G-7 FUNDAMENTAL ELEMENTS OF CYBER EXERCISE PROGRAMMES

Introduction and Overview

The financial sector is increasingly reliant on information technology services and their interdependencies to deliver most financial services. Disruption to those services, maliciously, inadvertently or otherwise, can cause significant impact on an organizations ability to deliver critical services. In order to better understand these dependencies and the ability of organizations to respond to and recover from incidents, it is important that both public and private financial sector entities regularly exercise their cyber incident response and recovery plans. These exercises allow different possible cyber scenarios to be rehearsed by organizations on an individual or collective basis, using a range of methodologies, to help prepare them to effectively respond to and recover from cyber incidents. To effectively rehearse those plans, financial entities and jurisdictions may choose to develop a comprehensive multi-year exercise programme. In recognition of the need for clearly defined and regularly rehearsed response and recovery procedures in case of disruptive cyber events, the G-7 developed this set of fundamental elements of effective cyber exercise programmes.

The *G-7 Fundamental Elements of Cyber Exercise Programmes* are non-binding, high-level building blocks that serve as tools to guide the establishment of cyber exercise programmes with internal and external stakeholders. They may also serve as guide for establishing cyber exercise programmes across jurisdictions and sectors.

The *G-7 Fundamental Elements of Cyber Exercise Programmes* are structured as follows:

- Part A outlines the fundamental elements for developing a multi-year exercise programme that comprises multiple exercise types and formats that build upon each other to increase the organization's incident response and recovery posture and capabilities.
- Part B outlines the fundamental elements for building, conducting, and assessing individual exercises within a cyber exercise programme.

Part A Fundamental Elements of Exercise Programmes

An exercise programme enables organizations to adopt a continuous improvement model, following a cyclical approach that includes exercising, evaluating, improving, and then re-exercising. Exercise programmes facilitate an understanding of the entity's ability to respond to and recover from a cyber incident. Exercises can build upon each other in a staged approach, (1) enabling the organisation to progressively enhance its cyber preparedness by tackling increasingly complex risk scenarios; (2) developing key risk indicators and metrics on improvements to the incident management process and procedures; (3) ensuring a common understanding of priorities, threats, and risks; and (4) validating or benchmarking incident recovery capabilities.

Organizations may need to develop a series of exercises to effectively measure improvement in responding to and recovering from a cyber incident. These exercises, when combined, (1) cover all necessary operations of the organization and the corresponding cyber threats; (2) assess the necessary response policies, procedures, and capabilities; (3) drive response and recovery improvement; and (4) capture improvements over time.

Effective exercise programme management typically includes the following elements:

- Stakeholder Engagement
- Multi-year Preparedness Priorities

- Improvement Planning

Exercise Programme Element 1: Stakeholder Engagement

As a first step, stakeholder engagement can help establish and maintain a successful exercise programme by securing the buy-in of key individuals in the organization. Generally, there are two types of stakeholders within an exercise programme: (1) the stakeholders for the exercise programme as a whole, and (2) the stakeholders for the individual exercises within the programme. By identifying stakeholders up front, exercise programmes can more effectively set the priorities for individual exercises. When trying to identify relevant stakeholders, planners of exercise programmes may assess their interconnections to other companies and the companies upon which they are operationally dependant, e.g., third party service providers, often referred to as an ecosystem scan. An exercise programme, as with individual exercises, may benefit from including stakeholders that are representative of the teams and organizations involved. Coordination across programme stakeholders can be achieved through establishing a joint exercising committee or group to oversee and deliver the programme.

An exercise programme may have a lead stakeholder who 'owns' the programme and coordinates across the other programme stakeholders. This should be a person with sufficient seniority within the organization to ensure the exercise programme has the support it requires, commit the organization to a course of action, and ensure that momentum and organisational buy-in for the multi-year plan is maintained. The lead stakeholder can also play a role in calibrating the risks that the exercise programme should focus on. To ensure consistency and stability for the exercise plan, planners of exercise programmes should avoid frequent changes of stakeholders where possible.

In addition to the programme stakeholders, individual exercises within a multi-year exercise plan will have their own set of stakeholders that will vary depending on the scope of each exercise or the scenario chosen. Reviewing and regularly refreshing the ecosystem scan can help to keep the group of relevant stakeholders for each exercise up to date.

Exercise Programme Element 2: Multi-Year Preparedness Priorities

Multi-year exercise planning provides substantial benefits to jurisdictions and organizations by allowing progress to be monitored over time. A key component of successful multi-year exercise programmes is the ability to incorporate lessons learned into the programme and action plans. A comprehensive multi-year exercise programme can help carry those lessons learned from system to system and exercise to exercise and update priorities accordingly. Exercise planners may consider basing the multi-year programme on risk assessments and multi-year priorities that have been approved by stakeholders and senior organizational leadership.

