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

Center for Asymmetric Threat Studies (CATS)

Nina Wilhelmson
Thomas Svensson

CATS
Center for Asymmetric Threat Studies

NATIONAL DEFENCE COLLEGE

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

NATIONAL DEFENCE COLLEGE

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

Nina Wilhelmson and Thomas Svensson
Center for Asymmetric Threats Studies (CATS)
Swedish National Defence College

2011 – Original text in Swedish
English translation by
Stephanie Young, CRISMART,
Swedish National Defence College (2013)

NATIONAL DEFENCE COLLEGE

CATS
Center for Asymmetric Threat Studies

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

Authors: Nina Wilhelmson and Thomas Svensson
Center for Asymmetric Threats Studies (CATS), Swedish National Defence College

2011 – Original text in Swedish, English translation by
Stephanie Young, CRISMART, Swedish National Defence College (2013)

Published by: The Swedish National Defence College

ISBN 978-91-86137-36-6

Printed by Elanders Sverige AB, Vällingby, 2014

Foreword

Exercises to reduce threats, risks, vulnerabilities and consequences and protect critical information infrastructures in contemporary information and cyber security environment are vital in establishing a resilient society. The need for exercises to train organisations and management at crises are obvious and there are lot of knowledge and experiences for how to develop Table-Top Exercises (TTX). When it comes to IT- and cyber incidents though is this not enough. There is in this environment normally a huge knowledge gap between the world of IT-technicians and the policy management which needs to be bridged, so that the injects in a TTX:es are relevant and realistic. Thus there is an obvious need to conduct technical exercises – normally called Cyber Defence Exercises (CDX) - focusing on the information technology of crisis management such as IT-incidents and cyber attacks.

The handbook for planning, running and evaluating information technology and cyber security exercises is an English translation of the Swedish handbook commissioned by the Swedish Civil Contingencies Agency (MSB). This unique handbook will guide actors working with critical information infrastructure to develop and enhance technical IT and cyber security exercises and decrease those risks and threats that pervade society, and public and private sectors in the information age.

The work on this handbook has been conducted by Nina Wilhelmson (now MSB) and Thomas Svensson at the Center for Asymmetric Threat Studies (CATS).

Lars Nicander
Director, Center for Asymmetric Threat Studies (CATS)

Summary

Information and cyber security combined with the skills to communicate problems and solutions in collaboration with others, even during difficult circumstances, can be improved by conducting exercises.

Such exercises – in this specific case, information technology and cyber security exercises – are a complement to regular preparedness and crisis management exercises. They can be designed in various forms and in many different ways, which this handbook will demonstrate.

This handbook is intended to be an aid in planning, running and evaluating information technology and cyber security exercises. One such area is exercises focusing on an organization's IT systems within a network in relation to other process-related aspects during a major IT incident. This is to improve information and cyber security as well as the ability to respond to incidents within the organization and serious IT incidents that impact many organizations and society at large.

This handbook was written heavily based on the Swedish Civil Contingencies Agency's (MSB) exercise handbook *Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar* [Crisis management exercises – A handbook on planning, running and processing feedback][1] published in 2009 where experiences from previous information technology and cyber security exercises are considered and discussed.

Above all, this handbook is meant to be an aid, in general, for those involved

[1] This handbook is only available in Swedish. The English translation of the title was made by Stephanie Young.

in information and cyber security and, more specifically, those involved in protecting the public critical information infrastructure.

The handbook is divided into a normative and an informative part. The normative section describes the interwoven project management and exercise planning process for planning, running and getting feedback from information technology and cyber security exercises, which is divided into ten steps. These are exercise preparations, the master plan, defining the assignment in a mission statement, planning the exercise, practical preparations, implementation, evaluation, feedback, reporting, and following-up (after-action review).

The handbook's informative section consists of practical experiences from previous exercises presented in the form of specific conclusions. A more in-depth presentation of the technical infrastructure used in simulated and 'live' information and cyber security exercises is found in the handbook's section on implementation.

Examples of templates and checklists for project management and for documenting the exercise planning process are provided in the handbook's appendices.

Among the handbook's recommendations are the following practical advice and tips:

- Start with the mission statement of the exercise assignment and determine feasible and measurable objectives for the exercise. Do not have too many objectives. Read the mission statement and see if the resources assigned for the exercise are sufficient to fulfill the purpose of the exercise. If not, the level of ambition for the exercise should be lowered or limited to certain aspects, or perhaps additional resources need to be allocated?

- Include and consider the legal aspects with respect to information management and documentation of the exercise (such as security and confidentiality issues) throughout the entire process of the project management and exercise (from planning, implementation, evaluation, getting feedback, and following up). Make time for establishing contracts and agreements between the parties involved in planning the exercise.

- Use a risk and impact assessment, which is continuously updated with exercise project. This can be used to illustrate the expected and unexpected risks with exercise. Information technology and cyber security exercises are often complex in structure, which requires relatively large resources of time, people and capital (purchase of hardware and software, etc.).

- Be sure to include the technology management team for support and communication (responsible for the infrastructure of the information and cyber security exercise) as well as the evaluation management team in planning the exercise and defining the purpose and objectives.

- With good planning (via a project management that establishes and can follow up agreed responsibilities and roles, a planning and implementing organization, and an evaluation organization), a proper foundation is in place to ensure a well-structured implementation.
- Be sure to have a coordinator for managing information in the exercise project, as well as a media and communications manager for visitors.
- Give attention to the traceability of information and communication management as well as the documentation of the exercise.
- Technology exercises should include the opportunity to update situation awareness and the extensive testing of the exercise environment and its systems before the exercise starts.
- In short, keep in mind that information technology and cyber security exercises are actually about people. If possible, have continuous planning meetings, briefings and conferences with the involved parties and give them the opportunity to meet during the planning stage as well as during the implementation and follow-up stages of the exercise.

It is our hope that this handbook will provide useful tools and practical advice both for those who are already carrying out information technology and cyber security exercises and for those who plan to start exercises in the above area.

Table of Contents

Figures and tables

Abbreviations and acronyms

BCS	Baltic Cyber Shield
CCB	Configuration and Control Board
CCD COE	Cooperative Cyber Defence Centre of Excellence
CDX	Cyber Defence Exercise or Computer Distributed Exercise
CERT	Computer Emergency Response Team
ISP	Internet Service Provider
IT	Information Technology
MSB	Swedish Civil Contingencies Agency
NISÖ	National Information Security Exercise
OTRS	Open-source Ticket Request System
SCADA	Supervisory Control and Data Acquisition

Disclaimer

The original manuscript of this publication was written in Swedish. The translation of it from Swedish to English was done by Stephanie Young in consultation with one of the authors Thomas Svensson. In the original publication, the authors cited often the book “Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar” [Crisis management exercises – A handbook on planning, running and processing feedback] which was published by the Swedish Civil Contingencies Agency (MSB) in 2009.

In order to help those readers who understand Swedish and have read the original, a list of the Swedish terms and the English translations is provided below.

Translations of Swedish terms

allmänspel – exercises and/or games that attempt to reflect and include public concerns and interests

attackvägar – threat paths

den manuella poängbedömningen – manual scoring

direktiv – mission statement, directives

erfarenhetsåterföring – processing experiential feedback and lessons learned

flertypsövning – multi-approach exercise

förhistoria – (prehistory) background information

genomförande – implementation

genomgång – briefing, trial run through, review

givare – messenger

inspelare – messenger

integritetsmål – intergrity objectives

kartskisser – map sketches

kartväggar – maps

konsultavtal – consulting agreements

krypterade tunnlar – encrypted tunnels

laborationsövning – controlled environment exercise

Lag (2009:1091) om offentlig upphandling för offentliga myndigheter – Swedish Public Procurement Act

larmövning – an unannounced live exercise

lokal övningsledare – local game controller

motspel – counterplay

motspelcentralen – counterplay headquarters

OH-bilder – slides

poängberäkning – scoring

praktiska förberedelser – practical preparations

projektledare – project leader

samarbetsavtal – agreements with involved parties

samband – communication

sambandbestämmelser – terms of reference for communication
sambandsprov – communication test
sambandsvägar – communication channels
samverkanövning – cooperation exercises
sekretessbestämmelser – confidentiality terms
sekretessmål – privacy/confidential objectives
skarp övning – 'live' exercise
spelledare – game controller
spelledning – game management
stabsövning – staff exercise
startövningar – initiation exercises
säkerhetsbestämmelser – security regulations
tekniska information – information technology
tekniskt stöd och samband – technical support and communications
tillgänglighetsmål – availability objectives
uppdrag – the mission statement
uppdragsbeställning – commissioned contract
uppdragsgivare /beställare – commissioning organization
uppföljning – after action review, following up, feedback
uppföljningstablåer – monitoring tables
utvärdering – evaluation
utvärderingsledare – head of the evaluation team
överensstämmelse – how well the objectives have been achieved, comparing objectives with results
övergripande projektplan – master plan
övningsansvarige – exercise controller, person responsible for the exercise
övningsförberedelser – exercise preparations
övningsbestämmelser – terms of reference for the exercise participants
övningsledare/övningsansvarig – exercise controller
övningsledning – exercise management
övningsledningsbestämmelser – terms of reference for the exercise management
övningsmoment – exercise phases
övningsutvärderare – exercise evaluator
övningsplanering – exercise planning
återkoppla – process feedback
återkoppling – processing feedback

1 Introduction

Below, an introduction of this handbook and its range of application are provided by presenting the purpose and target group as well as the limitations, methodology, definitions and guidelines for reading it.

Sweden's information and cyber security actors are found within both the private and public sectors of society. These actors ensure that data and information systems and networks are protected from intrusion and damage yet at the same time making them available to the right people at the right time.

Information and cyber security work is ongoing process within each organization. Besides ensuring that the operating activities function under normal circumstances with their ordinary incident management, private organizations and public agencies are also responsible to ensure that society's information infrastructure and the protection of it will function even during serious IT incidents.

When a serious incident increases stress on an organization, a sector, or a larger part of society, information and cyber security will also need to be maintained so that IT and communications systems can continue to operate, or can be quickly resumed in the event of an interruption. In normal mode as well as during extraordinary circumstances data and information will still need to be transferred without compromising confidentiality (unauthorized access), integrity (unwanted distortion), availability, or related liability or non-repudiation.

This work ranges from ordinary activities to preparing to manage a serious IT incident as well as actually dealing with an incident (crisis) when it occurs and concluding it by identifying lessons learned and following-up. In order for information and cyber security (from dealing with everyday matters to serious

IT incidents) to function properly, all involved parties including those from within an organization as well as external actors (i.e., public, private, national and international organizations) must be able to interact and communicate with each other.

Information and cyber security combined with the skills to communicate problems and solutions in collaboration with others, even during difficult circumstances (requiring decision-making under time pressure when significant values are at stake such as material wealth and human life), can be improved by conducting exercises. Exercises in the management of large scale IT incidents with extensive complexity, geographical breadth and impact on local, regional and national levels are, therefore, of great importance. Not least of which is the management of serious IT incidents require collaboration outside the organization and community sector.

Such exercises - in this specific case, information technology and cyber security exercises – are a complement to regular preparedness and crisis management exercises. They can be designed in various forms and in many different ways, which this handbook will demonstrate.

This handbook on information technology and cyber security exercises has been written largely based on the Swedish Civil Contingencies Agency's (MSB) handbook *Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar* [Crisis management exercises – A handbook on planning, running and processing feedback][2] where lessons learned from previous information technology and cyber security exercises have been documented.

1.1 What information technology and cyber security exercises can contribute

Exercises in the area of information and cyber security, like other recurring contingency and crisis management exercises, contribute to, among other things:

> Develop crisis management capabilities and leadership with responsible actors; improve the ability to interact with other actors in the crisis management system; increase the ability to make quick decisions and communicate situation information; maintain awareness of the complexity that is characteristic of crisis situations; examine and develop contingency plans that mirror reality; point out areas where further training or [... exercise] are needed; highlight weaknesses and strengths in resources and technology; increase public awareness of the

[2] MSB (2009). This handbook is only available in Swedish. The English translation of the title was made by Stephanie Young. The original in Swedish is available at: http://www.msb.se/RibData/Filer/pdf/25608.pdf

> skills, capabilities, vulnerabilities and needs; develop the participants' ability and confidence in their own competence; enable those in the network the opportunity to know and understand each other better.

In addition, information and cyber security exercises more specifically contribute by:

1. Increasing collaboration, through greater understanding and familiarity of interaction on the government level as well as between private and public sector by:

- Enabling the participants (professionals in the private and public sectors as well as students) to exchange experiences and information with each other, which in turn contributes to the team spirit among those involved in the exercise.
- Increasing the understanding of the national and international cyber environment with respect to policy, legal aspects and the need for international cooperation.
- Developing and expanding international collaboration in the ability to handle large-scale IT incidents/cyber incidents.

2. Identifying vulnerabilities in systems that have been exercised/tested in order to:

- Illustrate the desired security properties in information systems – for example to be able to withstand (secure and defend against) a particular form of viruses, DDoS attacks, etc.,
- Test preparedness and response plans.

3. Studying IT incidents and cyber attacks as well as the protection and defense of critical information infrastructures so that:

- Knowledge and skills for planning, implementing, and following up information technology and cyber security exercises can be improved.

1.2 Purpose

This handbook is intended to be an aid in the planning, implementation and evaluation, as well as getting feedback from experiences of information technology and cyber security exercises. This is to improve information and cyber security, and also the ability to respond to incidents within an organization and serious IT incidents that significantly impact many organizations and the society at large.

1.3 Target group for this handbook

This handbook is above all meant to be of help for actors (those responsible for exercises within an organization and operational management) in information and cyber security in general and those responsible for protecting the public critical information infrastructure more specifically, who already conduct exercises or are planning to begin exercises in the above area. This handbook can also be read by exercise participants as others interested in information and cyber security exercises.

1.4 Limitations

This handbook moves between the national management level (upper level) to IT operators and those responsible for network security (lower level) in both private and public organizations. It includes also a discussion of technology aspects. Such aspects are necessary to consider and they need to be clarified to those who commission exercises and the exercise controller s so they know what to require (in terms of technical specifications, privacy issues and so forth) of those supporting the technical environment. A well-functioning technical environment is a significant prerequisite for implementing information and cyber security exercises.

This handbook's point of departure is MSB's exercise handbook *Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar* [Crisis management exercises – A handbook on planning, implementing and processing feedback] which was published in 2009 and shares practical information and experiences of previous technology exercises. The exercises described in this handbook are foremost simulation exercises (exercises in a controlled environment with a counterplay), but seminar exercises and "live" exercises in the existing system in real time are also discussed. Thus, this handbook is not comprehensive or intended to provide an exhaustive picture of how information technology and cyber security exercises can or should be planned, implemented, and reported.

Finally, the authors of this handbook would like to emphasize that while references are made to cyber defense and cyber defense exercises in the text, they are not the focus of this handbook and therefore are not be described in great detail.

1.5 Method

The handbook is based on an expert-emphasized research approach. In addition, it was discussed and quality-checked in a workshop with participants who have worked and have valuable experience in national and international information and cyber security exercises. The background and material in this book are based on practical experiences from project and exercise management as well as from exercise controllers, exercise participants, and project reports from previous exercises. Among these are two simulated exercises: Baltic Cyber Shield 2010 (also called CDXII) and the 2008 Cyber Defense Exercise (CDXI), as well as the seminar exercise National Information Security Practice (NISÖ) in 2010 and a “live” information exercise completed a few years earlier.

As mentioned earlier, this handbook is heavily based on MSB’s exercise handbook since it addresses the planning, implementation, and getting feedback from information technology and cyber security exercises.[3]

1.6 Definitions and central concepts

- **Large-scale IT attack, large scale security incident in the network,**[4] **serious IT-incident, cyber incidents –** These relate to IT-related events (IT in the broad sense) that contribute to a serious disruption in essential

[3] MSB as well as other organizations have published related texts on these subject matters. For example, ”Handbok – Utvärdering av övningar” [Handbook – Evaluation of Exercises] published in 2010 by MSB. Additionally, the Swedish Standards Institute (SIS) has a handbook with checklists for scenario exercises and crisis management exercises in information security. Likewise the European Network and Information Security Agency (ENISA) has published a handbook for teachers, called “CERT Exercises Handbook”, which includes exercise documents for students called “CERT Exercises Toolset”. These documents are the basis for exercise managers (teachers) and participants (students) together with twelve different scenarios related to incident management.

Since 2008, NATO’s exercise series for cyber defense (Cyber Coalition) is compiled annually as new handbooks for future exercises. For the Cyber Coalition 2010 exercise (CC10) held in November 2010, the handbooks “Exercise Handbook for Exercise Controllers (EXCONs) and Local Trainers (LTs)” and “Exercise Handbook for the Training Audience (TA)” were used.

Another handbook is J.R. Vacca’s “Computer and Information Security Handbook. Here various exercise approaches are presented, such as the “Red Team/Blue Team Exercise” method.

[4] A more complete description appears in the *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on Critical Information Infrastructure Protection*, “Protection against large-scale cyber attacks and disruptions: Enhancing preparedness, security and resilience” (European Commission, 30 March 2009: p.10).

services or a crisis for society with an extensive geographic impact on the local, regional and national levels and require urgent action and cooperation with other organizations.[5]

- **Extra-ordinary event –** An "event that deviates from the norm, represents a serious disturbance or imminent risk of a serious disruption in important social functions, and requires urgent action by a municipality or a county."[6]
- **Critical functions of society –** "defined as a societal function of such importance that a loss or a severe disruption in it would entail significant risk or danger to inhabitants' well-being/lives, the overall functioning of society, and/or society's fundamental values."[7] Examples include "the distribution of electricity and water, rail transport, and petrochemical industry."[8]
- **Information security** – is a general term that encompasses both physical security (protection of premises, employees, etc.), data and IT security (protection of servers, data and communication via e-mail, etc.) and administrative security (policy, business continuity plans, regulations etc.).[9]
- **Cyber security –** includes the above as well as measures for the protection of data, computers or computer systems in a network (e.g., the Internet) against intrusions and attacks.[10]
- **Information technology and cyber security exercise** – relates to an exercise with a focus on an organization's IT systems within a network in relation to other process-related aspects (e.g., operational, legal, and policy-related) in the event of a major IT incident.

[5] A comparative description of serious IT incidents - it "differs from the normal; involves a serious disruption of essential services; and requires urgent action and coordinated action at the national level" (MSB, 2011-03-01, page 7).

[6] Chapter 1 4§ of the Swedish Act (2006:544) concerning local and county measures before and during extraordinary events in times of peace and times of heightened alert (LEH).

[7] MSB (2011).

[8] MSB (2010a).

[9] SIS (2007). Information security also includes personal safety (protection against threats, theft, fire) and communication security (protection of communication media, telephone, email, fax). Information security is more specifically security for information assets and their ability to maintain their intended confidentiality, integrity, availability, accountability and non-repudiation.

[10] Merriam Webster (2011-02-09).

- **Information Assurance (IA)** – is the protection of information systems and their contents; that is, "measures taken during peacetime, crisis or war to secure civil and military information, and information and communications systems vital to societal security."[11] IA also includes measures to detect and respond to intrusions, and measures to restore information.
- **Handbook** – "A book that provides a fairly concise but rather complete overview to be used as a guide to a specific subject area. The term 'handbook' is also often used for reference books, major textbooks, or compendiums. Both terms 'handbook' and 'guide' are used interchangeably throughout the text in this publication."[12]

1.7 Outline

The handbook is divided into a normative and an informative part. The normative section describes the interwoven project management and exercise planning process for planning, implementing and processing feedback from information technology and cyber security exercises, which is divided into ten steps. These are exercise preparations (Chapter 3), the master plan (Chapter 4), the mission statement (Chapter 5), exercise planning (chapter 6), practical preparations (Chapter 7), implementation (Chapter 8), evaluation (Chapter 9), feedback (chapter 10), reporting (Chapter 11), and the after action review (Chapter 12).

