ITUPublications

International Telecommunication Union
Development Sector

Operational framework and guidelines for the planning and execution of ITU regional cyberdrills

Operational framework and guidelines for the planning and execution of ITU regional cyberdrills

DISCLAIMER:

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ITU and of the Secretariat of ITU concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader.

The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of ITU or membership.

ISBN:

978-92-61-34791-8 (Electronic version)
978-92-61-34801-4 (EPUB version)
978-92-61-34811-3 (Mobi version)

Please consider the environment before printing this report.

Table of contents

List of tables and figures

Tables

Figures

1 Introduction

The International Telecommunication Union (ITU) improves cyber security readiness, protection and incident response capabilities by conducting cyberdrills at both regional and international levels. Cyberdrills are planned events during which cyber-attacks, information security incidents, and other disruptions are simulated in order to test the cyber capabilities of an organization, including detection, response, and resilience. Through cyberdrills, participants are able to assess the strength of policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations. In addition, cyberdrills encourage regional collaboration and increased communication between participating organizations in order to improve the continuity of regional cybersecurity postures.

Since 2011, ITU has conducted more than 30 cyberdrills around the globe.

This document is intended for host country organizers, co-organizers and partners. It contains good practices, event planning guidance, and suggested methods of developing and executing a successful regional cyberdrill, including, but not limited to, the recommended technologies, tools, methodologies, and responsibilities of the parties involved.

Section 1 introduces a baseline understanding of what a cyberdrill is and familiarizes the reader with common cyberdrill-related terminology.

Section 2 provides good practice guidance on cyberdrill planning and execution processes.

Section 3 gives a detailed description of cyberdrill roles and responsibilities for hosts.

Section 4 gives guidance on how to develop a cyberdrill programme.

Section 5 outlines cyberdrill scenario development instructions and gives an overview of the top-down methodology for a full cyberdrill.

Section 6 sets out recommendations and good practices for implementing virtual cyberdrills and methods to support and encourage virtual participation.

Section 7 offers instruction on logistics, including venue selection, recommended seating arrangements, technical requirements, and additional good practice recommendations.

What is a cyberdrill?

A cyberdrill is a planned event during which an organization simulates cyberattacks, information security incidents, and other types of disruptions to test cybersecurity capabilities including detection, response, and resilience. Cyberdrill simulations are delivered through specific scenarios. At the most basic level, a scenario combines a storyline, interactive simulations, competence objectives, user tasks and challenges, and can focus on a wide range of topics that generally fall under one of two types:

1. Table-top: These are discussion-based scenarios where participants role-play their reactions to real-life events. During table-top scenarios, a facilitator guides participants through a series of "injections", i.e. receiving a threatening email, a critical vulnerability alert, a threat declaration by hacktivists, and other similar events. Table-top exercises are traditionally paper based, but have evolved to include the use of laptops and mobile devices to better capture and track the actions and decisions taken by participants and facilitators.

2. Hands-on: These are operational scenarios where participants are required to interact with simulated systems to test their ability to carry out normal cybersecurity tasks. These can include, responding to a cybersecurity incident, performing malware analysis, or carrying out computer forensics.

Cyberdrill objectives

Cyberdrills can help achieve different objectives based on the priorities and thematic interests of stakeholders (such as the CIRT/CERT/CSIRT[1] teams, co-organizers, partners, organizations, and host country) including:

- testing the resilience of an organization to specific cyber threats;
- testing team capabilities;
- testing and identifying skill gaps for improvements;
- evaluating readiness and response capabilities to cyberattacks;
- improving coordination, communication and information sharing between internal and external teams, stakeholders, organizations and entities; and
- testing and validating existing incident response plans.

2 Organizing a regional cyberdrill event

This section contains a description of the phases involved in the overall planning and execution of an ITU regional cyberdrill, including details of the financial resources required to host the event.

2.1 Structure and format of regional cyberdrills

While the term cyberdrill generally just refers to cyberattack simulations or information security incidents, ITU regional cyberdrills include two days of capacity building sessions, a one-day plenary meeting, and two days of practical scenarios across several different cybersecurity

[1] CIRT/CERT/CSIRT (computer incident response team/computer emergency response team/computer security incident response team).

domains. Scenarios are performed in teams with each team representing a national CIRT/CERT/CSIRT from each Member State.

The five-day event is designed as a platform for cooperation, information sharing, discussion of current cybersecurity issues, and also a hands-on exercise for national CIRTs.

Table 1: Generic format of a cyberdrill

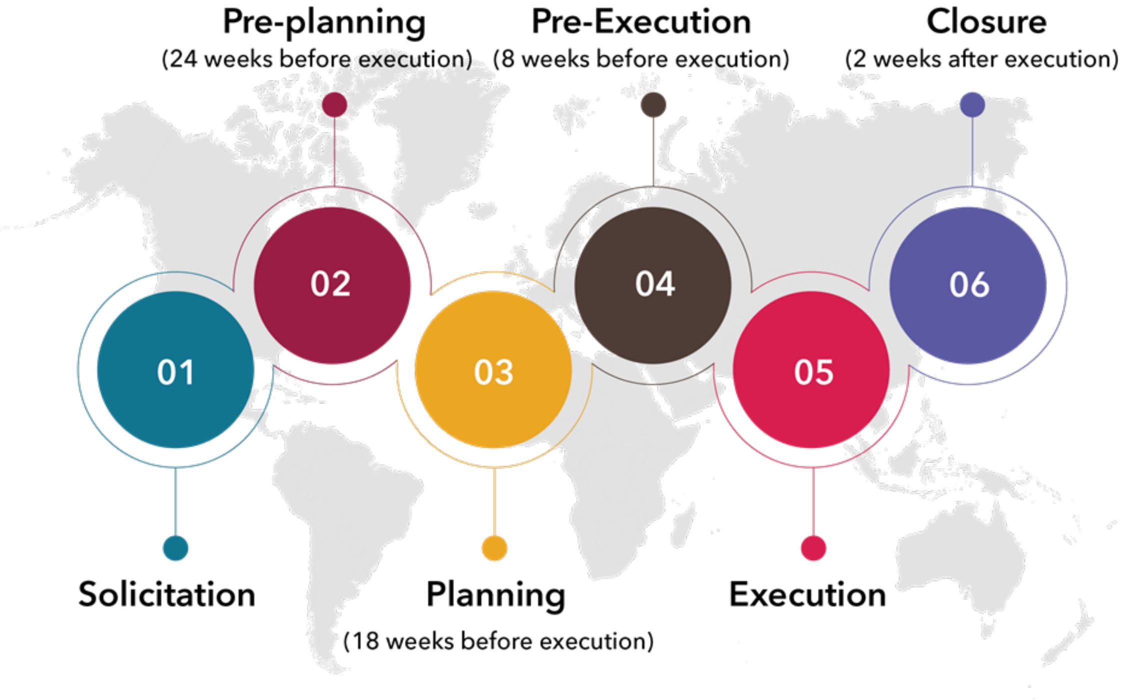
Day	Event	Description
1 and 2	Training	The first two days are dedicated to training in cooperation with one or more ITU partners.
3	Plenary session	This event is open to the general public and includes presentations and panel discussions on current cybersecurity issues, trends in cybersecurity threats, and other topics of relevance for CIRT/CERT/CSIRT professionals and security practitioners.
4 and 5	Cyberdrill scenario	The cyberdrill is open to national CIRT teams and is structured around scenarios delivered by ITU partners. Scenarios address specific cybersecurity domain and objectives.

