TLP CLEAR

September 2025

G7 FUNDAMENTAL ELEMENTS OF COLLECTIVE CYBER INCIDENT RESPONSE and RECOVERY IN THE FINANCIAL SECTOR

Introduction and overview

Cyber risks continue to grow, driven by rapid digital transformation, increasingly sophisticated threat actors, rising global tensions, geopolitical dynamics, and growing Information and Communication Technology (ICT) interconnectedness between financial entities, other essential economic sectors, and economies. Since major cyber incidents[1] increasingly have a global character, effective cyber incident response and recovery are ever-more dependent on collective efforts. This includes cooperation, both domestically and across borders, between financial authorities, financial entities and their relevant third-party service providers, as well as with actors from other sectors, including government authorities (e.g., law enforcement, cybersecurity agencies). The more jurisdictions align their cyber incident response and recovery approaches globally, the more effectively they can respond to widespread cyber incidents. To foster broad cooperation, the G7 Cyber Expert Group (G7 CEG) has developed this set of fundamental elements of collective cyber incident response and recovery ("**CCIRR**").

Coordinated CCIRR manifested in an arrangement -whether formal or voluntary- ("**CCIRR Arrangement**") offers significant advantages. These include increased situational awareness, more effective and timely information sharing, as appropriate and consistent with legal requirements, increased mutual trust among members of the CCIRR Arrangement (hereinafter referred to as "**members**"), joint development and dissemination of mitigation strategies, and reduced risk of misunderstanding or conflicting communications during crises. Coordinated response and recovery efforts help to better contain the impact of incidents, contribute to the stability of the financial system, and reinforce public confidence.

The *G7 Fundamental Elements of CCIRR in the Financial Sector* are non-binding, high-level principles that may guide the establishment and refinement of CCIRR Arrangements across the financial sector and beyond. These fundamental elements are not regulatory expectations, rather they aim to facilitate greater convergence and compatibility among different approaches, while allowing flexibility and tailoring to national, sectoral, or organizational needs based on the unique markets and regulations within each jurisdiction.

[1] For the purpose of this document, the following definition developed by the Financial Stability Board (FSB) has been retained: Cyber incident: A cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not (Source: FSB Cyber Lexicon - https://www.fsb.org/uploads/P130423-3.pdf).

The *G7 Fundamental Elements of CCIRR in the Financial Sector* are structured in three overarching pillars:

I. **Establishing** the CCIRR Arrangement
II. **Utilizing** the CCIRR Arrangement
III. **Maintaining and testing** the CCIRR Arrangement

The fundamental elements pillars leverage the same structure as the Financial Stability Board (FSB)'s practices for cyber incident response and recovery[2] and consists of three to four elements.

I. Establishing the CCIRR Arrangement

A CCIRR Arrangement clearly sets out governance structures, coordination protocols for CCIRR and how the plan interacts with other relevant frameworks.

Element 1: Governance

Establish strong governance with clearly focused objectives, scope, an appropriate group composition and defined roles.

Governance is crucial as it provides high-level direction for the setup, utilization, maintenance, and testing of the CCIRR Arrangement. Strong governance is key to enabling effective decision-making and achieving common goals.

Agreeing on objectives helps to provide clear direction, purpose, and focus for a CCIRR Arrangement. Objectives help ensure that all members understand what the CCIRR Arrangement seeks to achieve, enabling them to align their actions and prioritize tasks effectively. Objectives also enable better decision-making if they are paired with measurable goals against which progress can be evaluated.

Scope is another core aspect, since it is essential to ensure a shared understanding among members, including the types of incidents covered by the CCIRR.[3] The scope may define the thresholds for a CCIRR Arrangement (including activation criteria) and what aspects it will cover in case of an activation (e.g., exchange of technical information, alignment of external communications, discussion of measures to protect financial stability). The scope also has strong implications for determining potential members, including their skillsets (e.g., cybersecurity/digital operational resilience experts, business experts, business continuity managers) and their levels of seniority.

Regarding the group composition, potential members may be found in both the public and private sectors. In the public sector, potential members may be identified by their respective organization's objectives (such as supervising financial entities, protecting financial stability, or improving cybersecurity). It may be beneficial to distinguish between the public sector's role as a supervisory, oversight or resolution body and its potential role as a coordinator or catalyst in a CCIRR Arrangement to ensure smooth information sharing among members in a trusted

[2] See https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/
[3] For the purposes of this document, incidents refer exclusively to incidents covered by the CCIRR. Typically, these are rather severe incidents.

environment. Potential members from the private sector may include representatives of both financial entities and relevant third-party service providers that hold significant importance for the financial sector. Factors such as size, degree of interconnectedness, and relevance of the provided services to the functioning of the financial sector may serve as relevant factors.[4] It is beneficial to have designated and up-to-date points of contact for all members. It is beneficial to maintain up-to-date contact lists for other relevant forums to facilitate broader cooperation during incidents (see also Element 3: Interoperability with other frameworks).

