G-7 FUNDAMENTAL ELEMENTS FOR EFFECTIVE ASSESSMENT OF CYBERSECURITY IN THE FINANCIAL SECTOR

Executive Summary

Recognizing the continued pervasiveness of cyber risks and the need for sustained efforts to enhance cybersecurity in the financial sector, the G-7 developed a set of fundamental elements for the effective assessment of cybersecurity.

In October 2016, the G-7 published the *G-7 Fundamental Elements of Cybersecurity for the Financial Sector* ('*G7FE*'). The *G7FE* provide a set of effective cybersecurity practices within private entities, public authorities, and the financial sector ('entities'). They aim to build greater financial system resilience by supporting private and public entities as they design and implement cybersecurity policies and operating frameworks. The *G7FE* are non-binding, high-level building blocks that provide the foundation for private and public entities, as they develop their approach to cybersecurity, supported by their risk management and culture.

The *G-7 Fundamental Elements for Effective Assessment* promote the effective practices outlined in the *G7FE* by focusing on how well these practices are performed and assessed. The *G7FE* will be most impactful if they are accompanied by a set of desirable outcomes (Part A), and a process for their assessment and review (Part B). Specifically,

- Part A describes five **desirable outcomes** that a mature entity would likely exhibit and that less mature entities can aim for. The outcomes build on the *G7FE*, by encouraging entities to continue developing their cybersecurity, and providing further characteristics to assess the effectiveness of cybersecurity capabilities (the 'what').

- Part B sets out five **assessment components** which assessors can use to develop their approach to assessing progress as entities build and enhance their cybersecurity. The components aim to promote the quality of cybersecurity assessments, to facilitate a process of continuous improvement. They also provide confidence in the scope, execution, and communication of assessment results. Together, they help the assessment by describing the effectiveness of cybersecurity assessments (the 'how').

Desirable Outcomes	Assessment Components
1. The Fundamental Elements (G7FE) are in place.	1. Establish clear assessment objectives.
2. Cybersecurity influences organizational decision-making.	2. Set and communicate methodology and expectations.
3. There is an understanding that disruption will occur.	3. Maintain a diverse toolkit and process for tool selection.
4. An adaptive cybersecurity approach is adopted.	4. Report clear findings and concrete remedial actions.
5. There is a culture that drives secure behaviors.	5. Ensure assessments are reliable and fair.

The *G-7 Fundamental Elements for Effective Assessment* serve as tools to guide and drive internal and external discussions on risk management decisions critical to cybersecurity. For

example, they can help inform Board discussions and Board oversight. The *G-7 Fundamental Elements for Effective Assessment* are not meant to be prescriptive, and serve to inform entities, supervisors and independent assessors alike. They can also be of use in regulatory examinations, self-assessments, and independent review by third parties. Furthermore, these elements can promote conversations across jurisdictions and sectors to drive both technical and cultural conversations around effective practices for cyber risk management.

PART A: Outcomes associated with effective cybersecurity

Acknowledging that there are many ways to describe cybersecurity, the five desirable outcomes below set out broad characteristics that a financial sector entity with a mature understanding, delivery, and oversight of cybersecurity can demonstrate to an assessor.

Outcome 1: The *Fundamental Elements* (*G7FE*) are in place.

The *G7FE* provide the foundational elements for cybersecurity, both for entities who are in the early stages of building cyber resilience and for those who are more mature.

The *G7FE* are wide ranging, reflecting the nature of the challenge. Effective cybersecurity requires entities to maintain a cybersecurity strategy and framework (*Element 1*) and adapt or reinforce their governance processes (*Element 2*). It requires risk and control frameworks, including the relevant set of mitigation controls and protection mechanisms (*Element 3*) and effective monitoring (*Element 4*). Clearly defined and regularly exercised response (*Element 5*) and recovery (*Element 6*) procedures are in place in case of disruptive cyber events. Finally, information sharing (*Element* 7) and continuous learning (*Element 8*) reinforce each *G7FE* and contribute towards strengthening overall cybersecurity.

Outcome 2: Cybersecurity influences organizational decision making.

