sifma
Invested in America

FSSCC
Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Financial Services Sector Reconnection Framework

December 2025

Contents

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

The Financial Services Sector Coordinating Council, or FSSCC for short, was established in 2002 by financial institutions to work collaboratively with key government agencies while coordinating critical infrastructure and homeland security activities within the financial services industry. We are an industry-led non-profit organization and our mission is to bring together our members from financial services, trade associations, and other industry leaders to assist the sector's response to natural disasters, threats from terrorists, and cybersecurity issues of all types. The FSSCC partners with the public sector on policy issues to enhance the security and resiliency of the United States financial system. The U.S. Department of Homeland Security recognizes the FSSCC as the sector coordination council on behalf of the banking and finance sector. For more information, visit https://fsscc.org/ .

Purpose and Principles

Introduction

The Securities Industry and Financial Markets Association (SIFMA) and Financial Services Sector Coordinating Council (FSSCC) are pleased to announce the publication of the latest version of the Reconnection Framework. The Framework has been updated jointly by both organizations, addressing the scope of reconnection issues across the industry in order to produce a product suitable for broad adoption by the financial services sector.

There are many issues that a firm compromised by a cyber incident must first address in order to reconnect to the financial ecosystem after a cyber event has been contained and mitigated. Most importantly is how the firm should communicate, coordinate, and provide assurance to what could be dozens of business and trading partners in the most efficient and effective way to convey that the problem has been resolved and will not recur. This is crucial so the firm and its business and trading partners can resume normal Business as Usual (BAU) operations.

This document provides a five-step mitigation framework – Assess, Remediate, Assure, Reconnect, and Recover – and is intended to support and inform a technical view of reconnection as well as broader resilience planning.

The Reconnection Framework was originally published in 2020 with the endorsement of U.S. Treasury, the Analysis and Resilience Centre for Systemic Risk (ARC), the Financial Services Information Sharing and Analysis Center (FS-ISAC), FSSCC, trade organizations such as the Bank Policy Institute (BPI) and over thirty financial services firms. The original document set out expectations the financial sector has on global systemically important financial institutions in the event of a cyber incident that disrupts critical business operations.

Since then, the complexity of the financial services supply chain and the role of relatively small, but nonetheless critical, third-party providers have only increased. At the same time, the world is experiencing a more hostile cybersecurity environment than at any other time in modern history. Through this period, the sector has continued to experience incidents resulting in the disconnection of third parties and the subsequent process of attempting to gain enough assurances about the status of their security to allow for reconnection. As a result, SIFMA responded to broader concerns about third-party resilience by working with its members to update the Framework in 2023.

SIFMA's Framework has gained wide recognition across the financial sector, including internationally, where the United Kingdom Cross Market Operational Resilience Group (CMORG) and other systemically important financial institutions used it as the basis for their own Reconnection frameworks. The SIFMA-FSSCC and CMORG frameworks are now highly aligned, which demonstrates the demand for a holistic framework usable across the entire financial sector. Given this growing internationalization of the Reconnection issue, and the broad use of the Framework across the financial sector, the FSSCC and SIFMA are pleased to jointly release this update.

Purpose

'Reconnection' is the process of restoring access and integration to an organization that has been technically quarantined after suffering a material cyber incident. This document provides best practice guidance to aid the process of safely reconnecting an organization that has been technologically quarantined after suffering a material cyber incident. The Reconnection Framework attempts to reduce the time needed to recover by providing the sector with a structured way to facilitate efficient and effective communications. It is intended to support and inform a technical view of reconnection, based upon an understanding of the root cause, assurance that the impacted systems are operating in a known trusted state, and the execution of a controlled reconnection process; as well as to inform broader resilience planning.

The approach outlined in this framework is considered best practice and obtaining full assurance of system and data integrity may extend beyond business risk appetites. Levels of assurance required will vary by incident, depending on the compromised organization, the materiality of the business impacts, sophistication of the attack, etc. This Framework recognizes that specific events that may have a significant system impact may look different based on the details of the event, regulator(s) and impact to the financial ecosystem. Similar principles that are outlined in this Framework can be used but remain discretionary for an event of this kind.