The handbook's informative section consists of practical experiences from previous exercises presented in the form of specific conclusions. A deepening of the technical infrastructure in simulated and 'live' information and cyber security exercises is found in the handbook's section on implementation.

[11] SIS (2007), p. 73.

[12] See also ENISA's Good Practice Guide for Incident Management, European Network and Information Security Agency, 2002. Available at: http://www.ENISA.europa.eu

2 An Integrated Process for Exercise Planning and Project Management

The following section provides an introduction to an integrated process for exercise planning and project management with respect to information technology and cyber security exercises.

As previously mentioned, this handbook is intended for those within an organization responsible for exercises and the operational management of information and cyber security. This handbook focuses on exercises of physical security, IT security and administrative security (i.e., information security) as well as measures to protect important public data and information, computers, and computer and information systems in a network (the Internet) against attacks and intrusions (so-called cyber security). In addition, this book is a guide for matters regarding measures to secure, detect and respond to intrusions in information and communication systems (i.e., information assurance). Information assurance covers human behavior, information technology, and processes regarding policies in this area.

2.1 Exercise planning and project management processes

Exercises in general, and information technology and cyber security exercises, more specifically, are advantageously carried out as projects. This is why the integration of the project management process and exercise planning process has been made in this handbook.

The project management process usually includes these steps:[13]

- idea generation
- preliminary investigation
- establishment, divided into:
  - mission statement
  - dialogue about the mission statement
  - project planning, and
  - project organization
- project initiation and implementation
- completion and reporting
- following-up and evaluation of results.

In addition, the following steps are included in planning an exercise:

- defining the mission/assignment
- planning the exercise
- practical preparations
- implementation
- evaluation
- processing feedback
- reporting
- following-up
- a new mission/assignment

Ten general project management and exercise planning processes are highlighted in this handbook in order to provide a basis for discussion. They include the following:

1. Exercise preparation (Chapter 3)
2. Master plan (Chapter 4)
3. Mission statement (Chapter 5)
4. Exercise planning (Chapter 6)
5. Practical preparations (Chapter 7)
6. Implementation (Chapter 8)
7. Evaluation (Chapter 9)
8. Feedback (Chapter 10)
9. Reporting (Chapter 11)
10. After action review (Chapter 12)

[13] Based on Jan Wisén and Börje Lindblom (2009), p. 37 ff.

Moreover, the handbook's overall structure has been adapted to information technology and cyber security exercises. There are also a number of appendixes at the end of the book that include checklists and supplementary facts on information technology and cyber security exercises.

The overall structure of this handbook is illustrated in Table 1, which include activities for planning, implementation and feedback, and exercise documentation, integrated into project management and planning exercise. The table is read from left to right, while a guide to project management and exercise planning over time.

Table 1: The integrated process for exercise planning and project management

	PLANNING				**IMPLEMENTATION**				**FEEDBACK**	
PROJECT-(MANAGEMENT) PROCESS	Generating ideas and a preliminary investigation		Establishing a mission statement and a risk analysis	Establishing project plan and project organization	Launching and implementing the project				Concluding and making a report of the project	Following up and evaluating the results of the exercise
EXERCISE-PLANNING PROCESS	Exercise preparations	Master plan	Mission statement	Exercise planning	Practical preparations	Implementation	Evaluation	Feedback	Reporting	After action review
ACTIVITIES	• Take an inventory and establish the needs of the exercise	• Long-term exercise plan • Exercise as a learning process	• Cont. making an inventory of the needs surrounding the exercise.	• Purpose and objectives of the exercise • Exercise types and forms • Timings • Planning organization	• Implementing organization • Documentation of exercise • Scenario • Briefings	• Technical aspects of the exercise environment • Technical support and communications • External communication • Visitors and media coverage • Cont. different exercise formats.	• Cont. purpose and objectives of the exercise • Cont. evaluation and feedback	• Cont. evaluation and feedback	• Cont. making an inventory of the needs surrounding the exercise. • Cont. evaluation and feedback	• Follow-up and discuss new ideas for future assignments
EXERCISE DOCUMENTATION			• Mission statement • Consulting agreements • Agreements with involved parties	• Project plan (description of activities, project budget, time table) • Project discrepancies	• Terms of reference for the exercise • Terms of reference for the exercise management • Security terms • Confidentiality terms • Terms of reference for communications • Contact list for the exercise organization • Documentation for the evaluation				• Concluding the project (i.e., project report) • Report on the participants' evaluation of the exercise • Evaluation of the exercise project	

Planning (1 of 3)

	PLANNING			
PROJECT MANAGEMENT PROCESS	(1) Generate ideas and preliminary investigation		(2) Establish a mission statement and a risk analysis	(3) Project planning and project organization
EXERCISE PLANNING PROCESS	Exercise preparations	Master plan	Mission statement	Exercise planning
CHAPTER IN THE HANDBOOK	Chapter 3	Chapter 4	Chapter 5	Chapter 6
AKTIVITIES	• Take inventory and determine the needs of the exercise	• Long-term exercise plan • Exercise as a learning process	• Cont. taking inventory and determine the needs of the exercise	• The exercise's purpose and objectives • Exercise types and forms • Time tables • Planning organization
EXERCISE DOCUMENTATION			• Mission statement • Consulting agreements • Agreements with involved parties	• Project plan (description of activities, project budget, time table) • Project discrepancies

2.2 The project management process: Idea generation and preliminary investigation[14]

This step in the project management process corresponds to "Exercise Preparation" (Chapter 3) and "Master plan" (Chapter 4) in the exercise planning process.

Idea generation via brainstorming can yield fruitful ideas for looking and doing things in a new way. Some of these ideas will spark the interest of the management and the organization and therefore may be used directly, for example, in

[14] This section builds upon Chapter 3 ”Från idé till projekt”[From idea to project] in Wisén and Lindblom (2009), p. 42-48.

the exercise's mission statement or for defining the task at hand. Others can be put into an 'idea bank' for future consideration.

A brief inquiry regarding the background, purpose, expected results, limitations, and estimated time and costs can be conducted in order to provide a basis for prioritizing rendered ideas and future directives. If the inquiry reveals that there is insufficient evidence, a more comprehensive study can be done.

When selecting among project ideas, a project selection matrix can be a useful tool. This assists in assessing the ideas based on various criteria, such as their degree of usefulness, significance, and feasibility.

3 Exercise Preparation

3.1 Making an inventory and determining the needs of an exercise[15]

3.1.1 Initiatives and mission

Before planning an exercise, one should start by determining the guidelines and boundaries for the exercise, and the exercise planning process should be clearly formulated and anchored. It should be clear who the client is and who is initiating the exercise. Furthermore, there should be a set budget for the proposed exercise project and for the entire planning process (from planning and implementation to feedback) which allocates resources for staff, travel and technology costs.

3.1.2 Needs analysis – why should we have an exercise?

Before planning an exercise, the needs and reasons for having an exercise must be clearly formulated. A needs analysis may be helpful in doing this; for example, by performing a risk and vulnerability analysis of a particular function or certain activities. Even previous exercises can help clarify the needs for a new exercise as a single event or as many exercises in a series.

The needs analysis should highlight the organization, its operations, individual duties and responsibilities, changes in the organization/operations, and previous experiences during exercises and real events. It should also draw atten-

[15] This section builds upon Chapter 3 in MSB (2009), p. 18-19.

tion to the current capacity (knowledge, skills) of the exercise participants, and identify the knowledge and skills they need to perform their duties. Further analysis should answer the following questions:

- What should exercise achieve? Overall purpose of the exercise.
- Who should participate in the exercise? The target group for the exercise with consideration for what the purpose and objectives of their participation.
- What should be exercised? – Selecting the approach and content of the exercise.
- When should the participants exercise?
- How should the participants exercise? – Selecting the exercise format and the practical approach/methods for carrying out the exercise.
- Where should the exercise be?
- What resources are needed?

The needs analysis should help clarify the major questions regarding the reasons, needs, scope, and methods for the exercise.

4 The Master Plan

4.1 Long-term exercise plan[16]

In order to ensure continuity in exercise activities, a long-term exercise plan should be developed, spanning over several years. This, in turn, should be based on a competence development plan for the organization's employees. The exercise plan should be presented as a table in chronological order illustrating which exercises are intended to be completed and when they are supposed to take place. Furthermore, it should also reveal which functions within an organization (or in within different organizations) should be exercised at what times, and indicate when evaluation, feedback, and follow-up are planned to be implemented.

Considering the amount of time it takes to plan, implement, and process feedback from information technology and cyber security exercises, an exercise plan should stretch over several years, preferably over three to five years. Exercise activities structured in this way are easier to get an overview of and the path for fulfilling the objectives of the exercise is clearly laid out. For example, exercise activities can be represented in the form of development steps where information and cyber security exercises become increasingly more sophisticated and complex, [17] involving more features or elements within an organization, or with several different organizations within a larger area of cooperation.

[16] This section builds upon Chapter 2 in MSB (2009), p. 13-15 and p. 16-17.

[17] Within the framework of Sweden's participation in past international technological exercises on information security (so called Cyber Defense Exercises, CDXs), the overall goal has been to learn more about implementation and how this form of exercise can be set up.

With a good exercise plan in hand, all of the units or functions can be adequately and correctly adapted to the exercise at certain time intervals so that the stipulated levels of skills and knowledge are maintained in accordance with the established objectives that have been.

Exercise plans that extend over several years can be written for a specific sector (such as energy, communications, transportation, etc.), region, or organization (public or private).

As a project, the exercise plan should include:

- objectives for the exercise activities
- time table
- division of roles/responsibilities, and
- estimate of resources needed (funding, human resources, competencies, technology, equipment, etc.).

With respect to the resources, it is of great important to designate early on sufficient human (personnel and necessary skills), technology (equipment and other materials), and financial resources. These have a decisive influence on the exercise planning process from planning to implementation and following up. The financial situation (especially, the costs) of the exercise should be budgeted during the planning phase. In turn, this will help identify the appropriate ambition level. This will help decide the exercise objectives and scope as well as make it possible to implement changes if the economic situation should change and even assist in doing an evaluation of the exercise and in the follow-up stage. By documenting the economic outcomes of the exercise in the evaluation phase, this material can be used in the planning of the next exercise or even a new one.

While the long-term plan provides exercise managers with a way to structure and illustrate for management and decision makers how planned information and cyber security exercises fit into an organization's exercise and competence development plan as well as strategies for this, it should always be considered a living document.

The plan's scope (i.e., how many exercises are scheduled) is always a compromise between the needs, opportunities, level of ambition, time, and financial resources. A multi-year exercise plan may need to be revised due to what emerges from the evaluations of completed exercises or due to changing threats or other developments.

4.2 Exercise as a learning process

Whatever the objective of the exercise is, it should always be considered a learning process for both the exercise planners as well as for the exercise participants. A rewarding exercise for some can be a stressful and anxious experience for others. While the technology aspects and method of the exercise can easily become the focus, the human aspects should be highlighted in exercise planning. Among other things, this includes creating a good atmosphere throughout the entire exercise planning process so that the exercise participants feel well treated and are encouraged to participate.

Depending on the purpose and objectives of an exercise, the exercise participants can be involved in designing the exercise by sharing their ideas about what knowledge or skills in information and cyber security they would like to improve during the exercise. It is also important that the degree of difficulty is adapted to the prevailing technical conditions and the participants' skill level.

Scenarios of extreme situations including stress and uncertainty can easily give rise to strong feelings among the exercise participants during or after the exercise. The participants should not feel vulnerable or that their weaknesses have been exposed to their colleagues and superiors. Therefore, it is important that the exercise management creates a positive atmosphere for the exercise and have the ability to deal with such issues should they arise.

It is important to emphasize that it is allowed to make mistakes during an exercise.

Motivation is encouraged in the learning process by:

- involving the participants,
- adapting the exercise to their knowledge, and
- adapting the exercise to the technical requirements.

Reminders and helpful hints!

- Conduct a thorough needs analysis before planning an exercise. This should include answering questions regarding: what the exercise is meant to achieve and for whom; what should be exercised and when, where, and how; and the resources needed to do all of this.
- Make a long-term exercise plan – preferably between three to five years – that continually rotates information technology and cyber security exercises with a variety of other exercises. In order to be able to do this, it is important to have clear objectives, timetable, and division of labor/responsibilities for the exercise activities, as well as an estimate of the necessary resources needed for the entire exercise planning process.

Planning (2 of 3)

	PLANNING			
PROJECT MANAGE-MENT PROCESS	(1) Generating ideas and doing a preliminary investigation		(2) Establishing a mission statement and a risk analysis	(3) Project planning and project organization
EXERCISE PLANNING PROCESS	Exercise preparations	Master plan	Mission statement	Exercise planning
CHAPTER IN HANDBOOK	Chapter 3	Chapter 4	Chapter 5	Chapter 6
ACTIVITIES	• Taking inventory and determining the needs for an exercise	• Multiyear exercise plan • Exercise as a learning process	• Cont. making an inventory and determining the needs for an exercise	• Exercise's purpose and objectives • Exercise forms and types • Time table • Planning organization
EXERCISE DOCUMEN-TATION			• Mission statement • Consulting agreements • Agreements with involved parties	• Project plan (description of activities, project budget, time table) • Project discrepancies

Project management process: The mission statement and a risk analysis[18]

This step in the project management process corresponds to Assignment/ Mission (Chapter 5) in the exercise planning process.

Mission statement – Defining the assignment

The needs analysis identifies the need for an exercise from which an idea of an exercise is formulated into a mission statement (also called a commissioned order). The mission statement will guide future decisions and therefore should be clear, realistic and possible to evaluate as well as informative and

[18] This section builds upon Chapter 4 ”Direktivet – En uppdragsbeställning” [Mission statement – Commissioning an assignment] in Wisén and Lindblom (2009), p. 50-64.

problem-oriented. The mission statement is based on the client/customer's wishes and perspective and should be in writing.

The mission statement should contain the following elements:

1. a comprehensive title
2. background to the project origins
3. description of the mission in mandated terms (what to achieve?)
4. purpose, vision and objectives
5. clarification of the project boundaries and limitations
6. resources (rough estimate)
7. provisional timetable (with at least the final deadline)
8. instructions regarding with whom will be consulted and informed

Legal aspects with respect to information management and exercise documentation

The commissioned assignment/mission should specify requests regarding how information should be managed and how the exercise should be documented. This includes who has access rights to exercise documentation and data (including audio and video recordings) as well as how and where training materials should be stored during the preparation and implementation and after exercise. If data and information are stored in public forums and the project management system is open on the Internet, many digital footprints of the exercise are made in many locations. The information that is handled in the project management and exercise planning process can be sensitive. Therefore, issues related to security (accreditation) and secrecy[19] should be settled before exercise

[19] The agreement should also take into account confidentiality issues and how information and documents are intended to be addressed within the framework of the information and cyber security exercise. The issue of classified information is related to rules on public access to documents in the Swedish Freedom of the Press Act. The point of departure is that every document is an unrestricted document and therefore open to the public. Nonetheless, there are many exceptions with respect to public and private interests. Secrecy in Swedish law is treated in the Public Access to Information and Secrecy Act of Sweden (2009:400). This law provides exemptions to public documents and contains rules regarding professional secrecy. In order to be valid, all claims of secrecy must be supported by law.

"Secrecy means that there is a ban against disclosing information either verbally or in written word. The ban applies to authorities where information is confidential as well as to those persons who by their appointment, assignment or the like have learned of the information. Information can sometimes be accessed with the provision (penalty sanctioned) that it is not further distributed."

Different lengths of time are applied to the issue of secrecy in accordance to special regulations. Furthermore, the Act applies only to public activities. For private organizations, a special law exists regarding the protection of business and trade secrets (1990:409). Finally, an employee can be obliged to observe professional confidentiality according to employment contracts (National Encyclopedia of confidentiality, 2011-06-29: search word "sekretess").

planning continues. Just as it is important to exercise information and cyber security, it is important to maintain the determined level of security and confidentiality throughout exercise planning as a whole.

Thus, the mission statement clarifies, already in the beginning of the project, how this information should be handled in practice, where it can be used, and who has the right to use it. The mission statement is the governing document to so it focuses the project management and planning exercise efforts, and it is also the foundation for all decisions regarding contracts, plans, conditions, evaluation, and so on.

Analysis of the mission statement

After the mission statement has been formulated, the exercise/project manager analyzes it by looking at the title, background, assignment (purpose, amendments, contacts, time, etc.), and the demands it places on the organization and its financial position.

The second step is establishing a dialogue with the client about the mission statement. The client can be, for example, the organization's management group, a department within the organization, or another agency. The reason for emphasizing a meaningful dialogue in this phase obviously is to try to eliminate confusion and misunderstandings about the assignment (exercise) regarding what it is supposed to contribute to and how it is supposed to be implemented.

The mission statement, for example, raises specific questions about:

- Purpose, definition, and scope – What is the purpose? Why was this project established? What problems should be solved? What issues should we not attempt to address in this project (boundaries and limitations)?
- Objectives and target group – These should be discussed here, but they will also reappear in the next phase of the exercise planning.
- What results does the client expect? What do they want to achieve and have the ability to with the given resources? In what way should the results be presented?
- How does the time table look? When and if should there be debriefing sessions and points for decision-making?
- How should decision-making be made? (Who decides what?)
- Criteria for the evaluating the project (proposed exercise).
- Additional requirements regarding the project (maximum cost)?
- The role of the involved stakeholders (What is expected of them?)
- Need for cooperation with other organizations and the client's requirements regarding this issue should be stated at the outset.

- Intellectual property
- Security and confidentiality

The result of the above discussion can be used to reword the final mission statement, or it can be described in future project planning, the so called master plan.

Risk analysis[20]

In the beginning of the project before it is launched, it is a good idea to do a risk analysis of the factors that significantly influence the project as such (not its contents). This can be done by using a SWOT analysis where the strengths, weaknesses, opportunities, and threats are listed and summarized.[21] The risk analysis should be regularly reviewed and updated throughout the project. In the next step (exercise planning), there may also be a need to make separate risk analyses within each working group (for example, for the exercise management team, the game management team, the technical working group, evaluation groups, and so on).

The results of the risk analysis can affect the existing strategy for project implementation and also serve as a warning light for the project management and the commissioning organization in the ongoing process of dialogue.

[20] This section builds upon Chapter 4 ”Direktivet – En uppdragsbeställning” in Wisén and Lindblom (2009) p. 50-64.

[21] Another tool is a force-field analysis where the helping and hindering forces on the project are weighed against each other in the form of arrows corresponding to the power of influencing factors. A third way may be a risk matrix in which the identified risks are lined up with the possible consequences. The probability of the consequences are assessed (high, medium, and low), and then their potential impact on the project is assessed. The matrix should also consider proposals to address the risks, measures to be taken, allocating responsibility, as well as a time table for monitoring and managing the risks. The factors for the probability (p) and impact/effect (e) of the consequences can also be defined numerically from 1 (very unlikely and negligible) to 5 (very likely and alarming); of which, the risk is obtained by the formula: r = pxe.

5 The Mission Statement

5.1 Continuation of taking inventory and considering the needs of the exercise

Defining the mission statement involves a continuation of taking inventory and considering the needs of the exercise which were discussed in the exercise preparation phase.

During this step in the exercise planning process, the need for external resources (e.g., consultants) and cooperation with other parties for planning, implementation, evaluation, and feedback should be taken into consideration. This should be done so that additional resources can be ordered in a timely manner since some resources may have restricted access (such people power/ consultants and technology). Yet this will also allow ample time for the establishing contracts and agreements with other parties (organizations, agencies, and businesses).

5.2 Exercise documentation

Useful documentation for this step in the planning and project process includes:

- the mission statement
- consulting agreement(s), and
- agreements/arrangements with the other involved parties.

Suggestions for the contents of such documentation are available in this handbook's appendices. The handbook will also revisit the issue of documentation in a separate section; see Chapter 7.

Reminders and helpful hints!