Building on *Element 1* (Cybersecurity Strategy and Framework) and *2* (Governance), incorporating cybersecurity into entities' normal decision-making processes, specifically by including cyber risk management into these processes early, informs and facilitates strategic outcomes across the organization. Cybersecurity should not be viewed as separate from the concept, design, and operation of entities' core business processes but as into a key strategic consideration, both when developing new products and services, and when assessing the effectiveness of business operations that utilize existing technology or infrastructures.

Active senior management or board-level engagement implies oversight of the design, implementation and effectiveness of cybersecurity programs. Informed by information on threats and vulnerabilities and their entity's risk appetite, boards and senior management can drive risk-management decisions, oversight, and accountability in both the short and long term. As such, boards and senior management can use decision making to drive cybersecurity programs beyond the traditional views of compliance.

Outcome 3: There is an understanding that disruption will occur.

Building on *Element 3* (risk and control assessment), the layering of detective and protective controls is critical, and reduces the likelihood of loss of availability, integrity or confidentiality. However, mature entities recognize that it is impossible to guarantee a zero-failure environment. By adopting a mindset that operational disruptions will occur, key decision makers understand that strategy-aligned investment choices seek a balance across all aspects of the *G7FE*.

Entities that fail to recognize this concept may exhibit an imbalance by having an over reliance on perimeter controls, at the detriment of clearly defined and regularly exercised responses (*Element 5*) and a viable, tested contingency plan for the resumption of operations (*Element 6*).

Outcome 4: An adaptive cyber security approach is adopted.

Both cyber threats and the vulnerabilities which they exploit continue to emerge and evolve. Correspondingly, entities need to be adaptive and avoid a static fortress mentality to ensure their cybersecurity procedures reflect the ever changing landscape within which they operate.

Building on *Element 5* (response) and *Element 6* (recovery), incident response mechanisms need to be well-rehearsed such that economic functions can continue to operate through disruption or stress, whether at the entity, sector, cross-sector or international levels. As disruptions may impact the financial sector in unexpected ways, flexibility is key in reactive functions. Coupled with *Element 4* (monitoring), it is the agility and experience to rapidly identify and contain disruptions that largely influence the resulting impacts. Related, the overall focus should be on fostering an environment of continuous improvement and learning as part of the cybersecurity program.

Outcome 5: There is a culture that drives secure behaviors.

Building on *Element 7* (information sharing) and *Element 8* (continuous learning), a continuous focus on skills and behaviors is essential for embedding effective cybersecurity into the fabric of an organization.

In many cybersecurity incidents, flawed procedures or human factors play a key role (e.g. leveraging weak passwords, social engineering, poor security awareness, etc.). Effective cybersecurity strategies consider aspects of people and processes on an equal footing with technical solutions, and reflect this in investment decisions taken. Training and awareness are equally important, targeted at the end user, employee, and senior management.

In a world where individuals often trade security for convenience, the manipulation of human psychology is as relevant as an adversary's technological sophistication. Each individual understands that they have a role to play. Effective cybersecurity relies on engaging and educating people, and enabling them to handle information safely. Cybersecurity training and awareness can enhance technical knowledge as well as offer opportunities to change behaviors. Effective training aims for genuine and measurable change, shaping culture in a meaningful way, rather than seeking compliance with a set of policies. The adage that people are considered as the weakest link is reversed, instead promoted as the most valuable asset.

PART B: Promoting effective cybersecurity assessments

As entities embed the *G7FE* and strive to achieve the desired outcomes outlined above, there is a necessity to conduct regular assessments to measure the effectiveness of their cybersecurity programs.

Cybersecurity assessment can be defined as the systematic collection, review, and use of information on the cybersecurity practices and controls of individual financial sector entities (private or public) or sector participants collectively for the purposes of: (i) judging performance, measured against intended outcomes; and (ii) providing feedback and setting out areas for improvement, including remedial actions.

To meet these goals, the *G-7 Fundamental Elements for Effective Assessment* set out five high-level components for entities in the financial sector to consider and embed when developing cybersecurity assessment frameworks and conducting cybersecurity assessments.

Component 1: Establish clear assessment objectives.

Assessors establish explicit goals for assessment activities to provide clarity of motivation to both assessor and assessed entity and to facilitate accountability. Clearly defined objectives also support continuous improvement and learning.