Principles

No organization is immune to attack, and thus the following overarching imperatives apply to the reconnection protocol outlined within this document:

- All parties will engage in a non-judgemental fashion towards the compromised organization.
- All parties will assist the compromised organization to resume their business operations as fast as is safely possible.
- There will be zero tolerance for anti-competitive behaviour.
- The compromised organization should engage independent expertise where appropriate and openly provide evidence and assurance in support of technical considerations.
- To ensure transparency throughout the process, all major decisions and actions should be recorded and openly communicated between key stakeholders (see also Governance and Communication).
- Each firm will need to make their own disconnect/reconnect decision based on individual business processes and risk tolerance.

Structure

- The 'Reconnection Phases' section of this document outlines a five-step process for how the compromised organization can communicate its assessment of the impacts of the incident, the remediation activities it has undertaken and how assurance can be provided to client organizations. These steps will support the decision of client organizations in reconnecting to the compromised organization.
- Each phase includes a statement that articulates the target outcome.

Pre-planning – Recommendations to Consider Prior to any Incident

- Organizations should consider planning against this Framework, in the role of both compromised organization and impacted client organization.
- Before any disruption occurs, it is recommended that financial institutions meet with their key third parties and discuss expectations and procedures for a reconnection scenario, including sharing this framework, along with any relevant firm/client organization-specific processes.
- Third parties should consider maintaining a relationship with a reputable cyber incident response company. They could also consider a backup cyber incident response company to mitigate risks related to problems of availability or credibility with the primary cyber incident response company.
- Financial institutions should consider maintaining an internal framework or policy governing the decision to disconnect from a compromised organization. Financial institutions should also consider what playbooks or industry coordination may be necessary to resume business operations within certain sectors following a successful reconnection decision.
- To ensure clarity of decision making and communication, both financial institutions and their third parties should consider having clearly defined points of contact between them for both cybersecurity and business resilience purposes.

Governance and Communication

- Compromised organizations should communicate regularly with client organizations, relevant national cyber security agencies, sector incident response groups, regulators, law enforcement, and their supply chain throughout the incident.
- Progress through each of the phases of this framework could also be communicated via the relevant sector group(s) coordinating the response, as well as bilaterally to financial institutions, ensuring business and cyber related discussions are occurring.

Business Risks vs. Technical and Cybersecurity Risks of Reconnecting

- The Framework focuses on the technical and cybersecurity elements of reconnection. However, reconnection inherently involves business considerations as well and each firm will need to make their own disconnect/reconnect decision based on individual business processes and risk tolerance.
- The role of the cybersecurity function in the client organisation is typically to assess the residual cybersecurity risk based on information gathered from the compromised organisation and the client organisation’s own threat intelligence.
- The role of the accountable business is to assess business, banking and financial services, and market impacts and ultimately make the decision on whether to disconnect from or reconnect to a compromised organisation.
- While in urgent scenarios the cybersecurity function of the client organisation may initiate a disconnect, the decision to reconnect or not would typically remain with the accountable business within the client organisation, taking into account the cyber risk as articulated by the client organisation’s cybersecurity function.

Disconnection

A precursor and useful context to reconnection is disconnection; client organisations may decide to 'disconnect' from a compromised organisation, or vice versa.

Outcome

The compromised organisation is disconnected from the client organisation(s).

