G7 FUNDAMENTAL ELEMENTS FOR THIRD PARTY CYBER RISK MANAGEMENT IN THE FINANCIAL SECTOR
October 2022

Context and Scope

Private and public sector entities in the financial sector ('entities') continue to expand their use of third-party relationships to support their business operations. In recent years, this proliferation of third-party use has included the expanded utilization of Information and Communications Technology (ICT) providers. ICT providers may provide benefits to entities, which include strengthening operational resilience, reducing reliance on legacy IT systems, and increasing the potential for innovation, diversification, and efficiency in the provision of financial services. Further, the use of external ICT services allows entities to concentrate on their core business operations and efficiently manage IT expenditures.

The use of third parties, including ICT providers, may also introduce added cyber risks that entities should consider and manage. In recent years, cyber incidents have shown that critical parts of the ICT supply chain can involve cyber risk for an individual entity as well as systemic cyber risk to the financial sector. Cyber incidents resulting from third-party vulnerabilities could, for example, lead to fraud, disruption of entities' services, inappropriate access to sensitive customer or corporate information, or impact the safety and soundness of the financial markets. As the scale and complexity of these relationships continue to grow, understanding, measuring, and mitigating cyber risks becomes increasingly challenging for entities using third-party services.

Third-party relationships, within the definition of these Fundamental Elements, are any business relationships or contracts between an entity and an organization to provide a product or service, regardless of the organization being an intra-group company or an external provider. One important type of third-party relationship is outsourcing, whereby a third party provides a business function, service or process that would otherwise be provided by the entity itself.

The ICT supply chain, within the definition of these Fundamental Elements, comprises the interconnected web of third parties that form the ICT ecosystem that an entity uses in supporting its business. The ICT supply chain also contains all products, services, and infrastructure, as well as their providers, suppliers or manufacturers. Entities may consider maintaining adequate approaches for detection, recovery, ongoing testing and incident response for the ICT supply chain that supports critical operations.

Fundamental Elements

To help address cyber risks, the G7 Fundamental Elements of Cybersecurity for the Financial Sector were issued in October 2016, and the G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector were issued in October 2017. To further support the development of third-party cyber risk management in the financial sector, the G7 issued the Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector in 2018.

To address industry developments since 2018, the G7 has revised the 2018 Fundamental Elements so as to focus not only on the management of third-party relationships but also on ICT supply chain management. The updated Fundamental Elements stress the importance of extensive information sharing and transparency to cope with an ever-changing threat landscape. To draw attention to the increasingly important role of third parties in the financial sector, a new fundamental element (Element 7) has been added.

Entities should tailor the Fundamental Elements, as appropriate, to their specific risk profiles, operational and threat landscapes, roles in the sector, and legal and regulatory frameworks. The elements are non-binding and do not invalidate existing frameworks or prevent their continuous adaptation. The following Fundamental Elements consider the Third-Party Cyber Risk Management Life Cycle within an individual entity, the role of a third party to the financial sector, as well as system-wide monitoring of cyber risk. Moreover, these Fundamental Elements consider the Third-Party Cyber Risk Management within the entire ICT supply chain of an individual entity.

Entities and third parties can use these Fundamental Elements as part of their cyber risk management toolkit. In doing so, entities should apply a proportionate approach that takes into account the size, nature, scope, complexity and potential systemic significance of the third-party relationship.

Authorities within and across jurisdictions can use the Fundamental Elements to inform their public policy, regulatory, and supervisory efforts to address third-party cyber risks.

Third-Party Cyber Risk Management Life Cycle

Element 1: Governance

Entities' governing bodies are responsible and accountable for effective oversight and implementation of third-party cyber risk management.

Entities' governing bodies, such as boards of directors and senior management, are ultimately responsible and accountable for overseeing and implementing the management of the entities' cyber risks, including those posed by its third-party relationships. This oversight and implementation includes: a documented strategy addressing the reliance on third parties; third-party and cyber risk policies; setting a risk tolerance for third-party relationships; and clear roles, responsibilities, and accountabilities for third-party cyber risk management integrated into the enterprise risk control functions, managed in proportion to the level of risk and criticality of a given activity. It also includes appropriate communication and escalation processes as a normal course of business at all levels within the entity, and between the entity, the third party and relevant authorities.