Target audience

ITU regional cyberdrills are open to national CIRT/CERT/CSIRT experts from the region that hosts the cyberdrill. However, invitation to the cyberdrill security training and plenary sessions may be extended to other stakeholders in the region. Additional stakeholders include senior government officials, cybersecurity experts, industry related players, and other relevant stakeholder groups from the ICT and cybersecurity sectors. At the culmination of the drill, participants will have had an opportunity to build and extend their network of cybersecurity experts in the region.

2.2 Regional cyberdrill phases

Figure 1: Phases of a cyberdrill from solicitation to closure


Pre-planning
(24 weeks before execution)
Pre-Execution
(8 weeks before execution)
Closure
(2 weeks after execution)
01
02
03
04
05
06
Solicitation
Planning
(18 weeks before execution)
Execution

Source: ITU

2.2.1 Phase 1: Solicitation

Phase 1 objective: Identify and select the host country.

Solicitation includes the following:

1. A call for expression of interest is issued by the ITU regional office to identify possible candidates to host the cyberdrill.
2. The ITU regional office consults with interested Member States to ensure the availability of human and financial resources required to conduct a successful cyberdrill.
3. At the end of the consultation period, ITU regional office welcomes a Member State to act as host.
4. An official letter from the host country must be addressed to the ITU Telecommunication Development Bureau (BDT) Director requesting the organization of the regional cyberdrill.

Phase deliverable: Selection of host country.

2.2.2 Phase 2: Pre-planning

Phase 2 objectives:

1. Select the event date and venue.
2. Prepare the information to be shared with the event participants.

This phase contains multiple deliverables, which if delayed can potentially have a negative impact on the subsequence phases. The pre-planning phase ends with an official announcement of the cyberdrill. The official announcement must include:

- Confirmation of all cyberdrill dates.
- Confirmation of the event venue.
- A list of confirmed partner hotels (ideally with conference discount room rates for cyberdrill participants).
- Finalized official invitation letter.
- Finalized cyberdrill information pack.
- Preparation of the cyberdrill scenario specifications (see section 0 for guidance on the creations of these specifications). This activity is led by the scenario manager, who is responsible for coordinating the work of the different scenario authors and ensuring that the scenarios fit with the identified cyberdrill objectives.
- A list of co-organizers, scenario developers, and other event potential partners. This activity is led by the ITU cybersecurity team in cooperation with ITU regional office cybersecurity focal points.
- Curated list of official host country focal points such as Ministry representatives, regulators, and official agencies.
- Organization focal points for travel, visa, and additional logistics.
- Creation and secured launch date of an ITU cyberdrill event specific webpage. The ITU cyberdrill coordinator is responsible for launching the event website with stakeholder participation.
- Timely communication via all appropriate channels

Once all the above activities have been successfully completed, the event may be officially announced.

Phase 2 deliverables:

- Event date and selected venue.
- Cyberdrill information pack.
- Cyberdrill scenario specifications.
- Formal invitation letter.
- List of regional co-organizers, scenario developers, and event partners.
- List of regional and local ITU focal points.
- List of the organization, visa, and logistics focal points.

It is recommended that the pre-planning phase should be completed 24 weeks prior to the execution of the cyberdrill.

2.2.3 Phase 3: Planning

Phase 3 objective: Complete all media outreach and event communication plans to ensure the appropriate event visibility and ultimate participation by the intended stakeholders.

This phase includes the following activities:

- Send official invitations to all ITU cybersecurity focal points. This activity is the responsibility of the cybersecurity focal point in the ITU regional office;
- Publish comprehensive media and communications strategies to promote the cyberdrill within the region.

- Track and update the event registration roster;
- Finalize agenda in close cooperation with all stakeholders including the training agenda, list of cyberdrill scenarios, speaker agendas, etc.;
- Ensure proper and seamless integration of all cyberdrill scenarios, while guaranteeing that they meet scenario specifications and defined cyberdrill objectives.

Phase 3 deliverable: Draft cyberdrill agenda**.**

It is recommended that this phase should be completed 18 weeks prior to the cyberdrill.

2.2.4 Phase 4: Pre-execution

Phase 4 objective: This phase ensures that all logistical components of the cyberdrill are prepared in advance. This includes event agendas, cyberdrill scenario run-throughs, participant preparation meetings, and a detailed run-of-show (timing, programme, and content) for seamless cyberdrill experience. This phase includes:

- A cyberdrill agenda, which has been negotiated and approved by all key stakeholders (ITU, co-organizers, partners and the host country).
- Informing participants of all necessary competences and technical requirements, as well as sharing past cyberdrill scenarios, to assess levels of competence and readiness.
- Sharing user manuals and centrally locating any information about cyberdrill platforms that may be used by participants to practice prior to the event.
- Complete final run-though of all the cyberdrill scenarios from the event venue and distribute detailed run-of-show to affiliated partners.
- Complete the design and printing of the cyberdrill event roll-ups, and the official event backdrop.

Phase 4 deliverables:

1. Cyberdrill agenda.
2. Cyberdrill scenario.
3. List of participants.

It is recommended that the pre-execution phase should be completed eight weeks prior to the execution of the cyberdrill.

2.2.5 Phase 5: Execution

Phase 5 objective: This phase is where all the planning and preparation comes together. This phase includes the following activities, depending on the chosen drill format:

1. Preparation of the venue.
2. Training (day 1 and 2).
3. Cyberdrill conference (day 3).
4. Cyberdrill scenarios (day 4 and 5).

In order to ensure a smooth execution of the event, the required key stakeholders are presented in Table 2.

Table 2: Key stakeholders

ITU staff	Co-organizer	Host country
• Regional focal point • Cyberdrill manager • Scenario manager	• Co-organizer focal point	• Country focal point • Technical focal point • Audio-visual technician • Registration assistant • Master of ceremonies

2.2.6 Phase 6: Closure

Phase objective: This phase is where the cyberdrill results are shared and stakeholders are thanked. This phase includes:

1 A formal letter from the BDT Director to thank the host country and co-organizers.
2 A formal letter from the head of the ITU Cybersecurity Division to thank partners.
3 A formal letter of appreciation from the regional director to thank participants.
4 A mission report.
5 A feedback-survey report.
6 The cyberdrill results.
7 All available materials shared with participants.

It is recommended that this phase is completed two weeks after the cyberdrill.

3 Roles and responsibilities

The planning, delivery, and post-delivery of a cyberdrill requires collaboration, coordination, clear roles and responsibilities, with participants possibly located in different parts of the world and with different skillsets. This section describes the recommended roles, responsibilities and assignments required to develop and deliver a successful cyberdrill.

3.1 Stakeholders

A cyberdrill can have many stakeholders, each with specific responsibilities involving communication and collaboration standards for the successful planning and execution of a cyberdrill.