Pre-requisites

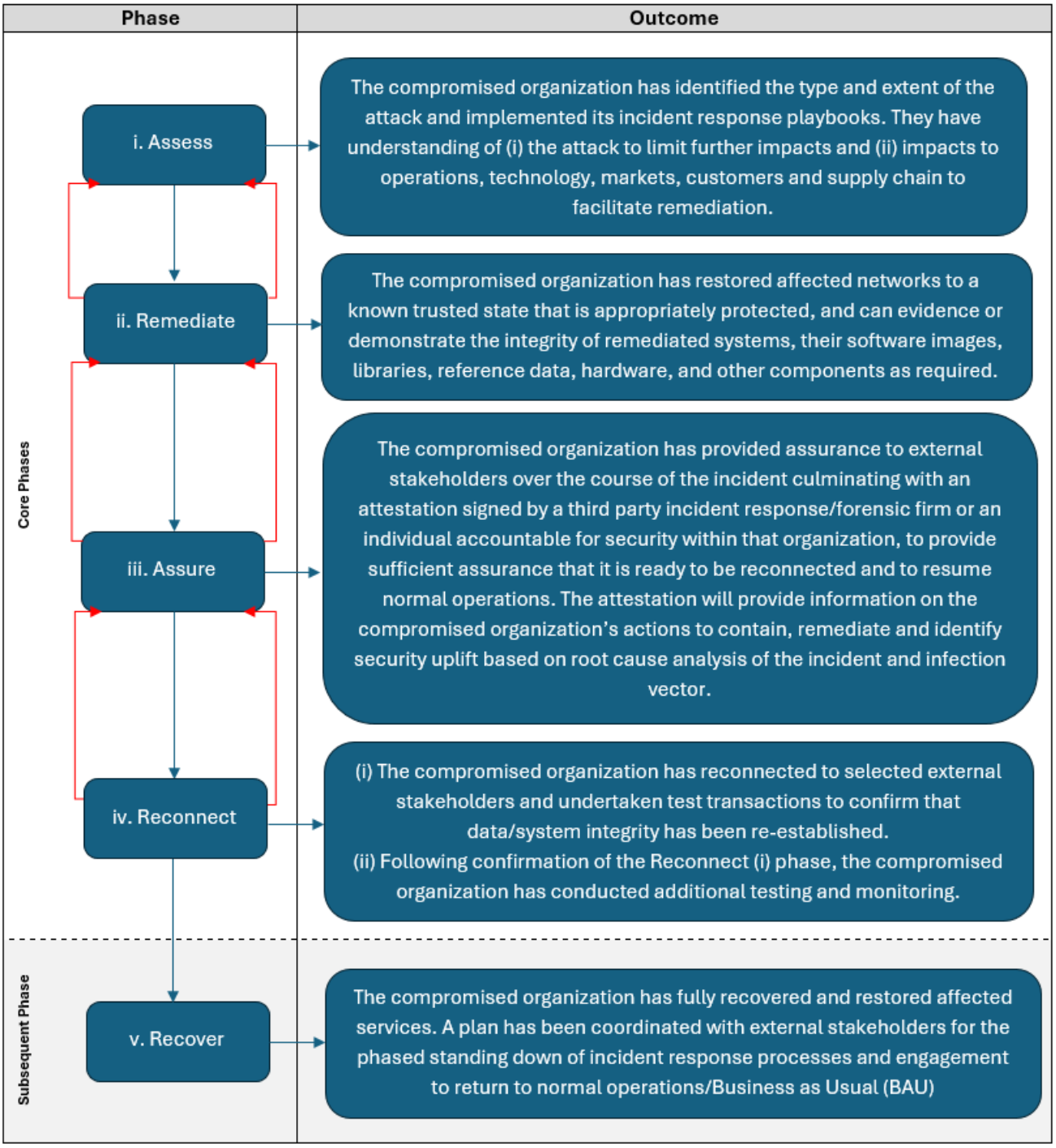
- Client organizations should consider having business-wide disconnection procedures in place to enable effective and targeted disconnection execution during an incident.
- There are several reasons a client organisation may choose to disconnect from the compromised organisation, including:
    - Intelligence suggesting the threat actor has not been removed from the compromised organization's network and that there is potential for further disruption or contagion.
    - When continuing to send sensitive information to the compromised organisation could result in a breach of that data.
    - When continuing to send data, especially transaction data, may complicate reconciliation and/or result in uncertain positions.
    - While fear of contagion could also lead to a disconnection decision, many financial institutions have made significant investment in compensating controls and monitoring capabilities that significantly reduce this risk. These should be considered in relation to the specifics of a given scenario to support optionality for decision-makers.

