# G-7 FUNDAMENTAL ELEMENTS FOR THIRD PARTY CYBER RISK MANAGEMENT IN THE FINANCIAL SECTOR

## Context and Scope

Private and public sector entities in the financial sector ('entities') use third parties for a variety of business reasons. Third parties introduce additional cyber risk management challenges to entities that they supply. Cyber incidents resulting from third party vulnerabilities could lead to fraud, disruption of services or access to sensitive customer or corporate information. As the scale, complexity and interconnectedness of third parties and their usage continues to grow, maintaining visibility of cyber risks becomes increasingly challenging, for both individual entities and the financial system as a whole.

Adding to the complexities of cyber risk management, entities may not yet have developed robust risk management techniques for third parties upon whom the organization relies.

Third parties are organizations that have entered into business relationships or contracts with an entity to provide a product or service. 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.

## Fundamental Elements

To help address cyber risks, the *G-7 Fundamental Elements of Cybersecurity for the Financial Sector* were published in October 2016, and the *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector* in October 2017.

To further support the development of third party cyber risk management in the financial sector, the G-7 developed the *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*. This is a set of Fundamental Elements for entities to tailor, as appropriate, to their specific risk profiles, operational and threat landscape, role 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 and system-wide monitoring of cyber risk. Entities and third parties can use them 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 cyber risks. 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 entity's cyber risk, including those posed by its third parties. This oversight and implementation includes: a documented strategy and risk tolerance for third party relationships; and clear roles, responsibilities and accountabilities for third party cyber risk management. It also includes appropriate communication and escalation 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 and monitor 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 contagion by third parties. Entities should understand the cyber risk management practices that critical third parties use, including where they rely on their own third parties, such as the 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 type and the sensitivity of the data they maintain or process; and their criticality to the operations of the entity.

### Cyber Risk Assessment and Due Diligence

*Before entering new third party relationships, 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 may introduce to their operating environment as well as risks associated with the third party's ability to deliver its product or service. Entities may consider risk factors such as: the third party's level of access (both physical and logical); sensitivity of the data or system accessed; and method of connection.

As part of the entity's overall due diligence, information gathered may include a review of the third party's prior performance related to cyber resilience. Entities should require that their third parties conduct due diligence in line with their own third party risk life cycle. 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.*

Entities should ensure that legal obligations and requirements of the relevant authorities and the expectations of the entity are included in a contract prior to entering into the relationship with a third party. This may include terms related to the retention, transfer and disposition of confidential data.

Entities may, in contract terms and conditions related to cyber security, include the scope of the relationship, performance standards, access and audit rights, reporting provisions, subcontracting 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 cyber incident reporting to the entity 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 review contracts to determine whether the third parties are performing as expected. The entity may collect and analyze 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.

**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**
*Entities have appropriate contingency plans 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 evaluate and use contingency planning to assist their ability to continue critical functions following a cyber incident related to the third party. As part of contingency planning options, entities should identify appropriate and workable alternatives to the provision of critical functions by third parties. Alternatives may need to be accessed quickly, which may require consideration of transferring business functions or services back to the entity or co-contracting with one or more alternative third parties. Where possible, entities should have termination clauses in third party contracts. Entities should also review and assess the contingency plans of their critical third parties and understand how these plans are validated.

## 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 potentially have systemic implications. These risks should be identified and assessed so that they can be managed.

Even where a third party does not provide a critical function to a systemically important entity, if the same third party supplies multiple entities, it may lead to a concentration risk. Similarly, the supply of multiple functions by a third party could lead to an aggregated or compound risk.

Measures to manage these risks and improve information sharing may include aggregating third party information across entities, and identifying where single points of failure, concentration risk, or transmission channels may occur. Substitutability of third parties may be a consideration in responding to these risks. In order to make such measures effective, entities and relevant authorities should endeavor 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 event 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.

Public and private entities 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.