Table 3: Cyberdrill stakeholders

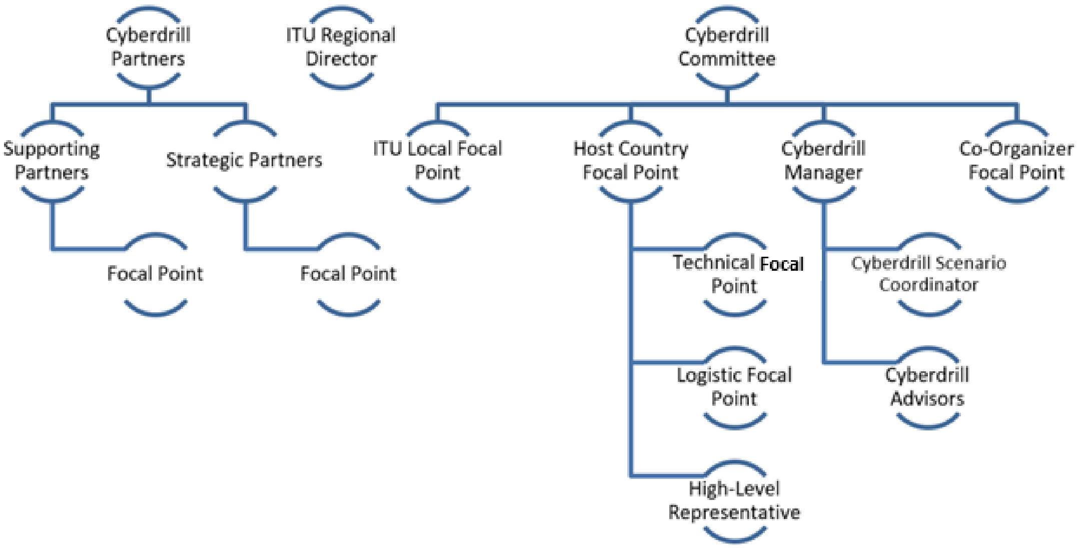
Stakeholder	Description
ITU Cybersecurity Division	The ITU Cybersecurity Division helps ITU membership to increase cybersecurity capabilities and contribute to building confidence and trust in the use of ICTs – making the digital environment safe and secure. The work and mandate of the cybersecurity programme is built on Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference (WTDC) and related resolutions.
ITU regional office	There are six ITU regional offices that represent ITU in each region. Within the context of these guidelines, the cybersecurity focal point in each ITU regional office is responsible for the coordination with the host country in all logistic and organizational aspects.
Host country	The ITU Member State hosting the regional cyberdrill.
Cyberdrill co-organizer	The co-organizer is a regional or international organization that can help to plan and organize the regional cyberdrill. Co-organizers contribute in a variety of ways, such as a financial contributions, training/workshops, and sponsorships.
Cyberdrill partners	Partners are commercial or non-commercial organizations that contribute to the cyberdrill through sponsorships or through contributions to the development of cyberdrill scenarios. There are two types of industry partner: • Strategic partners sponsor the event and may assist in scenario development. • Supporting assist in scenario development.

3.2 Cyberdrill committee

For each cyberdrill, stakeholder representatives are chosen to form a committee to:

- define the cyberdrill objectives;
- ensure effective collaboration between all the stakeholders;
- assure the quality of cyberdrill programme; and
- decide on issues to fulfil the objectives of the operational framework.

Figure 2: Key roles in the development and execution of a cyberdrill



Source: ITU

Cyberdrill manager

The cyberdrill manager is the cyberdrill project manager and focal point coordinator. The manager is an ITU Cybersecurity Division staff member and is appointed to the cyberdrill committee. Responsibilities include:

- cyberdrill administration and coordination between all stakeholders;
- tracking the event progress through logistical, organizational, and technical elements;
- coordinating with all host country partners and co-organizers;
- drafting of the agenda and the cyberdrill content;
- ensuring the availability of cyberdrill funds, human resources, and equipment.

Cyberdrill scenario coordinator

The scenario coordinator is responsible for the development, integration, and testing of scenarios. This role can be filled by an ITU staff member or assigned to a partner. Responsibilities include:

- ensuring that all scenarios address cyberdrill objectives;
- ensuring that scenarios are relative to specific competences;
- ensuring that all scenarios are developed in coordination with supporting partners; and
- ensuring the configuration of the delivery environment or platform.

ITU regional director

The ITU regional director oversees regional actions and must be consulted in all host country communications and organizational commitments at the regional level.

ITU regional office cybersecurity focal point

The ITU regional office cybersecurity focal point is a member of the cyberdrill committee and acts as the logistic and organizational coordinator between all the stakeholders. Responsibilities include:

- ensuring funds are available to conduct the cyberdrill;
- acting focal point for all participants from ITU Member States;
- assisting in the development of the agenda; and
- assisting in the promotion of the cyberdrill.

Host country focal point

The host country focal point is a member of the cyberdrill committee, acting as the project manager at the country level, coordinating cyberdrill logistics as well as serving as the liaison with ITU and other local authorities such as ministry officials and/or regulatory authorities. Responsibilities include:

- representing the host country in all coordination meetings;
- taking responsibility of all the logistical aspects of the cyberdrill, including participant travel arrangements and local transportation;
- ensuring the availability and management of local staff during the execution of the cyberdrill;
- assisting in the cyberdrill `agenda development; and
- assisting in promotion and execution of the cyberdrill.

This role is supported by other functions including technical and logistic focal points and a high-level representative from the host country.

Technical focal point

The technical focal point works in close cooperation with the ITU technical team and is responsible for setting up all technical requirements of the cyberdrill.

Logistic coordinator

The logistic coordinator is responsible for aspects such as transportation, cultural events and supports participant visa processing and hotel bookings.

High-Level Representative

The high-level representative from the host country delivers a speech during the opening session in the first day.

Co-organizer focal point

Co-organizer focal point is a member of the cyberdrill committee and is the official representative of the co-organizer in coordination meetings and during the cyberdrill. Responsibilities include:

- assisting in the development of the cyberdrill content;
- assisting in the development of cyberdrill agendas; and
- assisting in the event promotion.

Cyberdrill advisors

Advisors assist the cyberdrill team and can be chosen from any of the different cyberdrill stakeholders and partners.

Cyberdrill partner focal points

The partner focal points are the official representative of a cyberdrill partner. Responsibilities include:

- assisting in the development of the agenda; and
- assisting in the development of cyberdrill scenarios.

4 Developing the cyberdrill programme

This section contains recommendations and good practices for a cyberdrill event. A regional cyberdrill brings together national CIRT/CERT/CSIRT experts and cybersecurity professionals and practitioners from different countries. As such, developing a successful cyberdrill programme requires a good understanding of expectations, experience, levels of expertise, and effective communication between those involved in the delivery of the event.

4.1 Training

Training courses should match cyberdrill objectives and themes and focus on the functions and roles of a CIRT/CERT/CSIRT in preparation for the cyberdrill. Training should address the individual and team competences to be tested through the cyberdrill scenarios. It is important to ensure communication between the training course instructor and the cyberdrill scenario instructor, facilitated by the cyberdrill manager. The cyberdrill scenario can be adapted to match competence and experience levels of participating teams, for example, by controlling the number/timing of hints and guidance given during the scenarios or by moderating tasks or challenges, cyberdrill scenarios can be adjusted in real time to work with varying levels of technical ability.

Finally, cybersecurity training must be vendor agnostic, and therefore not based on products created by specific vendors.

It is not recommended to assume that participants have read the information related to the courses, including:

- the course syllabus and difficulty level;
- competence pre-requisites;
- technical pre-requisites (e.g., bringing a laptop with administrator access);
- joining instructions (e.g., registering on the training delivery platform).

Communication and validation of the course pre-requisites are key to the successful delivery of the training sessions:

1. Give participants a self-assessment period to help gauge their competency.
2. Provide instructions on how to complete the course pre-requisites.