Technical Process

- Consider the following factors when deciding to disconnect:
    - Type of security incident (i.e., malware, ransomware, business email compromise, insider threat, compromised website, non-malicious, unknown etc.)
    - Level of impact of the security incident to the compromised organisation
    - Current status of the security incident (i.e., remediated, not contained, unknown)
    - Level of cooperation from the compromised organisation
- Client organisations may have more than one connection with a compromised organisation e.g., multiple transactional connections, domain level connections (e.g., email), etc. Disconnecting does not necessarily mean complete termination of all connections between the two parties since different connections might present different levels of risk. Examples of disconnection might include:
    - Suspend connection – remain physically connected but switch off the systems which exchange data with the compromised organisation. This could be effected at the compromised organisation, the client organisation, or both.

- Suspend connection access – remain physically connected but remove or prevent the compromised organisation from accessing systems which exchange data, but which remain accessible to others e.g., FMIs' service platforms. This may also include removing the access rights of the client organisation to access data and systems.
- Pause traffic – remain physically connected and maintain access rights but agree to stop sending traffic e.g., stop submitting transactions or email exchanges. This can include pausing only incoming or outgoing traffic, or both.

Reconnection Phases: Five-Step Mitigation Framework



Phase 1: Assess

Guidelines

Outcome

The compromised organization has identified the type and extent of the attack and implemented its incident response playbooks. The compromised organization has sufficient understanding of (i) the attack to limit further impacts and (ii) impacts to operations, technology, banking and financial services, markets, customers and supply chain to facilitate remediation. Following customer identification, it has established communications with impacted client organizations.

Pre-requisites

- Organizations should have business-wide incident management procedures to quickly coordinate assessments during an incident.
- Organizations should consider having contractual arrangements in place with an appropriate cyber incident response company.
- Organizations should have an understanding of any incident reporting regimes related to the impacted service.
- Compromised organizations should be prepared to establish initial communications with impacted client organizations.
- Where appropriate, compromised organizations should engage with relevant security agencies.

Technical Process

The minimum information a compromised organization may want to provide to clients / authorities once an incident has occurred may include the following:

Information	Description
Timing of Incident	The time that the incident occurred or other relevant timeline information.
Type of Incident	The type of incident that has occurred, i.e., virus, distributed denial of service, ransomware, malicious attack, phishing, etc.
Nature of Incident	A concise description of the identified incident and its potential impact to clients (as detailed as possible). If data has been compromised or exfiltrated, provide an indication of the extent of the data exposure and classification of data.
Source of Incident Information	How the breach was discovered, i.e. through notification from another party, from self-discovery, etc.

Investigation Details	What actions have been taken as part of investigating the incident to confirm its potential scope and impact, including:
	• Identifying the tactics, techniques and procedures (TTPs) of initial infection
	  ○ Tactics (high level strategies of an attack) – reconnaissance, delivery, exploitation, espionage, insider threat
	  ○ Techniques (specific methods used to achieve tactics) – ransomware, phishing, brute-force attacks, SQL injection
	  ○ Procedures (detailed steps taken) – execution of the techniques above

Remediation Activities	Which actions have been taken, including what has been done to mitigate/remediate the incident; whether a third-party cyber assurance company has been engaged; whether legal authorities are informed; whether there is regulatory impact; etc. *(See 'Phase 3: Assure' for more examples)*
Impact Analysis	The impact to client organisation(s), including: • Operations – lines of business, business processes, geographic scope, services provided to industry. • Technology – infrastructure, applications (in house or third-party), data network, voice communications, cloud hosted services. • Data and Privacy – market or reference data, customer Personal Identifying Information (PII), Confidentiality, Integrity, Availability (CIA) impact (including corruption of data, backup data corruption, and data exfiltration).
Data Sharing	If available, share audit logs, Indicators of Compromise (IOCs), and/or forensic reports
Next Steps	This should include what actions remain for completion, along with a full timeline for remediation and wider service restoration.

Phase 2: Remediate

Guidelines

Outcome

The compromised organization has restored affected networks to a known trusted state that is appropriately protected and can evidence or demonstrate the integrity of remediated systems, their software images, libraries, reference data, hardware, and other components as required. The compromised organization has communicated these developments through ongoing engagement with impacted client organizations.