- Get a written mission statement from the client commissioning the assignment and maintain a dialogue where it can be analyzed before starting to plan the exercise.
- Conduct a risk analysis already in the project's commencement and before the project is officially launched. The risk analysis should be regularly reviewed and updated throughout the project.
- Consider and calculate the need for external resources (e.g., consultants), and the time needed for establishing contracts and agreements with other parties (organizations, agencies, and businesses).

Planning (3 of 3)

	PLANNING			
PROJECT MANAGEMENT PROCESS	(1) Generating ideas and doing a preliminary investigation		(2) Establishing a mission statement and a risk analysis	(3) Project planning and project organization
EXERCISE PLANERING PROCESS	Exercise preparations	Master plan	Mission statement	Planning the exercise
CHAPTER IN THE HANDBOOK	Chapter 3	Chapter 4	Chapter 5	Chapter 6
ACTIVITIES	• Taking inventory and determining the needs for an exercise	• Multiyear exercise plan • Exercise as a learning process	• Cont. taking inventory and determining the needs for an exercise	• Exercise's purpose and objectives • Exercise forms and types • Time table • Planning organization
EXERCISE DOCUMENTATION			• Mission statement • Consulting agreements • Agreements with involved parties	• Project plan (description of activities, project budget, time table) • Project discrepancies

Project management process: Establishing the project plan and project organization

This step in the project management process corresponds to "Exercise planning" (Chapter 6) in the exercise planning process.

Project planning is best done with the joint effort of the project group, and thereafter a project plan can be compiled. This plan (indicated with the respective version number) should contain:

- objectives, focus, and limitations
- strategy and methodology
- general activity plan and time table
- project budget

- project organization (who should be involved as well as roles and responsibilities)
- internal and external information and communication
- the expected end product
- anticipated effects

The project organization is set up. Within the exercise planning process, this includes the planning organization, the evaluation organization, and the implementation organization.

The project organization for information and cyber security exercises includes a planning organization, an implementing organization and an evaluation organization. Yet when the exercise is actual being carried out, the implementing organization has a more prominent role (See also examples of these in Chapters 6 and 7 below.)

6 Exercise Planning

6.1 The exercise's purpose, objectives, target group, and limitations

The first step in the planning exercise is to determine the exercise's purpose, general objectives, and limitations. This part of the planning is based on previously established directives and dialogue where the purpose has been clarified and possibly a discussion on some of the objectives, target group and limitations. However, here the actual formulation of the objectives (or the process for achieving the objectives, the so-called objectives) occurs.

The purpose of the exercise refers to why there should be an exercise and the reasoning behind it. It provides a general description of the direction without the need for measurability. The exercise's objective(s) should be fulfilled via the exercise. It is achieving a desired state/condition at a given time which is accomplished by the exercise. The target group includes those individuals or groups who should be trained. The limitations of the exercise are those things that cannot be achieved via the exercise and that are articulated in advance.

In order to carry out a proper evaluation of the exercise, it is important that the purpose and objectives are clear and comprehensible. The evaluation is important because it affects, and is affected by, all of the other components of an exercise. Thus, from the outset, the evaluation should be a part of the planning exercise.

6.1.1 Purpose – why we should have an exercise

The reason why an information and cyber security exercise is arranged and implemented can vary as well as the purpose. Examples of the purposes of the exercise may be to:

- educate by teaching something new to the participants – individuals or organizations should be given the opportunity to gain greater knowledge and skills
- test a new organization, technology or something else and thereby reveal strengths and weaknesses
- unconditionally develop activities (e.g., by cooperating or communicating with the outside world)
- measure ability and endurance.

6.1.2 Objectives – What we want to achieve with the exercise and formulating the objectives

The objectives of the exercise can be divided into main and intermediate objectives by [...] breaking down the objectives into more specific intermediate objectives. The person or people who will evaluate the exercise should be involved in the development and formulation of measurable objectives so that it is possible to assess and evaluate the objectives (i.e., determine whether or not if they are achieved).

Above all, the objectives should be measurable. There is a mnemonic rule for creating clear and observable objectives; that is, the objectives should be "SMARTA":

- Specific – clearly defined
- Measurable – detailed
- Accepted – approved by the clients, exercise management, and evaluators
- Realistic – reasonable and possible
- Time limited – a time should be determined for when the result/capability should be achieved
- Adequate – appropriate in relation to the purpose

The objective formulation can be simplified by using activity verbs in order to describe the results that the exercise should produce. These may include "know," "master," and so on. Moreover, it is important to spell out what is meant by "know," "have good knowledge of," or "have the ability to" in order to establish concrete criteria for assessing the ability to achieve these objectives in the evaluation.

The following questions can also provide support in the formulation of the objectives:

- What skills/ability should the participants have achieved after the exercise?
- What is the objective of the exercise as a whole and what are the intermediate objectives of the exercise?
- What limitations should be made?
- What are the shortcomings and weaknesses?

6.1.3 Target group – Who should participate in exercises?

The target group consists of those individuals or groups, units or the like who intend to participate in the exercise based on the defined purpose and objectives. An exercise can include different kinds of participants (such as IT technicians, security managers, lawyers, or members of the organization's management) or be conducted at different places within an organization, and consequently have multiple target groups. However, it should be clearly stated what the measurable objectives are and to which target groups they apply in order to enable a proper evaluation.

6.1.4 Limitations – what will not be addressed in the exercise

Limitations of the exercise include those things that in advance have been decided will not be addressed or realized during the exercise. For information technology and cyber security exercises, this may mean, for example, that the exercise intends to exercise an organization's internal incident response management in just one system, not all of them at the same time.

6.2 Exercise types and forms

When choosing a method for an exercise (that is, the exercise type and form), it is important to use the purpose and objectives of the exercise as the starting point. To that, the following questions may be helpful:

- How many people will be involved in the exercise simultaneously and in what function?
- How long will it take to plan, carry out, evaluate, and do a follow-up of the exercise?
- What financial resources have been allocated?
- How much experience has the organization had with exercises?

With the answers to the above questions in hand, the next step is to review and determine which exercise form and type are most appropriate.

6.2.1 Exercise forms

The most common exercise forms in information and cyber security exercises, which are also addressed in this handbook, are:

- seminar exercises (also called table-top exercises or workshops)
- simulation or 'controlled environment' exercises, with a counterplay
- a so-called 'live' exercise in the existing system(s) in real time.

All three exercise forms can be carried out either all on the same site or a distance exercise (distributed exercise). The exercise forms complement each other and an exercise may contain elements of different forms, if this is appropriate for achieving the purpose and objectives of the exercise.

6.2.1.1 Exercise seminar (table top exercise or workshop)

The simplest exercise form is a seminar exercise. A seminar exercise means that an instructor leads a discussion on a particular issue or scenario with the participants. A seminar exercise can be relatively simple if it is restricted to a specific area or limited task which can be exercised. Here there are fewer participants and the exercise requires less time so it costs less. Likewise, the ordinary operations are less affected by this exercise than with more advanced exercise forms. Another advantage is that those who participate in the exercise have the opportunity to deepen their thoughts on different issues. Everyone has the opportunity to discuss what happens in the exercise and by commenting, asking questions and raising objections.

Great demands are placed on the exercise seminar moderator, that is, the one who leads the exercise. The more complex problems that are discussed during the exercise, the greater the demands are on the moderator's expertise in the relevant areas. In this exercise form it is important to document the issues and problems that emerge during the exercise, which need to be investigated and worked on later. Therefore, a person should be appointed to take notes so that important details are not missed. The description of the scenario can either be given all at one time or in phases where the crisis situation gradually becomes more complex or changes depending on the participants' responses. A number of problems are presented, and participants, either all together or in smaller groups, discuss the potential dilemmas and solutions. The simplest variant of an exercise seminar is a group discussion based on for example a newspaper article. Questions may be raised regarding how the organization would have reacted in this case as well as what kind of support and help it would have needed.

In order to help describe the scenario or the event in which the seminar exercise has been designed, the exercise can be made more realistic by utilizing the following practical tools which may be based on real or fictional material:

- maps
- slideshows
- power point presentations
- film clips
- visual images and audio recordings

6.2.1.2 Simulation or 'controlled environment' exercises with a counterplay

Simulations controlled environment or games, as an exercise form, are as much as possible done in an environment with tasks that would appear in reality during a crisis caused by a major IT incident. In the case of information and cyber security exercises, exercises are advantageously conducted in a constructed, fictional game environment, where the infrastructure is set up separately from the organization's existing IT environment."

Based on the overall scenario, the participants should respond to the events which "are played" and act accordingly. It is important to remember that you cannot pretend that things have been done. Everything must be carried out as if it were a real event. It is extremely important to adhere to the information provided and refrain from replacing or excluding this information.

So that the participants have something to respond to, a counterplay is needed. The counterplay consists even of so-called messengers who provide the participants with events injects in the form of playing cards. Depending on the size of the exercise, the counterplay can consist of anything from a messenger with a telephone to a large counterplay headquarters with experts and advanced technical support.

The counterplay acts as the outside world in the exercise, playing the role of various people and organizations with whom/which the participants may need to come in contact. These roles may include individuals, businesses, organizations, and government agencies. The participants are enclosed by this simulated outside world. This means that all interaction is conducted between the participants and the counterplay. One exception is when fact-finding is done without the counterplay.

The information and actions that develop the course of events and create the simulation are known as injects. The messengers in the counterplay provide the participants with injects in the form of, for example, telephone calls, faxes, emails, radio announcements, and TV broadcasts.

In order to conduct such an exercise, major efforts are required in the planning and production of the game plan, including the instructions to the participants and those running the game, time tables, lists of performances, materials, and much more.

A simulation often provides a very high educational value both for the participants of the game and for those who are counterplaying. The amount of that is played vs that is simulated (counterplay) can vary greatly.

Counterplay exercises can, in fact, be implemented on a much smaller scale. For example, the simplest variant can be a counterplay consisting of just one or two people sitting in an adjacent room providing injects to the participants.

6.2.1.2.1 Injects during a simulation

An inject should always have a purpose. It should result in the participants react. The purpose may be, for example, to get the participants to initiate cooperation/contact or to apply a certain action, or simply to increase their workload. When the list of injects (menu) is established, the expected action of each inject should be written down; in part, to facilitate the messenger in conveying the event/action to the participants, and to enable a proper evaluation after the exercise.

A simulation can be more or less interactive depending on the counterplay's ability to play upon the development of the delivered injects in the form of new injects. This depends on the ability of the participants to act in their roles. Injects may consist of developing events, consequences and reactions from the outside world, and even the results of simulated operational initiatives.

The injects that are delivered to the participants are a predetermined course of events surrounding the crisis situation or event. This is done in accordance to a specific list of events (play plan or game book) so that injects are delivered in predetermined order. The data can alternatively be fed into any technical gaming support system (database).

The injects are delivered via realistically designed radio and telephone messages, fax, email, personal visits, and so on. The public and media reactions may be reflected by phone conversations and emails to the participants with continually recurring questions and requests for information. The injects should be thoroughly prepared in advance so that the messenger can easily read them out loud or act upon them. Additional injects can also be made during the game. They may be used, for example, in order to poke the participants in a certain direction or to get them to act if they are not taking the intended measures.

However, these must be agreed upon with the exercise *controller* so that they do not conflict with, for example, other injects. With the continuous flow of injects, the simulation exercise is carried out without stopping for discussion or for a retake if things goes wrong. The aspect of limited time is part of the exercise.

An important feature of the messengers and the counterplay is that they have an instinctive feeling of knowing when it's time for an inject and when they should just let the participants' reactions stimulate events so that the game becomes self-generating. The counterplayers must strike a balance between keeping the right amount of pressure on the participants – neither overstimulation nor understimulation (unless it is the purpose of the exercise). By maintaining contact with the observer, the evaluator, or the local exercise *controller* for the participants, the counterplayers can thus be adapted so that the desired amount of pressure is created.

The messengers should have a thorough knowledge of the organization and in the subject area relating to the scenario (the playback sequence of events). It requires creativity, factual knowledge, and empathy, and sometimes also a high threshold for stress in order to partake as a messenger in the counterplay.

6.2.1.2.2 Relation between the exercise's injects, major events and phases

Exercises often require a clear structure in order to be properly implemented. If the planned exercise is a simulation exercise with a wide variety of events, it may be a good idea to divide it up into different levels.

Based on the background scenario, a number of major events are established. The major events are then grouped into phases and respectively, each exercise phase provides the basis for formulating the individual injects.

6.2.1.2.3 Location and premises for the simulation

If the purpose of the simulation exercise is to increase the participants' knowledge and ability to handle a particular situation, it is beneficial to run the exercise on the ordinary premises, command center, or another place that is used for real crisis situations. Consequently, the participants will learn to use the ordinary means and devices that are intended for crisis situations and for providing technical assistance.

The simulated environment can also be arranged on another location provided that the simulation environment, namely the controlled environment, is mobile and that the "host site" has an appropriate technological infrastructure to support this. Another site can be located at a particular organization, at a training center, a hotel or a similar place. Likewise, technical support equipment and services should be adapted to the local conditions and needs.

The simulated environment can also be a specially prepared for the purpose of local such as an IT lab, and telephone lines can be pulled in. In this case, it is fitting if an adjacent group room is available for the communications equipment.

Suitable supplies for simulated exercises may consist of:

- telephones
- radio communications with frequencies designated for the exercise
- radio and TV
- Internet

- e-mail
- fax
- video conference equipment
- large screen projector for computer graphics and such
- maps, sketches, and monitoring tables
- plans
- plotting supplies
- hand books
- list of resource.

6.2.1.2.4 Counterplay headquarters

The place of counterplay – the counterplay headquarters – should be conveniently arranged on the premises with the necessary equipment (radio and telecommunications, etc.), similar to that being used by the participants. During large exercises with many functions or groups being exercised, many different kinds of technical assistance, perhaps even a technical game support system, may be needed.

The counterplay headquarters should be staffed by the game controller and a number of messengers who help control the game by maintaining the desired direction and focus via the counterplay. The messengers represent all the functions that the participants need to get in contact with during the exercise over and beyond those already in the exercise. The counterplay is led by the game controller.

6.2.1.3 Live exercises

A live exercise, also called a practical exercise, can in some ways be likened to a field exercise in that it is implemented in a real environment. A live information and cyber security exercise can be conducted in an organization's existing systems with the resources that would be used in a serious IT incident and a real crisis. A live exercise can also be used to test and identify vulnerabilities in existing systems while organizational functions (such as the management) are exercised in parallel.

For this kind of exercise it is even more important that the purpose and objectives of the exercise are anchored with the client and that sufficient time and resources are devoted to informing and instructing the participants and those involved about what they can and must do in order to prevent affecting their regular operations.

6.2.1.4 Seminar, simulation or live exercise?

A seminar exercise is a good exercise form for groups since they are able to theoretically analyze problems and discuss potential solutions in an atmosphere with less time pressure and stress; for example, regarding practical solutions to resource needs, management issues, and so on. Moreover, one does not need to put too much time or money in putting together (simulating) a course of events. One or just a few demonstrations given by the exercise controller (moderator) may be sufficient. Seminar exercises are a relatively simple and easy-planned exercise form with good efficiency.

Seminars can be used, for example, to

- highlight and develop:
  - roles
  - areas of responsibilities
  - tasks
  - the organization
  - working methods
  - priorities
  - cooperation
  - support functions
  - practical or technical needs
- analyze a particular risk or vulnerability
- evaluate a plan
- investigate and analyze potential problems in cooperation.

Simulation exercises are most suitable when the objective of the exercise is to test functions, organization, cooperation arrangements, and so on. It can also be used where seminars are appropriate. An experienced organization that has already done several exercises may choose a simulation exercise with counterplay. This usually requires that the organization is well established; that is, the structure, roles, tasks, and so on are clear and well-anchored.

A live exercise should be used with caution so that it does not interfere with regular activities. It is used, above all, to test an organization's existing systems and procedures as well as identifying vulnerabilities and weaknesses within them. This exercise form requires very good planning and careful preparation so that it does not put the organization in a compromising situation where the entire information system or parts of it are interrupted or shut down because of the exercise.

6.2.2 Exercise types

One exercise type that is commonly used for information and cyber security exercises is called the Red Team – Blue Team Exercise. This approach is suitable for all exercise forms (workshops, simulations and 'live' exercises) and is above all preferred in simulations/controlled environment exercises because it is flexible and able to support the different objectives of an information and cyber security exercise.

In addition, there are several other exercise types that can be useful. For example:

- unannounced 'live' exercises
- initiation exercises
- staff exercises
- decision exercises
- management exercises
- cooperation exercises
- red team – blue team exercises

The type of exercise (for example, an unannounced 'live' exercise, staff exercise, cooperation exercise, and so on) reveals the function or activity that the exercise primarily addresses. It can also be seen as a model or template for categorizing exercises. The type of exercise is determined most appropriately by the objectives and purpose of the exercise, as well as the size and scope of the exercise.

An exercise type can be carried out in various forms. For example, a staff exercise can either be done as a seminar exercise with discussions revolving around the staff members' work and tasks that should performed, or as a simulation with a counterplay. In some cases it may be sufficient to have the management team gathered around a table and in seminar setting have the exercise controller ask the participants what they would do in a specific situation with certain conditions.

6.2.2.1 Unannounced 'live' exercises

The purpose of an unannounced 'live exercise is to train an organization by alerting those likely affected by a certain situation and getting them to come to a designated place by a certain time. This may include a staff, a crisis management organization, or the like. This usually applies to an organization's own staff, but it may even apply to other contexts. This may need to be exercised recurrently so that the crisis management can begin its work early during a crisis.

6.2.2.2 Initiation exercises

An initiation exercise usually means that one builds upon an unannounced 'live' exercise in that the emergency management organization is quickly activated and is able to assume its tasks. An initiation exercise is thus a way to train and develop the ability to get the crisis management quickly started.

The following steps can be included:

- The exercise participants should meet on-site so the exercise controller can explain the terms of reference.
- The site should be in order and equipped.
- Every participant should prepare their workplace and ensure they have the necessary means.
- Computers, telephones and other equipment should be connected and tested.
- Plans, instructions, checklists, other written materials, and maps should be produced and checked.
- Contact information (including phone numbers and email addresses) for the individuals from the cooperating organizations should be listed and checked.
- Those responsible for providing technical services, catering and other support should be called to on- site.
- Weaknesses and uncertainties should be continuously noted by each and every one for they may be later rectified.
- Lastly, a staff orientation should be organized.

When there is a break or a time-out during the exercise, this is good opportunity to have a quick informal briefing.

Similar to unannounced 'live' exercises, initiation exercises should be conducted periodically so that the crisis management can be commenced early in a crisis.

6.2.2.3 Staff exercises

A staff exercise is designed to increase the ability to work with internal preparations as well as staff and information routines in order to create a common understanding and the ability to propose decisions. In cases where the structure and practices differ from ordinary procedures, it is particularly important to conduct staff exercises regularly.

6.2.2.4 Decision exercises

A decision exercise is mainly used to train decision-making within an organization; that is, despite time pressure, the ability to make early and clear decisions on measures as well as to initiate collaboration between those holding responsibility and the other stakeholders. The ability to make decisions in unfamiliar and stressful situation needs to be trained regularly.

The target group (for example, business managers, experts, advisers, and others) for this type of exercise consists of those who can do the groundwork and create a basis for decision-makers and who propose decisions. With a good support foundation, the ability to make quick and clear decisions is greatly accelerated.

A decision exercise should include the following considerations and situations that decision makers may have to face; for example:

- mandate
- actions/measures
- information management
- reporting
- cooperation.

6.2.2.5 Management exercises

A staff exercise can often be combined with a decision-making exercise, as well as an unannounced 'live' exercise and an initiation exercise. Such a combination is referred to as a management exercise. The focus is often on the roles, organization, procedures, priorities, and so on.

6.2.2.6 Cooperation exercises

In a cooperation exercise, coordination via collaboration is essentially trained. The authorities and organizations at different levels of government involved in a crisis need to exercise together in order to be able to cooperate in a real emergency.