Effective multi-year preparedness priorities should be clear, concise, measurable, realistic, and link directly to risk assessments. Risk assessments use vulnerability and threat analysis combined with mitigation controls or techniques to identify and prioritize risks to the organization, its employees, its operational capabilities, or its assets. In some cases, risks may reside in the external companies that the organization is dependent upon or which it has significant logical or physical connections to. Due to the interconnectedness of the financial sector, organizations looking to design an exercise programme may choose to develop an ecosystem scan as part of their threat and risk assessment process to identify risks stemming from external companies. For cyber security in particular, risks and threats to an organization can change rapidly and may require some multi-year priorities to be re-evaluated on a regular basis as new threat and risk assessments are conducted. However, organizations should be cautious when updating their multi-year priorities to ensure the updates are needed and do not disrupt the organizations' ability to track improvements in the incident response process. Additionally, when

identifying multi-year preparedness priorities, programme stakeholders may consider budget and resource constraints.

Exercise Programme Element 3: Improvement Planning

One of the primary reasons for conducting an exercise is to identify areas to improve the participants' ability to respond to and recover from cyber incident. An After-Action Report (AAR) can document the results of the exercise assessment and be used to issue specific recommendations for improvement based on the assessment. Once identified, areas for improvement are linked to measurable corrective actions with determined responsible parties and target dates for implementation.

Incorporating improvement planning into an AAR will help secure stakeholder buy-in to pursue the identified recommendations and can help show improvements in responding to and recovering from cyber incidents. Including improvement planning into an AAR can also strengthen the exercise programme itself by identifying gaps to correct in subsequent exercises.

Part B Fundamental Elements of Individual Exercises

Exercises provide a low risk, no fault environment for the rehearsing and assessing of plans, processes, and procedures, as well as allowing those responsible for incident management functions to become familiar with their roles during incidents, as well as meet and build relationships and understand how others are likely to approach an incident. Individual exercises within the multi-year programme may differ in size, type, complexity, objectives or area of focus.

For effective exercises, the following elements are commonly advised:

- Exercise Design and Development
- Exercise Conduct
- Exercise Assessment

Individual Exercise Element 1: Exercise Design and Development

The exercise design phase outlines the type of exercise, the participant's and their roles, the objectives, how it aligns with the multi-year programme plan, a scenario description, and identifies the team that will develop, run, and evaluate the exercise. While each exercise within a multi-year plan may be linked by common priorities, each exercise can have its own set of objectives and assessment criteria. Objectives are most effective when they are (1) clear, concise, and measurable; (2) achievable; (3) fit within the multi-year exercise plan; and (4) linked directly to the threat and risk assessment. Assessment criteria are a means to check how well the objectives are met. For more information on the types of exercises planners may consider, please see Appendix.

Participant selection is very important in ensuring effective exercises. The exercise planners may consider including a broad range of subject matter experts as each participant will bring a unique perspective to the exercise. In addition to technical experts, planners may consider including such experts from departments representing communications, legal, business line owners, sister agencies, law enforcement, and critical third parties such as internet service providers or telecommunications.

When designing a scenario, using risk assessments and input from threat intelligence analysis will add a level of reality. Illustrating the various threat actors and their capabilities against the assorted exercise scenarios will provide valuable insight and help tailor the scenario to the specific threat. To facilitate prioritization of risks to be addressed, the exercise programme can use the probability and severity of impacts as criteria. Scenarios can also be adjusted to add complexity, however exercises that are more complex may require additional planning/ education sessions with various stakeholders or participants. For example, due to the hands-on nature of **functional exercises**, additional training may be required to

ensure participants have clear lines of communication during the exercise. Communication rules and standards are critical during an exercise to reduce potential confusion between activities that are part of an exercise and activities that are part of a live event. Additionally, participants may need training on ways to call an emergency end to an exercise if a live event does take place during the execution of the exercise. These additional precautions are not needed in **tabletop exercises** or **seminar exercises** due to their discussion-based nature.

When training participants on how to act in the exercise, exercise planners may choose to prepare in advance for the possibility that the exercise could go off plan. Therefore, when developing the scenario, exercise planners may prepare additional scenario events, commonly referred to as injects, to help steer the exercise back on track if participants move in an unintended direction. It may be acceptable to allow the exercise to go off plan, but the decision to allow the divergence should be made in advance. If the objective is to exercise a specific process, then the exercise planners can bring the exercise back on track.

In addition to developing the scenario and identifying participants, the exercise planners may conduct regular planning and educational sessions with the participants throughout the process. The objective of these planning/education sessions is to confirm the entire stakeholder/participant group has a shared understanding of the various aspects of the exercise. Exercise planners are advised to confirm the lead stakeholder is supportive of the final design plan.

Finally, the exercise planners may choose to avoid solving problems and gaps found during the design process. Solving the gaps introduces a new risk, by obfuscating those problematic elements to the other stakeholders. Instead, exercise planners may choose to present the gap to the owner(s) of the systems as something to be addressed, or refrain from interfering and have the scenario played out and gaps discovered (or not discovered) by the participants during the exercise.

Individual Exercise Element 2: Exercise Conduct

Exercise conduct will vary depending on the type of exercise selected, the number of participants, and their respective roles. For all types of exercises, it is important that proper logistics measures are taken to ensure that locations, technology, communications capabilities, and participant safety are secured. Unless conducting an unannounced exercise, materials should be provided ahead of time and briefing meetings should be organized as appropriate. These considerations become more important when multiple jurisdictions are involved.