Regarding group size, it is beneficial to balance coverage and agility. A larger group offers better coverage, reducing the risk of excluding key stakeholders during a cyber incident. Conversely, a smaller group may offer greater agility through quicker coordination and decision making, while also encouraging active participation and maintaining a higher degree of confidentiality.

Finally, the governance structure may also define the working mode and key organizational aspects and roles, such as decision-making processes, leadership (e.g., a rotating chairperson), and key support functions like an internal secretariat, a crisis coordination team or technical support, as well as rules for maintaining these functions.

Element 2: Coordination protocols

Establish mechanisms and procedures to ensure efficient CCIRR coordination.

A CCIRR Arrangement may include clear and formalised rules, mechanisms and procedures that allow for a structured approach in the event of an incident ("**coordination protocol**"). It may define a response and recovery strategy in alignment with the governance set out in the CCIRR Arrangement.

The coordination protocol may contain defined criteria, triggers or thresholds for, among other things, activation, escalation, de-escalation and de-activation, consistent with the CCIRR Arrangement's scope. These may include both quantitative and qualitative (non-binding) criteria.

Further, the coordination protocol may support internal communications and coordination through the use of information sharing arrangements that ensure confidentiality and anonymity, where relevant, and other tools to strengthen the group's activities. For example, the coordination protocol may utilize an exchange platform to enable members to gather, share, synthesize, and extract information, as well as conferencing tools and alert systems. Additionally, the coordination protocol could account for scenarios in which information needs to be escalated to the highest decision-making levels among member organizations.

Existing coordination frameworks may be leveraged and customised to support the design of the coordination protocol.

Element 3: Interoperability with other frameworks

[4] In a different context conducted identification of key entities for the financial sector can be leveraged. For example, the BCBS (Basel Committee on Banking Supervision) publishes a list of Global systemically important banks; in the EU under Article 31 DORA critical ICT third-party providers are designated; in the UK, the Financial Services and Markets Act 2023 (FSMA 2023) where designated Critical Third Parties (CTPs) will be subject to regulatory oversight by financial authorities, once designated by HM Treasury.

Ensure frictionless coordination and foster synergies with other relevant forums.

Since the impact of a cyber incident is unlikely to be limited to the members, ensuring coordination and interoperability with other relevant forums may be beneficial. Planning for such coordination and interoperability may enable the identification and potential mitigation of conflicting goals or priorities, as well as overlapping responsibilities among multiple forums.

The CCIRR Arrangement may define links to other forums, domestically and internationally, where applicable, to facilitate broader collaboration during incidents, while ensuring information sharing remains appropriate and controlled according to agreed protocols. Aligning structures, such as through a common lexicon, standardized information sharing templates, or the nomination of observers participating in other forums, can enhance coordination. Furthermore, each member may consider its resource allocation on a staff level in the event members are participants in multiple frameworks that are activated at the same time. A single point of contact can enable centralized crisis management when participating in various relevant forums. However, risks of bottlenecks and single points of failure can be identified and addressed through appropriate advance planning and staffing.

To enhance overall preparedness and coordination, the CCIRR Arrangement may incorporate adaptable procedures for cross-sector and international scenarios.

II. Utilizing the CCIRR Arrangement

A CCIRR Arrangement defines resilient response tools and methods and prepares for clear, effective and timely crisis communication.

Element 4: Response and recovery tools and methods

Identify, define and establish potential response and recovery tools and methods in advance.

Effective and timely response and recovery is crucial during an incident. While not every situation can be anticipated, plausible scenarios and their potential impacts may be considered, to enable the preparation and inclusion and readiness of potential tools and methods in the coordination protocol to be ready to use[5]. These response and recovery tools and methods might consider:

- Impacts on critical operations/important financial services: Methods and tools may be designed to minimize disruptions to essential services and ensure the safe restoration of vital operations.
- Relevant third-party service provider risks: Response and recovery measures may need to be adapted for incidents originating from a relevant third-party service provider, as such crises may escalate and spread more rapidly.

[5] Response tools and methods refer to a set of structured procedures that may incorporate technical resources (e.g., containment), systems used to support crisis management activities or pre-defined actions (e.g., bank holiday). These tools can be designed and applied at the level of individual organizations or implemented collectively across a sector to ensure coordinated response and recovery actions.

- Disconnection, reconnection, and data restoration: Best practices[6] may guide the safe disconnection and reconnection of systems, as well as the reliable restoration of data.

The FSB's Effective Practices for Cyber Incident Response and Recovery is a helpful reference for potential response and recovery tools and methods[7].

Element 5: Crisis communication

Establish a crisis communication strategy among members to ensure timely and effective messaging to relevant stakeholders in the event of an incident, and prepare strategies to manage misinformation and disinformation, and customer communications.