Cooperation exercises can be performed on a large scale, such as between many agencies and companies in various areas of collaboration, as well as on a smaller scale between a few players (for example, on the sectorial or regional level). Cooperation exercises should be conducted regularly.

Such exercises can include:

- ’vertical’ cooperation between national, regional and local levels in society
- ’horizontal’ cooperation
- cooperation within one societal sector with both public and private actors
- cooperation involving several societal sectors
- cooperation between various societal sectors and geographic areas of responsibility

6.2.2.7 Red team – blue team exercises

The name of this type of exercise has its origins in the military's test of combat readiness. The exercise setup usually consists of two groups/teams that play against each other. For instance, the red team (e.g., consisting of professional security 'ethical' hackers) attack the blue (defensive) team's information systems. The blue team has the task of protecting its systems and detecting intrusions and serious incidents or incidents with the potential to escalate. This type of exercise has been used to test the physical security of vital infrastructures, such as nuclear power plants and high-tech laboratories. In the 1990s, experts began to use this type of exercise to test the security of information systems.

Red team – blue team exercises may have a variety of constellations. For example, an exercise may consist of several blue teams that, either individually or together, work together to protect their systems against one or more attacking red team(s). Another exercise may include just the blue team (one or more), without any red team, and be tasked to protect their systems, detect intrusion, and report incidents.

It is even possible to set up a so-called two-sided exercise where two or more teams are attacking each other and at the same time each team needs to protect its own systems. In this case, it is extremely important that the project management and exercise planning group clarify the purpose and objectives of the exercise. Since it is often unclear what is being exercised with this specific type of exercise, the two-sided exercise is not strongly recommended.

Red team – blue team exercises are flexible in that they can be modified depending on the team's knowledge of the system(s) in which they are exercising. Participants can thus go into the exercise with: no or very little knowledge of the system(s) in which they will be exercising, very good knowledge of these, or anything in between. The exercise method indicating the team's knowledge of the system(s) during the exercise is sometimes referred to as: White-box – with full knowledge and transparency of the systems prior to the exercise, or Black-box – without any knowledge of the systems prior to the exercise.

Red team – blue team exercises are also discussed in section 6.4.4.

6.2.3 A combination of exercise forms and exercise types

All exercise forms can be combined with the various exercise types. For example, an initiation exercise can be performed either as a seminar exercise, simulation exercise or live exercise. This also applies to staff, decision-making, management or cooperation exercises. However, some exercise types are better implemented in a particular exercise form. For example, it may be appropriate to conduct an unannounced 'live' exercise in the form of a live exercise where the participants have the opportunity to train the alarm chain (for example, for serious incident reports) in the organization's own systems to ensure that they function, can detect potential vulnerabilities, and also ensure that incident management plans/contingency plans work.

6.3 Time table for exercises

During the initial exercise planning and in the selection process regarding the exercise method (i.e., the form and type of exercise), it is also important to determine the amount of time needed for planning meetings, briefings, and more. The mission statement stipulates the purpose, objectives, and limitations of the exercise, which creates the framework for selecting the exercise form and types and to some extent even the time table for the exercise.

Seminars require less time whereas simulations and live exercises require significantly more time and resources. By having access to the technical infrastructure (exercise environment) and the real system(s), the time for preparing and planning simulation and live exercises is significantly shorter every time an exercise is carried out; whereas, more time is actually required for planning and developing scenarios.

However, it is important in the master plan to discuss and determine:

- The actual time for carrying out the exercise (how long and when will the exercise be run: one, two or more days; only during the day or around the clock; every day or just work days, etc.).
- The virtual/play time during the execution of the exercise. (This is related to the set-up of the exercise scenario and what is supposed to happen within the framework of the exercise. It is likely that the exercise's purpose and objectives will put certain requirements on the set-up of the exercise. For example, the exercise may need to be divided up into different phases. Doing this will make it possible to make a leap in time during the exercise which in turn may be known or unknown to the exercise participants.)
- Time for briefings during the exercise and feedback afterwards.
- Synchronized time (time zone and the actual time) for all systems during the execution of the exercise. Synchronized time is, above all, important for controlled environment exercises (distributed or not) and live exercises with multiple work stations and systems involved.

6.4 Planning organization

Planning for large exercises with many participating actors should start well in advance – in some cases several years in advance. Preliminary planning with an open discussion on exercise ideas and the level of ambition between the commissioning organization and project management are usually held during the phase "exercise preparation. In connection with the first meeting (kick-off meeting or the initial planning session), it is advisable to create an organization for planning the exercise with the actors (exercise management and counterplay organization) who will participate in the planning process. Also it is a good idea to determine early on which roles and responsibilities these actors should have.

See Figures 1 and 2 for examples of planning organizations for small and large information and cyber security exercises.

6.4.1 The commissioning organization

An exercise can be ordered by an authority responsible for a sector of society, municipal leaders, or business management. It is the commissioner of the exercise that stipulates the main focus of the exercise's purpose and objectives, and usually provides funding.

6.4.2 Steering committee

The steering committee is usually composed of individuals with senior positions in the administration or organization that has been commissioned to plan and carry out the exercise. The steering committee's tasks can be, for example, to decide on the project management's proposals for implementation (e.g., scope, funding, resources and limitations) and decide on the exercise's overall objectives. The steering committee should also, where appropriate, assist the client concretely formulating the mission.

6.4.3 Project management

The project management consists of the project leaders, project secretary and possibly several of the participants depending on the scale of the exercise. The main task is to manage and make priorities within the project considering the given constraints. This includes structuring the project into various working groups, making a schedule/work plan, answering to the project management, being responsible for the budget, organizing the kick-off meeting (the initial planning conference) for all of the participating organizations, reporting to their colleagues and the steering committees for all of the participating organizations, processing and compiling the proposals from the working groups, and providing guidelines for further work. It may be appropriate that the project management even establishes an exercise organization for carrying out the exercise.

The project secretary is responsible, for example, for documentation of the exercise plan as well as of the terms for the exercise and the exercise management. Other tasks may be to assist the project manager with meeting notices, keeping minutes of meetings, being responsible for the information on the web site, and so on.

During larger IT and cyber security exercises someone should be appointed to be in charge of information management, coordination, media and communication, and visitors before, during and after the exercise. Similarly, another task is coordinating the flow of information and ensuring that the necessary materials from the project management and the exercise planning process are available for the participants in the media which has been agreed on mutually. The media and communications manager writes and coordinates, among other things, press releases and invitations to the media and observers, as well as handles visitor programs, manages information to the media, and takes care of those invited on their own accord or coordinates this with other available for comment during exercise.

6.4.4 Working groups and colors of the working teams

The number of working groups usually varies depending on the size of the exercise. For a large and extensive exercise, it may be appropriate with a scenario group, a counterplay group, a group for technology and communications issues, a logistics group, a group for receiving invited visitors, and so on. Within the framework of the exercise objectives and scenario, a working group should actively participate in the exercise planning. Each working group should have person who serves as a liaison for the group with the project management.

For information and cyber security exercises using the red team – blue team approach, color designations are used for the working groups. The name red team is used for the counterplay group, and it can even be used to designate the scenario development group if the red team is not being trained. For these cases, and in major exercises, there tends to be a separate task force appointed for the scenario. During an exercise, the blue team is usually being trained. The white team is usually used to indicate the exercise management, and the green team is usually the working group for the technical training environment, technology, and communication issues.

Additional working groups, such as lawyers, the organization's management, and the evaluation team may also be fitting. (See Figures 1 and 2 below for examples of planning organizations.) It is entirely up to the project management to assess and determine the number of working groups and any color designation.[22] It is important to consider that the more groups there are, the greater the demands this puts on coordination, communication, and information sharing.

[22] The most common color designations include: the yellow team for the scenario development working group, the purple team for the legal working group, the orange team for the organizational management's working group, and the light green team for the evaluation team

6.4.4.1 Example of the planning and implementing organization for the Baltic Cyber Shield 2010 [23]

White team – exercise management
During planning, the white team was responsible for the development of rules, including scoring. During implementation, the white team together with the game management and the counterplay organization (red team) directed the exercise via injects from the prepared game plan (game menu). The white team took care of the manual scoring as well as the evaluation of the blue team's efforts. The white team was also responsible for visitors and the visitor program.

Red team – counterplay organization
The red team attempted to disable and impair the functionality of the systems that the blue teams were protecting. This was done in a controlled and consistent manner throughout the exercise. A preliminary list of the phases and objectives was compiled during the preparation stage in order to create a good structure for the implementation of the exercise.

Green team – technical exercise environment
The green team (group for the technical training environment as well as technology and communications issues) was responsible for preparing the technical infrastructure. This included VPN access to the game environment, the creation of systems for the blue team, the different arenas for presentations, logging in, and so on. During the implementation, the green team also served the role as the Internet Service Provider (ISP) for the blue team.

Blue team – exercise participants
The blue team consisted of the exercise participants, of which there were several during the exercise. Their job was to protect the IT infrastructure in the fictional organization from attacks by the red team.

[23] The section is an excerpt from Karlsson, J. (May 2010) ”Rapport efter CCD COE – Swedish CDX 2010” [Report after CCD COE – Swedish CDX 2010]. Report to MSB from the Center for Asymmetric Threat Studies, Swedish National Defence College.

6.4.5 Reference group

A reference group can be composed of representatives from all of the participating actors; that is, organizations being trained. The reference group can also include the client/commissioner of the exercise. The task may be to verify that the exercise's overall objectives are met and that the authority's or organization's purpose is taken into account."

The reference group can also be made up of experts and used as a sounding board before, during and after the exercise. The group ideally should be diverse in order to be able to assist the exercise management or the exercise controller.

6.4.6 Evaluation organization

The evaluation of the exercises and the process of developing and carrying out an exercises is described in more detail in the handbook for the evaluation of exercises that MSB has published.

Here, the various evaluation roles needed for an exercise are defined. See also Chapter 9.

6.4.6.1 Exercise evaluator – responsible for the evaluation of the exercise activities

The exercise evaluator is responsible for evaluating whether the participants achieved the exercise's objectives and purpose. The participants' actions are assessed. In order to be able to do this, it is necessary that the exercise objectives are measurable. The results should be compiled in a final report which is distributed to the exercise participants.

6.4.6.2 Project evaluator – responsible for the evaluation of the project

The project evaluator is responsible for evaluating the entire exercise project, including planning, cooperation between the involved actors, and so forth.

The project evaluator should support any local evaluators if there is a need for this.

Figure 1: An example of a planning organization for smaller information and cyber security exercises

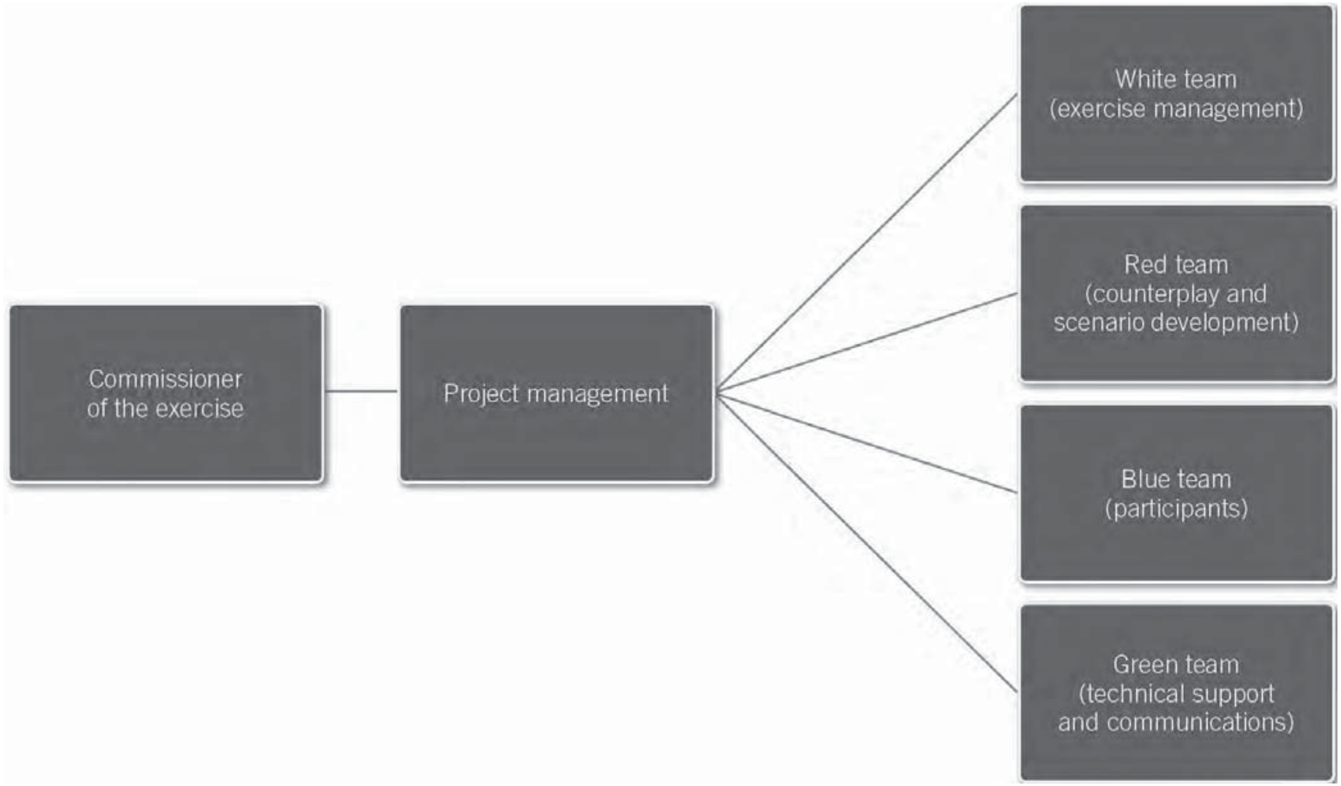
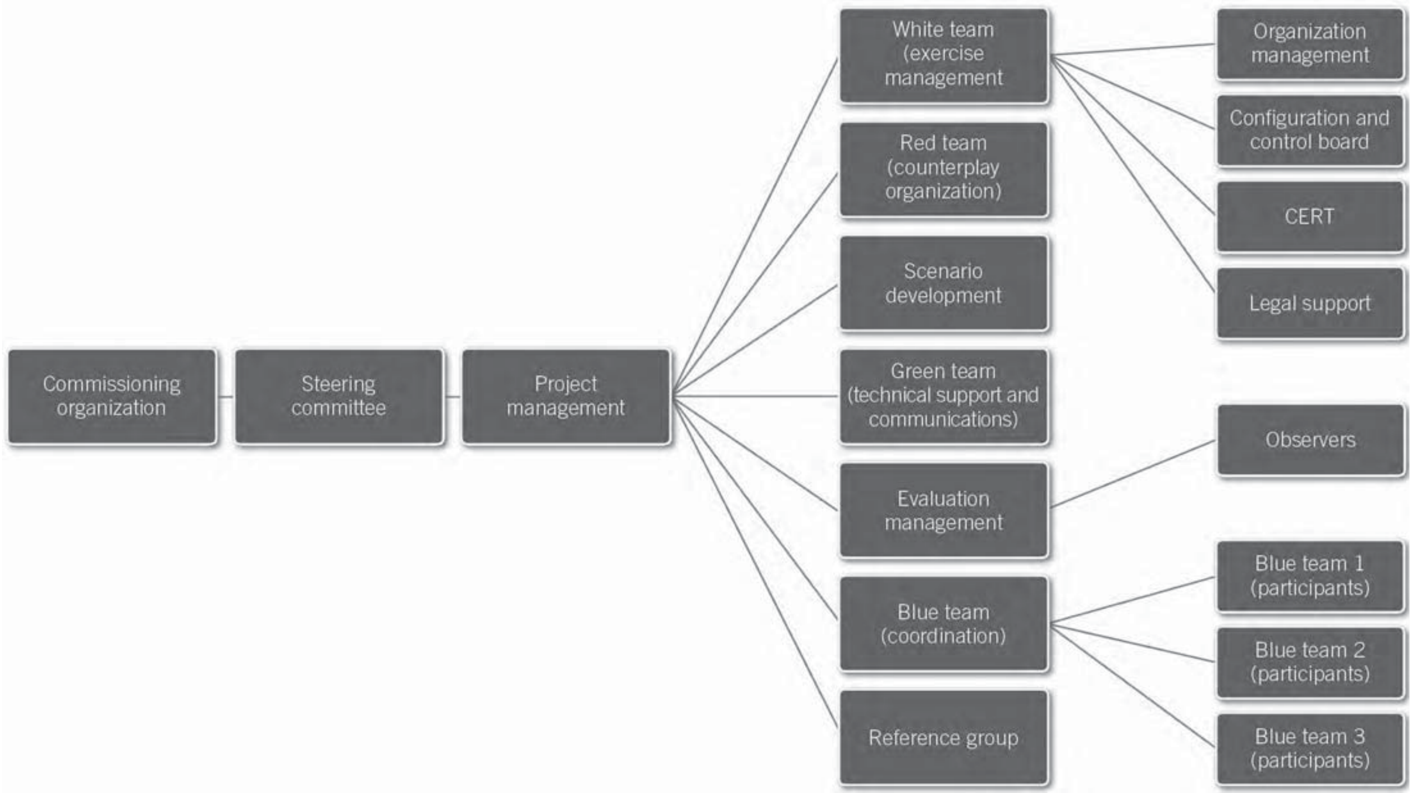


Figure 2: An example of a planning organization for a larger information and cyber security exercise


Commissioning organization
Steering committee
Project management
White team (exercise management
Red team (counterplay organization)
Scenario development
Green team (technical support and communications)
Evaluation management
Blue team (coordination)
Reference group
Organization management
Configuration and control board
CERT
Legal support
Observers
Blue team 1 (participants)
Blue team 2 (participants)
Blue team 3 (participants)

6.5 Exercise documentation

- Project plan (description of activities, project budget, time table, etc.)
- Project discrepancies

Reminders and helpful hints

- Establish "SMARTA" objectives. The exercise's purpose, objectives and target audience determine planning, implementation and feedback.
- Include the management for technical support and communications (responsible for the infrastructure used in information and cyber security exercises) in the evaluation management for the exercise planning and for defining the purpose and objectives.
- Select the exercise method (exercise form and type) based on the purpose and the objectives of the exercise. In IT and cyber security exercises, the exercise type red team – blue team is often fitting since it is suitable for all exercise forms (workshops, simulations and live exercises) and can support various exercise objectives. However, it is always the purpose and objectives of the exercise that determine the method of implementation.
- Establish a time table for when the exercise will be held as well as the duration of the exercise since these factors are significant for the scenario development of IT and cyber security exercises in the next step - practical preparations.
- Set up a planning organization with clear responsibilities in order to facilitate the coordination of the exercise and its implementation. If possible, physically assemble the planning organization (in particular, the project management, exercise management, and counterplay organization/game management) in order to simplify information and communication management within the planning organization.
- Collect and coordinate information and communications - if possible in one location for archiving, documentation, etc. (but still with the possibility for using numerous communication channels). This is important for creating a common situation awareness.

Implementation

	IMPLEMENTATION			
PROJECT MANAGEMENT PROCESS	Starting and carrying out a project			
EXERCISE PLANNING PROCESS	Practical preparations	Implementation	Evaluation	Feedback
CHAPTER IN HANDBOOK	Chapter 7	Chapter 8	Chapter 9	Chapter 10
ACTIVITIES	• Implementing organization • Exercise documentation • Scenario • Reviews	• Technical support and communications • Training external communication • Visitors and media coverage • Cont. exercise forms and types	• Cont. purpose and objectives of the exercise • Evaluation and feedback	• Cont. evaluation and feedback
EXERCISE DOCUMENTATION	• Terms of reference for the participants • Terms of reference for the exercise management • Security regulations • Confidentiality terms • Terms of reference for communications • Contact list for the exercise organization • Evaluation documentation			

Project management process: Initiating and carrying out the project

This step in the project management process corresponds to practical preparations (Chapter 7), implementation (Chapter 8), evaluation (Chapter 9) and feedback (Chapter 10) in the exercise planning process.