3. Send weekly correspondence to participants four weeks prior to the course with a checklist to ensure readiness.

4.2 Plenary conference

The conference programme should be developed with keeping the participants involved in mind (avoid presentations about specific products or solutions by commercial vendors, conference partners and sponsors). Where possible, the plenary conference should have at least one international keynote speaker addressing a current and relevant cybersecurity topic of interest to the wider cybersecurity community.

4.3 Cyberdrill scenarios

The development of cyberdrill scenarios requires coordination, communication and a specific methodology. Cyberdrill scenarios and good practice methodology are contained in section six of this document.

5 Cyberdrill good practice

5.1 Scenario delivery cycle

Each cyberdrill scenario typically lasts about an hour and a half to two hours. Shorter timeframes make it challenging to deliver a meaningful scenario, nor is it recommended to exceed four hours. When delivering longer scenarios coffee breaks should be held halfway through the scenario, either as a hard break (where the scenario delivery is interrupted for the duration of the break) or as a soft break (where individuals are free to come and go and continue working on the scenario). Table 4 outlines the delivery of a scenario in four parts:

Table 4: Scenario development lifecycle

Part	Description
1: Set-up	The scenario instructor ensures participating teams have access to the given scenario. This part depends specifically on the scenario delivery method, and includes instructor directions on download specifications, access to virtual machines, and answering participant questions related to scenario challenges and other related questions.
2: Brief	The scenario is introduced to participants by the instructor who explains the objectives of the scenario and participant expectations.
3: Play	Participants work on the scenario, carrying out the required tasks and addressing the different challenges a scenario may include.
4: Feedback	The instructor provides a walkthrough of the scenario sample answers while at the same time taking the opportunity to provide feedback to the participants. It is recommended not to share the document containing the walk through until the walk through has been delivered by the instructor.

A typical two-day cyberdrill will contain four to eight scenarios and it is important that the scenario design follows a methodology that ensures a successful user experience and to achieves the overall cyberdrill objectives.

5.2 Scenario delivery method

Each scenario is designed to use a specific set of tools and technologies including those used by the scenario authors and facilitators. Table 5 summarizes the key delivery methods that can be used during a cyberdrill to deliver and execute a scenario.

Table 5: Key method advantages and disadvantages

Delivery method	Advantages	Disadvantages
<u>**Local infrastructure**</u>: **All required files and virtual machines are made available through a local virtual infrastructure, which all participants have access to.**	• Ideal for scenarios that rely heavily on virtual machines. • Less reliance on Internet connectivity as everything is accessible locally.	• Scenarios have to be shared in advance with the organizers. • Difficult to test remotely by the scenario creator. • Not available to people after the conclusion of the cyberdrill.
<u>**File sharing**</u>: **All required files and virtual machines are shared with each team using memory sticks.**	• Requires little or no infrastructure set up since everything is run on user machines.	• Only applicable to a specific subset of scenarios (malware analysis, forensics). Complex scenarios cannot be expected to run on the end-user laptops. • Requires participants to install all the required tools on their individual laptops.
<u>**Cloud Infrastructure**</u>: **All required files and virtual machines are made available through either public (e.g., Amazon, Google etc.) or private cloud infrastructure services.**	• The scenario can be easily set up and tested prior to the cyberdrill.	• It can be costly, depending on the specifications of the virtual machines in the scenario. • It requires administration of the cloud environment which all Cyberdrill participants must have access to.

5.3 Cyberdrill planning and identification of scenarios

The design and development of cyberdrill scenarios begins with the identification of the cyberdrill objectives and ends with the identification of specific competences to be addressed in each scenario. Before scenarios can be developed or chosen for a cyberdrill, it is important to identify and document the learning objectives.

- A cyberdrill may have a specific theme or focus or cut across a range of domains. For example, in the case of a thematic cyberdrill, the focus could be on CIRT/CERT/CSIRT proactive services and specific objectives such as to assess the capability of national CIRT/CERT/CSIRT to handle cybersecurity incidents;
- and vulnerabilities.

Clearly identifying, documenting, and communicating cyberdrill objectives will allow Member States to assess the need to participate. Additionally, it helps to focus the design, development, and delivery of scenarios and focus of the cyberdrill objectives.

For example, an annual cyberdrill programme could include a series of five cyberdrills and the objectives may include assessing baseline capabilities of national CIRTs/CERTs/CSIRTs services and testing international cooperation and communication amongst national CIRTs/CERTs/CSIRTs.

Once the cyberdrill objectives have been identified and clearly defined and documented, they can be used to validate demonstrated competences of participating CIRT teams and to assess the capability of national CIRT/CERT/CSIRT to handle cybersecurity incidents, and if the event has been successful.

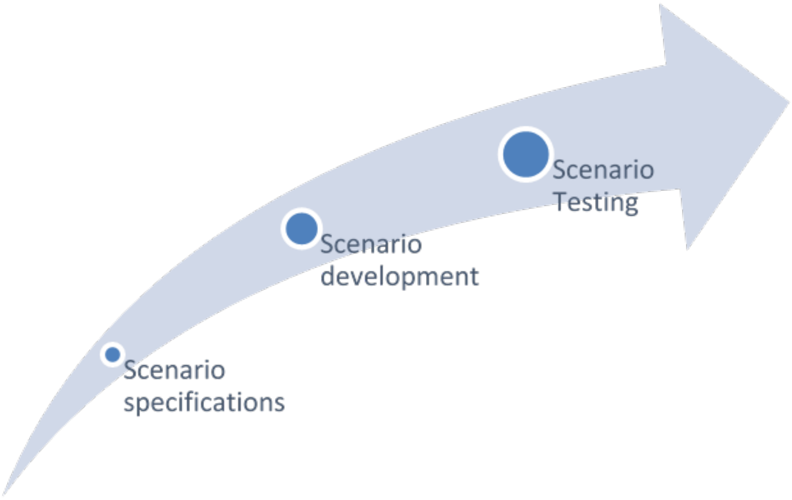
The capability of a national CIRT to handle cybersecurity incidents is based on having competences such as a demonstrated knowledge of common cybersecurity threats, and the ability to analyse and respond to cybersecurity incidents and vulnerabilities.

Once key competences have been identified, scenarios must be developed specifically to assess those competences. For example, a scenario focused on vulnerability assessment, incident investigation, or on the post-detection incident response process (triage phase) of the incident handling etc.

5.4 Scenario development methodology

Cyberdrill scenarios should be developed following a defined good practice methodology. A typical cyberdrill may involve scenarios developed by different partners, and it is therefore necessary to ensure the high-level coordination of both scenario development and delivery. This section contains good practice guidelines for cyberdrill organizers for the development of scenarios. Figure 3 illustrates the three phases of scenario development: specification, development and testing.

Figure 3: Scenario development: specification, development and testing



Source: ITU

5.5 Developing a cyberdrill storyline

Having a storyline that weaves across multiple scenarios is highly desirable, however, it is also resource intensive, particularly when there are multiple scenario authors. A scenario storyline must seamlessly dovetail all scenarios during the cyberdrill. This requires intricate levels of planning, coordination, and preparation before the start of the cyberdrill:

- The development of the storyline is the responsibility of the cyberdrill scenario coordinator.
- The storyline should not focus on a single sector and nor is it necessary that each scenario is mapped to different sectors.
- The storyline should have enough detail and context to create a realistic scenario and should be able to create a logical thread connecting each cyberdrill scenario.
- The storyline should also be anonymous and fictitious, making no reference to real people, organizations or Member States.