Pre-requisites

- Develop an inventory of trusted sources and back-ups for each of the systems to be remediated. This could remove potential obstacles to re-creating a trusted environment and develop safeguards to reduce the risks to the remediation process.
- Have an overarching plan for detailed testing to validate integrity at every stage of the process.
- Where possible, secure and preserve appropriate information for future investigative analysis and legal use, such as IoCs, for example privileged account irregularities, unusual outbound traffic, or geographic irregularities, as well as logs, images, and other forensic evidence.
- Collaborate with impacted client organizations on any business workarounds in place to reduce impact of the disruption.

Technical Process and Sequencing

Remediation efforts will vary based on the specific situation of the incident. However, compromised organizations should take into account the following considerations:

- Remediate immediate cyber impact
    - Take all affected systems offline
    - Identify tools and resources required to remediate impact
    - Eliminate malware and actor from all environments
    - Enable business continuity plans
    - Recovery to backup systems, if available
    - Potentially shift processes to other locations
- Remediate security control failures and enable monitoring
    - Industry best practice protections are deployed, tested and in place to minimize a recurrence of the compromise, prior to commencement of the restoration of systems and services
    - Where appropriate, patch relevant remaining systems to minimize chance of reoccurrence

  - Implement compensating controls, where appropriate
  - Isolate environments as necessary to prevent further impacts
  - Enable enhanced monitoring to detect whether issue might occur elsewhere in the network
- Remediate remaining incident impact
  - Undertake integrity checks to verify all components are ready to restore
  - Operations team identified corrupt transactions and contacts trading partners and/or other stakeholders where necessary
  - Validate that no other changes, incidents or events are occurring that could impact the restoration process

Phase 3: Assure

Guidelines

Outcome

The compromised organization has provided assurances to external stakeholders over the course of the incident culminating with an attestation signed by a contracted incident response/forensics firm or an individual accountable for security within that organization, to provide sufficient assurance that it is ready to be reconnected and to resume normal operations.

Pre-requisites

- IoCs/TTPs involved in the attack should have been explicitly shared with all impacted client organizations.
- Compromised organizations should consider developing and rehearsing an internal assurance and attestation framework to support efficiency throughout this phase.

Technical Process – Communication and Attestation

- The compromised organisation should consider leveraging an appropriate incident response company as part of their assurance activity to external stakeholders.
- The compromised organisation or a contracted incident response/forensics firm should consider providing an attestation to client organisations regarding the status of their actions to contain, remediate and identify security uplifts based on incident analysis derived from the root cause analysis of the incident and infection vector.
- The attestation may include (but is not limited to, nor is this an exhaustive list): [1]
    - That the compromised organisation is, to the best of their knowledge, ready to resume normal operations. This should be evidenced by steps taken in the first two phases of the framework, including assurance. that threat actor has been removed, containment has been successful, and key systems and datastores are recovered to pre-infection resilience
    - That assurance and integrity tests have been performed on the services, applications, systems, back-up systems and network to validate and certify all systems as operational and functioning normally

[1] See appendix 1 for FAQs to consider when developing an attestation

- Compromise assessment summary outcome report (e.g., incident review report), including information on any issues the firm has not completely recovered from – any aspects that have not been completed should be called out explicitly.
- Outline of lessons learned, and planned enhancements made to prevent similar incidents in the future.
- The compromised organisation should validate data transfer with select client organisations and validate integrity of any software code.
- In addition to engaging bi-laterally with client organisations, compromised organisations should leverage relevant sector response groups to enable faster and more effective communication with the sector.

Phase 4: Reconnect

The Reconnect phase has two outcomes:

i. For reconnecting to selected client organizations and testing transactions to confirm that data/system integrity has been re-established.
ii. And, following confirmation of Reconnect (i), for conducting additional reconnection and ramping up activity under heightened monitoring to normal levels.