7 Practical Preparations

7.1 The implementing organization

All games and exercises require a training organization of some kind in order to function during implementation. The requirements for such an organization naturally increase with the exercise's scope and complexity. The simplest organization for small simulations or games can be that the exercise management simply agrees on who does what. For larger exercises, an organization of 30 to 40 people may be needed. The actors and roles that generally exist in the exercise organization are presented below. Depending on the focus and scope of the exercise, some operations can be grouped or organized in various different ways.

See figures 3 and 4 for examples of implementing organizations.

7.1.1 Exercise controller – Person responsible for the exercise as a whole

The exercise controller has the ultimate responsibility for the exercise and is often appointed by the commissioning organization of the exercise. This person is the face of the exercise and during the actual exercise the one who makes major principle decisions on any changes in the implementation of the exercise based on external factors (such as weather or real-life matters) which affect some of the participating actors and the like. This, for example, can result in suspending the exercise prematurely.

The exercise controller is also responsible for external information and communication about the exercise to the media (press releases, etc.). Large exercises may also include a visitors' program for invited guests with tours and presentations of the exercise. The exercise controller may appoint a media and communications officer who is also in charge of the visitors' programs for exercise.

7.1.2 Exercise management – responsible for fulfilling the objectives

The exercise management leads the exercise during its implementation and is responsible that the exercise is carried out in the manner intended in accordance with the purpose and objectives. The exercise's size, scope and complexity will determine how large the exercise management needs to be.

In smaller exercises a person can assume several exercise management roles. In larger exercises, the roles may need to be kept separate or even divided.

7.1.3 Exercise management – responsible for implementation

The exercise controller is responsible for carrying out the exercise and ensuring that the exercise is conducted according to the mission statement. The exercise controller may even decide to suspend the exercise, for example, in order to clarify something that is unclear and that affects the entire or a large part of the exercise.

During the execution of the exercise, the exercise controller responsible for uniting the local exercise controllers if they are participating (for example, in a distributed information and cyber security exercise), game controllers, evaluators, contact people, observers, and the exercise management.

If it is a large exercise with a counterplay and counterplay headquarters, the exercise controller appoints a game controller to lead the counterplay headquarters. The exercise controller and the game controller asses how the exercise is progressing and decide whether or not changes in the exercise need to be made.

Considerations for the exercise controller before the exercise is carried out:

- Read the objectives and structure of the exercise. If the exercise controller was part of the planning team, these tasks will not be so extensive.
- Visit the sites for the proposed events, counterplay, place of live exercise etc. and commit to memory the environment and geography.
- Do a trial run with the participants and exercise management prior to exercise.

Considerations for the exercise controller during the exercise:

- Ensure that the exercise "flows" and that the workload of all the practicing functions are as intended.
- Ensure that the course of events provide the basis for the participants to achieve the exercise's objectives. The simulation exercise should be con-

ducted with the game controller, evaluator, observer, and exercise management. If it is a large exercise should include local training controllers to be with.

- Sometimes it may even be necessary to have "staff briefings" or the like during the actual exercise.

The exercise controller is responsible for the holding the briefings before and after the exercise.

During a seminar exercise, it is advisable that the exercise controller leads the seminar and asks the participants questions. The more complex problems addressed during the exercise, the higher demands there are on the exercise controller's competence in the relevant areas.

7.1.4 Game controller – responsible that the exercise goes as planned

The game controller can also be called the moderator. In smaller exercises, the exercise controller can even serve as the game controller.

In simulation exercises with a counterplay and counterplay headquarters, the game controller leads the activities taking place at the counterplay headquarters. It is important that game controller is involved when the scenario and game plan (game book) are developed in order to ensure that every inject has a purpose and that the game controller is aware of that purpose so that every inject is closely monitored and actually contributes to the intended results (i.e., fulfilling the objectives of the exercise).

During large exercises, the game controller may also need one or more assistant game controllers who follow the game and assist the game controller.

Considerations for the game controller during a simulation exercise:

- Give the messengers in the counterplay subsequently directions regarding how the situation is developing in order to ensure that the injects give the desired effect. This may be done by using some kind of technical support gaming system where the exercise stages and injects are clarified in relation to specified times when certain events will take place.Communication between the game controller, the local exercise controllers, and evaluators should be coordinated throughout the exercise so that everyone in the exercise organization has the same information.
- Be sensitive to the views that spontaneously arise. The messengers often have a lot of experience and therefore can significantly contribute.

7.1.5 Subject matter experts and observers

A subject matter expert (or observer, as the role is called sometimes) can have different roles during an exercise. (In information and cyber security exercises, this person may also be called an analyst or reporter.) A subject matter expert may even be invited to take notes that may contribute to the evaluation of the exercise. If the exercise is an educational/learning exercise, the task of the observer may be to contribute knowledge during the exercise and essentially increase the participants' opportunity to absorb the lessons of the exercise since an expert has expressed them.

During a simulation exercise with a counterplay, the observer is the game management 'eyes and ears' on the premises where the participants are and they are able to obtain data on how the participants are reacting and acting upon the injects and development of events. Based on the information from this person, the game management can increase or decrease the pressure for the participants, for example, by increasing or decreasing the number of injects sent to the participants. The observer, thus, has an important role in ensuring that the exercise objectives are achieved; however, they should not attempt to control or influence the participants.

If it is a large exercise with many participants at different levels, the role of the observer is to cooperate with the local exercise controllers, local evaluators, and game management so that the exercise objectives can be reached. Often, the role of the observer can be combined with the evaluator's role.

Yet the presence of too many observers, however, can risk disrupting the exercise participants and giving them the feeling that they are being watched over.

7.1.6 Local exercise controller – responsible for the local exercise management

If the exercise is conducted in different physical locations, each such location should have a local exercise controller. This person is responsible for making sure the participants (i.e., participating organizations) are well prepared to participate in the exercise.

During the actual exercise, the exercise controller oversees together with the observer, evaluator and exercise management that, among other things, the development of events (injects) give the participants a good basis for achieving the designated exercise objectives. The local exercise controller is responsible for briefings with the participants before and after the exercise (i.e., if the main exercise controller does not conduct briefings via video and telephone conference).

7.1.7 Media and communications manager as well as the person responsible for the visitor program

The media's interest often increases with major information and cyber security exercises and therefore, it is a good idea to designate a person who is responsible for communicating with the media and visitors during the exercise.

Figure 3: One example of an implementation organization for smaller information and cyber security exercises.

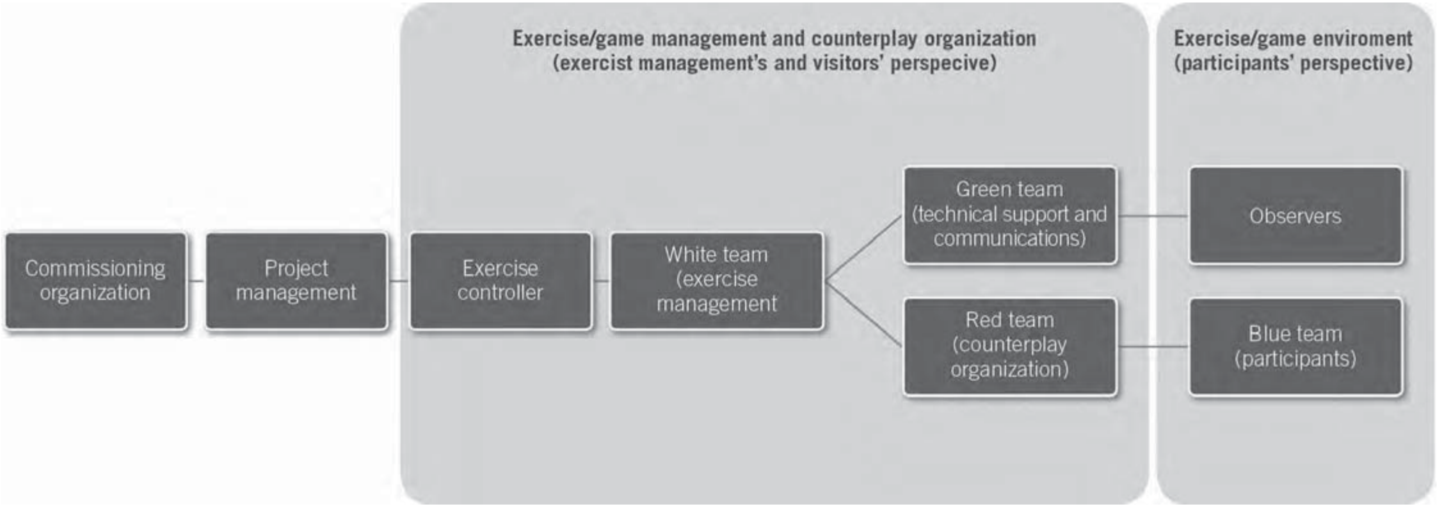
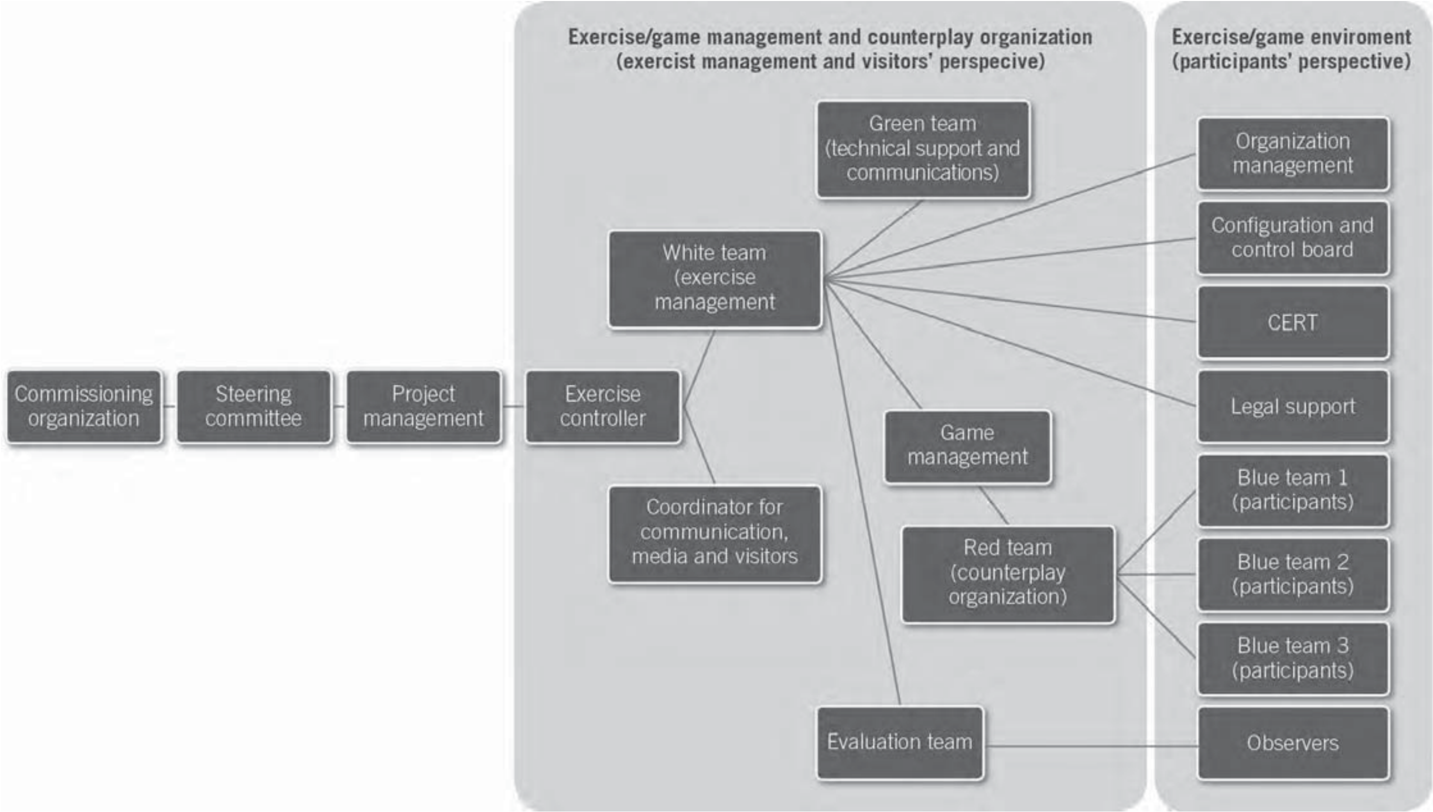

Exercise/game management and counterplay organization
(exercist management's and visitors' perspecive)
Exercise/game enviroment
(participants' perspective)
Commissioning organization
Project management
Exercise controller
White team (exercise management
Green team (technical support and communications)
Red team (counterplay organization)
Observers
Blue team (participants)

Figure 4: One example of an implementation organization for a larger information and cyber security exercise.


Exercise/game management and counterplay organization
(exercist management and visitors' perspecive)
Exercise/game enviroment
(participants' perspective)
Commissioning organization
Steering committee
Project management
Exercise controller
White team (exercise management
Coordinator for communication, media and visitors
Green team (technical support and communications)
Game management
Red team (counterplay organization)
Evaluation team
Organization management
Configuration and control board
CERT
Legal support
Blue team 1 (participants)
Blue team 2 (participants)
Blue team 3 (participants)
Observers

7.2 Exercise documentation

The purpose of the exercise documentation is that it should guide and govern the undertaking of the exercise, lay a foundation for the evaluation and processing feedback as well as provide a basis for planning the next exercise.

Listed below are a number of basic documents for exercises in general and information and cyber security exercises specifically. The documents on the top of the list indicated with a star (*) relate to the planning phase and have been described in *Mission Statement* (Chapter 6) and *Exercise Planning* (Chapter 7) in this book. Those on the bottom of the list are discussed in the section on *Feedback and Reporting* (Chapter 12) in this book. The other documents relate to carrying out an exercise and these are described below.

Useful documents for information and cyber security exercises:

- mission statement*
- consultancy agreement*
- agreements and understandings between the parties involved in the exercise (project)*
- project plan*
- description of the activities and the activity plan*
- project budget*
- time table*
- project deviations*
- terms of reference for the exercise
- terms of reference for the exercise management
- security and safety regulations
- privacy policy -terms of reference for confidentiality
- terms of reference for communications
- contact list for the participating organization
- evaluation documentation
- project completion (project report)
- evaluation report by the participants
- evaluation report of the exercise project

7.2.1 Terms of reference for the exercise – for everyone involved in the exercise from the participants to the management

The document concerning the terms of reference for the exercise is the open part of the two exercise documents guiding the implementation of an exercise. Here the specific objectives of the exercise are noted and how the exercise should be evaluated. All practical matters and instructions should be described in detail so that the participants have a clear overview of the exercise. Nothing of a secret nature should be included here, just those aspects that the participants need to know in order to get the most out of the exercise. The exercise terms should be sent to everyone involved in the exercise from the participants to the various working groups (technology, communication, counterplay, observers, etc.) in advance. In addition, a briefing of the exercise terms with the participants is strongly recommended.

The terms of reference for the exercise should include the following information:

- time table for the exercise (timings for carrying out the exercise)
- exercise form and method
- division of labor and responsibilities
- objectives – the main objectives and milestones
- organization, participants, exercise management
- scenario, past experiences and events, and the starting position
- time table – launch, run-throughs, and so on
- technical and communications matters
- security and safety regulations
- the conditions necessary for people to be able to work (food, drink, restrooms, etc.)
- funding issues
- evaluation and feedback
- visitors
- any necessary attachments.

7.2.2 Exercise management terms – limited disclosure

The exercise management terms are the ‘secret’ and closed part of the exercise documents. They should only be distributed to those in the exercise management. This limits the risk that the content of the exercise is spread to too many people. The exercise management terms govern the exercise management work in conjunction with the exercise and describe the scenario in detail with all of the background information that may be necessary. Furthermore, there should be a list of the injects with instructions for the counterplay messengers The game plan and possibly some images and map data on the course of events should also be found here. A general rule is that whatever is included in the exercise terms should not have to be repeated the exercise management terms.

The exercise management terms should include the following information:

- organization
- instructions, documentation, and reporting to exercise controller and evaluators
- technology and communications (over and beyond those stipulated in the exercise terms)
- scenario including the intended development of events
- anything that should be included or addressed in the evaluation
- information about the counterplay organization (if there is one)
- any necessary attachments, etc.

An early analysis of the contact list and the communications plan can give a good indication of the exercise’s organization and structure.”

7.2.3 Security and safety regulations

Ordinary employer insurance coverage and occupational safety should apply even during the exercise. The exercise controller is required to inform all of the exercise participants of the relevant security and safety regulations before the exercise begins. This can easily be done by including the security and safety regulations in the terms of the exercise.

In addition to the participants’ physical safety, guidelines should also be given regarding data/IT security and administrative security issues (policy, business continuity plans, regulations, etc.) so that the exercise can even apply, and not just train, information and cyber security.

7.2.4 Privacy Policy[24]

A privacy policy should take into account how information and documents are handled and archived during an information and cyber security exercise. The concept of privacy is addressed in the rules on public access to documents in the Freedom of the Press (Tryckfrihetsförordningen). The premise is that every document is a public document and therefore is open and unrestricted. Yet there are several exceptions in consideration for public and private interests. In Swedish law, confidentiality and privacy issues regarding public activities are addressed in the Public Secrecy Act (2009:400). This law prescribes exemptions from the principle of public access to official records and contains rules on professional secrecy. All claims to privacy or confidentiality must be supported by the law in order to be valid. There is a special law (1990:409) for private organizations regarding the protection of business and trade secrets. Finally, an employee may be required to observe professional confidentiality in accordance with employment contracts.

Considering this, the classification of information should be mentioned in the directives from the client or commissioning organization. In addition, if and how data should and can be obtained for the evaluation of the exercise and handled thereafter should also be discussed. For example, this includes requests regarding how data should be managed after the completion of exercise for future research. The existing terms for the privacy policy must be followed. If there is any uncertainty regarding which policy or rules apply, then the client or commissioning organization should always be consulted.

7.2.5 Terms of reference for communications

In the terms of reference for communications, it should be stated whether the ordinary communication and management support systems will be used or if other communication and management support will be provided in some another way during the exercise.

During major exercises, an exercise directory with contact information may be necessary; for example, including telephone numbers, fax numbers, e-mail addresses, videoconferencing accounts, information about encrypted connections, and so on to those functions that will be exercised.

It is important that it is stated in the terms of reference for communications or for the exercise whether or not the participants may only use the communication options listed in exercise directory. It may be possible to use a combination of the exercise directory and real communication channels.

[24] Nationalencyklopedin (2011-06-29). Search made in Swedish for the word "sekretess". http://www.ne.se/lang/sekretess

If confidential information needs to be sent during the exercise, it should be encrypted. This requires special numbers and codes (encryption keys). Details regarding whether or not ordinary encryption keys may be used during the exercise should be stipulated in the terms of reference for communications.

It should also be stated when and where the communication test is to be carried out before the exercise starts.

7.2.6 Contact information for the participating organizations

A contact list with participants' name, organization/company and department, role/position in the exercise, email address, telephone number, and possibly even account information for Skype, MSN, video conferencing, Jabber, and so on should be established as early as possible. It should also be apparent from the list where a person is supposed to be during the exercise (i.e., for distributed and major exercises that are not implemented in the same room). One person should be appointed to be responsible for the updating and distributing the list with the contact information.

7.2.7 Evaluation documentation

Evaluation documentation is outlined in chapter 10. See also the handbook for the evaluation of exercises that MSB published (2010b).

7.3 Scenario

A scenario is a description of an imaginary situation in a particular environment and at a given time, with a potential threat of an incident occurring. The threat or incident grows so that some immediate consequences occur and are followed by certain developments.

The scenario may be divided into:

- fixed conditions
- historical considerations (past events and developments)
- start position
- course of events
- immediate consequences
- development of the consequences
- game plan
- technical background material.