Element 2: Risk Management Process for Third-Party Cyber Risk
Entities have an effective process for managing third-party cyber risks through the entire third-party risk management life cycle.

Entities should identify, assess, monitor, and report to the appropriate level of management the cyber risks associated with their third parties, and manage them using a risk-based approach. They should adopt policies and control measures in order to protect themselves against contagious third-party cyber risks. Entities should understand the cyber risk management practices that critical third parties use, including risk management practices related to their use of subcontractors.

Identification of Third Parties and Criticality
Entities maintain an inventory of their third parties and an understanding of how these third parties are critical to their operations.

The inventory should contain: a list of all third parties; the services and functions they perform; the level of access each third party has to the entity's systems; and the type, sensitivity, and location of data maintained or processed by each third party.

Entities should be able to identify the criticality of the third party to the operations of the entity. The factors that determine criticality can include the degree to which the third party supports and has access to critical functions and core business lines. Entities are encouraged to further assess the ICT supply chain associated with their third parties using a risk-based approach. For example, a key step could be obtaining a software bill of materials from software suppliers, such as a list of software libraries that comprise the software and which are not strictly related to the relevant third-party relationship (e.g. open source).

Cyber Risk Assessment and Due Diligence
Before entering into new third-party relationships and during the lifespan of the engagement, entities conduct cyber risk assessments and due diligence to consider whether these relationships are consistent with their cyber strategy.

Entities should assess and manage the potential cyber risks and vulnerabilities that a third party and the ICT supply chain may introduce to their operating environments, as well as risks associated with a third party's ability to deliver its product or service. Entities may consider risk factors such as: the criticality of the supported business operations, the third party's level of access (both physical and logical); sensitivity of the data or system hosted or accessed; and method of connection.

As part of an entity's overall due diligence, information gathered may include a review of a third party's current cyber risk strategy and prior performance related to cyber resilience. Entities should conduct due diligence activities pertaining to cyber risks both prior to contractual agreements and during the lifespan of the third-party engagement on a risk-based approach, to provide proportionate up-to-date assurance that the third party's risk management programme is conducted in accordance with the entities' control environment, inclusive of legal and regulatory obligations. Entities may consider the use of common assessments of third parties to gain efficiencies in conducting risk assessments and due diligence activities identified above.

Contract Structuring
Entities' contracts with their third parties include terms and conditions to support the management of cyber risk and include cyber risks stemming from subcontracting.

Entities should ensure that legal obligations and requirements of relevant authorities and the expectations of the entity are included in a contract prior to entering into the relationship with a third party.

In contract terms and conditions related to cyber security, entities may include the scope of the relationship, performance standards, access, information and audit rights for the entity and its relevant authorities, reporting provisions, requirements about frequency and types of cyber resilience tests (e.g. penetration tests, threat-led penetration testing), conditions related to data location, storage, retention, transfer and disposition, subcontracting, and, to the extent possible, ICT supply chain provisions and termination options. If not otherwise provided for in law, contractual agreements should ensure that the entity and relevant authorities are provided with the information necessary to assess cyber risks arising from third-party relationships, including where there is a material change in the delivery of the contracted service.

Furthermore, expectations on reporting to the entity any event in the ICT supply chain that could negatively affect the cyber risk profile of the third party, including cyber incidents, should be articulated in contracts.

Ongoing Monitoring
Entities monitor changes in criticality and risk, and review contract performance of third parties on an ongoing basis to manage their cyber risks.

Monitoring should be proportionate to the materiality of the risk and should take into account changes in the nature of the relationship with the third party. Ongoing monitoring may include changes to the material cyber vulnerabilities and risks of the third party, its operating environment and the impact of any cyber threats or incidents. Entities should regularly monitor performance of the third parties to determine whether it meets the contractual expectations. The entity may collect and analyse cyber risk metrics and risk indicators to support monitoring.

Where the third party provides critical functions or poses a higher material level of risk to the entity, more rigorous and frequent monitoring with appropriate oversight should be considered.

Entities should continuously learn and develop their capability to respond to evolving cyber risks related to third parties and the ICT supply chain.

Element 3: Incident Response
Entities establish and exercise incident response plans that include critical third parties.