To avoid unnecessary disruption to operations, confusion, or panic, it is important to consider some key principles. When conducting an exercise, exercise planners may consider (1) labeling all exercise communications as such in a clear and prominent way; (2) choosing a date, time, location, and delivery method that will minimize potential impacts on normal operations; (3) distributing briefing books and other necessary written materials to all participants that outline roles, responsibilities, and a communication plan for the control staff; (4) communicating to external parties as appropriate that an exercise will be taking place; and (5) making provisions to allow for participants to exit the exercise to respond to real events.

Individual Exercise Element 3: Exercise Assessment

The goal of the assessment is to identify potential improvements to policies, procedures, operations, and systems, as well as to enhance the proficiency of conducting future exercises. During the assessment, the results are compared to the specified goals / objectives and the course of events recorded during the exercise is analyzed for weaknesses.

Effective assessment criteria are used to measure how well the objectives are met and to identify gaps in current plans and areas where improvement can be made, or areas that worked well. It is important not to encourage participants to play to pass or obtain high marks, altering the true outcomes of the exercise. This way designers and participants will be less inclined to "fix" a problem and allow it to be discovered during the exercise.

Effective assessment may include a short discussion session with assessors and participants immediately following the exercise to collect initial impressions and reactions. These meetings are often referred to as a "hotwash" or "hot debrief" and should be used to help shape the improvement planning process and allow for a wide range of feedback across the various roles.

When assessing an exercise, the assessors should observe the actions taken by participants and the outcomes with the aim of assessing (1) whether participants accurately judged the issue at hand; (2) whether the actions were in line with existing policies and procedures; (3) whether they were effective at addressing the issue; and (4) whether participants were aware of what others were doing and why. These questions form the foundation for the improvement plan.

APPENDIX: Terminology

Exercises can take many forms depending on the objectives of the specific exercise. However, exercises can generally be divided into two categories: (1) Discussion-based exercises and (2) Operations-based exercises.

Discussion-based Exercises: These types of exercises familiarize players with existing (or develop new) plans, policies, procedures, and agreements. Discussion-based exercises focus on strategic, policy-oriented issues, and facilitators or presenters lead the discussion, keeping participants moving towards meeting the exercise objectives[1]

> **Training and Awareness (Seminar/Workshop):** An exercise that orients participants to or provides an overview of authorities, strategies, plans, policies, procedures, protocols, resources, concepts, and ideas.[2]
>
> **Tabletop Exercise:** An exercise where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants on roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.[3]
>
> **Game:** An exercise that is a structured form of interactive play designed for individuals or teams in a competitive or non-competitive environment. It is an event players take part in and are guided by clear rules, data, and procedures for its execution. Games are designed to depict an actual or hypothetical situation to ensure that the participants make decisions and take actions that would be plausible.[4]

Operations-based Exercises: These exercises validate plans, policies, procedures, and agreements; clarify roles and responsibilities; and identify resource gaps. Operations-based exercises include a real-time response such as initiating communications or mobilizing personnel and resources.[5]

> **Functional Exercise:** An exercise that allow personnel to validate their operational readiness for emergencies in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects (e.g. communications, emergency notifications, IT equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements including timely recovery

---

[1] Derived from: U.S. Department of Homeland Security. (2020). Exercise and Evaluation Program (HSEEP) (Section 2-6). Retrieved from https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf,

[2] U.S. Department of Homeland Security. (2020). Exercise and Evaluation Program (HSEEP) (Section 2-6). Retrieved from https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf,

[3] National Institute of Standards and Technology (NIST) (2020). NIST Special Publication 800-84, (Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

[4] Derived from: U.S. Department of Homeland Security. (2020). Exercise and Evaluation Program (HSEEP) (Section 2-8). Retrieved from https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf,

[5] Derived from: U.S. Department of Homeland Security. (2020). Exercise and Evaluation Program (HSEEP) (Section 2-9). Retrieved from https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf,

of systems and operations. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency, but in a simulated manner.

Communication and Logistics exercise: An exercise that ranges in scope from simple examinations of the available communication technology to the assembly of the crisis team in the crisis team meeting room. In this exercise, the responsibilities and telephone numbers contained in the plans as well as the procedures, escalation strategy, ability to reach the corresponding people, and rules for substitutes are exercised. The exercise also checks if the plans available are up to date, understandable, and manageable; if the procedures are practical; and if the technologies to be used (e.g. alarm system, emergency telephone, Internet, radio or satellite communication device) are effective, appropriate, and ready for operation.[6]

Full-Scale Exercise (FSE): An exercise, based on a realistic situation that integrates all levels of the hierarchy, from management down to the individual employees, into the exercise. The time and expense required for preparation, execution, and assessment should not be underestimated. Despite this, full-scale exercises should be conducted if the organization places high requirements on business continuity management. Full-scale exercises should be performed regularly but with longer intervals between each business continuity exercise.[7]

[6] Derived from: Federal Office for Information Security (BSI) (2009). BSI-Standard 100-4. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

[7] Derived from: Federal Office for Information Security (BSI) (2009). BSI-Standard 100-4. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1