7.3.1 Fixed conditions

Select a place or geographic location for the event. Individuals or certain people who are near this area and who may be affected by the event and its consequences can be included. Determine the time of year and day. In many cases, climate and weather conditions will affect the sequence of events. Often it is easiest just to use the prevailing weather situation since maps as well as current satellite and radar image are quickly available.

Determine if the participants should carry out the exercise in their ordinary organizational roles/positions or if they should assume a fictitious role. For example, they may typically work as a systems developer or analyst, but during the exercise they may be asked to act in the role of the security director or in an incident management group.

Do not make the scenario more detailed and comprehensive than necessary. It takes a long time to read a comprehensive scenario and it is difficult to keep track of many details. The risk is that the time devoted to the exercise is significantly reduced and drowned out by all the details.

An important aspect in developing an exercise scenario is information security. Is there information that could harm the public or certain individuals if it is used in the exercise or if the scenario falls into the wrong hands or becomes a public document? If so, 'live' information should be replaced by fictitious information?

7.3.2 Background information – chain of events leading to a crisis / serious IT incidents

Prehistory (previous developments) is the course of events or series of circumstances leading up to the crisis or the event in the exercise. A reasonable prehistory is very important so that the event is not perceived as unrealistic, impossible or overly fabricated. Do not neglect presenting the prehistory, but avoid giving too many details. Make a distinction between the prehistory's 'open' and 'closed' parts.

The open part includes those facts that are obvious to everyone and that the responsible decision-makers are aware of when the exercise begins. Examples are the events and actions that have already occurred or been made before the exercise begins. Exercises are conducted rarely longer than one day. Sometimes you might want to train one sequence in a long chain of events which would create a situation where the crisis management (or the staff who started to deal with the event) is exhausted and resource shortages prevail after several days of work. Examples of this might be a threat that is increasing in scope shortly before the exercise date, malfunctions at a nuclear power plant, or an event that has received a lot of attention in the media.

The closed part includes certain information about the prehistory and the event that is available only after internal investigation. This is information that the participants must ask for and that is held by one of the messengers; that is, information that may be relevant for how efforts will be planned and implemented. Examples of this include: facts about a flight if the whereabouts of a missing aircraft are an issue in an exercise, details about dangerous goods in a train derailment, intelligence on extremist groups in the event of a terrorist attack, or the progression of a disease during a severe outbreak.

7.3.3 The starting position

The scenario's starting position is the time in which the exercise participants are expected to 'go into' the exercise and the game (or when the live exercise begins). This 'mode' can also be supplemented with instructions on what role the participants are expected to adopt during the exercise if they are not playing in their regular positions.

See Chapter 6.3 "Timetable for exercises" for more information about the dividing the exercise into phases and about fast forwarding the scenario.

7.3.4 Course of events

The course of events is often termed the operational phase. This is the technical process that, like the prehistory, must be reasonable and technically correct. The actual event can, for example, be described by using illustrations and images.

7.3.5 Immediate consequences

The immediate consequences are those consequences that arise in connection with the event(s) in the exercise. There may be damage that occurs or has occurred to people, property, and the environment. The consequences can be conveyed to the participants by an inject where a description is given of how it looks on the site of the incident.

7.3.6 Impact development

The impact development can be determined in advance until the point when the participants are expected to initiate their first measures. After that time, the participants' actions will determine the impact development. Alternative impact developments can obviously be described based on potential, possible, or predictable developments; however, in this case, it is usually better if the exercise controller or the counterplay improvise the impact development. This is one of the best educational instruments and therefore, it should not be restricted or hampered by an overly rigid structure.

The consequences that have no or little effect can also be described and delivered as injects.

7.3.7 Game plan

The game plan is the list of the injects in chronological order, which the counterplayer messengers intend to deliver to the participants. It is similar to a manuscript of events. Note that the game plan should only contain things that will occur regardless of the participants' actions. Besides the game plan, it is also a good idea to have a number of additional actions or injects on hand that can be used if necessary.

During exercise, it is the game controller's responsibility to ensure that the game plan is followed. During larger exercises, having some kind of technical support system for the game plan is very helpful in facilitating the exercise.

7.3.8 Technical background material

The material that is necessary to properly anticipate and describe the consequences is called the technical background material. It can include drawings, maps, weather prognoses, pictures, and descriptions of affected objects or a certain situation. This information can provide the messengers with a base for technical issues.

7.3.9 Presentation of the scenario

In a major exercise, it can be helpful to present the following parts of the scenario in the exercise document:

- **The fixed conditions:** time, location and weather (as stated in the exercise terms).
- **Prehistory – open sections:** facts that the participants should know before starting the exercise (as stated in the exercise terms).
- **Prehistory – closed sections:** the facts that have led up to the event which has occurred. This information is not presented to the participants at the beginning of the exercise, but it can be obtained upon request during the exercise (as stated in the exercise terms).
- **Course of events:** short 'prose description' of the event in its entirety with the major consequences, impact development, and potential future events beyond the control of the participants (as stated in the exercise terms).
- **Game plan:** a chronologically detailed list of all the injects that are to be delivered by messengers at the indicated time or during a certain phase of the exercise (as stated in the exercise terms).
- **A la carte list:** a non-time restrictive list of additional events that the exercise controller may use if necessary, in order to increase the workload

of certain functions being exercised or to increase the tempo of the entire exercise. This list should not be published in any document, but should only be available for those leading the counterplay.

- **Images:** photographs or drawn images of the events which can be used by the messengers to describe the course of events and consequences. These can be conveniently displayed as slides for the counterplay.

At the briefings prior to exercise as well as on later occasions, it is often necessary that the scenario is presented clearly and concisely. One suggestion might be to make a slide with a chart illustrating the horizontal time axis where the most significant events are marked. On the vertical axis, the different functions that will be affected can be illustrated.

7.3.10 Experience from past events and exercises

Experiences from real events that have occurred can provide a foundation for a scenario. Likewise, there are often photographs and newspaper clippings of the real event that can be used for background information in planning the scenario. The result of the exercise can be compared with the outcome of the real event.

7.4 Briefings

If many actors are involved in the exercise, briefings should be planned in good time as stated in the exercise terms regarding the schedule and time table for the exercise before the actual exercise is launched so that everyone has the opportunity to participate. The briefings are important in making sure the exercise is carried out in the most optimal way.

7.4.1 Briefings of smaller exercises

Smaller exercises usually do not require big meetings or briefings in connection with carrying out the exercise. However, the exercise's purpose, objectives, and approach should be discussed and anchored with decision makers and management well in advance before the exercise. After the exercise, the results can be presented in some form of debriefing.

7.4.1.1 Before the exercise

Before the exercise, the exercise management should double check communications, exercise methodology, roles, and so on with the working groups.

The participants should be informed of the purpose and objectives of the exercise as well as the benefits the exercise has for the individual and the organization.

Some of the necessary background information regarding geography, time, weather conditions, and the currently available resources can easily be presented in a written format at a joint briefing before the start of the game.

7.4.1.2 During the exercise

Usually there is no need separate briefings during the exercise. Problems that arise can usually be resolved through discussion or with a short break where the exercise controller announces the relevant changes in the exercise to the participants.

7.4.1.3 After the exercise

After the exercise, it may be appropriate to have a briefing with the participants where they have the chance to explain how they see their role in crisis management in the light of the current scenario. The participants should also be given the opportunity to reflect upon how they experienced the exercise and what they got out of it. As part of the evaluation process, they should also be given the opportunity to comment in writing on the planning and execution of the exercise.

7.4.2 Briefing of larger exercises

In connection with large exercises (for example, cooperation exercises), briefings before, during and after the exercise are very important in providing everyone involved in the project/exercise management, the counterplay, and the evaluation team a common picture of the exercise. In addition, the participants should be able to see the exercise terms and the other documentation well before the launching of the exercise.

Of course, those in the exercise organization - including the counterplay – have already during the planning process received information and instructions about their roles, exercise documentation, exercise method, and more. The briefings before, during and after the exercise should rather to be regarded as opportunities for checking and confirming the progress in these areas.

7.4.2.1 Before the exercise

Preferably a few weeks before the exercise, the exercise management should check in with the counterplay team in order to agree how the roles and policies of the counterplay should be implemented.

The exercise controller should also be in agreement with the participants on the starting position and how to organize the activities during the exercise. It is also the exercise controller’s responsibility that the exercise terms are discussed with the participants before the exercise.

The initial briefing should include the following points:

- exercise objectives
- scope and limitations (geography, weather conditions, available resources, etc.)
- time table for the exercise
- practical details (food, drink, etc.)
- location and premises
- evaluation and feedback

Even communications and technical issues should be tested in conjunction with the briefing.

Individuals who are unable to attend the briefings before the exercise should be contacted separately so that they know what role they will have and what is expected of them.

7.4.2.2 During the exercise

During the exercise, you may need short internal briefings (e.g., exercise management or counterplay team) in order to confirm details regarding a specific event. These are also called 'staff briefings.' The respective function within the counterplay team outlines the current situation - what has gone well, what has not, and so on. This is done so that the exercise controller has a good overview of how the exercise is progressing.

The better prepared the counterplay team is to do their tasks, the greater the chance is that the outcome of the exercise will be good.

When exercises last for several days, the exercise controller should take charge of getting feedback from the participants at the end of each exercise day. Comments from observers and evaluators should also be considered.

7.4.2.3 After the exercise

Directly after the exercise, a briefing should be held where the participants have the opportunity to do a self-evaluation. It can be very simple, such as a survey or an oral evaluation. The evaluator is responsible for making sure there is a final review with the participants. The exercise management should also at this time make a first assessment of the exercise.

7.5 Exercise documentation to consider in this phase

- exercise terms
- exercise management terms
- security and safety regulations
- privacy policy
- contact information for the participating organizations
- terms of reference for communications
- evaluation documentation

Reminders and helpful hints!

- Set up an exercise organization for implementing the exercise, which enables the physical coordination of the exercise management and the counterplay team/game management.
- Inform all of the participants during the exercise briefings of the preferred information and communications options and communication channels

8 Implementation

How an exercise is carried out is dependent upon how elaborate the exercise is and what exercise form and type are chosen as well as the planning and experience of previous exercises. A carefully planned exercise usually results in the fact that the implementation of the exercise is more or less carried out by itself.

Below is a list of criteria for the technical exercise environment in simulated and live information and cyber security exercises as well as technical assistance and communications. This is supplemented by an additional section on how to train communicating with the outside world as well as visitors and media coverage during an exercise.

Since technology is rapidly developing and there are many different technologies available on the market, no recommendations for specific products or providers are provided in this chapter.

8.1 Introduction

The technical exercise environment (gaming environment) for information technology and cyber security exercises may be more or less extensive depending on the purpose of the exercise and the selected method (exercise form and type). For exercise seminars, it may be sufficient with presentations and demonstrations made from a single computer without a network connection, while both simulated as well as live exercises require a network of interconnected computers. Live exercises can work in existing networks and in real time, while the technical infrastructure is fictitious in simulated exercises.

The game environment can be built by a single organization for its own exercise or it may be rented or purchased from an external supplier. For Swedish public authorities, Act (2009:1091) on public procurement applies.

8.1.1 Procurement

The procurement of technical infrastructure for information and cyber security exercises should take the following concerns into account.

Contracting authorities shall comply with the applicable law (2009:1091) on public procurement for public authorities which seeks competitive procurement. In the public sector, procurement can also be done between government agencies. It should always be sought with a commercially-sound customer and supplier relationship.

The contract should be divided into different sections depending on the requested service or product. An example of the breakdown might be:

- technical infrastructure and
- service (support) of the technical infrastructure.

The technical infrastructure (gaming environment or exercise network) consists of technical equipment such as network equipment, servers, PC clients, software, video conferencing equipment, and more. The infrastructure is relatively static and allows for procurement at a fixed price.

The planning and implementation of an exercise also requires service (support) of the technical infrastructure. It is difficult to plan in advance for this resource, making it difficult to procure a fixed price. Nevertheless, basic support for the parts that are specified in the technical infrastructure should also be included in the procurement of the technical infrastructure.

8.2 Technical exercise environment

8.2.1 Background

The following section is based on practical experiences from previous information technology and cyber security exercises. Among these are the simulated and distributed exercises Cyber Defence Exercise 2008 (CDX-I), Baltic Cyber Shield 2010, the Locked Shield series 2012 – 2013 and Swedish national exercises such as NISÖ and SAMFI.

The section is not inclusive or intended to provide an exhaustive overview of how information technology and cyber security exercises can or should be planned, conducted, or reviewed; however, it presents previously mentioned recommendations and proposals for technical exercises: how they may look and what should specifically be considered.

According to *Exercise Planning* (Chapter 6), the most common exercise forms for information and cyber security exercises are:

- seminar exercises (including table-top exercises and workshops);

- simulation exercises or controlled environment exercises with a counterplay, and
- live exercises in existing systems in real time.

All three exercise forms can be implemented either on the same site or as a distance exercise (distributed exercise). These exercise forms complement each other, and one exercise may have elements of several different forms depending on what is most appropriate for achieving the exercise's purpose and objectives.

One specific exercise approach commonly used for information technology and cyber security exercises is called the red team – blue team. Even though it is one type of exercise, it can also be used with other exercise approaches (e.g., unannounced 'live' exercises, initiation exercises, staff exercises, decision exercises, management exercises, and cooperation exercises). The red team – blue team exercise aims to train both team work and decision making during the same exercise. This makes it a 'multi-approach exercise.'

The seminar exercise form, discussed early in this handbook and now in this section, includes above all simulations but also live exercises in existing systems in real time. This section deals only briefly with the technical exercise environment for smaller simulated information and cyber security exercises. The relevant aspects of planning and practical preparations, technology, information and communication, planning and implementation of the counterplay, and the evaluation of major exercises are discussed here. In closing, there is a section on planning, threat paths, implementation, communication, and following-up live exercises.

8.2.2 Smaller simulation exercises with a counterplay

Simulation exercises can be performed in the form of smaller exercises where only one or few services is/are set up and where there is only one blue and one red team. In larger major exercises there are usually several blue teams and an extensive simulation environment with many services. A smaller exercise can be designed to highlight specific problems such as attacks against web services are orchestrated and how they can be detected.

Nevertheless, there are sections in the exercise manual that can be used for exercise activities conducted on a smaller scale. However, it is always important to first establish the purpose and the objectives of the exercise. The technology used for the exercise environment should be selected in accordance with these aspects so it can be determined how well these were achieved during the actual exercise and the evaluation.

The technology used in the simulated exercise network/environment may consist of a few computers that reflect a real environment. It may also, for example, include a copy of a web server, firewall, or something similar that is implemented in a secluded environment. The evaluation should be carried out throughout the exercise; for example:

- The red team implements one or several attacks.
- The blue team analyzes and reports what is happening.
- The exercise is interrupted, and the red and blue teams jointly review what has happened and what has been revealed.
- The exercise is resumed.

8.2.3 Larger simulation exercises with a counterplay

Exercises in a simulated environment place different demands on the implementation than in a 'live' exercise environment. The participants take part in the exercise detached from their ordinary activities.

The recommendations below are foremost based on the lessons learned from Baltic Cyber Shield 2010 (CDXII)[25] and the Locked Shield series of exercises 2012 and 2013. The exercises were a red team – blue team exercises, with predefined colors for the working groups. The name 'red team' was used for the counterplay team who during the exercise targeted the blue team's information systems for attacks and intrusions. The name 'white team' was used for the exercise management and the green team for the working group for the technical exercise environment, technology and communications as well as the collection of data for the evaluation and analysis. In the Locked Shield exercises a subgroup from white team was established to handle situation awareness and the collection of data for evaluation. This group was named Yellow Team.

8.2.3.1 Overview of the planning and practical preparations

The objectives of the exercise should be determined during the planning of the exercise so that they are crystal-clear before the practical preparations and planning of the technical environment/infrastructure begin. If the objective of the exercise, for example, is to increase awareness of generic attack techniques and appropriate security measures, the requirements put on the simulated environment are lower than if the exercise intends to mimic the real organization and is conducted in 'live' systems. In both cases, however, extensive planning and testing of above all the red team (counterplay team) are necessary as well as ensuring good coordination with the green team (working group for the tech-

[25] For a detailed description of the exercise, its organization, and implementation, see the report of the exercise "Baltic Cyber Shield Cyber Defence Exercise 2010, After Action Report" published 2010-10-06) which is available to the public at:
https://www.fhs.se/sv/forskning/centrumbildningar-och-forskningsprogram/cats/nyheter-och-artiklar/2010/

nical exercise environment, technology and communications) and the white team (exercise management).

The red team is responsible for the vulnerabilities that exist, or are implanted, in the simulated environment so they can be exploited in such a way that they do not adversely affect the simulation environment negatively from a technical exercise perspective. For example, vulnerability can result in a failure in the entire environment which in turn can require the exercise to be restarted. With the planned measures, the red team should be able to describe the blue team's ability to detect these.

The green team is responsible for the simulated environment. Close cooperation between the red team and white team should already be established during the planning process. Several blue teams will help facilitate that they also have the same simulated environment. If possible, this environment should be able to be re-established even on short notice.

The white team is responsible for the planning of the scenario for the exercise. This is advantageously done by establishing a separate working group that is tied to the white team. Cooperation with, in particular, the red team should be well-established already in the planning of the various exercise phases. The white team is also responsible for documentation (terms of reference for the exercise, terms of reference for the exercise management, security and safety regulations, privacy policy, terms of reference for communications, and contacts) which should be provided to the exercise participants before the exercise. Evaluation documentation should be prepared by the evaluation team in parallel with other documentation and should as well be issued to the participants before the exercise.

The yellow team that was introduced in the first Locked Shield exercise is responsible for the documentation, chat and the reporting system as well as the tools for situation awareness.

8.2.3.1.1 Communication

There are two types of communication for an exercise in a simulated environment:

- internal communication, and
- external communication.

Internal communication is all communication that takes place internally in the exercise network. This can be encrypted tunnels between the simulated environment/infrastructure and the different teams, or information sharing services in the exercise network (such as email, instant messaging, Voice over Internet Protocol VoIP) and so on.

External communication is the communication that takes place outside the exercise network, such as regular e-mail, telephony, chat, etc.

The appropriateness of what is to be selected for each exercise should preferably be decided in the planning phase, or at the latest during the practical preparations. Internal communication is usually protected against external exposure, but this depends on how easily the exercise network can be accessed. External communication can increase accessibility that is not dependent on the exercise network's availability, but this can create greater exposure to ongoing activities.

8.2.3.2 Technology during the planning and implementation phases

8.2.3.2.1 Exercise network

The exercise network can be centralized and/or distributed. Both approaches assume that the exercise network is separated from the other networks and using approved security mechanisms. In a distributed network, this may be done with approved encrypted tunnels to a physically separated centralized network. Rules for connecting devices to the endpoints in a distributed network must be clarified in order to avoid getting undesirable connections from other networks during the exercise.

When there is a need to connect to an external network (for example, downloading updates from the Internet) this should be done, if possible, with a controllable information transfer, on removable media offline. If galvanic coupling is required, then an approved mechanism (such as firewall with proxy server) should be used. An analysis of the risks, consequences and degree of vulnerability should be made for every type of connection to an external network. A connection point should be centrally located for the entire network and should be regularly monitored.

8.2.3.2.2 Equipment for the blue team

Equipment for the blue team should be specified so that all of the blue teams (if there are several) have the same opportunity to participate in the exercise. When using encrypted tunnels, the equipment should, if possible, be distributed in advance so that exercise network can be tested beforehand. This should be done together with the green team (which is responsible for technical support and communication).

8.2.3.2.3 Simulation environment

The environment in which the exercise is conducted may advantageously consist of virtual systems. In a virtual environment, there are often opportunities for so-called snapshots that can create a common configuration that can be quickly restored. Therefore, the exercise may be restarted from any given position during the exercise.

One challenge in having a simulated environment is adequately being able to reflect the real environment as much as possible so that the blue team is familiar with the environment and consequently the exercise feels realistic. The services and equipment used during the exercise should be similar to those found in the real network.

