Review on exercise guidelines

Master Thesis

For attainment of the academic degree of
Master of Science in Engineering (MSc)

in the Master Programme Cyber Security and Resilience
at St. Pölten University of Applied Sciences

by
Mr. Ashraf
52106373

First advisor: [Mr. Tjoa]

[Sankt Pölten, 20.09.2023]

Declaration

I hereby affirm that

- I have written this thesis independently, that I have not used any sources or aids other than those indicated, and that I have not made use of any unauthorised assistance.
- I have not previously submitted this thesis topic to an assessor, either in Austria or abroad, for evaluation or as an examination paper in any form.
- This thesis corresponds to the thesis assessed by the assessor.

....

Place, Date Signature

Abstract

Cyber exercises are increasingly being used as a means to test organisational preparedness for cyber incidents and evaluate incident response plans. Even though there are a fair amount of guides published, there are not many research papers reviewing these guidelines. This thesis aims to come up with a framework for designing cyber exercises by reviewing existing guides and reports. The review identifies the features provided by each guideline for the design, conduction and evaluation phase. After reviewing all the phases, the paper comes up with a framework including the best features from the design, conduction and evaluation phases for conducting a cyber exercise. The consolidated framework covers the full lifecycle of a cyber exercise from initial planning and design to post-exercise evaluation and improvement planning. If implemented, the proposed guidelines have the potential to bring greater structure, consistency and rigour to the process of conducting cyber exercises. They can help organisations derive maximum benefits from cyber exercises and better measure improvements in their cyber readiness over time.

Table of Content

1 Introduction

Cyber threats are becoming more prevalent and challenging to address. These threats pose risks to both the public and private sectors and can lead to serious consequences such as terrorism, crime, or industrial espionage.

It is essential to respond quickly and efficiently to security breaches to minimise damage to personal and business data. The computer security incident response is an accepted method to tackle these incidents. By following a consistent handling methodology, incident response helps in minimising losses or theft of information and service disruptions caused by security incidents. It also enables organisations to better prepare for future security breaches and protect their systems and data.

Incident response capabilities are useful in addressing any legal issues that may arise during a security breach incident [1]. It is, therefore, imperative to have a robust incident response capability to deal with the ever-increasing cyber threats.

The 2022 "Cost of a Data Breach Report" by IBM, highlighted the significant role of human errors in security breaches. Research has revealed that a significant portion, specifically 21%, of breaches can be attributed to unintentional incidents caused by the negligent actions of employees or contractors. [2]

Additionally, research and studies conducted in 2015 have indicated that human errors played a significant role in security breaches within industrial firms, with 31% of incidents being attributed to this factor. Additionally, a study found that social engineering attacks, such as e-mail phishing, were a common means of obtaining stolen data, and were the root cause of 80% of data breaches. These findings highlight the importance of user awareness and training as a key factor in preventing cyber-attacks from being successful. [3]

The modern world is faced with a growing threat of cyber-attacks like Conti cyber-attack[4] and WannaCry[5] ransomware attack and cybersecurity has become a top priority for governments, organisations, and individuals. To effectively protect against cyber threats, it is essential to develop and implement cyber exercises that can test an organisation's ability to respond to cyber

incidents. Cyber exercise manuals, also known as cybersecurity exercise guides, play a critical role in enabling organisations to create effective cyber exercises.

Cyber exercise manuals play a critical role in enabling organisations to develop and implement effective cyber exercises. These manuals provide guidance on the development of cybersecurity scenarios, the selection of appropriate exercise participants, and the implementation of exercises that can test the organisation's cybersecurity readiness. However, despite their importance, there has been limited research on their effectiveness and best practices for their development and use.

Therefore, the motivation for this research paper review is to bridge this gap in knowledge by providing a comprehensive review of the existing literature on cyber exercise manuals. By analysing the current guidelines and identifying gaps in knowledge, this review aims to inform the development and implementation of effective cyber exercise programs and contribute to the ongoing efforts to protect against cyber threats.

The aim of this research paper review is to provide a comprehensive analysis of the existing literature on cyber exercise manuals. Specifically, to identify best practices for the development and implementation of effective cyber exercise programs and to evaluate the effectiveness of current cyber exercise manuals in achieving their intended outcomes.

By synthesising the current research, the aim is to identify gaps in knowledge and areas for future research to enhance the effectiveness of cyber exercise programs.

This work provides guidance to provide guidance to organisations and governments on the development and implementation of cyber exercise programs that can better prepare them for the ever-evolving threat landscape of cyber-attacks.

The guiding research question for this study stems from the lack of research on the effectiveness and best practices of the cyber exercise manuals. The fundamental issue addressed by this study is the analysis of the established cyber exercise guidelines. This study derives criteria for the different phases of the cyber exercises and cross-checks with the guidelines to gather data.

This leads to the main research question of How should a framework look like for designing cyber exercises?

This study reviews different guidelines and try to answer questions such as what are the strengths and weaknesses of different guidelines? How much in-depth coverage does each guide provide for the design phase, conduction phase and evaluation phase?

To answer these questions the paper evaluates the existing literature on cyber exercise manuals, examining the effectiveness of different manuals and identifying best practices for their development and use. The review of cybersecurity exercise manuals involved comparing them based on specific criteria that were derived from this research on taxonomies. These criteria help to gain a comprehensive understanding of the different phases of cybersecurity exercises and provide readers with a wider view of the available manuals. This analysis is crucial in helping readers identify the best manual that matches their specific needs for conducting a successful cybersecurity exercise. Identifies areas where additional research is necessary, such as the creation of standardised evaluation frameworks for cyber exercises and the evaluation of the long-term effectiveness of cyber exercise programs.

The remainder of this thesis is structured as follows:

Chapter 2 provides a comprehensive overview of the research methodologies employed in the study, offering a transparent and rigorous framework for conducting the research and generating reliable findings.

Chapter 3 of the thesis provides an examination of the background information and related work relevant to the research topic.

Chapter 4 of the thesis focuses on the examination of multiple guides.

Chapter 5 of the thesis compares the features provided by the guides.

Chapter 6 of the thesis compares the features provided in the design phase of the guides.

Chapter 7 of the thesis compares the features provided in the conduction phase of the guides.

Chapter 8 of the thesis compares the features provided in the evaluation phase of the guides.

Chapter 9 of the thesis focuses on the examination of multiple after-action reports.

Chapter 10 of the thesis compares several after-action reports.

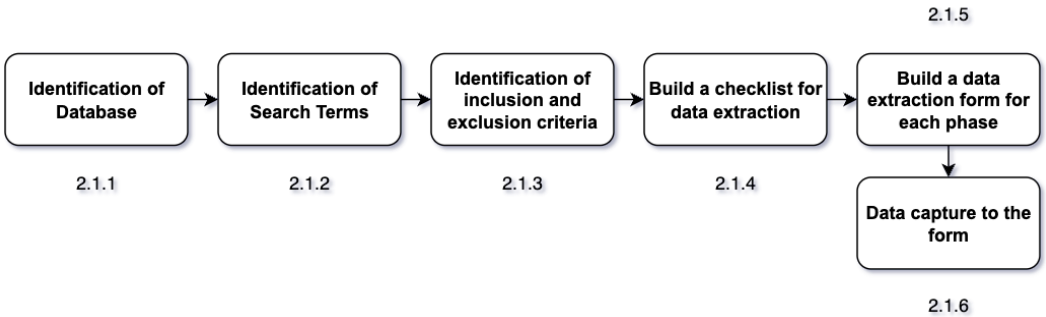
Chapter 11 of the thesis provides a framework for cyber exercise and specifically answers the research question.

Chapter 12 and 13 serves as the concluding section of the thesis, summarising the major findings, discussing their implications, and drawing overall conclusions.

Chapter 14 provides some definitions for some the terms used.

2 Research Method

Figure 2.1 Research method



This study used a literature review methodology, with a qualitative approach to data, to examine the current state of cyber exercise guidelines. The literature review is conducted in several stages, starting with the identification of relevant databases and search terms (as mentioned in 2.1.1 and 2.1.2 in Figure 2.1). The inclusion criteria for studies are established based on the research questions and hypotheses. Only studies published between 2011 and 2022 are included in the review, as this time period provides the most up-to-date information on cyber exercise guidelines.

The search process involves google search engine as well as electronic searches of academic databases such as IEEE Xplore, ACM Digital Library, and Google Scholar. Additional sources, such as industry reports and government publications, are also included in the search. The search results are managed using Zotero, a citation management software, and duplicates are removed.

The inclusion criteria for studies in this literature review were derived from taxonomies and ontologies related to cyber exercise guidelines. These taxonomies and ontologies were used to identify relevant terms and concepts related to cyber exercise guidelines and ensure that the inclusion criteria were comprehensive and consistent.

In conducting the research, reports from 2011 and earlier were excluded, focusing on more recent information. Additionally, guides published by reputable organisations were considered, ensuring a reliable and credible source of information. Non-English guides and reports were excluded from the analysis, as were blogs, newspaper articles, and magazine articles, which may lack the necessary rigor and authority. Reports and guides that did not meet the predetermined criteria for quality and relevance were also excluded, ensuring

that only the most suitable and reliable sources were included in the research (as mentioned in 2.1.3 in Figure 2.1).

Checklists have been developed to establish clear criteria for determining what should be included or excluded. These checklists serve as systematic tool to guide decision-making processes which helps to promote consistency, transparency, and efficiency in decision-making processes (as mentioned in 2.1.4 in Figure 2.1).

The data extraction process is conducted using a data extraction form developed specifically for this study and it is done manually. Data is extracted from the guides and reports based on the inclusion criteria and research questions. The collected data was organised into different categories based on the various stages involved in a cybersecurity exercise such as the design phase, conduction phase, and evaluation phase. This allowed for a more systematic and structured analysis of the information and helped to identify the specific strengths and weaknesses of different guidelines in each phase. When breaking down the data in this way, it is easier to compare and evaluate the effectiveness of different guidelines and determine which one is most suitable for a particular cybersecurity exercise (as mentioned in 2.1.5 and 2.1.6 in Figure 2.1).

This paper is structured as a systematic review that aims to identify the most up-to-date cybersecurity exercise guidelines and offer recommendations to readers on how to choose the most suitable ones. To achieve these objectives, collected data on exercise guidelines from various sources, analysed and categorised the information. The goal was to obtain as much relevant data as possible and present it in a way that can inform readers of the best practices for selecting cybersecurity exercise guidelines.

The study extends to cybersecurity exercises guidelines and national-wide best practices. Furthermore, the study included only exercise guidelines written in English. Google Search was the primary source of information for the exercise guidelines. Relevant literature was identified by searching keywords that identify all sources of information covering cybersecurity exercise guidelines

Search terms:

- “cybersecurity exercise guidelines”
- “cyber exercise guidelines”
- “cyber incident response exercises manuals”
- “cybersecurity tabletop exercises manuals”
- “cybersecurity scenario-based exercises manuals”

- “cybersecurity exercise after action report”
- “cyber exercise after action report”

In addition to collecting information from various sources, also consulted with the supervisor who provided some of the best guides used in the industry. This information was crucial in identifying the most effective cybersecurity exercise guidelines and developing recommendations.

Conducted a thorough search to find relevant taxonomies using popular databases such as IEEE Xplore, ACM Digital Library, and Google Scholar. Leveraging the powerful search functionalities of these databases, helped to find a variety of taxonomies that were applicable to this research on cybersecurity exercise guidelines. The insights gained from these taxonomies helped develop criteria for the guidelines.

Search terms:

- “cyber exercise taxonomies”
- “cybersecurity exercise taxonomies”
- “cyber exercise guidelines taxonomies”

Conducted a thorough search of popular databases such as IEEE Xplore and ACM Digital Library to locate ontologies that could be applicable to this research. While IEEE was the primary source for finding relevant ontologies, also recognised the value of exploring other databases to identify a diverse range of ontologies that could provide additional insights. Hence, also searched the ACM Digital Library to locate different ontologies that could be analysed.

Through the analysis of these ontologies, were able to gain valuable insights that helped to develop criteria for the guidelines.

Search terms:

- “cyber exercise ontologies”
- “cybersecurity exercise ontologies”
- “cyber exercise guidelines ontologies”

3 Background and Related Work

Cyber exercises are essential tools in the field of cybersecurity, allowing organisations to assess and improve their readiness and response capabilities when faced with cyber threats. Guidelines for conducting these exercises are crucial in ensuring their effectiveness and relevance. These guidelines cover the entire process, from designing and executing the exercises to evaluating their outcomes, providing a roadmap for organisations to follow.

Given the increasing frequency and sophistication of cyber-attacks, it has become imperative for organisations to be well-prepared in defending against such threats. Cyber exercises play a vital role in this aspect by helping organisations identify vulnerabilities, test incident response plans, enhance coordination and communication among stakeholders, and bolster overall cybersecurity posture.

As the cyber threat landscape evolves, so do the cyber exercise guidelines. Initially, tabletop exercises involving hypothetical scenarios were common. However, with the advancement of technology and the complexity of cyber-attacks, functional exercises and full-scale simulations have gained prominence, enabling participants to engage in hands-on activities and experience realistic cyber-attack scenarios.

Different types of cyber exercise guidelines exist, each with its specific focus. Some concentrate on exercise design and execution, while others emphasise the evaluation process. Currently, there is a diverse range of cyber exercise guidelines provided by governmental and non-governmental organisations. However, a lack of consensus on effective evaluation methods has resulted in varying practices across organisations.

Cyber exercises offer numerous benefits, including vulnerability identification, strengthened incident response capabilities, and improved collaboration among teams and departments. However, conducting effective exercises poses challenges such as resource allocation, complex scenario design, and ensuring the active participation and engagement of key stakeholders.

Some of the existing work related to this research is explained below,

Brilingaitė, Bukauskas and Juozapavičius [6] presented a framework that aids in the development and assessment of cybersecurity competencies of all teams

during hybrid cyber defence exercises by gathering data about a joint military-civilian cybersecurity exercise.

Chowdhury and Gkioulos [7] proposed a tabletop exercise framework for conducting cybersecurity exercises which is useful for students, security professionals and technical operators.

Patriciu and Furtuna [8] presented a number of steps and guidelines that should be followed when designing a new cybersecurity exercise including defining the objectives, choosing an approach, designing network topology, creating a scenario, establishing a set of rules, choosing appropriate metrics and learning lessons.

Patriciu, Furtuna and Bica [9] presented a step-by-step implementation of a cyber security exercise including design considerations for each of the steps and following a structured approach and can also be used as a guide for institutions who want to organise cyber security exercises for training purposes.

Seker and Ozbenli [10] discussed the concept of cyber defence exercises which are a very important tool when it comes to enhancing the safety awareness of cyberspace, testing an organisation's ability to put up resistance and respond to different cyber events to establish secure environment, gathering empirical data related to security, and looking at the practical training of experts on this subject.

Katt and Yamin [11] developed a software-based solution that helped to model and execute realistic cybersecurity exercise scenarios more efficiently, make cybersecurity exercise models adaptable to changing requirements, highlight operations in cybersecurity exercises that can be executed autonomously to reduce dependability on human teams, understand how much the exercise scenarios improve the skills of cybersecurity exercise participants.

Furtuna [12] discussed in depth about the design and implementation of a cyber defence exercise and closely followed its declared objectives.

Granåsen and Andersson [13] paper evaluated methods for assessing team effectiveness. Analysis results on performance and cognition are also included for a discussion of validity and applicability of the analytic tools and metrics used.

Alothman, Alhajraf, Alajmi, Farraj, Alshareef and Khan [14] presented a solution to enhance the security teams’ cyber-security offensive and defensive skills in the academic domain by facilitating real-life cyber-attack scenarios and hands-on cyber-attack and defence-learning practices.

Čeleda, Čegan, Vykopal and Tovarňák [15] provides a virtualised environment for performing complex cybernetic attacks against a simulated critical infrastructure.

Existing literature on cyber exercise guidelines provides valuable insights into best practices and the experiences of organisations in conducting such exercises. Researchers and cybersecurity experts have developed frameworks and methodologies to guide the planning, execution, and evaluation of cyber exercises.