If a single storyline cannot be used (which in many cases is likely) many cyberdrill objectives may be achieved by ensuring the scenarios are mapped to identified participant competences.

Competences can be mapped to existing international competence frameworks such as the NIST NICE[2] and to the service areas of a national CIRT as defined by the FIRST CSIRT Services Framework[3], or by specifying competences associated to the NIST Incident Response Process:

- preparation;
- detection and analysis;
- containment, eradication, and recovery;
- post-incident activity.

The selection and sequencing of scenarios should include one or more scenarios related to incident identification. This scenario would be followed by one where participants are exposed to a series of concurrent simulated attacks and would therefore need to decide on the best action to reduce the impact of the cybersecurity incident. A third self-contained scenario should then address end-to-end competences of participants. A scenario such as this could be either be placed at the beginning of the cyberdrill (to gauge the instructor's understanding of the participant competences) or at the end to carry out a final simulation. Such sequencing and choice of scenario must be decided by the cyberdrill scenario coordinator.

5.6 Scenario specifications

In many cases, when creating a scenario, the author focuses on the learning content. However, it is important to remember that scenarios involve people who need to know how to better prepare for a real-life scenario and understand and properly experience the simulation. Additionally, since every scenario may be different, knowing in advance what skills the scenarios will be testing and to what level, will help participating organizations choose which staff member to send to a cyberdrill event.

[2] The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. https://www.nist.gov/itl/applied-cybersecurity/nice/about

[3] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

The following table presents good practice guidelines when developing a scenario. This information should be shared with the cyberdrill scenario coordinator who may use it to create the cyberdrill agenda and storyline to be communicated to the participants.

Table 6: Cyberdrill scenario good practice guidelines

Section	Description	Guidelines	Example
Scenario title	This is the title that will appear in the cyberdrill agenda.	The title must be related to the theme of the cyberdrill, ideally the title will be eye-catching. Imagine picking a movie based on the title and the cover image. When choosing the title, beware, it may have already been chosen or is too similar to other titles being used.	The Night the Bank Was Hacked
Description	This is the short description of the scenario communicated to the participants in the cyberdrill agenda.	The description is simply a short summary of the scenario, a bit like a movie synopsis. Use this section to tell the perspective users about the scenario.	The Eco Bank website has been hacked and defaced and your team has been called to respond to the cybersecurity incident. The cybersecurity manager needs your help to quickly assess the impact of the attack and to understand which vulnerabilities have been exploited by the attacker.
Competences	This is a list of competences this scenario addresses.	Competences should be mapped to an international competence framework such as NIST/NICE or ideally mapped to the service areas of a National CIRT.	• Ability to categorize, prioritize, and create an initial assessment of an information security incident. • Ability to collect, catalogue, store, and track information related to the information security incident. • Ability to analyse information and events related to an information security incident. • Ability to identify the root cause of the information security incident. • Ability to correlate information about multiple information security incidents.
Difficulty	The rated and expected difficulty of the scenario. This is defined by the scenario author, and it can be any of four possible values: • Easy • Medium • Difficult • Expert	Authors tend to simplify scenarios in the creation process. When assigning a difficulty level, follow your instincts, and then choose the lower level. You may always adjust the level after the scenario has been tested by a few users.	Medium

Table 6: Cyberdrill scenario good practice guidelines (continued)

Section	Description	Guidelines	Example
Category	A category describes the high-level domain or body of knowledge a scenario is part of, for example: • Web Hacking • Computer Forensics • Incident Response • Malware Analysis, etc.	The category is provided by the cyberdrill scenario coordinator who ensures that all scenarios are mapped to the identified objectives of the cyberdrill.	Web Hacking
Keywords	Keywords are used to help refine a scenario. For example, if you are creating a scenario on web hacking linked to a competence, keywords help to specify the tools used in that scenario.	No more than 3 to 4 keywords should be provided.	SQL injection, ransomware, etc.
User pre-requisites	A list of competence pre-requisites must be satisfied by potential participants. These are required in order for them to fully engage and gain value from the scenario.	Pre-requisites should be based on international competence framework standards such as the NIST/NICE frameworks. Authors may also add additional pre-requisites based on experience.	N/A
Technical requirements	Similar to user pre-requisites, these are a list of technical requirements that must be met by the participant in order to fully engage with the scenario. Table-top scenarios may not have stringent technical requirements, or any at all. If this is the case, no technical requirements should be captured in the scenario specifications.	The technical requirements should be easy for the participant to carry out a self-test.	Examples include: • Specific laptop configuration. • Administration rights when required to install software. • Use of a VPN client.

5.7 Scenario development

In this phase, the scenario is developed according to previously defined specifications. It is important to stress that scenario development must take into consideration the delivery method and platform of the cyberdrill. For example, a scenario author may build out the scenario through the development of virtual machines, which are then shared with participants during the cyberdrill via a memory stick, however, all other scenarios should be delivered through a cyber range[4]. This causes a non-optimal user experience for the participants, and possibly raises integration issues in regard to the aggregation of results from different scenarios. Therefore, it is highly recommended that all scenarios are developed based on a common delivery platform capable of ensuring a seamless user experience and integration of scoring and reporting.

[4] Cyber ranges are simulated platforms and representations of networks, systems, tools, and applications. See https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf

Table 7 summarizes the deliverables that must be submitted by cyberdrill scenario authors. These are necessary to ensure effective and efficient use of the scenario within the cyberdrill context.

Table 7: Required deliverables

Deliverable	Description	Format
Scenario specifications	Information about the scenario presented in a brief paragraph or bulleted list for cyberdrill participants	.docx/. doc
Run of show	A detailed breakdown of timing for each element of the scenario for the facilitator and any other staff members working on the scenario.	Dependent on the delivery method. Examples include: • Word documents • PowerPoint presentations • Cloud-based virtual image • Conventional virtual machines • Set of files to be distributed
Sample answer	Where possible this should include a sample walk through of the scenario	.docx, .pptx
Competence framework mapping	The assessment envisaged for the scenario must be mapped to a competence framework so that the performance of the CIRT teams can be captured for each scenario. Specifically, whatever challenges, tasks or questions the scenario contains can be directly correlated to specific competences. For example, a scenario challenge related to incident response where the CIRT teams are called to perform triage could be mapped to the "skill in analysing memory dumps to extract information" (NIST NICE S0062)	Table with task and competence identified.

5.8 Scenario testing

Scenario testing refers to testing the scenario from both the participant and the facilitator perspectives, and especially from the viewpoint of the end user. In many cases, scenario authors test the scenario themselves. Such self-testing has some issues:

- The author makes assumptions about end participants that cannot be refuted. This is critical when the assumptions made are essential to the successful execution of the scenario. For example, the author may assume that participants have a Linux command line competence only to discover during the cyberdrill that the majority of participants lack this competence.
- What may appear to be obvious for a scenario author may be baffling or challenging for participants.
- The author may forget to provide important information required for the scenario. For example, the author will not need to read the access credentials to the simulation environment and will not notice if such information has not been provided to participants.