Assessment objectives confirm the scope of the assessment, ranging from a focused evaluation of a single entity (in part or in full) to an entire sector. Assessment scope also defines the aspects of cybersecurity under review. For example, assessors may choose to evaluate performance against a broad set of effective practices, such as the *G7FE*, or a specific subset.

A number of factors may be considered when setting scope, combining both qualitative and quantitative criteria, and minimizing gaps in the coverage. Scoping also establishes the assessment perimeter, confirming inclusions or exclusions with regards to interdependencies and supply chain relationships.

When establishing assessment objectives, assessors consider approaches to ensuring that assessments are efficient and effective. In addition, variations in legal frameworks and regulations are accounted for when spanning multiple jurisdictions. For complex entities such as cross-border groups, multiple assessors may have an interest in the evaluation outputs. Assessors with mutual interests and mandates are encouraged to liaise with each other to ensure that significant interdependencies are identified, responsibilities are clearly defined in advance, and conflicting requirements avoided.

Component 2: Set and communicate methodology and expectations.

Taking into consideration existing cybersecurity guidance and frameworks, assessors establish clear and measurable expectations against which cybersecurity assessments are to be conducted. These expectations are communicated to, and understood by, the entity or entities before the assessment commences.

The methodology selected by assessors is aligned to the stated objectives and the complexity of the entity under assessment. Proportionality of assessment can be achieved by following a risk-based approach, taking into account the complex and dynamic nature of the cyber risk.

Component 3: Maintain a diverse toolkit and process for tool selection.

Given the complex and diverse nature of the cyber risk, a diverse portfolio of assessment tools and techniques (‘toolkit’) permits effective cybersecurity assessments. Such a diverse toolkit contains assessment methods to reflect the specific breadth, depth of coverage, or maturity sought in a given assessment. It also gives assessors access to a variety of approaches, suitable for a wide range of circumstances.

Toolkits for cybersecurity assessment may include, but are not limited to, desktop reviews, self-assessments, on-site inspections, threat-based penetration testing, technical reviews (‘deep dives’), thematic reviews, and exercises. Each tool may provide assurance on different practices and each will have its own advantages and disadvantages. Use of multiple tools and

techniques in combination minimizes the risk of over-reliance on single methods of assessment.

To aid the matching of assessment tool or technique against defined objectives, a process for tool selection is recommended. As a minimum, this selection process uses factors such as the importance and inherent risk of entities to the wider sector; the specific nature and scope of the assessment; the resource and time to be expended on the assessment; and the level of assurance being sought. To assess the effectiveness of cybersecurity practices, assessors are recommended to select tools that actively demonstrate capabilities, going beyond a review of policies and procedures.

Assessment toolkits are evaluated regularly to ensure that they remain fit for purpose. The applicability of individual tools is regularly monitored and adapted in line with changes in the threat and business landscape, and the resources at hand.

Component 4: Report clear findings and concrete remedial actions.

Effective cybersecurity assessments deliver meaningful output to drive decisions and actions. This means developing clear conclusions and identifying concrete remedial measures and/or thematic findings that can lead to future action.

When drawing a key conclusion, assessors summarize observed practices and achievements, and identify gaps or shortcomings against expectations as they emerge from the facts gathered. Assessors describe any associated risks or other issues and the implications therein. Overall, the output of assessments provides value, supports decision making, and generates feedback that leads to significant and sustained improvement.

Component 5: Ensure assessments are reliable and fair.

Robust assessment methodologies can ensure reasonable parity between the judgments of different assessors and an overall consistency in approach. Proportionality further ensures that assessments performed are practical and realistic.

Assessments are carried out by competent individual(s) with defined skill sets and knowledge levels. Given the complex and diverse nature of cyber risk, a sound background in IT or cybersecurity is desirable, together with a deep understanding of the relevant business or sector. It can be useful to call on assessors that individually or collectively cover multiple disciplines. Moreover, to keep pace with the evolving landscape, assessors are recommended to continuously update the required skill sets, through training or other professional activities.

The overall quality of the assessment process is maintained through independent reviews (i.e. assessing the assessor) of assessments performed and methodologies adopted; knowledge sharing between assessors; and individual assessor evaluations. To promote fairness and freedom from bias, entities under assessment are afforded process transparency, whilst being assured confidentiality of assessment scope, methodology, and findings.