Clear, effective, and timely external crisis communication following an incident is key to prevent further impacts on the market and its participants. A communication strategy can define in advance general rules for external communications (e.g., to inform members before publishing a statement, or refrain from communicating about other members without their consent, etc.). In addition, it can define the extent to which crisis communications might be harmonized (e.g., timing, templates, platform to share common elements). Preparing for different scenarios in advance can facilitate clear, effective and timely communications during an incident. The crisis communication strategy might identify and assign key roles and responsibilities for developing and disseminating crisis communications, along with suitable tools and media on how to reach the appropriate audience. The direct involvement of communication experts in the CCIRR Arrangement is recommended, as it will help to ensure that crisis communication is an integral part of CCIRR.

Element 6: Resilience of the CCIRR Arrangement

Ensure the resilience of the CCIRR Arrangement by identifying fallback solutions and ensuring sufficient resources for CCIRR.

In the case of a crisis disrupting information and communication systems (e.g., prolonged telecommunications or power outages), response and recovery tools and communications may also be impaired. Members might prepare for such scenarios by identifying and implementing alternative tools or workarounds, to ensure a minimal level of coordination, such as technical fallback solutions or a reduced functionality mode.[8] Regular testing of these contingency measures during non-crisis periods helps maintain their effectiveness.

III. Maintaining and testing the CCIRR Arrangement

Regular testing, exercises and continuous improvement strenghten a CCIRR Arrangement. Moreover CCIRR Arrangements function more effectively when supported by established trust relationships and threat intelligence.

[6] See G7 Cyber Expert Group: Reconnection Framework Best Practice; https://home.treasury.gov/system/files/216/G7-CEG-Reconnection-Framework-Best-Practice.pdf
[7] See footnote 2.
[8] Further fallback solutions might consider people, processes, facilities and/or data.

Element 7: Testing and exercising

Conduct regular tests and exercises to ensure the effectiveness of the CCIRR Arrangement and coordination protocol.

Regular testing of the CCIRR Arrangement and the coordination protocol contributes to its effectiveness and to ensure that members are familiar with how it operates. Furthermore, tests may verify the proper functioning of tools (including fallback solutions) and activation/alerting, and other aspects of the arrangement.

Simulation exercises are particularly valuable, as they provide realistic testing and training under stress and foster anticipation and preparedness. Additionally, such exercises can strengthen members' cohesion and offer opportunities to refine the CCIRR Arrangement, including the coordination protocol. Other exercise types (e.g., table-top exercises or logistic tests) may also be useful, including in preparation for a broad simulation exercise. The G7 CEG has published guidance on best practices in the design of exercise programmes[9].

After-action reports following tests and exercises are beneficial for identifying lessons learned and potential areas for improvement. Findings may also be shared with other groups, where appropriate, to compare learnings, share best practices and achieve common response and recovery outcomes.

Element 8: Continuous improvement

Continuously improve the established CCIRR Arrangement and sustain members' activities outside of a crisis.

To uphold and improve its effectiveness and ensure long-term relevance, the CCIRR Arrangement and underlying protocols benefit from regular review and updating (e.g., based on post incident reports and their recommended actions and remediation measures, capturing and incorporating lessons learned from past incidents and exercises, and looking ahead to future developments in policy, regulation and requirements). A structured review process may support these efforts and is important for sustaining activities beyond times of crisis. Member involvement in identifying improvement opportunities and future areas of development cultivates a feeling of shared ownership and alignment with the protocol, thereby increasing their engagement and willingness to actively contribute to its evolution and implementation. In addition, strategies to foster ongoing engagement during non-crisis periods, such as the creation of working groups (e.g., for designing and conducting exercises), regular meetings, or collaborative projects, help preserve the group's cohesion, ensure continued relevance, and enhance readiness for future incidents.

Element 9: Continuous threat intelligence

Build and strengthen threat intelligence capabilities.

Active and sustained collaboration within and outside of the CCIRR Arrangement relating to threat intelligence is important to preserving adaptability to address an evolving threat landscape.

[9] See G-7 Fundamental Elements of Cyber Exercise Programmes

Exchanging threat intelligence and information of emerging trends (e.g., potential impacts from emerging technologies) affecting jurisdictions or specific parts of the sector can help members prepare for future threats and challenges.

Threat intelligence may guide the CCIRR Arrangement's further evolution and feed exercising activities.

Element 10: Trusted community

Create and maintain an environment of mutual trust among members.

Effective cooperation during an incident is enhanced when members know and trust each other. To cultivate a network of trusted partners and foster an environment where people feel comfortable speaking openly, it may be beneficial to establish clear rules for sharing data/information and ensuring confidentiality and anonymity, where relevant and appropriate. This can be accomplished, for example, through the establishment of information sharing arrangements and/or a classification system to indicate the level of confidentiality when sharing information (e.g., Traffic Light Protocol, Chatham House Rule), which consider members' jurisdictional, legal or other constraints applicable to the sharing of information.

To foster the trust required for sharing sensitive information in times of crisis, it may also be beneficial to have regular touchpoints, such as through exercises, threat intelligence exchange or other working groups during non-crisis periods. In particular, in-person meetings allow individuals to become better acquainted with the members and to enhance communications.