It is recommended for scenarios to be tested by sample users with a similar professional profile as the intended audience. This will more closely mimic a realistic execution of the scenario. It is also recommended that scenario testing is completed by more than one sample end user, and for the author to carry out one or both of the following:

- Update the scenario, such as including missing files or information, updating system configuration, adding or changing challenges/questions/tasks etc.
- Update the scenario specifications such as the scenario competence pre-requisites or tool requirements. For instance, if the feedback from scenario testing reveals that Linux command line competence cannot be assumed, the author can add a competence pre-requisite to the scenario and some suggested reading or tutorials or other learning resources.

It is recommended for scenario testing to be carried out using the same delivery method and simulation environment to be used by participants of the cyberdrill. This is particularly recommended for technical scenarios involving simulation environments such as ICT infrastructures, applications and networks. Changing the delivery environment of such scenarios can have serious implications for the successful delivery of live scenarios. This could be as simple as missing a required configuration or more dramatically that the final delivery environment does not have all the required tools or software for the scenario.

5.9 Sample cyberdrill scenarios

Scenario I	**Threat intelligence**
The national CIRT has been tasked with the responsibility of monitoring current threats and issuing relevant threat reports for various organizations and business domains, to proactively identifying and managing threats. In order to provide the requested service of Cyber Threat Intelligence, the CIRT needs to collect information about specific business domains and organizations. Information about a wave of ransomware attacks have been reported to the CIRT and the CIRT is now tasked with the responsibility of performing a threat analysis somehow linking the observed attacks with organizations from different business domains in order to provide actionable intelligence that will help those organizations proactively manage their specific threats.	
Level	*Competences*
Intermediate	• Ability to explain the Threat Intelligence process and its activities • Ability to explain Threat Intelligence related terms such as observables, indicators, TTP, campaign etc. • Ability to explain the characteristics of different threat actors (e.g., technical capabilities, intentions, typical targets etc.) • Ability to analyse threat data • Ability to generate advisories with actionable intelligence
Scenario II	**Log Analysis – Web Attacks**
Over the past months the national CIRT has received numerous notifications of attacks and breaches of a multiple websites across the country. The attacks are carried out using a range of techniques and tools. The CIRT has been tasked with assisting constituents in learning about different web attack techniques and developing competences to analyse web server logs that investigate breaches and cybersecurity incidents. In this scenario students are presented with a wide range of web server logs and are asked to analyse them in order to identify the tools and techniques used by the attacker, as well as gaining a better understanding of the type of threat actors involved.	
Level	*Competences*

(continued)

Intermediate -Advanced	• Ability to describe different attack vectors for the exploitation of web vulnerabilities • Ability to investigate web attacks • Ability to analyse web server logs

Scenario III	**Log Analysis – Website Defacement**
The national CIRT has received notification about a defacement of the website of the Revenue Authority. Upon discovering the incident, the IT Team from the Revenue Authority was able to reinstall the website from a backup. However, a few minutes later the website was once again defaced. The Revenue Authority has requested help from the CIRT team to analyse the logs from the website and understand the root cause of the incident so that appropriate corrective actions can be put in place and the attack stopped.	
Level	*Competences*
Intermediate	• Ability to describe different attack vectors for the exploitation of web vulnerabilities • Ability to investigate web attacks • Ability to analyse web server logs
Scenario IV	**Intrusion Detection**
The CIRT has been asked to assist its constituents in learning about different attack techniques as well as being tasked with developing competences to detect such attacks. Specifically, many organizations have implemented the opensource Network Intrusion Detection System (NIDS) Snort or Suricata, but they need assistance in deploying it and using it efficiently to detect attacks. In this scenario students are presented with a wide range of NIDS alert logs and are asked to analyse them in order to identify attacker tools and techniques. They should also gain a better understanding of the type of threat actors involved.	
Level	*Competences*
Intermediate	• Ability to describe different attack vectors for the exploitation of network, system and application vulnerabilities • Ability to investigate common attacks • Ability to analyse network intrusion alert logs • Ability to configure and tune Snort/Suricata NIDS
Scenario V	**Log Analysis – Internal Breach**
The National CIRT has received a notification from the Central Bank about a serious internal breach. Their internal database has been breached and the attackers have posted a small subset of data from the database onto *pastebin* as a proof. The database contains sensitive financial information and the Central Bank needs help handling the incident. They would like to understand how the breach occurred, and who could be behind the attacks. The CIRT is given access to Central Bank Log Management System (SIEM) and to the logs of the compromised systems.	
Level	*Competences*

(continued)

Intermediate	• Ability to describe the common methodology followed by attackers to compromise systems and applications • Ability to investigate information security breaches • Ability to analyse different types of operating system and application logs • Ability to identify indicators from a range of tools and techniques used by hackers

Scenario VI	**Incident Response – Bank Fraud**
A computer fraud has been reported by one of the local banks. The fraudsters were able to steal a large sum of money by issuing an unauthorized bank transfer. The Bank IT security team has requested the help of the national CIRT to handle the incident. The initial investigation carried out by the Bank IT security team has not led to any substantial result and the national CIRT has been contacted to help lead the investigation. The CIRT team has been given the results of the initial investigation and is being asked to validate those results and continue with the investigation.	
Level	*Competences*
Advanced	• Ability to correlate information from different sources • Ability to handle incidents in a dynamic environment • Ability to analyse different types of operating system and application logs
Scenario VII	**Computer Forensics**
After analysing the computer logs, the CIRT has been able to reach some conclusions with regards to the attack. However, during the investigation it becomes clear that one of the internal systems used in the attack has been carefully wiped of important data that needs to be recovered in order to find the missing puzzle piece to fully analyse the incident. The Central Bank requires assistance in performing the forensics analysis of the compromised system. The result of the analysis will help clearly establish the attribution of the attack to a specific threat actor and decide if the ransom should be paid or not.	
Level	*Competences*
Advanced	• Ability to explain the computer forensics methodology • Ability to carry out the dead-system analysis • Ability to analyse artifacts of the Windows operating system and a number of common applications
Scenario VIII	**Malware Analysis**
During the course of forensics investigation, a piece of malware is discovered installed on the compromised system. The malware appears to be a keylogger, but it is unclear which keylogging technology is being used. The malware could be a simple keylogger readily available in the black market or a custom made. Malware analysis is required that will reveal more information about the potential threat actor.	
Level	*Competences*
Advanced	• Ability to explain malware analysis methodology • Ability to identify suitable tools and techniques to perform malware analysis • Ability to analyse malware • Ability to correlate malware analysis to threat actor identification.

6 Virtual cyberdrills and virtual participation

While the concept of a virtual cyberdrill may be understood, it is important to define how it differs from traditional cyberdrills, and how it enables virtual participation.

A virtual cyberdrill allows participants to interact through a virtual environment on the Internet, rather than meeting in a physical location.

Similar to other virtual events, a virtual cyberdrill includes a number of multiple sessions, either in sequence or in parallel, usually delivered through webinar or webcasting, with no physical location, and is highly interactive with all stakeholders, including organizers, partners and the participants taking part remotely.

A cyberdrill supporting virtual participation uses a physical location to bring participants together but which also supports remote participation.

It is important to appreciate that supporting virtual participation is not the same thing as running the entire cyberdrill online. Supporting virtual participation should not be considered as a simple extension of virtual cyberdrills. A cyberdrill with virtual participation is a physical event where most of the participation and interaction occurs but which allows remote virtual participation. The biggest challenge of a cyberdrill supporting virtual participation is the interaction of the participants at the physical venue with remote participants.

Table 8 summarizes the key use cases for virtual cyberdrills and cyberdrills supporting virtual participation.