By reviewing and analysing the existing literature, this thesis aims to offer a comprehensive overview of current best practices, identify gaps or areas for improvement, and provide recommendations to organisations seeking to enhance their cybersecurity preparedness through effective cyber exercises.

4 Cyber Exercise Guidelines

The following subsection briefly describes the most notable 21 cyber exercise guidelines used in the survey.

4.1 Homeland Security Exercise and Evaluation Program (HSEEP)

The Homeland Security Exercise and Evaluation Program (HSEEP) offers a foundational framework of principles that guide exercise programs. It also presents a standardised method for managing programs, designing and developing exercises, their execution, evaluation, and the subsequent planning for improvement. The guide was published in 2020. The guide provides a comprehensive set of tools and materials that can be customised to create a simulated cyber incident scenario and test the organisation's response capabilities. [16]

4.2 The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide

The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide is a resource developed by the Health Information Trust Alliance (HITRUST) and the U.S. Department of Health and Human Services (HHS) to help healthcare organisations test their readiness for a cyber-attack. The guide was published in 2015.

The guide provides step-by-step instructions and guidance for both participants and facilitators of the exercise. The CyberRX 2.0 Level I Playbook exercise simulates a cyber-attack on a healthcare organisation's information systems. The scenario is based on real-world cyber-attacks that have occurred in the healthcare industry and is designed to test the organisation's ability to detect, respond, and recover from a cyber-attack. [17]

4.3 Center for Security Studies Cyber Defense Report

The report is based on research and analysis conducted by the Center for Security Studies (CSS), which is part of the Swiss Federal Institute of Technology Zurich (ETH Zurich), as well as contributions from cybersecurity experts and practitioners from around the world. The report was published in 2018.

The CSS Cyber Defense Report is an annual report that provides an overview of the current state of cybersecurity threats, trends, and challenges facing governments, organisations, and individuals. [18]

4.4 Cyber Exercise Playbook

The cyber exercise playbook was developed by MITRE, a non-profit organisation that operates research and development centres sponsored by the U.S. federal government. It was published in 2014.

The Cyber Exercise Playbook is a comprehensive guide that provides a framework for organisations to plan, design, and execute cybersecurity exercises. The playbook is designed to help organisations improve their incident response capabilities and better prepare for cyber-attacks. [19]

4.5 NCSS Good Practice Guide

National Cyber Security Strategies (NCSS) Good Practice Guide is a publication by the European Union Agency for Cybersecurity (ENISA). The guide was published in 2016.

NCSS Good Practice Guide provides guidance on developing and implementing national cybersecurity strategies (NCSS) in the EU member states. The guide is intended for policymakers, government officials, and other stakeholders involved in the development and implementation of NCSS. [20]

4.6 WHO Simulation Exercise Manual

The WHO Simulation Exercise Manual is a guide developed by the WHO Health Emergencies Programme (WHE) Country Health Emergency Preparedness & IHR (CPI) department, IHR Capacity Monitoring and Evaluation Team (IHR

MEF), with contributions from the WHO regional offices and other headquarters departments to assist countries in conducting simulation exercises for public health emergency preparedness and response.

The manual provides a framework and guidelines for developing, implementing, and evaluating simulation exercises at the national and sub-national levels. [21]

4.7 Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training

Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training is a research paper that presents a meta-level framework for scenario-based training in cybersecurity incident response for organisations. The paper is authored by Ashley O'Neill, Sean B. Maynard, Atif Ahmad, and Justin Filippou.

The framework is designed to provide a comprehensive approach to incident response training that takes into account the technical, organisational, and human factors involved in responding to cybersecurity incidents. [22]

4.8 Healthcare System Cybersecurity Readiness & Response Considerations

Healthcare System Cybersecurity Readiness & Response Considerations is a document developed by the Office of the Assistant Secretary for Preparedness and Response (ASPR) in the U.S. Department of Health and Human Services. The document was originally published in February 2021 and then Updated later in October 2022.

The document provides a comprehensive framework for healthcare organisations to assess their cybersecurity readiness and develop effective strategies for responding to cyber threats and incidents. [23]

4.9 Indiana Emergency Manager Cybersecurity Toolkit

The Indiana Emergency Manager Cybersecurity Toolkit is a comprehensive set of resources developed by the Indiana Office of Technology and the Indiana Department of Homeland Security to help emergency managers in Indiana improve their cybersecurity preparedness. The toolkit was published in October 2019.

The toolkit is designed to provide practical guidance and resources that emergency managers can use to develop and implement effective cybersecurity programs for their organisations.

The toolkit is intended for use by a wide range of organisations, including government agencies, businesses, and non-profit organisations. It provides a practical and comprehensive resource for organisations looking to improve their cybersecurity posture and respond effectively to cybersecurity incidents. [24]

4.10 Instructions for Organising Cyber Exercises - A Manual for cyber exercise organizers

Instructions for Organising Cyber Exercises is a manual developed by the Finnish Transport and Communications Agency (TRAFICOM) to provide guidance and support to organisations in Finland in planning, preparing, and conducting cyber exercises. The manual was published in 2020.

It provides valuable guidance and best practices for organisations looking to improve their cybersecurity readiness through the use of cyber exercises. The manual is specifically tailored to the needs of organisations in Finland. [25]

4.11 The Department of Defense Cyber Table Top Guide

The Department of Defense Cyber Table Top Guide is a resource developed by the United States Department of Defense (DoD) to help organisations conduct tabletop exercises to test their cybersecurity incident response plans. The resource was initially published in 2nd of July 2018 and then revised in 16th September 2021.

The Department of Defense Cyber Table Top Guide is a valuable resource for organisations looking to improve their cybersecurity readiness through tabletop exercises. While the guide is primarily targeted at organisations in the U.S. Department of Defense, the principles and practices described in it can be applied to organisations in other sectors as well. [26]

4.12 A Guide to Cyber Exercises: Plan + Conduct + Evaluate

A Guide to Cyber Exercises: Plan + Conduct + Evaluate is a resource developed by the Victoria State Government in Australia to help organisations plan, conduct, and evaluate tabletop exercises for cybersecurity incident response.

The purpose of this guide is to assist organisations within the Victorian Government in creating and executing efficient cyber exercises. [27]

4.13 How to develop a cyber table top exercise: A Practical Guide

How to Develop a Cyber Security Table-Top Exercise: A Practical Guide is a resource developed by the National Cyber and Information Security Agency of the Czech Republic to help organisations plan and execute tabletop exercises for cybersecurity incident response. The guide was published in 2019.

The target audience of this handbook is individuals who are in charge of safeguarding and managing crucial information infrastructure, significant information systems, or any other type of valuable assets. [28]

4.14 Computer Security Incident Handling Guide

The Computer Security Incident Handling Guide (NIST Special Publication 800-61) is a publication by the National Institute of Standards and Technology (NIST) that provides guidelines for incident response planning, detection, analysis, containment, eradication, and recovery. It was published in 2012.

The guide is intended to be a comprehensive resource for organisations of all sizes and industries to effectively respond to security incidents and protect their

information systems and data. It provides a systematic approach to incident handling, with an emphasis on timely response, effective communication, and continuous improvement. [29]

4.15 Cybersecurity Tabletop Exercise Guide

The Cybersecurity Tabletop Exercise Guide by NARUC (National Association of Regulatory Utility Commissioners) is a publication that provides guidance on how to plan and conduct tabletop exercises to help utilities prepare for respond to cybersecurity threats. The guide was ordinally published in October 2020 and then revised in October 2021.

The guide outlines the benefits of tabletop exercises, describes the planning process, and provides sample scenarios and discussion questions. It emphasises the importance of collaboration and communication among stakeholders, including utility personnel, regulators, and other industry partners. [30]

4.16 Organising A Cyber Crisis Management Exercise

Organising a Cyber Crisis Management Exercise is a guide published by the French National Agency for the Security of Information Systems (ANSSI) to help organisations plan and conduct cyber crisis management exercises. The guide was published in September 2021.

The guide outlines the benefits of exercises and provides guidance on selecting the appropriate exercise type. It serves as a useful resource for organisations looking to enhance their preparedness for cyber crises through the use of exercises. [31]

4.17 Guide To Developing A National Cybersecurity Strategy

The Guide to Developing a National Cybersecurity Strategy was developed by twelve partners, including the NATO CCD COE, to help countries establish and implement their own cybersecurity strategies. The guide provides comprehensive resources and actionable guidance to national leaders and policy-makers. It was published in September 2018.

The guide focuses on strategic engagement as a key component of a national cybersecurity strategy, and provides practical steps for developing a national cybersecurity strategy through collaboration and stakeholder engagement. This guide is a one-stop resource for countries to understand the purpose and content of a national cybersecurity strategy. [32]

4.18 Handbook for planning, running and evaluating information technology and cyber security exercises

The Handbook for Planning, Running, and Evaluating Information Technology and Cyber Security Exercises was written by Nina Wilhelmson and T. Svenssony, Center for Asymmetric Threats Studies (CATS), Swedish National Defence College and it was published by The Swedish National Defence College in 2011.

The handbook provides practical guidance on how to plan, design, and execute effective IT and cybersecurity exercises, as well as how to evaluate their outcomes. The guide is intended for anyone involved in organising or participating in IT and cybersecurity exercises, including government agencies, private sector organisations, and academia. [33]

4.19 Conducting Table-Top Exercises

The Conducting Table-Top Exercises in response to a terror attack at the workplace guide was developed by the Singapore Police Force (SPF) and the Ministry of Manpower (MOM) to provide guidance on conducting table-top exercises for response to a terror attack in a workplace setting.

The guide aims to help organisations develop and enhance their crisis management and emergency response capabilities through the use of table-top exercises. It provides a step-by-step process for planning, conducting, and evaluating table-top exercises, as well as sample scenarios and discussion points for facilitators to use during the exercises. [34]

4.20 Handbook 3: Managing Exercises

The Australian Disaster Resilience Handbook Collection is a series of guides developed to assist in the management of disaster resilience in Australia by the Australian Institute for Disaster Resilience. The third handbook in this collection, "Managing Exercises," provides a comprehensive guide on how to plan, conduct, and evaluate exercises that test disaster response plans. The guide was published in 2012.

The "Managing Exercises" handbook is a valuable resource for anyone involved in disaster resilience and response, providing practical guidance and tools to effectively test and improve disaster response plans. [35]

4.21 Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context

"Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context" is a publication by the Department of Homeland Security. This document provides a framework for conducting cyber wargames that incorporate realistic business contexts. The document was published in 2018.

The main objective of this framework is to enhance the effectiveness of cyber wargames and make them more relevant to the real-world challenges faced by businesses. This is achieved by integrating business processes, operations, and strategies into the design and execution of the wargames. [36]

5 Comparison of Guides

This section compares all the guides on 5 axes:

5.1 the type of exercise supported by the guides

5.2 Is the guideline designed for organisational or nationwide

5.3 the phases covered by the guides

5.4 strengths and weaknesses of the guides

5.5 the type of materials provided by the guides

5.6 the examples and samples provided by the guides.

5.1 Type of exercise

Out of the 21 guides analysed, 15 guides provided recommendations and guidance for conducting tabletop exercises, which are discussion-based exercises that test the response capabilities of organisations in a hypothetical scenario.

Twelve of the guides provided support for functional exercises, which are more complex and involve the deployment of personnel and resources in a simulated scenario.

Finally, ten of the guides provided guidance for conducting full-scale exercises, which are the most comprehensive and realistic type of exercise involving real personnel, equipment, and resources in a real-world scenario.

These findings shown in the Table 5.1 Comparison of guides based on the type of exercise supported, suggest that the majority of the guidelines reviewed prioritise the use of table top and functional exercises, which can provide valuable insights and training without the significant resources required for full-scale exercises.

Table 5.1 Comparison of guides based on the type of exercise supported

No:	Guides	Tabletop Exercise	Functional Exercise	Full-Scale Exercise
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✓	✓
3	Cyber-Report	✓	✓	✓
4	Cyber Exercise Playbook	✓	✓	✓
5	NCSS Good Practice Guide	✗	✗	✗
6	WHO Simulation Exercise Manual	✓	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓	✓
10	A Manual for Cyber Exercise Organisers	✓	✓	✗
11	The Department of Defense Cyber Table Top Guide	✓	✗	✗

12	A Guide to Cyber Exercises	✓	✓	✗
13	How To Develop a Cyber Table Top Exercise	✓	✗	✗
14	Computer Security Incident Handling Guide	✗	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✓	✓
17	Guide To Developing a National Cybersecurity Strategy	✗	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology And Cyber Security Exercises	✓	✓	✓
19	Conducting Table-Top Exercises	✓	✗	✗
20	Handbook 3: Managing Exercises	✓	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✗	✗

5.2 Designed for organisational or nationwide

As shown in the Table 5.2 Guide Comparison: Organisational vs Nation-wide, all 21 guides examined in the analysis were specifically designed to cater to organisational needs in the context of cybersecurity exercises. These guides offer guidance, best practices, and recommendations to assist organisations in planning, conducting, and evaluating their cybersecurity exercises effectively.

Moreover, among the 21 guides, 15 of them extend their support beyond organisational boundaries and provide insights and recommendations for conducting cybersecurity exercises at a national level. These guides take into account the larger scale and complexity of exercises involving multiple organisations, sectors, and critical infrastructure components within a nation. The inclusion of nation-wide support in these guides demonstrates the recognition of the importance of collaborative and coordinated efforts in addressing cybersecurity challenges on a broader scale.

Table 5.2 Guide Comparison: Organisational vs Nation-wide

No:	Guides	Organisational	Nation-wide
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✗
3	Cyber-Report	✓	✓
4	Cyber Exercise Playbook	✓	✓
5	NCSS Good Practice Guide	✓	✓
6	WHO Simulation Exercise Manual	✓	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✓	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✓	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓
10	A Manual for Cyber Exercise Organisers	✓	✓
11	The Department of Defense Cyber Table Top Guide	✓	✗
12	A Guide to Cyber Exercises	✓	✓

13	How To Develop a Cyber Table Top Exercise	✓	✓
14	Computer Security Incident Handling Guide	✓	✓
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising a Cyber Crisis Management Exercise	✓	✓
17	Guide To Developing a National Cybersecurity Strategy	✓	✓
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓	✓
19	Conducting Table-Top Exercises	✓	✓
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✗

5.3 The phases covered by the guides

As shown in the Table 5.3 Comparison based on the phases covered, among the 21 guides analysed, a significant majority of 14 guides provide comprehensive support for all three phases of cybersecurity exercises: the design phase, conduction phase, and evaluation phase. These guides offer detailed recommendations and guidelines for effectively planning, executing, and assessing the various aspects of a cybersecurity exercise.

By covering all three phases, these guides enable organisations to approach their cybersecurity exercises in a systematic and holistic manner. In the design phase, organisations can leverage the guidance to develop exercise objectives, define scenarios, and establish realistic constraints. During the conduction phase, the guides assist in implementing the exercise, coordinating participants, and managing the exercise environment. Finally, in the evaluation phase, organisations can utilise the guidance to assess the exercise outcomes, identify areas for improvement, and develop lessons learned.

Table 5.3 Comparison based on the phases covered

No:	Guides	Design Phase	Conduction Phase	Evaluation Phase
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✓	✓
3	Cyber-Report	✗	✗	✗
4	Cyber Exercise Playbook	✓	✓	✓
5	NCSS Good Practice Guide	✗	✗	✗
6	WHO Simulation Exercise Manual	✓	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework For Scenario-Based Training	✗	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓	✓
10	A Manual for Cyber Exercise Organisers	✓	✓	✓
11	The Department of Defense Cyber Table Top Guide	✓	✓	✓
12	A Guide to Cyber Exercises	✓	✓	✓

13	How To Develop a Cyber Table Top Exercise	✓	✓	✓
14	Computer Security Incident Handling Guide	✗	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✓	✓
17	Guide To Developing a National Cybersecurity Strategy	✗	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology And Cyber Security Exercises	✓	✓	✓
19	Conducting Table-Top Exercises	✓	✓	✓
20	Handbook 3: Managing Exercises	✓	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✗	✗

5.4 Strengths and weaknesses of the guides

5.4.1 Homeland Security Exercise and Evaluation Program (HSEEP)

The "Homeland Security Exercise and Evaluation Program (HSEEP)" stands as a highly comprehensive and invaluable resource, providing excellent guidance for conducting cybersecurity exercises within the healthcare industry. This guide offers a wealth of practical insights and realistic scenarios, allowing healthcare professionals to simulate and respond to cyber threats in a controlled environment.