Guidelines

Outcome (i)

The compromised organization has reconnected to selected external stakeholders and undertaken test transactions to confirm that data/system integrity has been re-established.

Pre-requisites

Organizations should consider preparing protocols for each type of managed system disconnection and reconnection they may need to undertake, to include:

- Types of messages to be exchanged, and with which other critical stakeholders.
- Success criteria for those exchanges to demonstrate data/system integrity.
- Mitigation process for an unsuccessfully managed reconnection (e.g., to what phase the wider reconnection process should be rolled back), both internally and with sector peers.

Technical Process – Communication and Attestation

- Establish connectivity with selected stakeholders, agree on process for a test exchange of data and validate that these data exchanges are as expected.
- Reconcile data, transactions and settlements
    - Reconcile corrupt transactions and confirm mismatches on existing, pending and completed transactions
    - Identify and ring-fence all pending/inflight/future dated transactions
    - Identify and resolve extant liquidity concerns
    - Conduct final clearance and settlement activities
- Make low-value test transactions with key stakeholders.

- Tests should replicate the range and behaviour of data expected in business-as-usual and should test the end-to-end process.[2] It is also recommended to use low value test transactions, to use current dates (no future transactions) and to test data file transfer, software and code as required by the incident and relationships with key stakeholders.
- Where relevant, compromised organisation to define a strategy to validate connectivity and data integrity.
- These tests should ideally be conducted first in the test system, then out-of-hours in the production system.
- Undertake heightened transaction monitoring across all relevant organisations for an agreed period.

Outcome (ii)

Following confirmation of Reconnect (i), the compromised organization has conducted additional testing and begun ramping up activity under heightened monitoring to normal levels.

Pre-requisites

- Compromised organizations should have protocols in place establishing the criticality of key partners (for example, if reconnection needs to be phased, which partners will be prioritized).
- Appropriate test and roll-back plans should be prepared and approved prior to reconnection attempts/activities.
- Organizations should consider testing full reconnect and restore activities on a regular basis as part of an organization's incident response plan.

Technical Process

- Full connectivity with key stakeholders should be re-established using a phased approach, where relevant.
- Transaction/activity testing should be considered prior to reconnection with each partner, where relevant.
- Validate transactions are handled normally.
- Heightened monitoring and enhanced support across all relevant organizations should continue for an agreed period of time.

[2] Where data is exchanged bidirectionally, the test should replicate those types of transactions.

Phase 5: Recover

Though not necessarily specific to the technical elements of the reconnection process, business resumption and recovery could be occurring while the reconnection process is taking place.

Outcome

The compromised organization has fully recovered and restored affected services, and business / service levels reach an effective resilience position.

Pre-requisites

- Full reconnection and restoration activities should be included and tested on a regular basis as part of an organization's incident response plan.

Technical Process

- Service is restored following successful results from the Reconnect phase.
- Client organizations have removed remaining barriers to the compromised organization.
- Isolation mechanisms are reset.
- Communications are issued to internal and external parties, particularly any interested parties who have experienced downstream impacts.

Appendix – Attestation Guidance and Frequently Asked Questions

What does an internationally recognized cyber incident response provider look like?

- Internationally recognized cyber incident response providers can be vetted effectively by considering multiple factors. Personnel may hold relevant cybersecurity qualifications that are aligned with international standards and have a proven track record in resolving incidents.
- Compromised organizations should verify that the cyber incident response provider has documented processes for detecting, containing, and recovering from incidents.
- The compromised organization should consider whether the cyber incident response provider has experience responding to incidents where the firm has experienced disconnection by their third parties.
- A cyber incident response provider should have the ability to communicate effectively with the compromised organization's third parties and to produce detailed attestations and forensic reports to facilitate the assurance process of reconnection.
- If the compromised organization has cybersecurity insurance, the insurer will likely provide a list of pre-vetted cyber incident response providers.
- Organizations providing services to regulated firms should consider maintaining a relationship with multiple cyber incident response providers to mitigate the risk that one cyber incident response provider does not have the resources available to support their incident or the scenario in which confidence in the cyber incident response provider is lost by the compromised organization or its clients.
- Organizations should also consider seeking contract terms with their cyber incident response provider that specify the requirements necessary to satisfy the assurance expectations set out in this framework.