Table 8: key use cases for virtual cyberdrills

Cyberdrill Type	Use cases
Virtual cyberdrill	• Organization of a large-scale event which would be otherwise logistically and financially challenging to host it at a physical location. • Organization of an event where the logistics of running a physical event are no longer possible due to unforeseen events (natural disasters, pandemics.
Cyberdrill with virtual participation	Remote participation of one or more event stakeholders due to logistic challenges or unforeseen events. Examples include: • Participation of one or more guest speakers to present at the event. • Delivery of training by a remote trainer. • Allowing participants who could not come to the physical venue to attend all or some of the cyberdrill presentations, panel discussions, training sessions, scenarios.

It is recommended that support for virtual participation is always built into a cyberdrill as a contingency plan to ensure participation in the face of unpredictable events and to extend invitations to stakeholders who would not normally consider participation.

Technologies

The choice of technology is key for a successful cyberdrill involving virtual participation. Specifically, the following aspects must be carefully considered:

- **Delivery of the cyberdrill conference**: This refers to the technology that enables conference sessions such as speaker presentations, demos, panel discussions, round tables, and other typical activities. It also includes the support for sponsor and partner virtual exhibitions and allows for interaction with virtual participants to showcase their solutions and engage in demonstrations or discussions with remotely.
- **Delivery of cyberdrill training sessions**: This refers to technology that supports a remote trainer and remote participation. The complexity faced in the delivery of training increases if the course includes hands-on sessions that require access to simulation environments and groupwork, if the trainer interacts with each group separately, and if members of a group interact.
- **Delivery of the cyberdrill scenarios**: This refers to the technology that delivers the different scenarios including the provision and management of the cyberdrill environment.

The following table summarizes the proposed technologies and associated solutions for an effective delivery of a virtual cyberdrill or of a cyberdrill supporting virtual participation.

Table 9: Technologies supporting virtual participation

Cyberdrill event	Recommendations
Conference	• Webinar
Training	• Webinar • Cloud-based cyber ranges*
Cyberdrill	• Webinar • Cloud-based cyber ranges*

***For an in depth understanding of cyber ranges, see** *Understanding Cyber Ranges: From Hype to Reality*: https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf

Webcasting and webinars

The technical means used to deliver aspects of the cyberdrill, such as the conference, the training sessions and the scenarios, are similar for on-premises (physical) or remote (virtual) events. However, there is a difference between the use of webcasts and webinars, and which is best suited for a virtual cyberdrill:

- Webcasts are typically used when broadcasting a physical event to a remote audience (not physically present at the location) with no interaction with the live event. Interaction with the audience is usually carried out through out-of-band means.
- Webinars are better suited to virtual cyberdrills as they include options available with online meetings, such as question and answer sessions, polls, and whiteboards, beyond the baseline screen sharing and streaming content.

Today, commercial webinar solutions can support hundreds of participants, and enable session moderation allowing virtual participants to raise hands and speak. Such functionality becomes important when delivering cyberdrill scenarios.

7 Cyberdrill logistics and technical requirements

Working language

Regional cyberdrill events are conducted in English with simultaneous translation to other languages if sponsored by the host country or by a co-organizer.

Collocation with other events

Collocation of the event is acceptable if it is a back-to-back event, and if it meets the overall requirements for the organization of the cyberdrill.

Finance

Funding plays a very important role in cyberdrill management. While successful cyberdrills can be carried out with different budget sizes, it is important to understand that significant financial resources are required for the successful delivery of a cyberdrill.

Sources of financing

There are two main funding sources for ITU regional cyberdrill events:

- ITU Operational Plan: The first source of funding is the regular budget of BDT (operational plan).
- Voluntary contributions: The cyberdrills can also be financed by voluntary contributions from strategic partners or from the co-organizers. Funds received from co-organizers can be directed either to specific cyberdrills or to the global project; there is no limit to how much a partner may contribute.

All financial contributions and all cyberdrill-related activities funded from such contributions, shall be administered by the ITU Cybersecurity Division in accordance with the applicable ITU rules, regulations and procedures.

Management of funds

The responsibility of cyberdrill funds is shared between the ITU Cybersecurity Division and the ITU regional office. In order to ensure the efficient management and proper use of these funds, ITU funds are prioritized in order to give more flexibility in budget management. This also allows voluntary contributions to be used for subsequent cyberdrills in regions that lack funding.

Travel provisions

All travel expenses of ITU staff and recruited experts should be covered by the cyberdrill budget.

Research and development fund

To ensure sustainable development of cyberdrill activities, it is highly recommended that the remaining voluntary contributions be reserved for the research and development of cyberdrills, or to improve BDT cybersecurity initiatives across all regions.

The implementation of regional and national cyberdrills can also serve to build a knowledge base that supports the implementation of a cybersecurity strategy, as well as an approach for the protection of critical information infrastructures. This will also support and develop a cybersecurity culture and related awareness raising initiatives, as well as enhance cybersecurity capacity through regional collaboration and cooperation; It will also further enable Member States to develop and enhance incident response and management capabilities.

Cyberdrill breakout events

The host country shall be responsible for cover expenses relating to breakout events that it organizes in conjunction with the meeting. Furthermore, it shall be responsible for expenses relating to all coffee breaks and luncheons (hot meals) provided during the on-premises event, including a coffee break area and a lunch area. The host country is expected to host a welcome cocktail reception and a cultural event such as a networking dinner, or a demonstration of its culture, customs, and traditions to all cyberdrill participants. Subject to consultation with ITU, the host may find suitable sponsors for these coffee breaks/luncheons and cultural programmes in full or in part.

Travelling to the host country

The host is required to coordinate travel arrangements for all cyberdrill participants. Good practice information to be provided includes:

- providing information regarding travel regulations to the host country, such as health restrictions, recommended vaccines, and all other health related needs related to travel;
- providing information regarding local visa requirements may require the facilitation of group visas, visa delivery on arrival, providing invitation letters for visa purposes, and assistance with general immigration issues of the host country;
- welcoming delegates at the airport and providing round trip shuttle services from the airport to the meeting venue for all delegates.

Local transportation

The host country is required to coordinate local transport arrangements for participants including:

- transportation to and from the meeting venue to pre-selected hotels accommodating delegates;
- arranging transport to and from the airport for delegates;
- arranging transportation to any of the side events – dinners, cocktails, social events – for all delegates;
- arranging transportation for ITU staff during event for any necessary errands that need to be conducted off-site.

Onsite assistance

Local staff to help facilitate the cyberdrill is to be provided by the host. The following roles should be filled by local staff provided by the host. It should be noted that the list below may change depending on the requirements of the meeting:

- at least one technician to assist in the setting-up of the servers and network;
- at least one technician for the audio/visual equipment in the meeting room;
- at least one person at the participants registration desk that is also able to provide assistance elsewhere as and when required;
- at least one master of ceremonies (a person who acts as host at the event) to make the welcoming speech and introduce other speakers;
- security personnel for the event.

Service providers: The host must obtain around the clock maintenance support from service providers for critical components.

Premises setup

The physical setup of venues chosen to host the event is critical for the success of the cyberdrill. Seating arrangements are particularly important and should be chosen according to the events being hosted on the day, whether it is training, the conference, or the cyberdrill scenario.