One of the notable strengths of this guide is its coverage of all phases of the exercise. From the initial planning and design phase to the execution and evaluation phases, the guide ensures that healthcare organisations can effectively navigate each stage of the exercise.

Furthermore, the guide demonstrates a commitment to continuous improvement and knowledge sharing. By actively seeking feedback from the community, it embraces a collaborative approach, incorporating real-world experiences and best practices into its materials.

5.4.2 The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide

One of the standout features of this guide is its detailed coverage of various scenarios. It presents a wide range of realistic situations that participants can encounter, allowing them to immerse themselves in simulated cyber threats and practice their response strategies.

Additionally, the guide excels in its facilitator instructions. It offers a well-structured and comprehensive facilitator guide, ensuring that exercise organisers have the necessary information and tools to effectively plan, execute, and debrief the cybersecurity exercise.

This resource is lacking in the area of comprehensive injects, which are essential to ensure a thorough and realistic exercise. Additionally, it has limited guidance for post-exercise evaluation, which is crucial for identifying areas of improvement and refining the incident response plan.

5.4.3 Center for Security Studies Cyber Defense Report

It stands as an exceptional resource that draws upon the expertise of renowned professionals in the field. Through a meticulous data-gathering process, this report captures valuable insights from these experts.

One of the notable strengths of this report is its thorough analysis of the different types of exercises employed in the realm of cyber defence.

Moreover, the report offers insightful details about the participants involved in these exercises.

5.4.4 Cyber Exercise Playbook

One of the notable strengths of this playbook is its meticulous attention to exercise planning.

The inclusion of numerous samples further enriches the playbook, providing practical examples that organisations can adapt to their specific needs.

However, it is important to note that the playbook may have some limitations in terms of its coverage of the conduction and evaluation phases. While it excels in exercise planning, it may provide less detailed information or explanation in these subsequent phases.

5.4.5 NCSS Good Practice Guide

The "NCSS Good Practice Guide" serves as a pivotal resource in the realm of national cybersecurity strategy, providing valuable guidance on designing and developing robust frameworks to safeguard digital environments.

The guide emphasises the importance of organising cyber exercises, establishing of public-private partnerships, and raising awareness.

5.4.6 WHO Simulation Exercise Manual

It provides explanations of the different phases involved in various types of cybersecurity exercises.

One of the notable strengths of this guide is its inclusion of proper templates. These templates serve as practical tools that organisations can utilise to streamline their exercise planning and execution processes.

However, it is important to note that the guide may have limited guidance specifically focused on the evaluation phase. While it covers the preceding

phases in detail, such as the design and conduction phases, the guidance pertaining to evaluating the effectiveness and outcomes of the exercises may be relatively limited.

5.4.7 Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training

The scenario-based training approach presented in this resource offers a commendable emphasis on incident response, recognising its critical role in effectively addressing and mitigating cyber threats.

One of the notable strengths of this training approach is its method for scenario development. It offers a systematic and structured process that enables organisations to create scenarios that mirror real-world situations.

5.4.8 Healthcare System Cybersecurity Readiness & Response Considerations

One of the notable strengths of this guide is its comprehensive coverage of preparedness, mitigation, and response aspects in cybersecurity. It recognises the importance of addressing these three key areas to effectively combat cyber threats and minimise their impact on organisations.

Firstly, the guide provides valuable insights and guidance on preparedness. It emphasises the significance of proactive measures and planning to enhance an organisation's resilience against potential cyber incidents.

Secondly, the guide offers detailed information on mitigation strategies. It recognises that despite preventive measures, cyber incidents may still occur. Therefore, it emphasises the need for effective mitigation techniques to minimise the potential damage caused by these incidents.

Lastly, the guide delves into the crucial aspect of response. It recognises that a swift and effective response is vital in minimising the impact of cyber incidents.

5.4.9 Indiana Emergency Manager Cybersecurity Toolkit

The exercise planning section of this resource is commendable, offering extensive coverage of various aspects related to designing and organising cybersecurity exercises.

One of the notable strengths of this resource is its comprehensive approach to scenario development. It emphasises the importance of crafting scenarios that

closely resemble real-world cyber incidents, enabling participants to engage in realistic and immersive exercises.

However, it is important to note that the resource may have relatively less focus on the evaluation and improvement phase of the exercises

5.4.10 Instructions for Organising Cyber Exercises - A Manual for cyber exercise organizers

This resource provides a comprehensive and insightful overview of various types of cybersecurity exercises.

The resource delves into the details of exercise planning and demonstrates a strong understanding of the key considerations involved.

Moreover, the resource offers valuable insights into the conduction phase of cybersecurity exercises.

However, it is important to note that the resource may have certain limitations, particularly in terms of the evaluation phase. While it provides an overview of the evaluation process, it may lack in-depth details on measuring exercise performance, capturing lessons learned, and identifying areas for improvement.

Additionally, the resource may benefit from incorporating more scenario examples to enhance its practical applicability.

5.4.11 The Department of Defense Cyber Table Top Guide

This resource stands out for its comprehensive and detailed coverage of the design phase of cybersecurity exercises.

Furthermore, the guide offers valuable insights into the post-exercise analysis and reporting process. It emphasises the importance of evaluating exercise outcomes, capturing lessons learned, and identifying areas for improvement.

However, it is important to note that the resource may have limitations in terms of the availability of scenarios and injects. While it offers detailed explanations of the design and evaluation phases, the specific inclusion of scenario examples and injects may be relatively limited.

5.4.12 A Guide to Cyber Exercises: Plan + Conduct + Evaluate

While this resource provides information on all phases of cybersecurity exercises, it may not offer the level of detailed guidance that some exercise planners may

seek. Although it touches upon each phase, including the design, conduction, and evaluation stages, the resource may not delve deeply into specific methodologies or techniques to navigate these phases effectively.

5.4.13 How to develop a cyber table top exercise: A Practical Guide

This comprehensive guide offers valuable insights into all phases of cybersecurity exercises. It serves as a reliable resource for exercise planners, providing detailed explanations and guidance throughout the entire exercise lifecycle.

One notable strength of this guide is its excellent explanation of the training audience. It recognises the importance of tailoring exercises to specific audiences and provides guidance on how to effectively engage and train participants.

One area that may present limitations is the availability of materials and injects. Exercise planners might find the resource lacking in terms of providing comprehensive materials or specific examples of injects that can enhance the realism and complexity of their exercises.

5.4.14 Computer Security Incident Handling Guide

One of the notable strengths of this guide is its comprehensive approach to incident handling. It takes into account the entire lifecycle of an incident, from initial detection and assessment to containment, eradication, and recovery.

Moreover, the guide emphasises the importance of incident response preparedness, highlighting the significance of developing robust incident response plans, establishing clear roles and responsibilities, and conducting regular training and exercises.

Additionally, the guide underscores the criticality of information sharing in incident response. It emphasises the need for effective communication and collaboration among relevant stakeholders, both within and across organisations.

5.4.15 Cybersecurity Tabletop Exercise Guide

One notable strength of this resource is its provision of practical and user-friendly exercise checklist templates. These templates serve as valuable tools for exercise planners, offering a structured framework to guide them through the process of exercise planning.

Furthermore, the resource offers detailed insights and guidance for the design and conduction phases of cybersecurity exercises. However, one area where the resource could benefit from further development is the evaluation phase.

5.4.16 Organising A Cyber Crisis Management Exercise

One of the notable strengths of this guide is its consistent use of a single example throughout. By presenting a continuous example scenario, the guide helps readers better relate to and visualise the concepts being discussed. This approach enhances the reader's comprehension and allows for a more practical application of the guidelines provided.

However, one area that could be further improved is the coverage of the evaluation phase. While the guide excels in explaining the design, preparation, and conduction phases, it may fall short in providing a comprehensive evaluation procedure.

5.4.17 Guide To Developing A National Cybersecurity Strategy

This resource offers a unique perspective as it has been collaboratively developed by 12 partners, capturing a diverse range of views and expertise. The involvement of multiple stakeholders enhances the credibility and comprehensiveness of the content, providing a well-rounded approach to cybersecurity practices.

One of the notable strengths of this resource is its coverage of Good Practice for Governance, Risk Management, Preparedness, and Resilience. It offers valuable insights and guidelines on how to effectively govern and manage cybersecurity risks within an organisation. It also emphasises the importance of preparedness and resilience, providing practical advice on how to enhance an organisation's ability to prevent, detect, respond to, and recover from cybersecurity incidents.

5.4.18 Handbook for planning, running and evaluating information technology and cyber security exercises

This comprehensive guide provides thorough explanations of all the phases involved in cybersecurity exercises. It offers in-depth insights into the design, preparation, conduction, and evaluation phases, ensuring a holistic understanding of the entire process.

However, one area that could benefit from improvement is the inclusion of examples, scenarios, and injects. These elements play a crucial role in

enhancing the practicality and applicability of the guide. By providing concrete examples, realistic scenarios, and meaningful injects, practitioners can better grasp the concepts and translate them into their own exercise settings.

5.4.19 Conducting Table-Top Exercises

This guide is notable for providing insightful examples that help illustrate the concepts and principles of cybersecurity exercises. These examples serve as valuable reference points for practitioners, offering practical insights into how exercises can be designed and executed effectively.

However, one area where this guide could be further enhanced is in providing more detailed information regarding the conduction and evaluation phases.

5.4.20 Handbook 3: Managing Exercises

This guide provides comprehensive details on all the 3 phases of cyber exercise. One notable strength is the templates provided. These templates helps the organisation as tools to conduct the exercise.

5.4.21 Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context

One of the notable strength of the guide is the details about the different exercises conducted before. And it also explains in-detail about the cyber wargaming Scenarios.

5.5 Type of materials provided by the guide

Out of the 21 guides examined, it was found that 10 of them primarily provide non-editable materials. These non-editable materials offer valuable information, guidance, and best practices related to cybersecurity exercises but may not allow for easy adaptation to specific organisational requirements or preferences.

On the other hand, as shown in Table 5.4 Comparison of guides based on the type of materials provided, only 5 of the guides provide editable materials. These materials are likely in a format that allows organisations to customise and tailor the content to better suit their specific needs. This could include editable templates, checklists, or editable electronic documents that organisations can modify, update, and integrate into their own exercise planning and execution processes.

The availability of editable materials in these guides provides organisations with the flexibility to adapt the content to their unique circumstances, organisational structure, and specific exercise objectives. It allows for a more personalised approach and enables organisations to align the materials with their existing policies, procedures, and documentation.

Table 5.4 Comparison of guides based on the type of materials provided

No:	Guides	Non-Editable Materials	Editable Materials
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✗
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✓	✗
5	NCSS Good Practice Guide	✓	✗
6	WHO Simulation Exercise Manual	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✓	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓
10	A Manual for Cyber Exercise Organisers	✗	✗
11	The Department of Defense Cyber Table Top Guide	✗	✗

12	A Guide to Cyber Exercises	✗	✗
13	How To Develop a Cyber Table Top Exercise	✗	✗
14	Computer Security Incident Handling Guide	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✗	✗
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✗

5.6 Examples and sample questions provided by the guides

As shown in the Table 5.5 Comparison of guides based on the sample questions and examples provided, out of the 21 guides analysed, it was found that 8 of them provide support to organisations by offering sample questions for the participants of cybersecurity exercises. These sample questions serve as valuable resources to guide the facilitators and trainers in designing and conducting effective exercises.

By providing sample questions, these guides help organisations ensure that participants are engaged and actively involved in the exercise. The sample questions can cover a wide range of topics, including incident response procedures, threat detection and analysis, decision-making processes, and communication protocols.

These sample questions serve multiple purposes. Firstly, they help participants understand the objectives and expectations of the exercise, enabling them to focus on relevant aspects of cybersecurity. Secondly, they promote critical thinking and problem-solving skills by challenging participants to analyse and respond to realistic scenarios. Lastly, the sample questions facilitate discussions and knowledge sharing among participants, fostering a collaborative learning environment.

Table 5.5 Comparison of guides based on the sample questions and examples provided

No:	Guides	Sample Questions	Examples
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✓
3	Cyber-Report	✗	✓
4	Cyber Exercise Playbook	✗	✓
5	NCSS Good Practice Guide	✗	✗
6	WHO Simulation Exercise Manual	✗	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓
10	A Manual for Cyber Exercise Organisers	✗	✗
11	The Department of Defense Cyber Table Top Guide	✗	✗

12	A Guide to Cyber Exercises	✗	✗
13	How To Develop a Cyber Table Top Exercise	✓	✓
14	Computer Security Incident Handling Guide	✗	✓
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✓
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✓	✓
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✓

6 Comparison of the design phase

In this section, delve into the crucial design phase of all the guides. The design phase plays a pivotal role in shaping the overall structure and objectives of a cybersecurity exercise. It encompasses the careful planning and formulation of exercise goals, scenarios, and desired outcomes.

Each guide offers valuable insights and recommendations for navigating the design phase effectively. It emphasises the importance of aligning the exercise objectives with the organisation's cybersecurity goals and priorities. Furthermore, it highlights the significance of considering the specific context, resources, and constraints of the organisation when developing the exercise design.

Throughout this phase, attention is given to defining realistic and challenging scenarios that mimic potential cybersecurity threats and incidents. The guides provide guidance on selecting appropriate scenarios and injects that stimulate critical thinking, decision-making, and collaboration among participants. They emphasise the need for well-structured exercise plans that consider various aspects, including exercise duration, participant roles, communication protocols, and technology requirements.

Moreover, the guides emphasise the importance of incorporating a diverse range of stakeholders and subject matter experts during the design phase. By involving key individuals from different departments, organisations, and sectors, the exercise design can benefit from a broader perspective and foster a collaborative approach to cybersecurity preparedness.

Ultimately, the design phase sets the foundation for a successful cybersecurity exercise, ensuring that the objectives are clear, the scenarios are relevant, and the participants are engaged. By following the guidance provided in the respective guides, organisations can develop robust and tailored exercise designs that effectively enhance their cyber resilience and response capabilities.

The comparison of the design phase in the various guides is based on several key criteria. These criteria serve as a framework for evaluating and assessing the effectiveness and comprehensiveness of the design phase in each guide.

The comparison of the guides is based on the following criteria:

6.1 The goals defined by each guide

6.2 Does the guideline support public and private sector participation?

6.3 Do the guidelines specify about participant skill requirements and roles of the participants

6.4 Do the guidelines provide injects, scenarios, and methodologies to develop them

6.5 Structure for Master sheet event list

By considering these criteria, a comprehensive comparison can be made to assess the strengths and weaknesses of each guide's approach to the design phase of cybersecurity exercises. These criteria address important aspects such as goal setting, stakeholder engagement, participant management, scenario development, and documentation, which are vital for effective planning and execution of the exercises.

6.1 Goals defined

As shown in the Table 6.1 Comparison of guides based on the goals defined, among the 21 guides examined, 11 of them prioritise raising awareness among the participants as a key goal. These guides recognise the importance of educating individuals about cybersecurity risks, best practices, and the potential impact of cyber-attacks. By raising awareness, they aim to empower participants to make informed decisions and take proactive measures to protect themselves and their organisations.

Additionally, 13 of the guides focus on improving current policies and practices. They aim to enhance existing cybersecurity policies and frameworks to address emerging threats and challenges. These guides provide recommendations for developing robust cybersecurity strategies, implementing effective risk management measures, and establishing appropriate governance structures.

Furthermore, 16 of the guides emphasise the evaluation of incident response capabilities. They recognise the critical importance of assessing and enhancing an organisation's ability to detect, respond to, and recover from cyber incidents. These guides provide methodologies, frameworks, and assessment criteria to evaluate incident response plans, identify areas for improvement, and strengthen overall incident response capabilities.