What is the best way to share the attestation and forensic reports?

- The compromised organization should consider communicating on an ongoing basis with the disconnected firms. Through this communication, channels should be established to the relevant team(s) within the disconnected firms. These channels should be utilized for sharing the final attestation and forensic reports.
- Where the compromised organization does not have a direct line of communication to the disconnected firm, it should consider utilizing the appropriate industry bodies to disseminate information regarding assurance activities, up to and including the attestation and forensic report.
- Failure to communicate or provide the attestation and/or forensic reports directly to the disconnected firm(s) may delay the reconnection process.

Do you want to work with sector organizations to stand up conference calls to share information?

- Compromised organizations should consider utilizing financial sector industry groups to share information related to the breach, as well as activities undertaken to assess and remediate the incident, in accordance with Phases 1 and 2 of the Reconnection Framework.
- The compromised organization should consider sharing assurance details and final attestation documentation with sector groups.
- Information sharing may take the form of participating in crisis calls or providing written communications to those groups for circulation to its members.
- However, the compromised organization should not view communication to industry groups as a substitute for bilateral communication to disconnected firms.
- Many disconnected firms will require bilateral live conversations with the compromised organization before any reconnection decision is made. For these disconnected firms, the industry group calls serve to provide a baseline rather than the full assurance picture they require.
- The compromised organization should consider consulting National Institute of Standards and Technology (NIST) guidelines for the secure sharing of sensitive information, such as Indicators of Compromise (IoCs).

When should the attestation be ready?

- The formal signed attestation is typically the final step in the assurance phase. For some disconnected firms, it may serve as a formality following extensive bilateral communication, while for others, it may be the basis for a reconnection decision. The scenario, as well as the individual firm's risk appetite, will dictate whether a firm chooses to reconnect to a compromised organization before an attestation is received.
- Significant communication regarding the status of remediation activities is expected to occur between the compromised organization and disconnected firm(s) before the final attestation is shared.
- While the specific timeline for the final attestation will depend on the scenario, the compromised organization should communicate with disconnected firms through established channels to clarify when they expect the final attestation to be available. This timeline estimate may evolve over the course of remediation activities.
- Proactive and timely information sharing by the compromised organization is likely to reduce the total time required to reach a reconnection decision.

When should the forensics report be available?

- The forensics report is typically the result of a more extended process and is not available during the assurance phase.
- Disconnected firms should consider making a reconnection decision before the forensics report is available. For most firms, the forensics report is not deemed necessary to make that decision.

What is the difference between an attestation and forensics report?

- An attestation is a record of the assurance steps a compromised firm has undertaken to identify, contain and remediate security enhancements based on the root cause analysis of the incident and infection vector.
- The forensic report is a third-party created or attested report that outlines every aspect of Containment, Remediation, Restoration, Immediate Security Uplifts and Future Security Uplift Roadmaps.

Who should sign the attestation?

- The attestation should be signed by an individual accountable for security or operations within the compromised organization. This individual should possess the technical proficiency to discuss in detail all information included in the attestation.
- The signee should have appropriate levels of seniority and familiarity with the products and be reputable and well-known to the disconnected firms.
- Alternatively, and depending on the incident, the compromised firm may chose to empower a third party incident response/forensics firm to provide attestation.
- The compromised organization should consider in advance who would sign an attestation, depending on a range of scenarios, how that decision will be made, and whether multiple accountable individuals from different responsible functions would sign.

Have you provided the IOCs or other intelligence to the customer base?

- The compromised should consider providing IoCs, where possible, in line with Phase 2 of the Framework. Other intelligence such as tactics, techniques, and procedures (TTPs) should be considered for sharing.
- The compromised organization should consider in advance its process for sharing such information, including familiarity with NIST or other relevant guidelines for the sharing of sensitive information.
- The compromised organization should consider sharing IoCs before the final attestation to facilitate the reconnection decision. The attestation should confirm that IoCs have been shared.