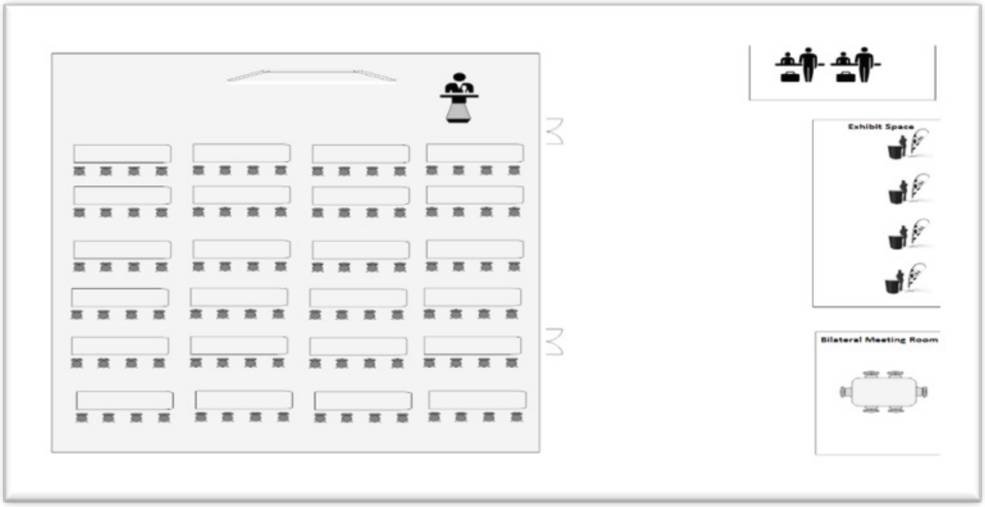
The following guidelines concern the physical set-up of the cyberdrill venue:

- Seating arrangements should give people room to shift comfortably without disturbing others.
- Accessible access must be considered.
- Allow easy access to and from seating; consider factors like aisle locations (and widths), distance between rows of chairs, location of seating in relation to room entrances and exits.
- Multiple entry and exit doors to ease access to and from the conference room.
- Bottled mineral water should be available for participants.
- All rooms should be operational at 8 a.m.

The room layout can change to reflect the agenda. Generally, hosts should prepare for two configurations:

- **C**lassroom style: Allow rows of conference tables with chairs facing the front of the auditorium and provide writing space for each person. This setup is recommended for day 1, 4 and 5.

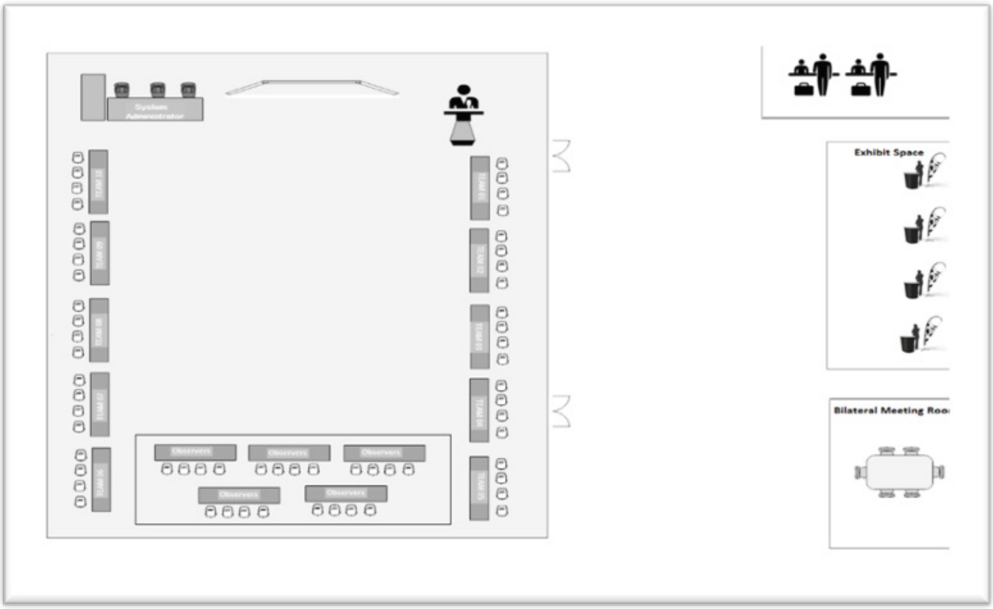
Figure 4: Sample classroom style



Source: ITU

- **U-shape style:** A series of conference tables and chairs set in the shape of a classic boardroom setup that enables members to both face each other and the speaker. The setup in the shape of the letter 'U' is also useful to provide power plugs for laptops (1 per seat). This setup is for day 2 and day 3.

Figure 5: U-shape style



Source: ITU

IT requirements

Table 10: IT requirements

Type	Role	Quantity
Laptops	• One laptop for projection on the podium. • One laptop for the registration desk. • One laptop for the secretariat.	3
Printer	• At least one ppm robust network printer, black and white, colour, recto-verso, with A4 and A3 paper capability. • Robust and higher speed network printers, black and white, exact specification to be defined at project definition to be used by the teams involved in document preparation. • Toners, including on-site spares.	2
Power extension cables	• 15 metre units.	7 units
Gang power extension	• Minimum four-way mains trailing socket. • minimum length 1.5 metre.	15 units

Technical and audio-visual (AV) requirements

- One microphone in the podium for the presenter.
- At least two wireless microphones.
- At least one large projection screen, clearly visible to all the participants.
- At least one projector (XVGA, BNC, HDMI), adequate for projecting a clear image on the large projection screens, with direct wired connection via split video cables to the presentation laptop (at/or near the podium).

- One laptop for projections either on the podium or in the AV control room: the laptop should have an international keyboard (Microsoft Word and PowerPoint and USB ports).
- Line audio connected to the PC or laptop for projections, in case of video/audio presentations.

Internet access requirements

Internet access during cyberdrills is crucial and should be provided through wired Ethernet and a public wireless network. The local host must be able to obtain a minimum of two different connectivity providers:

- A LAN designed to provide seamless Internet connectivity for all meeting participants.
- Two network ports with internet connection on the podium.
- Sufficient wireless LAN access points to support approximately one hundred (150) wireless devices.
- The wireless LAN capacity for each meeting room and work area must be at least equal to the seating capacity of the room (i.e., consider the possibility that everyone may wish to connect their laptops, PDAs and smartphones at the same time).
- A minimum Internet download and upload speed of 100 Mbit/s and 50 Mbit/s.
- The wireless LAN needs to be 802.11a, b, g, n and Wi-Fi compliant (plus any new generally adopted standards at the time of the Meeting).
- The wireless LAN needs to support common encryption protocols (e.g., WEP, WPA, WPA2).
- The target average ping response time from the PCs to the gateway should not exceed twenty (20) milliseconds during normal load conditions.
- The target average throughput for each associated laptop needs to be 3 Mbit/s or above.
- The wireless access points need to be centrally controlled to allow rapid, if possible, auto reconfiguration of the access points to adapt to change load conditions in the meeting rooms and to block individual laptops in case of virus problems.
- The broadcast SSID shall be set to that requested by ITU.

Software licences

It is the responsibility of the host to arrange for the necessary software licences installed on PCs and laptops provided by the host.

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt

International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand

International Telecommunication Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication Union (ITU) Area Office
Sapta Pesona Building
13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation

International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-34791-8

9 789261 347918

Published in Switzerland
Geneva, 2021
Photo credits: Shutterstock