The comment columns of the guides reveal additional objectives and focus areas that are highlighted throughout the documents. These objectives and focus areas may vary from guide to guide but often provide valuable insights and perspectives on specific aspects of cybersecurity exercises.

By addressing these goals, the guides contribute to a comprehensive approach to cybersecurity. They aim to foster a culture of awareness, continuous improvement, and resilience in the face of evolving cyber threats. Through education, policy enhancement, and evaluation, these guides strive to empower organisations and individuals to effectively navigate the complex landscape of cybersecurity and mitigate the potential impacts of cyber incidents.

Table 6.1 Comparison of guides based on the goals defined

No:	Guides	Raise Awareness	Improve current policies	Evaluate Incident response	Comments
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓	✓	Enhance roles and responsibilities, Validate plans and procedures, assess types of systems in a defined incident, explore and address cybersecurity challenges
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✓	✓	Improve the maturity of the cyber security program, Engage and educate the executives on cyber security, Establish partnerships across the healthcare industry
3	Cyber-Report	✗	✓	✗	Highlighting and identifying vulnerabilities, procedural flaws and information-sharing mechanisms, ensure readiness in the event of an actual incident occurring, Increase Communication and Co-operation
4	Cyber Exercise Playbook	✓	✓	✓	Determine the effectiveness of the cyber education,

					Assess the organisation's capability to determine operational impacts of cyber attacks, Determine the success of scenario planning and execution between the ECG, RT, and training audience, Understand the implications of losing trust in IT systems and capture the workarounds for such losses, Expose and correct weaknesses in cyber security systems, Determine if the injects meet the objectives of the training
5	NCSS Good Practice Guide	✓	✓	✓	
6	WHO Simulation Exercise Manual	✗	✗	✗	Support decision-making on which type of simulation exercise to use, Support users in key steps in planning, designing, implementing, and evaluating simulation exercises, Provide guidance, templates, tools, and checklists to support exercise implementation, Ensure consistency in conducting and designing exercises
7	Cybersecurity Incident Response in Organisations: A Meta-Level	✗	✗	✓	

	Framework for Scenario-Based Training				
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗	✓	
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓	✓	
10	A Manual for Cyber Exercise Organisers	✗	✓	✓	Developing crisis leadership, Identifying threats, Reporting, Testing communication methods and backup methods
11	The Department of Defense Cyber Table Top Guide	✗	✓	✗	Bridges the gap between the IT and functional mission viewpoints,
12	A Guide to Cyber Exercises	✗	✓	✓	
13	How To Develop a Cyber Table Top Exercise	✓	✓	✓	
14	Computer Security Incident Handling Guide	✗	✗	✓	Detecting, analysing, prioritising, and handling incidents
15	Cybersecurity Tabletop Exercise Guide	✓	✗	✓	Public Affairs, Supporting Recovery, Supporting Service Restoration, Information Sharing

16	Organising a Cyber Crisis Management Exercise	✓	✓	✓	Test the crisis communication strategy, Educating or training staff
17	Guide To Developing a National Cybersecurity Strategy	✗	✗	✗	
18	Handbook For Planning, Running and Evaluating Information Technology And Cyber Security Exercises	✓	✗	✗	Educate by teaching something new to the participants, Test a new organisation, technology, or something else and thereby reveal strengths and weaknesses
19	Conducting Table-Top Exercises	✗	✗	✓	Link up procedures with Police, Roles and responsibilities of all relevant personnel during an attack, Key information that would be useful for Police
20	Handbook 3: Managing Exercises	✓	✓	✓	Practice interoperability, Validate training, Identify gaps, Evaluate equipment, techniques and processes
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✓	✓	

6.2 Public and private sector participation

As shown in the Table 6.2 Comparison of guides based on the private and public sector participation, out of the 21 guides analysed, a significant number of them, specifically 16 guides, offer valuable guidance and recommendations on private sector participation in cybersecurity exercises. These guides recognise the crucial role played by private sector organisations in safeguarding their own networks and assets, as well as contributing to the overall cybersecurity posture of the broader ecosystem.

Additionally, 12 of the guides specifically address the participation of the public sector in cybersecurity exercises. These guides recognise the unique challenges and responsibilities faced by government agencies and public entities in protecting critical infrastructure, sensitive information, and ensuring public safety.

By providing guidance on both private sector and public sector participation, these guides aim to promote a comprehensive and coordinated approach to cybersecurity exercises. They recognise the importance of bridging the gap between different sectors, fostering information sharing, and leveraging the collective expertise and resources available in both the private and public domains. Such guidance serves to strengthen the overall resilience and effectiveness of cybersecurity preparedness and response efforts, ensuring a holistic and collaborative approach to mitigating cyber threats and enhancing the security posture of organisations and the broader community.

Table 6.2 Comparison of guides based on the private and public sector participation

No:	Guides	Private Sector	Public Sector
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✗
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✗	✗
5	NCSS Good Practice Guide	✓	✓
6	WHO Simulation Exercise Manual	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓
10	A Manual for Cyber Exercise Organisers	✓	✗
11	The Department of Defense Cyber Table Top Guide	✓	✓

12	A Guide to Cyber Exercises	✓	✓
13	How To Develop a Cyber Table Top Exercise	✓	✓
14	Computer Security Incident Handling Guide	✓	✓
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓	✗
19	Conducting Table-Top Exercises	✓	✓
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✓

6.3 Participant skill requirements and roles of the participants specified

As shown in the Table 6.3 Comparison of guides based on the specification of participant skill and roles, among the 21 guides examined, it was found that 6 of them provide specific details regarding the required skills and competencies of participants in cybersecurity exercises. These guides recognise the importance of ensuring that participants possess the necessary knowledge, technical expertise, and capabilities to effectively engage in the exercises. By specifying the participant skills, these guides aim to facilitate the selection and preparation of individuals who can contribute effectively to the exercises and enhance the overall learning and improvement outcomes.

Furthermore, 10 of the guides delve into the roles and responsibilities of participants in cybersecurity exercises. These guides highlight the diverse functions and contributions that individuals or teams can play during the exercises. By clarifying the roles, these guides help in assigning responsibilities, fostering collaboration, and ensuring a coordinated and efficient response during the exercises. They also facilitate a better understanding of the various perspectives and expertise that participants bring to the table, thus promoting a holistic and well-rounded exercise experience.

The inclusion of participant skills requirements and roles in these guides reflects the recognition of the crucial role played by individuals in the success of cybersecurity exercises. By providing such guidance, the guides aim to ensure that participants possess the necessary skills, knowledge, and clearly defined roles to effectively contribute to the exercises' objectives, promote effective teamwork, and maximise learning and improvement outcomes.

Table 6.3 Comparison of guides based on the specification of participant skill and roles

No:	Guides	Participant Skill	Participant Roles
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✗	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✓
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✗	✗
5	NCSS Good Practice Guide	✓	✓
6	WHO Simulation Exercise Manual	✗	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✗
10	A Manual for Cyber Exercise Organisers	✗	✗
11	The Department of Defense Cyber Table Top Guide	✓	✓
12	A Guide to Cyber Exercises	✗	✗

13	How To Develop a Cyber Table Top Exercise	✗	✗
14	Computer Security Incident Handling Guide	✓	✓
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising A Cyber Crisis Management Exercise	✗	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✗	✓
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✓

6.4 Injects, scenarios, and methodologies to develop the scenarios specified

As the Table 6.4 Comparison of guides based on the injects, scenarios, and methodologies to develop the scenarios shows, out of the 21 guides examined, it was found that 8 of them offer preparation material injects. These injects serve as valuable resources for the readers, providing them with specific content or information that can be incorporated into the cybersecurity exercises. These materials can include simulated incidents, threat scenarios, or relevant data that add realism and complexity to the exercises. By providing such injects, the guides aim to enhance the quality and effectiveness of the exercises by offering ready-made content that can be tailored to meet specific training objectives or simulation requirements.

Similarly, 8 of the guides provide sample scenarios, which serve as practical examples to help readers grasp the concept and structure of cybersecurity exercises. These scenarios outline a sequence of events, challenges, or incidents that participants may encounter during the exercises. By presenting these sample scenarios, the guides aim to facilitate a better understanding of how to design and develop realistic and engaging exercise scenarios. Readers can draw inspiration from these examples and adapt them to their specific needs, ensuring that the exercises align with their organisation's goals and desired outcomes.

Additionally, 9 of the guides offer methodologies or guidelines on how to build effective exercise scenarios. These methodologies provide step-by-step instructions or frameworks that readers can follow to develop their scenarios from scratch. By providing these methodologies, the guides aim to assist readers in creating robust and engaging scenarios that align with their specific training objectives and simulate realistic cybersecurity incidents.

The inclusion of preparation material injects, sample scenarios, and scenario-building methodologies in these guides reflects the recognition of the importance of well-designed and engaging exercise scenarios in cybersecurity training. By offering these resources, the guides aim to support readers in developing comprehensive and impactful exercises that effectively simulate real-world cybersecurity challenges, enhance participant learning, and improve incident response capabilities.

Table 6.4 Comparison of guides based on the injects, scenarios, and methodologies to develop the scenarios

No:	Guides	Injects	Scenarios	Methodologies
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✓	✗
3	Cyber-Report	✗	✗	✗
4	Cyber Exercise Playbook	✓	✗	✗
5	NCSS Good Practice Guide	✗	✗	✗
6	WHO Simulation Exercise Manual	✗	✗	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗	✓
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✓	✗
10	A Manual for Cyber Exercise Organisers	✗	✗	✓
11	The Department of Defense Cyber Table Top Guide	✗	✗	✗

12	A Guide to Cyber Exercises	✗	✗	✗
13	How To Develop a Cyber Table Top Exercise	✓	✓	✓
14	Computer Security Incident Handling Guide	✗	✓	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✓	✓
17	Guide To Developing a National Cybersecurity Strategy	✗	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗	✗
19	Conducting Table-Top Exercises	✓	✗	✗
20	Handbook 3: Managing Exercises	✗	✗	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✓	✓

6.5 MSEL structure

As show in the Table 6.5 Comparison of guides based on the MSEL structure, among the 21 guides analysed, it was identified that 7 of them provide a structured framework or template for a master sheet event list. This component plays a crucial role in organising and tracking the various events, incidents, or injects that occur during a cybersecurity exercise. The master sheet event list serves as a central reference point for exercise coordinators and facilitators, enabling them to manage the flow of the exercise and ensure that all planned activities are executed smoothly.

The structure provided in these guides for the master sheet event list typically includes columns or sections to capture essential information related to each event. This involve specifying the event type, time of occurrence, description or scenario context, associated objectives or goals, responsible parties or actors, and any additional relevant details. By following this structured format, exercise organisers can effectively document, monitor, and evaluate the progress and outcomes of the exercise.

Having a predefined structure for the master sheet event list brings several advantages. It enhances the overall organisation and coordination of the exercise by providing a systematic approach to manage multiple events concurrently. It also facilitates better communication among exercise participants and stakeholders by offering a common reference point for discussing and analysing events. Furthermore, a structured master sheet event list enables exercise evaluators to assess the participants' responses, performance, and decision-making during the exercise accurately.

By including a template or framework for the master sheet event list, these 7 guides aim to support exercise planners and facilitators in streamlining the execution and management of cybersecurity exercises. This feature provides a valuable resource for maintaining order and coherence throughout the exercise, ensuring that all relevant events are accounted for and properly executed. It ultimately contributes to the overall effectiveness and success of the exercise in achieving its intended training objectives and enhancing cybersecurity preparedness.

Table 6.5 Comparison of guides based on the MSEL structure

No:	Guides	MSEL Structure
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✓
5	NCSS Good Practice Guide	✗
6	WHO Simulation Exercise Manual	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓
10	A Manual for Cyber Exercise Organisers	✓
11	The Department of Defense Cyber Table Top Guide	✗
12	A Guide to Cyber Exercises	✗

13	How To Develop a Cyber Table Top Exercise	✗
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✓
16	Organising a Cyber Crisis Management Exercise	✗
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗
19	Conducting Table-Top Exercises	✗
20	Handbook 3: Managing Exercises	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗

7 Comparison of Conduction Phase

In this section, delve into the comparison of the conduction phase across the different guides. The conduction phase represents the actual implementation and execution of the cybersecurity exercise, where participants engage in various activities to simulate real-world scenarios and test their response capabilities. By examining this phase, gain insights into how each guide approaches and guides the conduction process.

Among the analysed guides, variations can be observed in terms of the level of detail and guidance provided for the conduction phase. Some guides offer comprehensive instructions, providing a step-by-step approach to conducting the exercise. These guides often outline the sequence of events, recommend specific methodologies or techniques, and offer practical tips for facilitating the exercise effectively.

On the other hand, some guides emphasise the importance of maintaining a realistic and immersive exercise environment during the conduction phase. They advocate for creating scenarios and injects that closely mimic actual cyber threats and incidents, ensuring that participants can actively apply their skills and knowledge in a simulated yet lifelike setting.

It is worth noting that while the majority of the guides address the conduction phase, there are instances where the level of guidance provided in this area is relatively limited. These guides focus more on other aspects of the exercise, such as design, planning, or evaluation, and provide less explicit guidance for the actual execution of the exercise.

Overall, the comparison of the conduction phase highlights the diverse approaches and emphasis across the different guides. Exercise planners and facilitators can leverage this information to select a guide that aligns with their specific needs, preferences, and organisational context. By considering the available guidance for the conduction phase, they can ensure a smooth and

effective execution of the cybersecurity exercise, fostering valuable learning experiences and enhancing preparedness in the face of cyber threats.

The criteria used for the comparison are as follows.

7.1 Is there a checklist for the exercise

7.2 Are there forms for the observers and handouts for the participants

7.3 Is there guidance on exercise venue setting and seating charts

7.4 Is there guidance to set up registration facilities

7.5 Is there guidance for testing exercise systems

7.6 Is there guidance for the preparation of key control functions, evaluation functions, and logistics function

7.7 Is there guidance about exercise briefing

7.8 Does the guide suggest preparing supplies and food and refreshments

By comparing the guides based on these criteria, it becomes possible to assess the comprehensiveness and level of guidance provided during the conduction phase of the cybersecurity exercises. These criteria address key aspects that contribute to the smooth and effective execution of the exercise, ensuring that organisers have the necessary tools, resources, and instructions to facilitate a successful and impactful training experience for the participants.

7.1 Checklist for the exercise

As shown in the Table 7.1 Comparison of guides based on the checklist provided, out of the 21 guides analysed, 8 of them include a comprehensive checklist that covers the entire exercise. This checklist serves as a valuable tool for exercise planners and facilitators to ensure that all necessary elements and tasks are addressed throughout the exercise lifecycle.

The inclusion of a checklist in these guides indicates a focus on thorough planning and organisation. The checklist typically outlines key components and considerations for each phase of the exercise, including the design, conduction, and evaluation phases. It serves as a reference point to ensure that critical aspects such as participant coordination, resource allocation, documentation, and logistics are adequately addressed.

By providing a checklist, these guides offer a structured approach to the overall exercise process. It helps exercise planners to stay organised, track progress, and ensure that no important steps or requirements are overlooked. The checklist acts as a guide to facilitate smooth coordination and execution of the exercise, enhancing its effectiveness and efficiency.

Exercise planners can utilise the provided checklist as a starting point and customise it to fit their specific exercise objectives, scope, and requirements. It serves as a valuable tool to ensure consistency and completeness in the planning and execution of cybersecurity exercises.

Having a comprehensive checklist helps exercise planners streamline their efforts, minimise the risk of overlooking crucial elements, and contribute to the overall success of the exercise. It enhances the exercise's readiness, effectiveness, and ability to achieve the desired outcomes.

Therefore, the inclusion of a checklist in 8 out of the 21 guides highlights the importance of a systematic and structured approach to the entire exercise process, contributing to a more organised and successful cybersecurity exercise.