The incident response plan of the entity should include ways to detect and collect information about cyber incidents involving third parties and to communicate with third parties and appropriate authorities. The plan should also contain roles and responsibilities, and triggers for reporting to relevant authorities, including national cyber incident response teams.

Periodic exercises can help to identify weaknesses, test cyber resilience, and evaluate the adequacy of response and recovery. Where possible, the incident response plan should be exercised among entities, third parties and relevant partners. The incident response plan should be reviewed to take into account organizational changes and lessons learned.

Element 4: Contingency Planning and Exit Strategies
Entities have appropriate contingency plans and exit strategies in place to address situations where third parties fail to meet cyber-related performance expectations or pose cyber risks outside the entity's risk appetite.

Entities should develop and maintain viable contingency plans and exit strategies that assure the entities' ability to deliver critical functions. Scenarios affecting the cyber risk of the entity may include the following: a material third-party operational event, changes in the third party's ability to operate, changes to the third party's commercial or business strategy, and/or performance. Considerations may include transferring the service(s) back to the entity or to another third party. An entity should evaluate options best suited for its operations and to best promote the safety and soundness of the financial system and limit consumer harm.

Contingency plans and exit strategies should be tested as appropriate and to the extent feasible. Entities should also understand and validate the existence of their critical third parties' contingency plans, in addition to the governance policies and standards supporting these plans and strategies.

System-wide Monitoring of Cyber Risk and Cross-Sector Coordination Management

Element 5: Monitoring for Potential Systemic Risks
Third-party relationships across the financial sector are monitored and sources of third-party cyber risk with potential systemic implications are assessed.

Third-party cyber risk assessment goes beyond individual entities. Where a third party provides a critical function to a systemically important entity, or where multiple entities use common third parties (concentration risk), third-party cyber risks could have systemic implications. These potentially systemic risks should be identified and assessed so that these risks can be managed.

Even where a third party does not provide a critical function to a systemically important entity, if the same third party provides services to multiple entities, it may lead to a concentration risk. Similarly, the supply of multiple functions by one third party could lead to aggregated or compound risk. Entities should identify, assess and monitor concentration risk from their perspective concerning their use of third parties and share relevant information with their relevant authorities.

Relevant authorities should try to identify, assess and monitor concentration and potential systemic risks both at the entity and sector levels, as appropriate. For systemic and concentration risk approaches, relevant authorities should consider implementing appropriate measures to manage these risks and improve information sharing, such as the aggregation of third-party information across entities and the identification of where single points of failure, third-party concentrations, or transmission channels may occur. Entities may consider substituting a third party to mitigate said risks. In order to make such measures effective, entities, third parties and relevant authorities are encouraged to improve information sharing on third-party relationships across the financial sector.

Element 6: Cross-sector Coordination
Cyber risks associated with third-party dependencies across sectors are identified and managed across those sectors.

The financial sector is dependent on third parties in other sectors. A disruptive cyber incident in one of these sectors could affect the ability of entities to deliver their core business functions. Appropriate steps should be taken to facilitate cross-sector coordination in order to identify and manage these cyber risks.

Efforts to improve information sharing across sectors on cyber risk should be encouraged, so that entities can monitor and manage cyber risks stemming from third parties in other sectors.

Entities and relevant authorities should continue to seek opportunities to work with their respective counterparts in other sectors and critical infrastructure forums to promote sound cyber risk management, improve cyber resilience, support the sharing of effective practices and, if appropriate, pursue coordinated responses.

Element 7: Third Parties to the Financial Sector
Third parties that enter into contractual relationships with an entity should be aware that risk management requirements of these entities might have implications for their provision of services and goods.

Entities remain responsible for ensuring the safe and sound operation of services provided to them by third parties. However, third parties should support entities in identifying, assessing, monitoring, and mitigating cyber risks and in complying with relevant risk management requirements. This especially applies to third parties that support ICT and cybersecurity services. To this extent, third parties should make available information necessary to facilitate effective management of cyber risk, including third-party cyber risk. This includes information potentially affecting an entity and its customers such as that related to material incidents, the intent to terminate a service or the support for a service or product, and the intent to enter into a critical third-party relationship with another party in the ICT supply chain.

Where applicable, third parties are encouraged to use these Fundamental Elements to address third-party risk emanating from their respective third parties in the ICT supply chain.