The red team (the counterplay organization) in cooperation with the green team creates the simulation environment for the platform where vulnerabilities are presented. The vulnerabilities should mirror realistic threats that could even appear in a real situation. These vulnerabilities should be tested so that they give expected results.

8.2.3.2.4 Following up

Procedures for following up incidents (actions/attacks) must be planned and tested if they are dependent on technological systems. For example, if a bug tracking system is typically used in an operation, a similar system should also be included in the exercise.

For every action the red team executes in the simulated environment, there should be planned procedures for how to follow up on these: what is the expected outcome of the action, how is the blue team expected to react, and what are the grading guidelines for the blue team. Extra consideration should be given to those measures that may affect things beyond the scope of the exercise. For example, an attack on the DNS (Domain Name System) may also knock out reporting lines and access to the system which technically supports the functioning of the exercise.

8.2.3.2.5 Scoring

An exercise can be performed with or without scoring. Often, however, the participants' level of motivation is raised when an exercise is designed with scoring for defense (blue team).

An important part of monitoring the implementation of the exercise is, thus, scoring. The exercise's objectives determine what should be prioritized in the assessment. The white team, which is responsible for scoring the implementation of the exercise, should be supported as much as possible by an automated system. Feedback (regarding, for example, the availability of services) requires extensive human resources if several blue teams are to be assessed equally well.

Objectives with scoring can include but not limited to:

- availability objectives
- integrity objectives
- privacy/confidential objectives.

Below are examples of an automated system for scoring these objectives.

Availability objectives – Maintaining internal and external services can, for example, be included in the exercise objectives. These services can usually be controlled with software that can automatically detect whether or not they are active. Examples of these services include: web, email, FTP, data base, and so on.

Integrity objectives – Monitoring integrity can be done by automatically checking to see if changes have been implemented in system files. File Integrity Monitoring (FIM) software can be used to do this.

Privacy/confidential objectives – This can be indirectly measured as an integrity objective. A change by the red team in a "secret" file or downloading some "secret" data, in most cases, is often considered sufficient to prove a breach of privacy.

8.2.3.3 Information and communication solutions during the planning and implementation phases

An information and communication model should be developed already when beginning to plan the practical preparations for an exercise. The procedures for planning may differ from those used to carry out the exercise.

8.2.3.3.1 General points to consider when selecting information and communication solutions for the exercise project

- **Minimize the number of places where information is stored**. Lessons learned from early exercises shows that combining peer-to-peer networks with a centralized system entails unnecessary risks for information inconsistencies. Choose one technology. There should be no doubt about where the most recent information is. Managing different versions of information should be supported by appropriate software. For example, Subversion, or the equivalent, can provide a basis for storing information. A wiki based system has proven to work quite well during the Locked Shield exercises.
- **If possible, choose solutions that have a independent platform.** Dependence on special technology or specific programs should be avoided. Users should be able to use a system with which they are familiar. The selected solutions should be compatible and able to work in Microsoft Windows, Linux, and MacOS.
- **Educate those involved and participating in the exercise on the selected communication solutions and information strategy.** Already at the startup of the exercise project (i.e., during the practical preparations) sup-

port for and education on the solutions that will be used for the exercise should be available. This should include how to work with information, version management, classification, distribution, templates, naming, quality assurance, confirmation, and so on.

- **Privacy/Confidentiality.** When selecting information and communication solutions, confidentiality requirements and needs should be met.

8.2.3.3.2 Information and communication solutions when carrying out the exercise

The general recommendations listed above also apply when implementing the exercise, conducting the evaluation and processing feedback.

The implementation of an exercise demands more technology and personnel for the information and communication solutions. Exchange of information between the participating teams can thus be done both inside and outside the exercise network. Both approaches should be planned in order to allow for redundancy.

The exchange of information between the white team and the blue team will primarily be done via e-mail and if possible a ‘ticket system’, which is a reporting system with templates for reporting. Access should be made possible both within and outside the exercise network.

In order to facilitate the exchange of information between the other units in the exercise management, subgroups should be established. If this cannot be done, then video conferencing should be set up with the ability to share displays and multi-party connection (if the units are spread out in different locations). Even if the exercise management is divided into subgroups, video conferencing can be useful between the different teams.

Things to consider when selecting information and communication solutions for implementing an exercise:

- **Decide in advance what should be saved in order to be able to evaluate the exercise.** Different solutions provide different options for saving information for evaluation and feedback. Text-based information (such as emails, a ‘ticket system’, electronic documents, etc.) is easier to store than real time communication such as telephone conservations

- **Timing**. One common time source should be used for all of the technical equipment in order to facilitate time consistency among the different sources of information. This time source can be used advantageously with NTP (Network Time Protocol). It is not critical that it is absolutely the correct time, but rather that all units are using it to determine what time it is.

- **Minimize the number of systems in which information is stored**. In order to avoid inconsistencies in information exchange and storage, efforts should be made so that information is located in one place (or two if you count the 'backup' which of course must be included).

8.2.3.4 Planning of the counterplay organization – the red team

Planning to implement the counterplay organization's activities is dependent on several factors. Some examples of these include:

- the objectives of the exercise
- the exercise participants' skills and the type of equipment available for the exercise
- how the exercise network is constructed
- the mission statement and any other directives that should be followed

8.2.3.4.1 Agreement between the objectives and how the exercise is set up

The activities that the red team (counterplay) performs during the exercise should have a clear connection to the objectives of the exercise. The objectives can be broken down so they are consistent with the different phases, which are initiated and controlled by the white team (exercise management).

An example of this is how the blue team (participants) exercise system can be built up of three components:

- **DMZ** is the zone in which public services are normally placed. This is the part that is connected to the Internet.
- **INTERNAL** is the ordinary organization network which should only be accessible to authorized personnel.
- **SCADA** (Supervisory Control And Data Acquisition) is a type of industrial control system with both process control equipment and user interface.

The exercise can be divided into three phases focusing individually on DMZ, INTERNAL and SCADA.

8.2.3.4.2 Monitoring and Controlling the Exercise – The Exercise Management

The white team (exercise management) should be aware of the measures planned by the red team (counterplay) so that they have the necessary resources in order to follow up the blue team's (the participants) responses. This planning should also include rules for scoring, if applicable.

The white team is responsible for providing the necessary reporting tools for the blue team. There should be a limited number of reporting lines since this simplifies coordinating the white teams. As previously suggested, a 'ticket system' should be used (such as OTRS, Open-source Ticket Request System), if possible.[26] Adapting OTRS, or the equivalent, to the exercise should be done well in advance. In addition, participants on both the white team and blue team should get instructions on how the system works. There may also be a need for the red team to report in the same system.

The exercise management's coordination of the different teams (white team such as CCB and CERT, red team, green team and blue team) during the implementation of the exercise is of great importance for creating flow in the exercise and maintaining good structure.

A good understanding of the situation is required so that the white team and green team are able to perform their tasks, and this issue should be given adequate consideration, especially in terms of practical preparations. A common understanding is crucial for enabling the white team to lead the exercise and conduct fair scoring, and for aiding the green team in making good decisions. It is also useful for informing visitors to the exercise. Some parts of the situation awareness may also need to be communicated to the blue team's observers. Situation awareness can easily be displayed in a matrix where the intermediate objectives are given for each of the participating teams.

8.2.3.5 Tools for evaluating information technology and cyber security exercises

The evaluation work should begin already in the planning phase (by creating the evaluation organization in parallel with the other teams) and should continue throughout the entire exercise. Evaluating exercises helps to identify lessons learned by processing feedback which can be integrated into the work of planning and carrying out new exercises.

Although the evaluation process of most exercises is relatively similar, information technology and cyber security exercises differ slightly. According to the chapter on evaluating exercises (Chapter 9), data collection can be done in several ways. Yet, technical exercises provide better conditions for using various technological tools and systems since data is automatically collected via on-line surveys to exercise participants, data logs of the system traffic in the exercise network, and recordings (audio and video), which complement the observers' accounts of the participating teams (blue, red, green, and white).

However, it is worthwhile as well as necessary during the planning phase of the exercise to determine what the evaluation will focus on (in connection to the exercise's purpose and objectives) since data collection after a completed exercise is costly in terms of time as well as technological and human resources.

[26] More information on Open-source Ticket Request System (OTRS), see www.otrs.com

8.2.4 A live exercise in existing systems in real time

This type of exercise is suitable for training emergency preparedness and for example how well incident management and reporting activities work. This exercise form puts high demands on carrying out an exercise since security in the real systems should not be jeopardized or affected. In addition, this exercise form requires that risk and impact assessments are made both before and during the implementation of the exercise. This is done so that no weaknesses can be implanted in the exercise systems in advance. Implications for how detected weaknesses can be exploited during the exercise should be assessed in terms of how they can impact general activities as a whole. People with good knowledge of the business activities of the participating organizations (e.g., security and operations) should be included in the exercise management and involved in assessing, for example, whether or not a particular server can be shut down.

Information about the implementation of an exercise typically has limited circulation. The participating organizations usually do this within their own organizations.

8.2.4.1 Planning

When planning exercises in an organization's 'live' environment, two groups should be involved: the red team (the counterplay organization) and the white team (the exercise management) together with at least one security director (or equivalent) who is from the organization participating in the exercise and who has good knowledge of the technology infrastructure (IT, network, etc.) and its management system. Good knowledge of what may adversely affect the management needs to be discussed before the exercise in order to be able to conduct a risk analysis. Likewise, the red team must be able to assess all of the planned actions (attacks) in order to be able to properly do an impact analysis.

Information regarding the network diagrams, information systems and networks, management system components, versions of the operating systems, application information, and so on provide the red team (counterplay organization) with a solid foundation for counterplaying.

8.2.4.2 Threat paths

During the implementation of an exercise in a live environment, one must take into account the level of exposure caused by every action played by the red team (counterplay organization). Actions carried out by participating organizations' non-controllable networks should be avoided, if possible, in order to reduce potential exposure to vulnerabilities.

8.2.4.3 Implementation

During the implementation of an exercise, only those attacks that during the preparation phase were approved by the white team (exercise management) may be played. If there is a desire or need to play a move or injects that were not planned in the preparation phase, an impact and risk assessment should first be carried out and approved by the white team before the action is activated.

8.2.4.4 Communication

The ordinary routines for internal reporting can be used for communication from the participating organization (blue team). The white team and red team (i.e., exercise and game management as well as the counterplay organization) should sit together in order to simplify communications regarding the exercise. The participating organization may have, for example, members from the management and legal support in the counterplay who participate in the exercise in terms of their regular positions and who are a part of the regular chain of communications.

8.2.4.5 After action review

Throughout the planning process, consideration should be given to what is expected of the participating organization and how this can be checked in the exercise's after action review. A follow-up meeting with the blue team, white team and red team (i.e, participants, exercise and game management, and counterplay organization) should be planned to take place in the final phase of the exercise, when a review can be made of what technically happened in the systems. This includes the actions played by the red team and how these actions affected the participating organizations on the white team (exercise management and participants on the management level). During this follow-up meeting, discussions should include appropriate measures for improvement that can be implemented by the participating organizations.

8.3 Technical support and communications

8.3.1 Technical reporting system

For information technology and cyber security exercises, a technical reporting system can be built into the simulated exercise environment while simultaneously the existing systems can be used/tested in the live exercise. Here the exercise's purpose and objectives should govern how the reporting system should be developed to work during the exercise and how it can contribute to the evaluation of the exercise. A reporting system may be relatively simple and consist of an email system which may or may not be integrated into the exercise infrastructure.

Obviously, the technology that is used in real-life situations should also be used in an exercise, for example management and information reporting systems. One such system is WIS (web-based information system) which was developed by MSB so that various actors could better manage societal crises. In this case, it is about giving the participants the opportunity to sustain and enhance their ability to use technical management and information support systems.

8.3.2 Web site for exercise planning

A separate web site can be created for larger exercises so the participants are able to access information (e.g., minutes from the meetings) and keep up-to-date throughout the project. Ideally, the web site should be protected with login and password functions.

8.3.3 Exercise web pages during the exercise

Many municipalities and authorities create special web pages in connection with exercises, where the participants can share with others information that they would publish in the context of a real event. It is important to note that only the exercise participants should have access to these password-protected web pages.

8.3.4 Gaming support systems – Ensuring the right injects at the right time

There are various technical gaming support systems available on the market. Most of them show how various the exercise phases can be set up and how injects can be used at different times throughout the exercise. The assumption is that exercise phases and injects are timed in the data bank so they can be easily displayed on a timeline. With that, the game controller and the counterplay have a better overview of the exercise so that the correct inject is played at the right time. Another advantage is that detailed information about certain resources, and such, can be directly connected to a certain phase or inject.

In addition, it is good if the exercise phases and injects can be connected to some kind of evaluation tool. If during the exercise the evaluators can report their observations and assessments directly into a gaming support system, then more of the exercise is retained and can be fed into the evaluation process after the exercise.

While a technical gaming support system can be helpful for the exercise management and counterplay organization during exercise, it can also serve as a basis for the evaluation of the exercise, as described above. It can also be linked to a technical situation awareness function (software) that both shows where in the exercise the team is and whether and how the participants have reacted to previous injects as well as which injects are in line to be played. This technical/

computerized visual situation awareness function can be programed so that the game management, counterplay organization, and visitors have access to it.

8.3.5 Film

A film clip (animated or recorded) of a sequence of events can be a great tool, for example when the exercise starts. It can either be used by the counterplay in order to give a picture of the event or by the participants in order to paint a picture of the event. Films can also be a means to increase the exercise management's and participants' engagement and provide valuable insight.

8.4 Training external communication

Crises often generate a large demand for information from the involved actors – in particular authorities. When a crisis becomes known, the media, public and other stakeholders immediately need fast and accurate information about the course of events and how they are being managed. The ability to communicate in a crisis means that an authority or another actor has the ability to reach out to their target audiences with relevant information even under adverse conditions. It also means the ability to receive and analyze important information from the media, the public and other stakeholders and be able to incorporate this information into the crisis management. One the one hand, the media is often a very demanding audience yet one the other, it is the fastest channel for reaching the general public. For most of those who are not eyewitnesses to the incident, their main source of information is the media, even if the authorities and other actors are in charge of dealing with the situation. Therefore, the responsible actors should in parallel manage the crisis at hand as well as the image of the crisis.

Training these aspects puts high demands on planning, an organization, and imagination. The crisis managers must be capable of handling a crisis as well as anticipating the information needs that might arise along the way. It also places high demands on cooperation since those authorities who go out with different messages will immediately be held accountable for this in the media and by the public.

8.4.1 Media

Giving realism to the challenges of this task can be created by including the media and the public in the exercise. The purpose of such a game can also be to increase pressure on the participants during the exercise. Journalists or other people can be asked to play different roles (e.g., the general public, victims or their relatives) with various means in order to activate the participants.

Freelance journalists can be called in to play the role of the media during the exercise. One option is to engage journalism students. Often, journalism colleges and high schools like to contribute to such exercises. Those playing media representatives can, among other things, run press conferences and interviews with the participants. Often, there may be a need – and desire – to give media training to certain key people during the exercise. Interviewing techniques and talking in front of a camera can be easily organized with the help of experts and consultants on the topic. Doing this on a smaller scale with fewer people enables more personal feedback and, therefore, a better opportunity for absorbing and internalizing the media training.

8.4.2 Public interests

In order to train communicating with the public, an exercise can include elements aimed at representing the public's interests. For example, a few individuals can play victims, concerned relatives, employees or other affected actors during the exercise. They can also pretend to be eyewitnesses, or the like, who have important information they would like to report and can be available for interviews with the media group. If there are not staff members available for this task, volunteers can be engaged from various civilian and military organizations: such as students, senior citizens, or theater students.

Likewise, it is meaningful if a few people can follow what the media is reporting and what information the participants are presenting or publishing (e.g., on their web sites) during the exercise. In addition, individuals can be encouraged during the exercise to contact the authorities regarding the public's interests.

Note that such exercises and games are intended to simulate the interests of the media and the public and that the ability to truly reflect these interests on any given issue is limited.

8.4.3 Methods and channels

Depending on what you want to accomplish with the exercise and what should be trained, media and public games can utilize different channels during (and possibly before) the exercise. For example, a technical system may be tested or perhaps various forms of cooperation and networking should be rehearsed.

8.4.3.1 Online newspaper

By having a web newspaper on the Internet, information that would in reality be published online can be made available to the participants, under the premises that it is easily accessible during the exercise and that there are press journalists available for this. In connection with having a web newspaper, the participants could, for example, be asked to be interviewed for the newspaper in order to practice their interviewing skills.

8.4.3.2 Role-playing press conferences

More pressure can be created for the participants by organizing a press conference. The purpose of a press conference is primarily to provide the opportunity to experience what it entails to plan and meet several journalists at the same time and to practice delivering coordinated information. Students of media and journalism are often able and willing to assume the role of journalists when role-playing a press conference, or alternatively, freelance journalists can be hired.

Press conferences and media activities are coordinated most appropriately by the exercise management. For practical reasons, these should be planned well before the exercise as well as the details surrounding them (e.g., timings, location, meetings if many players are involved, etc.). It is also a good idea if those from the exercise management who are in charge of the media game get a review of the press conference so they in turn can provide constructive feedback to those who played the journalists and if needed, adjustments can be implemented in the exercise.

8.4.3.3 Radio exercises

The Swedish National Radio regularly exercises its organization for crisis preparedness, often in cooperation with other agencies and organizations. The Swedish National Radio's own journalists participate in the exercise and provide news reports, which are then transmitted on a dedicated web site which is password protected and only available for the exercise participants. The radio segments can be recorded in advance or they can be created by interviewing the participants during the exercise.

8.4.3.4 TV exercises

TV broadcasts can also be effectively used in exercises. During an exercise a TV team with news reporters, for example, can actively call upon certain individuals from the participating organizations. The TV team can also cover the press conferences. In addition, TV segments (interviews and edited press conferences) can be posted on the exercise web site so that the participants have access to them.

8.5 Visitors and media coverage

Exercises can often be interesting to visit and, for the media, to report on. The question is how the exercise manager and exercise management should handle this. In many cases it may be good publicity if the media covers an exercise in a particular area. In other cases, there may be sensitive information during an exercise, which should not be disclosed outside the circle of participants. The same applies to visitors. On the one hand, it can be beneficial for those who are organizing an exercise or are experts in the subject area to be able to utilize the experiences of others. On the other hand, certain exercises are not suitable for visitors.

For information technology and cyber security exercises that are open to the public or invited visitors and observers, a visitors' program should be established. If there are visitors during an exercise, it is therefore important to have a coordinator for media and communication as well as for visitors in order to avoid disturbing the exercise. This person should be knowledgeable about and well versed in the exercise and be able to provide a good overview of the exercise. The same person should also be responsible for coordinating press releases and for booking interviews with media representatives (radio, TV, newspapers, and etc.).

8.5.1 Visitors

If visitors are invited to an exercise, there should be an organization that takes care of them. For major exercises, a visitors' center can be established. There visitors can get information about the exercise, have the opportunity to ask questions, and can even get a guided tour of the exercise site.

Specially invited guests may need a visitors' program with information about the specific functions being exercised, press conferences and so on.

Before guests are invited to visit the exercise, it is appropriate to consider who should have access to the exercise. Should only people with certain functions or positions be invited, and, if so, in what form? Is there any sensitive information that should not be disclosed? Security aspects should be included in planning, receiving and showing around visitors.

8.5.2 Mass media

Media, communication, and visitor activities related to the exercise can put heavy demands on the exercise management and the exercise participants. Therefore, a plan should be developed for dealing with these issues. Where, when and how should the media be received so that they do not influence the exercise participants in a negative way or interfere with fulfilling the exercise objectives and purpose? Who has the responsibility for informing the real mass media and providing them with requested information about the exercise?

During larger exercises, it may be appropriate to arrange a press and information center where external public relation and media representatives can receive real information about the exercise.