Table 7.1 Comparison of guides based on the checklist provided

No:	Guides	Checklist
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✓
5	NCSS Good Practice Guide	✗
6	WHO Simulation Exercise Manual	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗
10	A Manual for Cyber Exercise Organisers	✗
11	The Department of Defense Cyber Table Top Guide	✗
12	A Guide to Cyber Exercises	✗

13	How To Develop a Cyber Table Top Exercise	✓
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✓
16	Organising A Cyber Crisis Management Exercise	✓
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology And Cyber Security Exercises	✗
19	Conducting Table-Top Exercises	✓
20	Handbook 3: Managing Exercises	✗
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗

7.2 Forms for the observers and handouts for the participants

As shown in the Table 7.2 Comparison of guides based on the observer forms and participant handouts, among the analysed guides, it is notable that 5 of them specifically provide guidance on forms for the observers, while 9 guides offer handouts for the participants. These provisions demonstrate a focus on facilitating effective observation and active participation during cybersecurity exercises.

The inclusion of guidance on forms for observers indicates a recognition of the importance of capturing relevant information and observations during the exercise. These forms serve as structured templates that observers can use to record their observations, document key findings, and provide valuable feedback. By providing such guidance, the guides emphasise the significance of gathering comprehensive data and insights for later analysis and improvement purposes.

On the other hand, the provision of handouts for participants highlights the intention to enhance their engagement and understanding throughout the exercise. These handouts often contain relevant information, instructions, or reference materials that participants can refer to during different phases of the exercise. By offering handouts, the guides aim to provide participants with necessary resources to perform their roles effectively, encourage active involvement, and ensure a shared understanding of the exercise objectives and processes.

Both the observer forms and participant handouts contribute to the overall effectiveness of the cybersecurity exercise. Observer forms enable systematic data collection, while participant handouts facilitate informed and prepared participation.

It is worth noting that while not all guides include specific guidance on observer forms or participant handouts, the 5 guides providing observer forms and 9 guides offering participant handouts demonstrate a recognition of the value in supporting these aspects of the exercise. Exercise planners and facilitators can refer to these guides to leverage the provided resources and tailor them to their specific exercise requirements.

By focusing on the observer experience and participant engagement through forms and handouts, these guides contribute to creating a more structured, organised, and immersive cybersecurity exercise environment.

Table 7.2 Comparison of guides based on the observer forms and participant handouts

No:	Guides	Observer Forms	Participant Handouts
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✓
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✓	✗
5	NCSS Good Practice Guide	✗	✗
6	WHO Simulation Exercise Manual	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✓
10	A Manual for Cyber Exercise Organisers	✗	✗
11	The Department of Defense Cyber Table Top Guide	✗	✓

12	A Guide to Cyber Exercises	✗	✗
13	How To Develop a Cyber Table Top Exercise	✗	✓
14	Computer Security Incident Handling Guide	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology And Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✗	✗
20	Handbook 3: Managing Exercises	✗	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✓

7.3 Exercise venue setting and seating charts

As shown in the Table 7.3 Comparison of guides based on the exercise venue setting and seating charts, out of the 21 guides analysed, it is noteworthy that 10 guides specifically provide guidance on setting up exercise venues. This demonstrates a recognition of the importance of creating an appropriate physical environment to conduct cybersecurity exercises effectively. The inclusion of such guidance emphasises the significance of considering logistical factors in order to facilitate a smooth and successful exercise.

Additionally, among these 10 guides, 3 of them go into further detail by providing a detailed explanation about seating arrangements. This level of specificity suggests a deeper focus on optimising the seating layout and configuration within the exercise venue. The guides that offer this level of guidance understand the impact that seating arrangements can have on communication, collaboration, and overall participant engagement during the exercise.

By providing guidance on setting up exercise venues, the guides aim to ensure that the physical space is conducive to the objectives and requirements of the cybersecurity exercise. This include considerations such as the layout of tables, chairs, and equipment, the arrangement of workstations, the availability of necessary infrastructure (e.g., power outlets, internet connectivity), and the overall ergonomics of the space.

The inclusion of detailed explanations about seating arrangements further underscores the importance of optimising the seating layout to enhance communication and interaction among participants. It takes into account factors such as visibility, accessibility, and the formation of working groups or teams.

It is important to note that while not all guides provide explicit guidance on setting up exercise venues or detailed explanations about seating arrangements, the 10 guides that do offer such guidance provide valuable insights for exercise planners and facilitators. These resources can serve as references to help ensure that the physical aspects of the exercise are well-organised, comfortable, and conducive to achieving the exercise objectives.

By considering the guidance provided in these guides, exercise organisers can create an environment that promotes participant engagement, facilitates effective communication, and ultimately enhances the overall quality and outcomes of cybersecurity exercises.

Table 7.3 Comparison of guides based on the exercise venue setting and seating charts

No:	Guides	Exercise Venue Setting	Seating Charts
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✗
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✓	✗
5	NCSS Good Practice Guide	✗	✗
6	WHO Simulation Exercise Manual	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✗
10	A Manual for Cyber Exercise Organisers	✓	✓
11	The Department of Defense Cyber Table Top Guide	✓	✗

12	A Guide to Cyber Exercises	✓	✗
13	How To Develop a Cyber Table Top Exercise	✗	✗
14	Computer Security Incident Handling Guide	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✗
16	Organising A Cyber Crisis Management Exercise	✓	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✗	✗
20	Handbook 3: Managing Exercises	✓	✗
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✗

7.4 Set up of registration facilities

As shown in the Table 7.4 Comparison of guides based on the registration facilities, among the 21 guides analysed, it is notable that only 2 guides specifically provide guidance about the setup of registration facilities for cybersecurity exercises. While this may seem like a relatively small number, it still demonstrates the recognition of the importance of efficient and well-organised registration processes in the context of conducting such exercises.

The inclusion of guidance on registration facilities suggests that these guides acknowledge the significance of properly managing participant registrations to ensure smooth logistics and effective coordination. Registration facilities typically encompass various elements such as registration desks or booths, sign-in sheets, badges or identification cards, and related administrative processes.

By addressing the setup of registration facilities, these guides aim to assist exercise organisers in efficiently managing participant registrations, which is crucial for maintaining an accurate record of participants, controlling access to exercise venues, and ensuring a smooth flow of activities throughout the exercise.

Although the number of guides providing explicit guidance on registration facilities may be limited, exercise organisers can still benefit from consulting these resources to gain valuable insights and practical recommendations. By leveraging the guidance offered, organisers can optimise the setup of registration facilities and improve the overall efficiency and effectiveness of the cybersecurity exercise.

It is worth noting that while not all guides provide specific guidance on registration facilities, exercise organisers can draw from the expertise and experience shared in the 2 guides that do offer such guidance. Additionally, organisers can also consider general event management principles and best practices to tailor the setup of registration facilities to their specific exercise requirements and objectives.

By ensuring a well-designed and well-executed registration process, exercise organisers can effectively manage participant logistics, enhance security measures, and create a positive experience for all participants involved in the cybersecurity exercise.

Table 7.4 Comparison of guides based on the registration facilities

No:	Guides	Set up registration facilities
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✗
5	NCSS Good Practice Guide	✗
6	WHO Simulation Exercise Manual	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗
10	A Manual for Cyber Exercise Organisers	✗
11	The Department of Defense Cyber Table Top Guide	✗
12	A Guide to Cyber Exercises	✗

13	How To Develop a Cyber Table Top Exercise	✗
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✗
16	Organising a Cyber Crisis Management Exercise	✗
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗
19	Conducting Table-Top Exercises	✗
20	Handbook 3: Managing Exercises	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗

7.5 Testing exercise systems

As shown in the Table 7.5 Comparison of guides based on the testing of exercise systems, out of the 21 guides analysed, approximately 6 of them provide guidance on testing the exercise systems prior to the start of the cybersecurity exercise. This aspect highlights the recognition of the importance of ensuring the functionality and readiness of the systems involved in conducting a successful exercise.

The inclusion of guidance on testing the exercise systems indicates that these guides emphasise the significance of conducting thorough testing procedures to identify and address any potential issues or vulnerabilities before the actual exercise takes place. This proactive approach aims to minimise disruptions during the exercise and ensure the smooth operation of the systems involved.

By emphasising the importance of testing the exercise systems, these guides seek to enhance the overall preparedness and quality of the cybersecurity exercise. Thorough testing helps identify and mitigate potential technical challenges, software glitches, or configuration errors that could impact the exercise's objectives, functionality, or realism.

Exercise organisers and practitioners can benefit from consulting the guides that offer guidance on testing the exercise systems. By following the recommended testing procedures, they can ensure the stability and reliability of the systems, minimise the potential for unforeseen disruptions, and create a more realistic and effective exercise environment.

It is worth noting that while not all guides provide explicit guidance on testing exercise systems, exercise organisers can still draw from the insights and recommendations provided in the 6 guides that do address this aspect. Additionally, exercise organisers should also consider industry best practices, technical expertise, and their specific exercise requirements when designing and implementing the testing procedures for the exercise systems.

By conducting thorough testing of the exercise systems, exercise organisers can enhance the credibility, effectiveness, and overall success of the cybersecurity exercise.

Table 7.5 Comparison of guides based on the testing of exercise systems

No:	Guides	Test exercise systems
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✗
5	NCSS Good Practice Guide	✗
6	WHO Simulation Exercise Manual	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗
10	A Manual for Cyber Exercise Organisers	✗
11	The Department of Defense Cyber Table Top Guide	✓
12	A Guide to Cyber Exercises	✗

13	How To Develop a Cyber Table Top Exercise	✗
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✓
16	Organising a Cyber Crisis Management Exercise	✗
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓
19	Conducting Table-Top Exercises	✗
20	Handbook 3: Managing Exercises	✗
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓

7.6 Preparation of key control functions, evaluation functions, and logistics function

As the Table 7.6 Comparison of guides based on the preparation of key control, evaluation and logistics functions shows, out of the 21 guides analysed, 7 of them provide guidance on control functions, 6 guides offer guidance on evaluation functions, and 8 guides provide guidance on logistics functions. These aspects highlight the recognition of the importance of well-structured control, evaluation, and logistics processes in conducting a successful cybersecurity exercise.

The inclusion of guidance on control functions in 7 of the guides indicates that they emphasise the need for establishing and managing key control mechanisms during the exercise. These controls include protocols for monitoring and regulating the exercise progress, ensuring adherence to predefined objectives and rules, and managing the flow of information and communication among participants.

The 6 guides that provide guidance on evaluation functions underscore the significance of evaluating the exercise's performance, outcomes, and effectiveness. They offer recommendations on developing evaluation criteria, establishing evaluation teams, defining evaluation methodologies, and collecting relevant data for analysis.

Additionally, 8 of the guides offer guidance on logistics functions, which encompass the planning, coordination, and management of various logistical aspects of the cybersecurity exercise.

By providing guidance on control, evaluation, and logistics functions, these guides aim to enhance the overall structure, efficiency, and effectiveness of the cybersecurity exercise. Well-defined control mechanisms facilitate proper exercise management and ensure that participants adhere to the exercise objectives and rules. Effective evaluation functions enable the assessment of the exercise's performance, identification of strengths and weaknesses, and generation of actionable insights for improvement. Efficient logistics functions support the smooth operation and logistical support necessary for the exercise's success.

Exercise organisers can benefit from consulting the guides that offer guidance on control, evaluation, and logistics functions. By following the recommended practices, they can establish robust control mechanisms, conduct comprehensive evaluations, and ensure efficient logistical arrangements. These measures contribute to the overall quality and effectiveness of the cybersecurity exercise.

Table 7.6 Comparison of guides based on the preparation of key control, evaluation and logistics functions

No:	Guides	key control function	Evaluation function	Logistics function
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✗	✗
3	Cyber-Report	✗	✗	✗
4	Cyber Exercise Playbook	✗	✗	✓
5	NCSS Good Practice Guide	✗	✗	✗
6	WHO Simulation Exercise Manual	✓	✓	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✗	✗
10	A Manual for Cyber Exercise Organisers	✗	✗	✗
11	The Department of Defense Cyber Table Top Guide	✓	✓	✓

12	A Guide to Cyber Exercises	✗	✗	✗
13	How To Develop a Cyber Table Top Exercise	✗	✗	✗
14	Computer Security Incident Handling Guide	✗	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓	✓
16	Organising A Cyber Crisis Management Exercise	✓	✗	✓
17	Guide To Developing a National Cybersecurity Strategy	✗	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗	✗
19	Conducting Table-Top Exercises	✗	✗	✗
20	Handbook 3: Managing Exercises	✓	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✓	✓

7.7 Exercise briefing

As the Table 7.7 Comparison of guides based on the exercise briefing shows, among the 21 guides reviewed, 12 of them provide detailed information and guidance on conducting briefings before the cybersecurity exercise takes place. The inclusion of this aspect in a significant number of guides highlights the recognised importance of conducting pre-exercise briefings to ensure effective communication, understanding, and alignment among the participants.

The guides that emphasise the briefing phase recognise that it serves as a crucial opportunity to set expectations, provide essential information, and establish a common understanding of the exercise objectives, rules, and procedures. The briefings typically involve communicating the exercise scenario, outlining the roles and responsibilities of the participants, explaining the exercise timeline and logistics, and clarifying any specific instructions or guidelines relevant to the exercise.

Conducting a thorough pre-exercise briefing helps ensure that all participants are well-informed, aligned, and prepared to actively engage in the exercise. It sets the foundation for a common understanding of the exercise goals, promotes effective communication and collaboration, and helps participants to navigate the exercise scenarios and activities more effectively.

Exercise organisers are encouraged to consult the guides that provide guidance on conducting briefings before the exercise. By following the recommended practices and incorporating relevant briefing elements, they can enhance the overall readiness and engagement of the participants, fostering a more effective and productive cybersecurity exercise.

It is worth noting that while not all 21 guides explicitly address the briefing phase, exercise organisers can still benefit from the insights and recommendations provided in the 12 guides that do cover this aspect. Additionally, exercise organisers should adapt the briefing process to suit their specific exercise objectives, participant requirements, and available resources, ensuring that the briefings are tailored to meet the unique needs of their cybersecurity exercise.

Table 7.7 Comparison of guides based on the exercise briefing

No:	Guides	Exercise Briefing
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✗
5	NCSS Good Practice Guide	✗
6	WHO Simulation Exercise Manual	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗
10	A Manual for Cyber Exercise Organisers	✓
11	The Department of Defense Cyber Table Top Guide	✓
12	A Guide to Cyber Exercises	✓

13	How to Develop a Cyber Table Top Exercise	✓
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✓
16	Organising a Cyber Crisis Management Exercise	✓
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓
19	Conducting Table-Top Exercises	✓
20	Handbook 3: Managing Exercises	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗

7.8 Preparation for supplies, food and refreshments

As the Table 7.8 Comparison of guides based on the supplies and food and refreshments provided shows, out of the 21 guides analysed, 5 of them provide guidance on ensuring the availability of necessary supplies during the cybersecurity exercise. These guides acknowledge the importance of having essential materials, equipment, and resources readily accessible to support the smooth execution of the exercise. The guidance includes recommendations on identifying and procuring relevant supplies such as stationery, communication tools, technical equipment, or any other materials specific to the exercise requirements.

Furthermore, among the reviewed guides, 3 of them specifically address the provision of food and refreshments during the exercise. These guides recognise that the participants' physical well-being and comfort play a vital role in their overall engagement and performance during the exercise. The provided guidance cover aspects such as planning meals, accommodating dietary restrictions or preferences, organising breaks, and ensuring an adequate supply of refreshments to keep participants energised and focused.

It is essential for exercise organisers to consider the scale, duration, and specific requirements of their cybersecurity exercise when planning for supplies, food, and refreshments. The guidance provided in the applicable guides can serve as a valuable reference to help organisers create a comfortable and conducive environment for participants, ultimately contributing to the effectiveness and success of the exercise.

Table 7.8 Comparison of guides based on the supplies and food and refreshments provided

No:	Guides	Supplies	Food and Refreshments
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✗
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✗	✗
5	NCSS Good Practice Guide	✗	✗
6	WHO Simulation Exercise Manual	✗	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✗
10	A Manual for Cyber Exercise Organisers	✓	✓
11	The Department of Defense Cyber Table Top Guide	✗	✗

12	A Guide to Cyber Exercises	✓	✗
13	How To Develop a Cyber Table Top Exercise	✗	✗
14	Computer Security Incident Handling Guide	✗	✗
15	Cybersecurity Tabletop Exercise Guide	✓	✓
16	Organising a Cyber Crisis Management Exercise	✓	✗
17	Guide to Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✗	✗
20	Handbook 3: Managing Exercises	✗	✗
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✗

8 Comparison of Evaluation Phase

In this section, delve into the comparison of the evaluation phase across the different guides. The evaluation phase plays a critical role in assessing the effectiveness of the cybersecurity exercise and identifying areas for improvement. By examining this phase, gain insights into how each guide approaches and guides the evaluation process.

