFMA frameworks; however, it features minor adjustments to reflect G7 authorities and industry reflections of recent incidents.

Element 4: Governance & Communication

Ensure clear communication, both on a bilateral basis between a compromised organisation and its clients and more broadly as part of any sector-wide engagements, and support accountability throughout the reconnection process.

Effective communication and governance are critical for facilitating an effective reconnection process, particularly when addressing complex disconnection scenarios. This section outlines key governance components and best practice to support organisations in managing reconnection efforts.

Communication: As touched on in Element 2: 'Principles', regular and transparent communication is essential during reconnection efforts to foster trust and align actions across stakeholders. Impacted organisations, specifically the compromised organisation but also client organisations, where relevant, should:

- Collaborate with sector response groups: Participate in sector-specific groups to ensure alignment with industry standards and collective response strategies. Progress against each of the phases of this framework should ideally be communicated via the relevant sector group(s) coordinating the response.

- Structured communications: Enhances clarity and confidence among stakeholders during the reconnection process. Best practice includes:

    - Phase-by-Phase Updates: Share progress transparently against each phase of the reconnection framework with client organisations and relevant sector groups.

    - Timely and Transparent Messaging: Use available information-sharing channels, bilateral engagements, and response coordination platforms to communicate updates in real-time to clients and partners.

- Engage with national cyber security agencies: Where appropriate, maintain consistent updates with relevant national cyber security agencies to receive guidance and share situational awareness.

- Work with regulators and law enforcement: Again, where appropriate based on jurisdictional requirements, communicate with financial authorities and regulators to meet compliance obligations and with law enforcement when legal or security issues arise.

- Coordinate with the supply chain: Notify supply chain partners of disruptions and reconnection timelines, if possible, to minimise downstream impacts. This applies to both the compromised organisation and relevant client organisations.

Sector response: Sector-wide collaboration is crucial for ensuring a unified response to disruptions and supporting effective the broader incident management process. Key actions include:

- Leveraging sector response groups: As alluded to above, utilise established sector response groups to communicate assurances and share information across the sector.

- Synchronising business resumption efforts: Facilitate discussions on business resumption through sector-wide meetings and forums, aligning technical and strategic decision-making. Many of these discussions will continue once the technical reconnection process has been completed and support wider sector incident management and business resumption efforts. It is good practice to establish these engagements before reconnection is achieved to support alignment between technical and strategic or business-level response activities.

- Aligning cyber security and operational responses: Establish mechanisms to integrate technical cybersecurity responses with broader operational and strategic frameworks, especially during severe disconnection scenarios. These frameworks are likely to vary depending on jurisdictional requirements and approaches to sector response.

Attestation: Provides a declaration of readiness for reconnection, ensuring accountability and confidence in the process. The compromised organisation should confirm the status of previous phases (e.g., remediation and testing), where feasible, with a signed attestation by an individual accountable for security and/or operations and responsible for reconnection within that organisation. The attestation may include:

- Timeline of attack including method and initial infection vector.
- Impact to services, data, endpoints, servers, supply chain, etc.
- Remediation activity – including detail on steps taken in the first two phases of the framework. Any aspects that have not been completed should be called out explicitly.
- Where possible, timeline of next steps including planned enhancements to security posture.
- Where possible, evidence of cyber incident response activities undertaken should be provided.
- Compromise assessment summary outcome report (e.g. incident review report).
- Additional information needed as required by either the compromised or client organisations depending on the specifics of the scenario.

Roles and responsibilities: Clear delineation of roles and responsibilities is essential for reconnection efforts. Both compromised and client organisations have critical roles to play:

- <u>Compromised organisations:</u>
    - Take the lead in implementing reconnection protocols, including communicating progress and providing attestations.
    - Liaise with sector response groups to ensure alignment with industry standards.
    - Share lessons learned and refined processes for future incidents.
- <u>Client organisations:</u>
    - Support recovery efforts by engaging collaboratively with the compromised organisation. This might include, where possible, providing resources or assistance, such as technical expertise or operational support.
    - Maintain transparent and constructive communication with the compromised organisation. This might include responding promptly to

requests for information or adjustments to operations, while also avoiding placing undue pressure on impacted organisations during recovery.

- Collaborate in information-sharing fora to address sector-wide challenges.

Appendix

1. **UK Cross Market Operational Resilience Group (CMORG) System Integrity Reconnection Framework (March 2023)** System Integrity Reconnection Framework | Cross Market Operational Resilience Group (cmorg.org.uk)

   This document offers guidance to support the safe resumption of business operations and reconnection of an organisation that has been technically isolated following a significant cyber incident. The outlined steps support and inform a technical view on reconnection and ensure a secure recovery and service restoration by addressing the root cause, providing assurance that affected systems are operating in a trusted state, and following a controlled reconnection process.

2. **SIFMA Reconnection Framework: Guidelines for Remediating Cyber Events Impacting the Financial Ecosystem (November 2023)** SIFMA Reconnection Framework - Guidelines for Remediating Cyber Events Impacting the Financial Ecosystem

   This guidance offers best practice to help organisations safely resume operations and reconnect after being technically isolated due to a significant cyber incident. It aims to provide technical insights for reconnection, while also contributing to broader resilience planning efforts.

3. **Canadian Centre for Cyber Security Ransomware Guidance: How to Prevent and Recover (2024)** Ransomware Guidance: How to Prevent and Recover

   This guidance covers how ransomware infects devices, offers strategies for strengthening cybersecurity defences, minimising risk, and ensuring a swift, effective recovery in the event of an incident. It also addresses the risks of paying a ransom, along with other key considerations.

4. **Options Clearing Corporation (OCC) Reconnection Rules (2024)** OCC Rules (theocc.com)

   This document, specifically pages 22-23, includes OCC requirements to provide a reconnection attestation and reconnection checklist, as well as procedures for connecting following a security incident.

5. **G7 Fundamental Elements of Ransomware Resilience for the Financial Sector (2022)** G7 Fundamental Elements of ransomware resilience for the financial sector

   This document provides financial entities with high-level building blocks for addressing the ransomware threat. It is non-prescriptive & non-binding, and is meant to incorporate current policy approaches, industry guidance, and best practice in place throughout the G7 member countries.