When analysing the evaluation phase, it becomes apparent that there is variation in the level of detail and guidance provided by the different guides. Some guides offer comprehensive frameworks and methodologies for evaluating exercise outcomes. These guides emphasise the importance of defining clear evaluation criteria, collecting relevant data, and employing appropriate analysis techniques. Provide templates or tools to facilitate the evaluation process, enabling exercise organisers to systematically assess the performance of participants, systems, and processes.

It is important to note that while many guides address the evaluation phase, there are instances where the level of guidance provided in this area is relatively limited. Some guides place greater emphasis on the design, planning, or execution of the exercise, and provide less explicit guidance for the evaluation process. In such cases, exercise organisers are encouraged to adapt and tailor evaluation approaches based on best practices and their specific objectives.

Furthermore, several guides highlight the importance of continuous improvement and follow-up actions based on the evaluation findings. They emphasise the need for incorporating feedback into future exercises, updating policies and procedures, and enhancing overall cybersecurity posture.

By comparing the evaluation phase across the guides, exercise planners and facilitators can gain valuable insights and guidance for effectively assessing the outcomes of the cybersecurity exercise. They can select approaches and techniques that align with their goals, resources, and organisational context,

ultimately driving continuous improvement and strengthening their overall cyber resilience.

The criteria used for the comparison are as follows

8.1 Is there a structure for After Action Report

8.2 Is there metrics stated for the evaluation

8.3 Does the guide provide guidance on public and private dissemination

8.4 Does the guide provide guidance on the evaluation of plan, policy and procedure

8.5 Does the guide provide guidance on the evaluation of agreement and skills

By comparing the evaluation phase across the guides based on these criteria, exercise planners and evaluators can gain insights into the level of detail, guidance, and emphasis placed on each aspect of the evaluation process. This allows for informed decision-making when selecting a guide that aligns with their specific evaluation requirements and objectives.

8.1 Structure for After Action Report

As the Table 8.1 Comparison of guides based on the AAR structure provided shows, out of the 21 guides analysed, 9 of them provide a structured approach or framework for creating an After Action Report (AAR) during the evaluation phase. An AAR is a comprehensive document that captures the key observations, findings, and recommendations derived from the exercise evaluation. It serves as a valuable tool for documenting lessons learned, identifying strengths and areas for improvement, and guiding future exercises and incident response efforts.

The guides that offer a structured approach for the AAR typically outline the key sections or components that should be included in the report. This includes sections such as executive summary, exercise objectives, methodology, observed strengths and weaknesses, identified issues or gaps, recommended actions, and an appendix with supporting documentation or evidence. By providing a predefined structure, these guides help ensure that the AAR is comprehensive, consistent, and focused on capturing essential information.

Having a structured AAR is beneficial for several reasons. It promotes a systematic and organised approach to evaluating the exercise, ensuring that all relevant aspects are adequately addressed. It enables easy sharing and dissemination of evaluation findings to relevant stakeholders. It also facilitates the review and comparison of AARs across different exercises, allowing for the identification of trends, common challenges, and best practices.

Exercise planners and evaluators can consider the availability of a structured AAR framework when selecting a guide that aligns with their evaluation needs. Such a framework can streamline the AAR development process, enhance the quality and usefulness of the report, and support effective learning and improvement in cybersecurity preparedness and response efforts.

Table 8.1 Comparison of guides based on the AAR structure provided

No:	Guides	AAR Structure
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✓
5	NCSS Good Practice Guide	✓
6	WHO Simulation Exercise Manual	✓
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✓
10	A Manual for Cyber Exercise Organisers	✗
11	The Department of Defense Cyber Table Top Guide	✗
12	A Guide to Cyber Exercises	✗

13	How To Develop a Cyber Table Top Exercise	✗
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✓
16	Organising a Cyber Crisis Management Exercise	✓
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓
19	Conducting Table-Top Exercises	✗
20	Handbook 3: Managing Exercises	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗

8.2 Is there metrics stated for the evaluation

As the Table 8.2 Comparison of guides based on the metrices for evaluation shows, out of the 21 guides analysed, 8 of them include metrics or criteria for evaluating the effectiveness and performance of cybersecurity exercises during the evaluation phase. These metrics serve as measurable indicators or benchmarks to assess the achievement of exercise objectives, measure the capabilities of participants, and identify areas for improvement.

The guides that provide metrics for evaluation typically define specific performance indicators or criteria that can be used to evaluate various aspects of the exercise. By incorporating metrics into the evaluation process, these guides enable a more objective and systematic assessment of exercise performance.

Having defined metrics for evaluation offers several benefits. It allows exercise planners and evaluators to set clear expectations and standards for performance, enabling a more consistent and structured evaluation process. It facilitates the collection of quantitative data that can be analysed to assess the strengths and weaknesses of the exercise and identify areas that require improvement. It also supports the establishment of baselines and allows for the comparison of performance across different exercises or iterations.

When selecting a guide for conducting cybersecurity exercises, exercise planners should consider whether it provides relevant metrics for evaluation that align with their exercise goals and objectives. The availability of metrics can enhance the evaluation process, provide valuable insights into exercise performance, and help drive continuous improvement in cybersecurity preparedness and response capabilities.

Table 8.2 Comparison of guides based on the metrics for evaluation

No:	Guides	Metrics for Evaluation
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✗
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗
3	Cyber-Report	✗
4	Cyber Exercise Playbook	✗
5	NCSS Good Practice Guide	✓
6	WHO Simulation Exercise Manual	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗
10	A Manual for Cyber Exercise Organisers	✗
11	The Department of Defense Cyber Table Top Guide	✓
12	A Guide to Cyber Exercises	✗

13	How To Develop a Cyber Table Top Exercise	✓
14	Computer Security Incident Handling Guide	✗
15	Cybersecurity Tabletop Exercise Guide	✓
16	Organising A Cyber Crisis Management Exercise	✓
17	Guide To Developing a National Cybersecurity Strategy	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓
19	Conducting Table-Top Exercises	✗
20	Handbook 3: Managing Exercises	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗

8.3 Public and private dissemination

AS the Table 8.3 Comparison of guides based on the private and public dissemination shows, among the 21 guides analysed, 17 of them offer guidance on the private dissemination of information obtained during the evaluation phase of cybersecurity exercises. Private dissemination refers to the sharing of evaluation findings, insights, and lessons learned within a limited and controlled audience, typically within the organisation or participating stakeholders.

These guides recognise the importance of sharing evaluation outcomes with relevant parties in order to facilitate organisational learning, improve response capabilities, and drive corrective actions. They provide guidance on the appropriate channels, methods, and formats for sharing evaluation reports, after-action reviews, and other evaluation findings within the private sphere. This involve distributing reports to key personnel, conducting debriefings and workshops, or utilising internal communication platforms for knowledge transfer.

On the other hand, 5 out of the 21 guides also provide guidance on the public dissemination of evaluation results. Public dissemination involves sharing evaluation findings, best practices, and lessons learned with a broader audience beyond the organisation or participating entities. This include sharing insights with industry forums, conferences, or publishing reports for public access.

The guides that offer guidance on public dissemination recognise the value of sharing evaluation outcomes with the wider cybersecurity community to promote transparency, collaboration, and knowledge exchange. They provide recommendations on anonymizing sensitive information, adhering to data protection regulations, and leveraging appropriate platforms for sharing evaluation reports and insights in the public domain.

When selecting a guide for conducting cybersecurity exercises, exercise planners should consider their organisation's specific needs and objectives regarding the dissemination of evaluation outcomes. Guides that provide comprehensive guidance on both private and public dissemination can offer valuable support in effectively sharing evaluation findings to drive improvements in cybersecurity practices and foster collaboration within the broader cybersecurity community.

Table 8.3 Comparison of guides based on the private and public dissemination

No:	Guides	Private Dissemination	Public Dissemination
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✓	✗
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✓	✗
5	NCSS Good Practice Guide	✓	✗
6	WHO Simulation Exercise Manual	✓	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✓	✓
9	Indiana Emergency Manager Cybersecurity Toolkit	✓	✗
10	A Manual for Cyber Exercise Organisers	✓	✗
11	The Department of Defense Cyber Table Top Guide	✓	✗

12	A Guide to Cyber Exercises	✗	✗
13	How To Develop a Cyber Table Top Exercise	✓	✗
14	Computer Security Incident Handling Guide	✓	✓
15	Cybersecurity Tabletop Exercise Guide	✓	✗
16	Organising a Cyber Crisis Management Exercise	✓	✗
17	Guide To Developing a National Cybersecurity Strategy	✓	✓
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✓	✗
19	Conducting Table-Top Exercises	✗	✗
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✓	✗

8.4 Evaluation of plan, policy and procedure

In the evaluation phase of cybersecurity exercises, it is crucial to assess various aspects of the organisation's cybersecurity framework, including plans, policies, and procedures. As shown in the Table 8.4 Comparison of guides based on the plan, policy and procedure evaluation, among the 21 guides examined, 7 of them specifically address the evaluation of plans. These guides provide guidance on how to assess the effectiveness, completeness, and suitability of cybersecurity plans considering the exercise objectives and identified vulnerabilities. They outline criteria, checklists, or evaluation methodologies to support the evaluation process.

Furthermore, 3 out of the 21 guides focus on evaluating policies during the evaluation phase. These guides emphasise the importance of evaluating the organisation's cybersecurity policies to ensure they align with industry best practices, regulatory requirements, and exercise objectives. They provide evaluation criteria, guidelines, or tools to assess policy compliance, clarity, and effectiveness in addressing cybersecurity risks.

Similarly, 7 out of the 21 guides include guidance on evaluating procedures as part of the evaluation phase. These guides emphasise the assessment of operational procedures, response protocols, and incident handling processes. They provide evaluation frameworks, checklists, or scenarios to evaluate the adequacy, efficiency, and consistency of procedures in addressing simulated cyber incidents during the exercise.

By evaluating plans, policies, and procedures, organisations can identify areas for improvement, gaps in their cybersecurity framework, and potential vulnerabilities. This evaluation helps in refining and enhancing the organisation's response capabilities, ensuring that plans are effective, policies are comprehensive, and procedures are robust.

Exercise planners and evaluators can benefit from selecting guides that provide specific guidance on evaluating plans, policies, and procedures, as these guides offer a structured approach and evaluation criteria tailored to these key components of the cybersecurity framework.

Table 8.4 Comparison of guides based on the plan, policy and procedure evaluation

No:	Guides	Plan Evaluation	Policy Evaluation	Procedure Evaluation
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✗	✗
3	Cyber-Report	✗	✗	✗
4	Cyber Exercise Playbook	✗	✗	✗
5	NCSS Good Practice Guide	✓	✗	✓
6	WHO Simulation Exercise Manual	✗	✗	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✗	✗
10	A Manual for Cyber Exercise Organisers	✗	✗	✗
11	The Department of Defense Cyber Table Top Guide	✗	✗	✗

12	A Guide to Cyber Exercises	✓	✓	✓
13	How To Develop a Cyber Table Top Exercise	✓	✗	✓
14	Computer Security Incident Handling Guide	✓	✗	✓
15	Cybersecurity Tabletop Exercise Guide	✓	✗	✓
16	Organising a Cyber Crisis Management Exercise	✗	✗	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗	✗
19	Conducting Table-Top Exercises	✗	✗	✗
20	Handbook 3: Managing Exercises	✓	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✗	✗

8.5 Evaluation of agreement and skills

Within the evaluation phase of cybersecurity exercises, the assessment of agreements and skills plays a significant role in ensuring comprehensive and effective cybersecurity practices. As the Table 8.5 Comparison of guides based on the agreement and skill evaluation shows, among the 21 guides examined, 4 of them focus on evaluating agreements as part of the evaluation process. These guides emphasise the assessment of agreements, contracts, or partnerships related to cybersecurity, such as information-sharing agreements, mutual aid agreements, or public-private collaborations.

Furthermore, 7 out of the 21 guides highlight the evaluation of skills during the evaluation phase. These guides emphasise the assessment of personnel capabilities, technical proficiencies, and cybersecurity skills required to effectively respond to cyber threats and incidents. Evaluating skills helps identify skill gaps, training needs, and opportunities for improvement to enhance the overall cybersecurity posture.

By evaluating agreements and skills, organisations can ensure that their collaborative efforts and partnerships are robust, well-defined, and aligned with cybersecurity objectives. Additionally, assessing skills enables organisations to identify strengths and weaknesses in their workforce's capabilities, allowing for targeted training programs and skill development initiatives.

Exercise planners and evaluators should consider guides that provide specific guidance on evaluating agreements and skills, as these guides offer insights into assessing the effectiveness of partnerships and the competence of personnel. Such evaluations contribute to enhancing the organisation's ability to respond to cyber incidents, foster information sharing, and build a skilled cybersecurity workforce.

Table 8.5 Comparison of guides based on the agreement and skill evaluation

No:	Guides	Agreement Evaluation	Skills Evaluation
1	Homeland Security Exercise and Evaluation Program (HSEEP)	✓	✓
2	The CyberRX 2.0 Level I Playbook Participant and Facilitator Guide	✗	✗
3	Cyber-Report	✗	✗
4	Cyber Exercise Playbook	✗	✗
5	NCSS Good Practice Guide	✗	✓
6	WHO Simulation Exercise Manual	✗	✗
7	Cybersecurity Incident Response in Organisations: A Meta-Level Framework for Scenario-Based Training	✗	✗
8	Healthcare System Cybersecurity Readiness & Response Considerations	✗	✗
9	Indiana Emergency Manager Cybersecurity Toolkit	✗	✗
10	A Manual for Cyber Exercise Organisers	✗	✗
11	The Department of Defense Cyber Table Top Guide	✗	✗

12	A Guide to Cyber Exercises	✓	✓
13	How To Develop a Cyber Table Top Exercise	✗	✓
14	Computer Security Incident Handling Guide	✓	✓
15	Cybersecurity Tabletop Exercise Guide	✗	✓
16	Organising a Cyber Crisis Management Exercise	✗	✗
17	Guide To Developing a National Cybersecurity Strategy	✗	✗
18	Handbook For Planning, Running and Evaluating Information Technology and Cyber Security Exercises	✗	✗
19	Conducting Table-Top Exercises	✗	✗
20	Handbook 3: Managing Exercises	✓	✓
21	Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context	✗	✗

9 After Action Reports

The following subsection briefly describes the most notable 9 After action report guidelines used in the survey.

9.1 Cyber Storm VIII: After-Action Report

Cyber Storm VIII: After-Action Report summarises the findings and lessons learned from Cyber Storm VIII, conducted by the U.S. Department of Homeland Security. The exercise is held in March 2022 and report is published in August 2022.

The report makes recommendations to improve planning, information sharing, coordination, and public-private partnerships to strengthen the nation's cyber resilience. [37]

9.2 Cyber Europe 2022: After Action Report

The Cyber Europe 2022: After Action Report provides key findings and lessons learned from the Cyber Europe 2022 cybersecurity exercise organised by the European Union Agency for Cybersecurity (ENISA). It is published in December 2022.

The report is aimed at both the public and private sectors from the EU and EFTA Member States. [38]

9.3 Pre-Symposium Cyber TTX AAR

Pre-Symposium Cyber Tabletop Exercise After action report/ Improvement plan provides key findings and lessons learned from the Pre-Symposium Cyber Tabletop exercise organised by the U.S. Department of Homeland Security. The report was published in October 2021.

The report makes recommendations for preparedness, response, and recovery. [39]

9.4 NYS Healthcare Cybersecurity Exercise AAR

New York State Healthcare Cybersecurity Exercise After Action Report provides key findings and lessons learned from the New York State Healthcare Cybersecurity Exercise hosted by the Greater New York Hospital Association and Healthcare Association of New York State. The report was published in May 2017.

The report makes recommendations for planning, information sharing, operational coordination, and public messaging. [40]

9.5 State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR

State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise After Action report provides key findings and lessons learned from Oregon Gremlins in the Gears Cybersecurity Tabletop Exercise/Functional Exercise hosted by DHS Cybersecurity and Infrastructure Security Agency (CISA). The report was published in March 2022.

The report makes recommendations for operational communications, operation coordination, and cybersecurity. [41]

9.6 Quantum Dawn VI AAR

Quantum Dawn After Action report provides key findings and lessons learned from SIFMA's global Quantum Dawn VI exercise hosted by the Securities Industry and Financial Markets Association (SIFMA) on November 2021. [42]

9.7 Baltic Cyber Shield Cyber Defence Exercise AAR

Baltic Cyber Shield Cyber Defence Exercise After Action report provides key findings and lessons learned from Baltic Cyber Shield (BCS). The exercise was organised in collaboration with several organisations coordinated by the Cooperative Cyber Defence Centre of Excellence (CCDCOE) and Swedish National Defence College (SNDC) in 2010. [43]

9.8 NISÖ AAR

The National Cyber Security Exercise series (NISÖ) After Action report provides key findings and lessons learned from The National Cyber Security Exercise series (NISÖ). The exercise was organised The Swedish Civil Contingencies Agency (MSB).

It aims to strengthen Sweden’s crisis management capability and its capability to manage major IT-related crises and collaboration in the crisis management system.[44]

10 Comparison of After-Action Reports

This section compares the after-action reports (AARs) across the different exercises. The AAR is a crucial component of the evaluation phase in cybersecurity exercises, as it provides a comprehensive analysis of the exercise outcomes, observations, and recommendations for improvement. Examination of the AARs gives insights into how each guide approaches and structures the reporting process.

When comparing the AARs, it becomes apparent that there is variation in the level of detail, structure, and content for different exercises. These exercises outline sections such as executive summary, exercise objectives, methodology, findings, recommendations, and lessons learned. It emphasise the importance of a structured approach to ensure consistency and facilitate the effective communication of evaluation outcomes.

Exercise planners and evaluators should consider the available guidance on AARs when selecting a guide that aligns with their reporting requirements and organisational context. By following established frameworks and incorporating best practices, exercise organisers can ensure the creation of comprehensive, insightful, and actionable AARs that drive continuous improvement and enhance cybersecurity preparedness.

The criteria used for the comparison are as follows

10.1 Focuses on the goals

10.2 Inclusion of key findings, key observations, and key achievements

10.3 Covered design phase, overview, and outcome of the design phase

10.4 Covered conduction phase, overview, and outcome of the conduction phase

10.5 Covered evaluation phase, overview, and outcome of the evaluation phase

10.6 Includes participant list

10.1 Focuses on the goals

As the Table 10.1 Comparison of AAR based on the goals shows, out of the 8 analysed after-action reports (AARs), 6 of them have the goal of information sharing as a prominent objective. These AARs recognise the importance of sharing evaluation findings, lessons learned, and best practices with relevant stakeholders to facilitate knowledge exchange, enhance collective understanding, and promote collaboration in the cybersecurity domain.

Furthermore, 7 of the AARs aim to evaluate the effectiveness of plans and policies. These reports focus on assessing the alignment, comprehensiveness, and suitability of existing plans and policies in addressing cybersecurity challenges and achieving exercise objectives. By evaluating plans and policies, these AARs provide valuable insights into areas that require improvement or enhancement to ensure more effective incident response and cybersecurity governance.

Moreover, 6 of the AARs focus on fostering public and private partnerships. These reports highlight the importance of collaboration, coordination, and information sharing between public and private entities in responding to cyber threats. By emphasising the evaluation of partnerships, these AARs aim to strengthen the collaborative approach to cybersecurity, promote shared responsibilities, and enhance the collective resilience of the cybersecurity ecosystem.

Table 10.1 Comparison of AAR based on the goals

No:	Guides	Information Sharing	Evaluate Effectiveness Of Plan And Policies	Foster Public And Private Partnerships
1	Cyber Storm VIII: After-Action Report	✓	✓	✓
2	CYBER EUROPE 2022: AFTER ACTION REPORT	✓	✓	✗
3	Pre-Symposium Cyber TTX	✗	✓	✗
4	NYS Healthcare Cybersecurity Exercise AAR	✓	✓	✓
5	State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR	✗	✓	✓
6	QUANTUM DAWN VI AAR	✓	✓	✓
7	Baltic Cyber Shield Cyber Defence Exercise AAR	✓	✗	✓
8	NISÖ AAR	✓	✓	✓

10.2 Inclusion of key findings, key observations, and key achievements

As the Table 10.2 Comparison of AAR based on the key findings, key observations and key achievements shows, out of the 8 After Action Reports (AARs) analysed, 5 of them provide a detailed explanation of the key findings derived from the evaluation of the cybersecurity exercises. These reports aim to identify and articulate the main discoveries, lessons learned, and areas of improvement that emerged during the exercise. By highlighting the key findings, these AARs enable stakeholders to gain insights into the strengths, weaknesses, and critical aspects that need attention in future exercises and cybersecurity practices.

Additionally, 3 of the AARs focus on explaining the key observations made during the evaluation. These reports emphasise the significant points, patterns, or trends observed throughout the exercise that provide valuable insights into the performance, effectiveness, and challenges encountered by the participants and systems involved. By highlighting key observations, these AARs enable stakeholders to understand the exercise dynamics and derive actionable insights for enhancing preparedness and response capabilities.

Furthermore, 3 of the AARs emphasise the key achievements resulting from the cybersecurity exercises. These reports highlight the successful outcomes, milestones, or positive aspects that were accomplished during the exercise. By acknowledging key achievements, these AARs not only celebrate the accomplishments but also serve as motivation for future exercises and foster a culture of continuous improvement and excellence.

The distinction between key findings, key observations, and key achievements in these AARs ensures a comprehensive and balanced understanding of the exercise outcomes.

Table 10.2 Comparison of AAR based on the key findings, key observations and key achievements

No:	Guides	Key Findings	Key observations	Key achievements
1	Cyber Storm VIII: After-Action Report	✓	✓	✓
2	CYBER EUROPE 2022: AFTER ACTION REPORT	✓	✗	✓
3	Pre-Symposium Cyber TTX	✓	✓	✗
4	NYS Healthcare Cybersecurity Exercise AAR	✗	✓	✓
5	State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR	✓	✗	✗
6	QUANTUM DAWN VI AAR	✓	✗	✗
7	Baltic Cyber Shield Cyber Defence Exercise AAR	✗	✗	✗
8	NISÖ AAR	✗	✗	✗

10.3 Covered design phase, overview and outcome of the design phase

As the Table 10.3 Comparison of AAR based on the design phase coverage shows, out of the 8 After Action Reports (AARs) examined, 5 of them provide coverage of the design phase of the cybersecurity exercises. These reports delve into the specifics of the design phase, highlighting the process, considerations, and decisions that went into crafting the exercise. By covering the design phase, these AARs offer insights into the foundational aspects of the exercise and provide a comprehensive understanding of how the exercise was structured.

Additionally, 2 of the AARs offer an overview or summary of the design phase. Rather than providing an in-depth analysis, these reports provide a high-level view of the design phase, outlining the key elements, approach, and considerations taken into account during the exercise design. While they may not provide extensive details, they still offer valuable insights into the design phase and its role in shaping the overall exercise.

Furthermore, only 1 of the AARs covers the design phase outcome specifically. It assesses whether the design phase objectives were met, the appropriateness of the scenario, and the alignment of the exercise design with the desired outcomes. By examining the design phase outcome, this AAR provides valuable feedback on the effectiveness of the design process and its impact on the exercise.

Table 10.3 Comparison of AAR based on the design phase coverage

No:	Guides	Design phase	Design phase Overview	Design phase Outcome
1	Cyber Storm VIII: After-Action Report	✓	✓	✓
2	CYBER EUROPE 2022: AFTER ACTION REPORT	✗	✗	✗
3	Pre-Symposium Cyber TTX	✗	✗	✗
4	NYS Healthcare Cybersecurity Exercise AAR	✓	✗	✗
5	State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR	✓	✓	✗
6	QUANTUM DAWN VI AAR	✗	✗	✗
7	Baltic Cyber Shield Cyber Defence Exercise AAR	✓	✗	✗
8	NISÖ AAR	✓	✗	✗

10.4 Covered conduction phase, overview, and outcome of the conduction phase

As the Table 10.4 Comparison of AAR based on the conduction phase coverage shows, out of the 8 After Action Reports (AARs) examined, 4 of them provide coverage of the conduction phase of the cybersecurity exercises. These reports offer detailed insights into the execution, management, and operations during the conduction phase. They discusses the activities, actions, and events that took place, as well as the challenges, successes, and lessons learned encountered during this phase. By covering the conduction phase, these AARs provide valuable information about the actual implementation and execution of the exercise.

Additionally, 2 of the AARs offer an overview or summary of the conduction phase. Instead of delving into the details, these reports provide a high-level view of the conduction phase, outlining the key elements, approach, and considerations taken into account during the exercise execution. While they may not provide extensive information, they still provide a broad understanding of the conduction phase and its role in the overall exercise process.

Furthermore, 2 of the AARs specifically cover the outcome of the conduction phase. These reports focus on evaluating the results, effectiveness, and impact of the conduction phase on the overall success of the exercise. They assesses the coordination, communication, decision-making, and performance of the participants and systems involved during this phase. By examining the conduction phase outcome, these AARs offer valuable feedback on the effectiveness of the execution and its contribution to the exercise objectives.

Table 10.4 Comparison of AAR based on the conduction phase coverage

No:	Guides	Conduction Phase	Conduction Phase Overview	Conduction Phase Outcome
1	Cyber Storm VIII: After-Action Report	✓	✓	✓
2	CYBER EUROPE 2022: AFTER ACTION REPORT	✗	✗	✗
3	Pre-Symposium Cyber TTX	✗	✗	✗
4	NYS Healthcare Cybersecurity Exercise AAR	✗	✗	✗
5	State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR	✓	✗	✓
6	QUANTUM DAWN VI AAR	✗	✗	✗
7	Baltic Cyber Shield Cyber Defence Exercise AAR	✓	✓	✓
8	NISÖ AAR	✓	✗	✗

10.5 Covered evaluation phase, overview, and outcome of the evaluation phase

As the Table 10.5 Comparison of AAR based on the evaluation phase coverage shows, out of the 8 After Action Reports (AARs) examined, 4 of them provide detailed coverage of the evaluation phase of the cybersecurity exercises. These reports offer comprehensive insights into the evaluation process, methodologies, and criteria used to assess the exercise outcomes. They discusses the data collection methods, analysis techniques, and evaluation frameworks employed during this phase. By covering the evaluation phase, these AARs provide valuable information about the assessment of exercise performance and the identification of strengths, weaknesses, and areas for improvement.

Additionally, 2 of the AARs offer an overview or summary of the evaluation phase. These reports provide a high-level view of the evaluation phase, highlighting the key objectives, approaches, and considerations taken into account during the evaluation process. While they may not provide extensive details, they still provide a broad understanding of the evaluation phase and its role in shaping the exercise outcomes.

Furthermore, 3 of the AARs specifically cover the outcome of the evaluation phase. These reports focus on evaluating the results, effectiveness, and impact of the evaluation process on the overall success of the exercise. They assesses the quality of data collected, the accuracy of analysis, and the relevance of evaluation findings. By examining the evaluation phase outcome, these AARs offer valuable insights into the effectiveness of the evaluation methods and their contribution to improving future exercises.

Table 10.5 Comparison of AAR based on the evaluation phase coverage

No:	Guides	Evaluation Phase	Evaluation Phase Overview	Evaluation Phase Outcome
1	Cyber Storm VIII: After-Action Report	✓	✓	✓
2	CYBER EUROPE 2022: AFTER ACTION REPORT	✗	✗	✗
3	Pre-Symposium Cyber TTX	✗	✗	✗
4	NYS Healthcare Cybersecurity Exercise AAR	✗	✗	✗
5	State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR	✓	✓	✓
6	QUANTUM DAWN VI AAR	✗	✗	✗
7	Baltic Cyber Shield Cyber Defence Exercise AAR	✓	✗	✗
8	NISÖ AAR	✓	✗	✓

10.6 Includes participant list

As the Table 10.6 Comparison of AAR based on the participant list provided shows, out of the 8 After Action Reports (AARs) examined, 6 of them provide information about the participant lists involved in the cybersecurity exercises. These reports recognise the significance of documenting and understanding the composition of participants to gain insights into the roles, responsibilities, and expertise contributed during the exercise.

These AARs include details such as the names or titles of participants, the organisations they represent, and their respective roles or functions within the exercise. Additionally, the AARs discusses the inclusion of participants from different sectors, such as government agencies, private organisations, or industry associations, to promote collaboration and information sharing.

Table 10.6 Comparison of AAR based on the participant list provided

No:	Guides	Participant List
1	Cyber Storm VIII: After-Action Report	✓
2	CYBER EUROPE 2022: AFTER ACTION REPORT	✗
3	Pre-Symposium Cyber TTX	✓
4	NYS Healthcare Cybersecurity Exercise AAR	✓
5	State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise AAR	✓
6	QUANTUM DAWN VI AAR	✗
7	Baltic Cyber Shield Cyber Defence Exercise AAR	✓
8	NISÖ AAR	✓

11 Results

The Table 11.1 design phase framework for exercise guidelines, provides a comprehensive framework on the design phase, offering insights into the essential features that should be incorporated within the phase and elaborates on the key elements that need to be addressed during this phase.

Table 11.1 design phase framework for exercise guidelines

No:	Features	Explanation
1	What is an objective	specific statements describing what is to be achieved by individuals, groups, or agencies participating in the exercise
2	Types Objectives	Raise awareness, validate plans and procedures, engage and educate your executives on cybersecurity, establish partnerships, information-sharing mechanisms and evaluate incident response
3	Objective formulation	SMART model (Specific, Measurable, Achievable, Relevant, Task-Related)

4	Type of exercise	Tabletop exercise, functional exercise, full-scale exercise
5	Planning team composition	Exercise leadership team, planning team, facilitation team
6	Leadership team	Exercise director, lead designer, lead evaluator, logistics lead
7	Planning team	leadership team, representatives from stakeholder organisations, relevant individuals from the public utility commissions, lead facilitator from facilitation team
8	Facilitation team	Lead evaluator, co-facilitator(s), lead evaluator, evaluator(s)
9	Exercise planning meetings	Concept development meeting, initial planning meeting, msel planning meeting, mid-term planning meeting, final planning meeting

The table 11.2 conduction phase framework for exercise guidelines, presents a thorough framework for the conduction phase, providing valuable insights into the critical aspects that should be integrated into this stage. It goes into detail about the key elements that require attention throughout the execution of this phase.

Table 11.2 conduction phase framework for exercise guidelines

No:	**Features**	**Explanation**

1	Exercise Logistics	Facility and room, audio/visual requirements, supplies, food and refreshments, registration and badging, table and breakout identification, parking, media, public affairs, and vips
2	Exercise Preparation	Situational manuals, presentations, audio/visual equipment, table tents for each tables, name tents for participants, badges exercise participant, sign-in sheets, feedback forms
3	Exercise conduct activities	Opening statements, discussion based on a scenario, objectives, or goals, taking notes and observations
4	Briefing	briefings for senior leaders, controllers and evaluators, actors, players, and observers
5	Wrap-up Activities	Player hotwash, debrief

The Table 11.3 evaluation phase framework for exercise guidelines, offers a comprehensive structure for the evaluation phase, delivering valuable perspectives on the essential components that should be incorporated during this phase.

Table 11.3 evaluation phase framework for exercise guidelines

No:	**Features**	**Explanation**
1	Evaluation planning	Including electing the evaluation team, developing the evaluation documentation

2	Evaluation documentation	Facilitator/evaluator handbook, controller/ evaluator handbook, evaluation plan, exercise evaluation guide, participant feedback form
3	Data Collection Methods	Direct observation, documentation review, feedback forms and surveys, interviews, hotwash and debrief: enable group discussion with participants
4	Data Analysis	Consolidation of data collected to determines whether participants performed critical tasks and met capability targets
5	Data Analysis techniques	Data synthesis, event reconstruction, trend analysis, root cause analysis
6	After-Action Report	Including exercise overview, analysis of capabilities, and list of corrective actions
7	Improvement Planning	The areas for improvement from the exercise are turned into concrete, measurable corrective actions that strengthen capabilities

12 Discussion

The literature collects data from 21 cyber exercise guidelines published from 2011 to 2022 which provides useful guidance for designing, conducting, and evaluating phases of cyber tabletop exercises. All the guidelines published before 2011 was excluded. There is a substantial lack of research on the effectiveness and best practices for the development and use of these guidelines. Therefore this research explains how the framework should look like, what all things should be included in the design phase, conduction phase and evaluation phase.

The design phase should include the objectives of the exercise, different types of the exercise and exercise planning.

Resources such as the Homeland Security Exercise and Evaluation Program (HSEEP) offered by the DHS and the Cybersecurity Tabletop Exercise Guide from Naruc provide a substantial number of objectives. They also incorporate the SMART model, which aids in formulating these objectives.

Guides like Instructions for Organising Cyber Exercises the Finnish Transport and Communications Agency (Traficom) and the Homeland Security Exercise and Evaluation Program (HSEEP) by DHS provides details about different type of exercise and explains the focus of different exercises.

In design phase it is important to have exercise planning composing of team composition, planning meetings and establishing timelines.

Guides such as the Cybersecurity Tabletop Exercise Guide by Naruc and the Department of Defense Cyber Table Top Guide by the United States Department of Defense (DoD) provide in-depth insights into team composition and the roles played by each team.

Guides like Handbook 3: Managing Exercises by the Australian Institute for Disaster Resilience and the cyber exercise playbook by MITRE explains different types of planning meeting, the participants, discussion topics in the meeting and the products of the meeting.

The conduction phase should structure in a way including logistics, preparation, activities during exercise and wrap-up.

Guides like the Homeland Security Exercise and Evaluation Program (HSEEP) by DHS and WHO Simulation Exercise Manual by WHO gives in-depth knowledge about the exercise logistics explaining venue setting and other resources which should be arranged for the exercise.

Guides such as Handbook 3: Managing Exercises by the Australian Institute for Disaster Resilience and Homeland Security Exercise and Evaluation Program (HSEEP) by DHS provides details about the necessary exercise materials and equipment given to the participants.

Guides like Instructions for Organising Cyber Exercises the Finnish Transport and Communications Agency (Traficom) and the Homeland Security Exercise and Evaluation Program (HSEEP) by DHS stresses on the activities during the exercise explaining the things to be done and role of facilitators in different scenarios.

Guides such as Handbook 3: Managing Exercises by the Australian Institute for Disaster Resilience and Cybersecurity Tabletop Exercise Guide by Naruc stress the importance and gives details about the wrap-up activities like hot-wash.

The evaluation phase should be constructed in such a way that it includes evaluation planning, documentation, data collection methods, data analysis, after action report and improvement planning.

Guides such as Handbook 3: Managing Exercises by the Australian Institute for Disaster Resilience and Homeland Security Exercise and Evaluation Program (HSEEP) by DHS explains about evaluation planning and shows how important is it to have evaluation team and different documentations like evaluation guide, evaluator plan.

Guides like Organising a Cyber Crisis Management Exercise by ANSSI and Homeland Security Exercise and Evaluation Program (HSEEP) by DHS provides more in-depth details about different data collection methods.

Resources like the Handbook for Planning, Running, and Evaluating Information Technology and Cyber Security Exercises by CATS and Homeland Security Exercise and Evaluation Program (HSEEP) by DHS describes about data analysis and the techniques which can be used for analysing data.

Resources such as the cyber exercise playbook by MITRE and the WHO Simulation Exercise Manual by WHO gives the structure and details about the after action report which covers important points of the exercise.

The Homeland Security Exercise and Evaluation Program (HSEEP) by DHS provides improvement planning details for the future.

There is an opportunity for future research to explore quantitative metrics and assessment techniques that can measure the effectiveness and impact of cyber exercises. In addition, the literature would be improved if the sources provided more guidance for organisations on how to integrate their cyber exercises into a holistic training program that includes other security initiatives like security awareness training, incident response planning, and policy development, in order to maximise the effectiveness of the exercises. The exercises can help reinforce lessons from other initiatives, and vice versa. This type of integrated approach could help organisations develop a more mature cybersecurity program.

13 Conclusion

The literature collects information from 21 cyber exercise guidelines published from 2011 to 2022. There is limited research on the effectiveness and best practices for the development and use of these guidelines. Therefore this research explains how the framework should look like for designing cyber exercises which is specifically explained under results.

The design phase should include the objectives of the exercise, how should it be formulated. It should explain what are the different type of the exercise available and what are the benefits of each exercise. It should also explain teams which should be formed and the roles played by them. It should also explain the details about the planning meetings and their estimated outcomes.

The conduction phase should include detailed explanation about exercise logistics to create a smooth and seamless exercise. It should explain about necessary preparation of exercise materials and equipment delivered by planning team. It should also include different activities performed during the exercise and at wrap-up.

The evaluation phase should include evaluation planning including developing evaluation documentation and selecting the evaluation team. It should include details about different data collection methods. It should explain how data can be analysed and what all methods can be used for it. It should include details about the after action report containing all the results and it should also include an explanation about improvement planning.

The Results part of the research mainly helps the organisations who wants to build a new guide as it points out the critical features each phase should have. Meanwhile, organisations seeking to utilise this research as a guide for conducting cyber exercises can refer to the sections titled "Comparison of the Design Phase," "Comparison of the Conduction Phase," and "Comparison of the Evaluation Phase" as it covers each feature in detail.

14 Definitions

NIST defines Cybersecurity as “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation” [45].

NIST defines Resilience as “The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents" [46].

NIST defines Cyber Resiliency as “The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources” [47].

NIST defines Cyber Tabletop Exercise as “Tabletop exercises are discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation” [48].

References

[1] G. Makrodimitris, P. Kotzanikolaou, and C. Douligeris, “Preliminary design of a new approach to choose cyber exercise methodologies for critical infrastructures,” in *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, Athens Greece: ACM, Nov. 2018, pp. 40–45. doi: 10.1145/3291533.3291542.

[2] IBM, “Cost of a Data Breach Report 2022.” [Online]. Available: https://www.ibm.com/downloads/cas/3R8N1DZJ

[3] N. Chowdhury and V. Gkioulos, “Cyber security training for critical infrastructure protection: A literature review,” *Computer Science Review*, vol. 40, p. 100361, 2021, doi: https://doi.org/10.1016/j.cosrev.2021.100361.

[4] S. Alzahrani, Y. Xiao, and S. Asiri, “Conti Ransomware Development Evaluation,” in *Proceedings of the 2023 ACM Southeast Conference*, in ACMSE 2023. New York, NY, USA: Association for Computing Machinery, Jun. 2023, pp. 39–46. doi: 10.1145/3564746.3587004.

[5] L. J. Trautman and P. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*. SSRN, 2019. [Online]. Available: https://books.google.at/books?id=zKUAzwEACAAJ

[6] A. Brilingaitė, L. Bukauskas, and A. Juozapavičius, “A framework for competence development and assessment in hybrid cybersecurity exercises,” *Computers & Security*, vol. 88, p. 101607, Jan. 2020, doi: 10.1016/j.cose.2019.101607.

[7] N. Chowdhury and V. Gkioulos, “A Framework for Developing Tabletop Cybersecurity Exercises,” in *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers*, Berlin, Heidelberg: Springer-Verlag, Feb. 2023, pp. 116–133. doi: 10.1007/978-3-031-25460-4_7.

[8] V.-V. Patriciu and A. Furtuna, “Guide for designing cyber security exercises,” Jan. 2009.

[9] A. Furtună, V.-V. Patriciu, and I. Bica, “A structured approach for implementing cyber security exercises,” in *2010 8th International Conference on Communications*, Jun. 2010, pp. 415–418. doi: 10.1109/ICCOMM.2010.5509123.

[10] E. Seker and H. H. Ozbenli, “The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation,” in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Jun. 2018, pp. 1–9. doi: 10.1109/CyberSecPODS.2018.8560673.

[11] M. M. Yamin and B. Katt, “Modeling and executing cyber security exercise scenarios in cyber ranges,” *Computers & Security*, vol. 116, p. 102635, May 2022, doi: 10.1016/j.cose.2022.102635.

[12] A. Furtuna, “Design and Implementation of a Cyber-Defense Exercise,” *Journal of Mobile, Embedded and Distributed Systems*, Jan. 2010, Accessed: Aug. 27, 2023. [Online]. Available: https://www.academia.edu/64030994/Design_and_Implementation_of_a_Cyber_Defense_Exercise

[13] M. Granåsen and D. Andersson, “Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study,” *Cognition, technology & work*, vol. 18, no. 1, pp. 121-, 2016, doi: 10.1007/s10111-015-0350-2.

[14] B. Alothman, A. Alhajraf, R. Alajmi, R. A. Farraj, N. Alshareef, and M. Khan, “Developing a Cyber Incident Exercises Model to Educate Security Teams,” *Electronics*, vol. 11, no. 10, Art. no. 10, Jan. 2022, doi: 10.3390/electronics11101575.

[15] P. Čeleda, J. Čegan, J. Vykopal, and D. Tovarňák, “Kypo–a platform for cyber defence exercises,” *M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization*, 2015.

[16] United States. Department of Homeland Security, “Homeland Security Exercise and Evaluation Program,” 2020. [Online]. Available: https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

[17] Health Information TRUST Alliance, “CyberRX 2.0 Level I Playbook Participant and Facilitator Guide,” 2015. [Online]. Available: https://www.vita.virginia.gov/media/vitavirginiagov/about/pdf/itac-and-hitsac-archives/HITRUSTCyberRX2Playbook.pdf

[18] D. R. S. Dewar, “CYBER DEFENSE REPORT,” Zürich, 2018. [Online]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf

[19] J. Kick, “Cyber Exercise Playbook,” Wiesbaden, Germany, 2014. [Online]. Available: https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf

[20] European Union Agency for Network and Information Security, “NCSS Good Practice Guide,” 2016. [Online]. Available: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[21] World Health Organization, “WHO Simulation Exercise Manual,” World Health Organization, Geneva, WHO/WHE/CPI/2017.10, 2017. [Online]. Available: https://apps.who.int/iris/handle/10665/254741

[22] A. O’Neill, A. Ahmad, and S. Maynard, *Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training*. 2021.

[23] Administration of Strategic Preparedness and Response, “aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf,” 2021. [Online]. Available: https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf

[24] Indiana Executive Council on Cybersecurity, *Indiana Emergency Manager Cybersecurity Toolkit*. 2019. [Online]. Available: https://www.in.gov/cybersecurity/files/Indiana-Emergency-Management-Cybersecurity-Toolkit_FINAL_Oct-2019.pdf

[25] Finnish Transport and Communications Agency Traficom National Cyber Security Centre Finland, “Instructions for organising cyber exercises,” 2020. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf

[26] United States Department of Defense, “The Department of Defense Cyber Table Top Guide,” 2021. [Online]. Available: https://ac.cto.mil/wp-content/uploads/2021/09/DoD-Cyber-Table-Top-Guide-v2.pdf

[27] Victoria State Government, “A guide to cyber exercises.” [Online]. Available: https://www.vic.gov.au/sites/default/files/2019-08/Vic-Gov-Cyber-Exercise-guide.pdf

[28] M. Ulmanová, “How to Develop a Cyber Security Table-Top Exercise: A Practical Guide,” 2019. [Online]. Available: https://cybilportal.org/wp-content/uploads/2020/07/N%C3%9AKIB-How-to-Develop-a-Cyber-Security-Table-Top-Exercise-a-Practical-Guide.pdf

[29] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-61 Rev. 2, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.

[30] L. P. Costantini and A. Raffety, “Cybersecurity Tabletop Exercise Guide,” 2021. [Online]. Available: https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

[31] ANSSI, “Organising a cyber crisis management exercise,” 2021. [Online]. Available: https://www.ssi.gouv.fr/guide/organising-a-cyber-crisis-management-exercise/

[32] International Telecommunication Union *et al.*, “GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY,” 2018, [Online]. Available: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[33] Wilhelmson, T. Svensson, and Nina, “Handbook for planning, running and evaluating information technology and cyber security exercises,” 2011. [Online]. Available: https://www.semanticscholar.org/paper/Handbook-for-planning%2C-running-and-evaluating-and-Wilhelmson-Svensson/21d8d0352cff1025494990779e6b7d575c3a1451

[34] Singapore Police Force and Ministry of Manpower, “Conducting Table-Top Exercises in response to a terror attack at the workplace.” [Online]. Available: https://www.police.gov.sg/-/media/Spf/Archived/2021-11-17/CPD/TTX-Guide-for-Workplaces.ashx

[35] The Australian Institute for Disaster Resilience, “Managing Exercises,” Austrailia, 2012. [Online]. Available: https://knowledge.aidr.org.au/media/3547/handbook-3-managing-exercises.pdf

[36] D. B. Fox, C. D. McCollum, E. I. Arnoth, and D. J. Mak, “Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context,” The Homeland Security Systems Engineering and Development Institute, 2018. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/pr-18-1636-ngci-cyber-wargaming.pdf

[37] Cybersecurity and Infrastructure Security Agency, “Cyber Storm VIII: After-Action Report,” 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-02/final-cyber-storm-viii-after-action-report-082022.pdf

[38] N. Christoforatos, I. Lella, E. Rekleitis, C. Van Heurck, and A. Zacharis, “Cyber Europe 2022: After Action Report,” Report/Study, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

[39] Homeland Security Exercise and Evaluation Program, “Pre-Symposium Cyber TTX,” 2021. [Online]. Available: https://www.setrac.org/wp-content/uploads/2021/10/Cyber-TTX-IP-After-Action-Report-Improvement-Plan-Final-10-19-2021.pdf

[40] Greater New York Hospital Association and Healthcare Association of New York State, “GYNHA & HANYS NYS Healthcare Cyber Security Exercise After Action Report,” 2017. https://www.gnyha.org/wp-content/uploads/2018/10/GNYHA-HANYS-NYS-Healthcare-Cybersecurity-TTX-AAR-Final-20170718-v00.pdf

[41] Cybersecurity & Infrastructure Security Agency, “State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise After Action Report and Improvement Plan,” 2022. [Online]. Available: https://www.oregon.gov/siec/SiteAssets/Pages/Lessons-Learned/Oregon%20Cybersecurity%20TTX%20FE%20AAR_Final.pdf

[42] Protiviti and SIFMA, “QUANTUM DAWN VI AFTER-ACTION REPORT,” 2022. https://www.sifma.org/wp-content/uploads/2022/02/Quantum-Dawn-VI-After-Action-Report.pdf

[43] The NATO Cooperative Cyber Defence Centre of Excellence, “Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report,” 2010. https://ccdcoe.org/uploads/2018/10/BCS2010AAR.pdf

[44] Swedish Civil Contingencies Agency)MSB=, “NISÖ 2018 After Action Report,” 2018. [Online]. Available: https://www.msb.se/siteassets/dokument/publikationer/english-publications/niso-2018---after-action-report.pdf

[45] M. Powell *et al.*, “Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector,” National Institute of Standards and Technology, Mar. 2022. doi: 10.6028/NIST.SP.1800-10.

[46] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing Cyber-Resilient Systems:: A Systems Security Engineering Approach,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-160v2r1, Dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[47] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, and G. Guissanie, “Protecting controlled unclassified information in nonfederal systems and organizations,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-171r2, Feb. 2020. doi: 10.6028/NIST.SP.800-171r2.

[48] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good, “Guide to test, training, and exercise programs for IT plans and capabilities,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-84, 2006. doi: 10.6028/NIST.SP.800-84.

List of Figures

List of Tables