8.6 Continuation of exercise forms and types

Implementation is a continuation of the discussion on exercise forms and types that was previously presented in the section exercise planning.

8.7 Exercise documentation applicable to this phase (as mentioned earlier)

- Terms of reference for the exercise participants
- Terms of reference for the exercise management
- Security regulations
- Confidentiality terms
- Terms of reference for communication
- Contact list for the exercise organization
- Evaluation documentation

Reminders and helpful hints!

Set up an exercise organization for implementing the exercise that enables the physical coordination of the exercise management and the counterplay organization/game management

9 Evaluation

The overall idea of evaluating exercises is to create opportunities for increasing individual and organizational learning. The evaluation process is an ongoing effort that stretches over the entire project management and exercise planning process from planning and implementation to the after action review.[27]

9.1 Continuation of exercise's purpose, and objectives

The evaluation is a continuation of the exercise planning's purpose and objectives. (See also Chapter 7.1.) It is important that the purpose (why you are doing an exercise) and the objectives-(what you want to achieve with the exercise) are specific, measurable, adequate, realistic, and time-specific (i.e., in accordance with the "SMART" rule). The exercise revolves around the stated purpose and objectives and consequently, the evaluation revisits them frequently in order to see if they were achieved and to provide feedback. Thus, the evaluation work begins already in planning the exercise and therefore, the evaluation leader should be included in this phase.

[27] This chapter is based on MSB's comprehensive exercise handbook published in 2009. For further reading on the subject of exercise evaluations, see MSB's "Handbook on the Evaluation of Exercises" (2010).

9.2 Evaluation and processing feedback

After an exercise has been carried out, there is a risk that many people can be under the impression that the job is done. Those individuals who have worked hard with the exercise planning may be looking forward to some time off and those who actively participated in the exercise may also need some time for thought. However, this is when the real learning phase begins. After the exercise is completed, there is time to take a step back and reflect on what went well and what needs to reworked. Here is the opportunity to reflect on the ways and means by which improvements can be made.

There are many different definitions of evaluation. In general, an evaluation is the examination to secure, maintain and/or improve the quality of efforts, activities, and actions.

For exercises MSB suggests the following definition of evaluation: A systematic post-assessment and examination of an operation or activities. More specifically, it is a post assessment and examination of the design of an exercise as well as of the performance and organization of the exercise. MSB also stresses the importance that the exercise evaluation should be independent from the planning and execution of the exercise.

For information technology and cyber security exercises, a combination of technical and manual systems for data collection and analysis may be preferable. The technical data collection may consist of audio and video recordings, computerized surveys (online forms), and data logs. The system(s) for data collection can be either developed within the exercise organization or purchased via a third party. (See Procurement in Chapter 8.1.1.) After completing an exercise, a "data set" can be collected that contributes to reconstructing the exercise for a more detailed analysis.

The manual data collection often consists of direct observations from one or more observers on the participating teams/working groups during the exercise. These observers may be involved in both the technical data collection (managing audio and video recordings) and keeping notes of their observations of the participating teams during the exercise.

The observers may also help to update the exercise and game management's situation awareness during the implementation of the exercise, by reporting on how the injects have been received and what actions have been taken. In cases where technology fails, the observers may also contribute to situation awareness and provide additional material for the evaluation by interviewing the exercise participants.

9.2.1 The nine steps of the evaluation process

The evaluation process can be described by a list of nine steps:

1. Appoint the head of the evaluation
2. Plan and organize the evaluation together with the exercise management
3. Formulate evaluation questions
4. Educate and prepare the evaluators
5. Observe the exercise and collect experiential feedback
6. Analyze the collected data
7. Compile and disseminate the evaluation report
8. Process lessons learned
9. Start planning the next exercise.

Processing experiences can be seen as part of getting feedback after the exercise. Similarly, processing lessons learned can be part of the after action review which takes place after the exercise."

9.2.1.1 Appoint the exercise evaluation person/team

A natural place to begin is to appoint an evaluation function. It is important that this takes place as early as possible in the exercise process. This function (one or more people depending on the scale of the exercise) is then part of the exercise and evaluation planning.

9.2.1.2 Plan and organize the evaluation together with the exercise management

The evaluation approach should be developed at the same time as the exercise purpose and objectives are formulated. It is important that planning for the exercise and evaluation are developed in parallel since they significantly influence each other. The purpose and objectives of the exercise must be clearly worded and they should be accepted by those involved. This is significant for two reasons. Firstly the exercise form (I.e., how the exercise is carried out) locks the function of the evaluation in how the exercise can be observed and assessed and whether the exercise fulfills the purpose and reaches its objectives. Secondly it must be possible to observe, analyze and evaluate the issues, which the exercise and the scenario are meant to address. The earlier this is done in the planning of the exercise, the better.

The function of the evaluation is to assess whether it is feasible to address the issues, based on the available resources and on the conditions that the selected exercise format presents. This assessment is very important for the future planning of the exercise.

An evaluation of high quality is labor intensive. Therefore, the resource issue is important to highlight early on since it provides the framework for which efforts (in terms of people, time, and technology) can be used during the exercise to collect relevant information linked to the exercise questions. Already at an early stage the exercise planning team needs to discuss with the evaluation team what the aim of the exercise is and which exercise form is most suitable for achieving this. This is significant since different exercise forms require different resources for the evaluation. The choice of exercise form provides an indication of how resource intensive evaluation becomes.

Since an evaluation contains many elements, it is a good idea to develop a timeline and a resource plan for the process of designing the evaluation template and for collecting, processing, analyzing and disseminating the evaluation results. Even external evaluators, experts, and technical equipment should be included in the cost estimate.

9.2.1.3 Formulate the evaluation questions

What is a good evaluation question? First and foremost, the evaluation questions should be linked to the exercise purpose and objectives. In addition, it should be possible to observe and evaluate them, which in turn brings us back to the discussion that the evaluation should be an integral component in the exercise structure and in determining the method for implementation.

Once the evaluation questions are formulated, they should be examined in regards to how well they can be answered. Can the questions be answered with the existing resources (people, expertise, time, and technology)? Is there knowledge available that can facilitate analyzing and measuring the observations?

There is often a need to prioritize the questions that an exercise aims to answer. Neither an exercise nor an evaluation should attempt to have too many purposes at the same time; otherwise, there is a great risk that the quality will suffer.

Some elements that can be evaluated in staff and decision exercises include the following:

- how the staff works and operates
- how the organization and the management work
- issues related to cooperation
- internal and external communication
- information management
- stress management.

It is also important to emphasize that no assessment should be done mechanically. Often, unexpected events that occur in an exercise can be well worth highlighting for discussion.

9.2.1.4 Educate and prepare the evaluators

In order for an evaluator to be able to collect the necessary information during the exercise, s/he must know the organization(s) and the participants. Likewise, a few individuals should be appointed and prepared for the task of collecting useful material during the exercise that can be used later for the evaluation.

Examples of materials that can be submitted and presented to the evaluators include:

- the key background documents, which contain the purpose of the exercise and the objectives
- the terms of reference for the exercise
- the exercise scenario
- relevant legislation
- documentation of the organization's previous crisis experiences
- documentation that describes the organizational processes
- responsibilities and job descriptions
- crisis plan(s)
- the organization's previous exercise experiences.

In order to make sure the information collected for the evaluation is relevant, the evaluator(s) should be given specifics on what should be observed. They can be provided with a list on the most important exercise phases. This list can also serve as a time line so that the evaluator(s) know when such events are expected to occur during the exercise. Additional support can be provided by formulating the criteria for the questions which should be addressed; for example, what should the evaluator be looking for and how should certain actions and conduct during the exercise be assessed?

9.2.1.5 Observe the exercise and process experiential feedback

The evaluators' documentation of the course of events as well as the collection of the exercise participants' impressions and reflections are crucial for evaluating and understanding how the participants acted during the exercise, how the exercise's arrangement affected the exercise, and if the exercise was useful for the participants.

Various types of materials can be used to evaluate an exercise:

- **Primary (first hand) materials:** observations of the participants, logs, the participants' notes, e-mails as well as telephone, audio and video recordings, and so on.
- **Secondary materials:** various types of materials produced for the exercise, such as orientation documents (exercise objectives), terms of references, scenario documents, and so on.

- **Experiential feedback:** After the exercise's active phase, the participants can be given the opportunity to verbally communicate their impressions and reflections on what happened during the exercise.
- **Data from personal interviews:** Interviews can also provide valuable information on insights and impressions of the exercise. Interviews can be done with both participants and persons in the exercise management regarding questions about the exercise itself and the method chosen for the exercise.
- **Observation notes:** Observers, who are often subject matter experts or people from other agencies, are often invited to share their thoughts based on their knowledge or professional point of view. Observers may be asked to keep notes of their impressions which could benefit and enrich the evaluation.
- **Surveys:** Questionnaires can be distributed to the participants and those included on the evaluation team.
- **Technical log files:** Technical log files show the extent to which communication took place during the exercise, what kind of technology was used for this, how well this technology worked, and how well security and confidentiality issues were respected.

The evaluator should carefully reflect on the most ideal place to be during the exercise so that participant observations can be done in the best possible way. However, it is important to note that it is not good to be too close to the participants since this can disturb them or since this runs the risk that the evaluator is "drawn into" the exercise.

A very significant part of processing feedback is discussing experiences. Everyone who participated in the exercise should be allowed to take part in the evaluation process. Early in the planning of the evaluation, time should be devoted to how and where this can happen.

If possible, processing feedback should take the form of a dialogue in which the participants can provided their comments and reflections in both oral and written form. A rule of thumb – the so-called 50-50 rule – is that half of time for the exercise should be devoted to collecting and processing experiential feedback.

A skilled discussion leader can get the exercise participants to reflect upon their performance during the exercise and can formulate a number of the lessons learned which they can take back with them. It is possible to dig deep into the process of what happened and why, what the consequences were, what lessons need to be highlighted, and so on. It is important to point out that collecting experiential feedback should be seen as a process, that is, as something that not only takes place on one single occasion. For example, spreading out the opportunities when the participants can discuss their experiences is one good way to encourage participant involvement in the evaluation process. This creates favorable conditions for success and for achieving the desired results; namely that, lessons learned are identified, accepted and used to make improvements.

Examples of the experiential feedback process:

- **Collecting experiential feedback and debriefing:** Just after the closure of the exercise, the participants, under the direction of a discussion leader, are given the opportunity to talk among themselves and describe their experiences during the exercise.
- **Seminar:** After a few weeks, a seminar is conducted with all of the exercise participants so they can share their exercise experiences and discuss which lessons should be raised and included in ongoing discussions. By this time, the participants have had time to digest their first impressions and also had time to reflect on what went well, what was problematic and, not least, what should be done in order to get an even better outcome next time. Furthermore, the evaluators should present their first preliminary conclusions and give the participants a chance to reflect on these.
- **Presentation of the final evaluation:** Once the evaluation report is finalized, there should be an opportunity to present the findings and conclusions. On this occasion, it is good if the evaluators give a clear picture of how the lessons learned can be worked on and developed, or at least provide a later time when this discussion can be facilitated. Otherwise, there is a risk that the learning process loses momentum or is completely discontinued after the final report is presented.

9.2.1.6 Analyze the collected data

When the exercise is completed, the next step is to analyze how the participants performed and how the selected exercise format affected the outcome. To facilitate this analysis, criteria should be formulated for the questions to be answered. A critical issue is how the impressions of the exercise can be evaluated. Issues may, for example, include the following: How well did the participants deal with stress and information overload? Did they organize themselves in an appropriate manner considering the situation at hand? Could decisions be made in an efficient manner? Did the participants behave/react in a “good” or “unsatisfactory” way, in relation to the desirable result, and what determined that?

Of course it is not always so simple, or black or white, to evaluate performance or ability; but rather, the appraisal is usually influenced by the situation.

Therefore, it is important to pay attention to the difficulty of analyzing and evaluating the behavior and actions of the exercise participants. Likewise, it is crucial that the participants feel they have been fairly evaluated so that they can accept and make use of the evaluation. Consequently, it is important to clarify, as much as possible, how the analysis will be conducted and with which criteria the participants' performances will be assessed.

9.2.1.7 Compile and disseminate the evaluation report

An evaluation report generally contains the following items:

- Summary
- Background to exercise
- Purpose and objectives of the exercise
- Exercise form - why this method was selected and what the pros and cons of it are
- Scenario – the major events in the exercise
- A review of the purpose and objectives - an account of the exercise performance and of any deviating events
- Lessons learned
- Proposal for how the results can be utilized
- The next step in the exercise process.

How then can the lessons learned be utilized and disseminated to the stakeholders? A good basis for this is establishing good communication between those responsible for the evaluation and the commissioning organization. This can advantageously be done by creating a mutual exchange of information during the evaluation process so that a sense of inclusion is created.

Other important aspects for the evaluators to consider are:

- Evaluators must a good understanding for the fact that the participants have different prerequisites for partaking in the exercise. Some cannot or do not want to embrace more advanced analyses. There are different ways to report their performances - from complex analyses and wordy reports to shorter oral presentations. Most importantly, the method should be tailored to the recipient.
- The evaluation should be completed while the memory of the exercise is still intact. The challenge is to find a balance between thoroughness and quality, on the one hand, and time and accessibility, on the other.
- Plans for how the evaluation will be used and disseminated should be included from the outset by making them a part of the evaluation design.

- An important aspect is that the evaluator finds a balance between praise and criticism.

9.2.1.8 Process lessons learned

Exercises and assessments are done to improve operations. One such improvement can be achieved only when one makes the step from identifying the lessons learned to addressing and changing the conditions that the evaluation highlighted. In order to achieve this, the key messages must be highlighted and receive significant attention. It is also advantageous if the lessons learned are presented as concrete suggestions for improvement rather than vague and general trends or patterns. What equipment is needed? What technology is required? What skills and competencies should be acquired? What competence development and education will get us there?

Another important question is who will ensure that the evaluation is disseminated, read and, consequently, produces the desired effect. One suggestion is to appoint early a working group with this task that will continue to work on making use of the identified lessons learned even after the exercise is completed. In doing so, this group will create a good starting point for the next exercise, for example, by encouraging that the lessons learned be exercised or by highlighting suggestions from the evaluation that have been neglected.

9.2.1.9 Start planning the next exercise

Make sure to utilize the results from previous evaluations to create a basis for planning future exercise efforts.

9.2.2 Good advice for evaluating exercises

- An evaluation is an essential part of the exercise process as a whole – not just something that comes at the end. The evaluation is important because it affects, and is affected by, all other components of the exercise. Therefore, the evaluation should be included already from the onset in the planning exercise.

- The purpose and objectives of the exercise must be clearly worded in order to enable a proper evaluation. If the objectives and purpose of the exercise are unclear, there is a great risk that the evaluation will also be.

- Involve the management – By doing this, it sends a strong signal to the entire organization that exercises should be taken seriously. The management is also the major beneficiary and user of the exercise evaluation.

- Use the 50-50 rule – half of the time should be used for the actual exercise and half of the time for collecting and processing experiential feedback, in which the events during the exercise can be discussed and reflected upon. The individuals' knowledge is deepened if there is sufficient time allocated for discussion and reflection.

- Allocate time and resources to identifying and establishing contacts with the recipients of the exercise evaluation. This makes it easier to understand what information they consider relevant and how they want information packaged and presented.
- The evaluation should weigh the participants' experiences, education, and training in relation to how they are evaluated. Remember to highlight both good and less favorable efforts in order to provide a balanced view of the participants' performances.
- Appoint a working group that is tasked with following the exercise process and that can later facilitate that the lessons learned from the exercise have an impact on and within the organization.
- Compile concise and relevant information about the organization's crisis plans and past crisis experiences that can be given to new employees.
- If there are people in an organization who "always" are observers during an exercise and conduct the evaluations, it is a good idea to occasionally allow them to participate in exercises in order to provide inspiration and to enable the organization to take on new experiences.
- Exercise evaluations have a greater value than just for their own organization. They are also important for the society at large since such work can support the development of standards and guidelines for "good" crisis management.
- Each organization participating in the exercise should make a deeper analysis of the organization's participation in the exercise in order to draw more specific lessons and experiences.

9.3 Exercise documentation that should be included in this phase (according to the previous section)

- Terms of reference for the exercise participants
- Terms of reference for the exercise management
- Security regulations
- Confidentiality terms
- Terms of reference for communication
- Contact list for the exercise organization
- Evaluation documentation

Reminders and helpful hints!

The exercise's purpose and objectives determine which data should be collected (the what). Thereafter, decide the method of data collection (the how) (technical/automatic and/or manual data collection) and then inform the exercise participants of this.

10 Processing Feedback

Processing feedback is easier if it is conducted shortly after the exercise is completed. This allows the evaluator to gather experiences from the participants via direct experiential feedback or debriefing after the exercise as well as from a review of the material collected during the exercise observations. Processing feedback can be done by having a seminar where the evaluator presents the initial findings from the exercise and then discusses them with the exercise participants before completing the final evaluation report.

10.1 Continuation of evaluation and processing feedback

Processing feedback is a continuation of the evaluation process that was addressed in the previous section on evaluating the implementation of the exercise.

10.2 Exercise documentation that should be included in this phase (according to the previous section)

- Terms of reference for the exercise participants
- Terms of reference for the exercise management
- Security regulations
- Confidentiality terms
- Terms of reference for communication
- Contact list for the exercise organization
- Evaluation documentation

Reminders and helpful hints!

Have a simple feedback section, a so-called *quick wash-up*, with the exercise controller right after the exercise has been completed in order to be able to capture the participants' experiences.

Processing feedback (1 of 2)

	FEEDBACK	
PROJECT MANAGEMENT PROCESS	(1) Completing and debriefing of the project	(2) Project follow-up and evaluating the results
EXERCISE PLANNING PROCESS	Reporting	After action review
CHAPTER IN THE HANDBOOK	Chapter 11	Chapter 12
ACTIVITIES	• Cont. taking inventory and discussing the need for training • Cont. evaluation and feedback	• Follow-up and generate ideas for new assignments
EXERCISE DOCUMENTATION	• Completion of project (project report) • Evaluation report of the participants • Evaluation report of the exercise project	

The project management process: Completing and debriefing as well as performing the after action review and evaluating the results[28]

This step in the project management process corresponds to feedback (Chapter 11) in the exercise planning process.

[28] See Chapter 13 ”Uppföljning och utvärdering” [After Action Review and Evaluations] in Wisén and Lindblom (2009), p. 163-180.

11 Reporting

After the results of the exercise have been analyzed and summarized, a report (a so-called After Action Review) is delivered to the commissioning organization. It may include the results and experiences of what was exercised as well as the experiences of the exercise process and the choice of the exercise form, etc.

11.1 Continuation of taking inventory and discussing the need for training

Reporting is a continuation of taking inventory and discussing the need for training both of which were previously mentioned in the section on exercise preparations in the planning process.

11.2 Continuation of evaluating and processing feedback

Reporting is also a continuation of evaluating and processing feedback both of which were previously mentioned in the section on evaluating while implementing an exercise.

11.3 Exercise documentation

- Project completion (project report)
- Evaluation report of the participants
- Evaluation report of the exercise project

Processing feedback (2 of 2)

	FEEDBACK	
PROJECT (MANAGEMENT)-PROCESS	(1) Completing and reporting of the project	(2) Project follow-up and evaluating the results
EXERCISE PLANNING PROCESS	Reporting	After action review
CHAPTER IN THE HANDBOOK	Chapter 11	Chapter 12
ACTIVITIES	• Cont. taking inventory and discussing the need for training • Cont. evaluating and processing feedback	• Follow-up and generate ideas for new assignments
EXERCISE DOCUMENTATION	• Project completion (project report) • Evaluation report of the participants • Evaluation report of the exercise project	

The project management process: Completing and reporting as well as following up and evaluating the results[29]

This step in the project management process corresponds to following-up (Chapter 12) in the exercise planning process.

[29] See Chapter 13 ”Uppföljning och utvärdering” [Following up and Evaluations] in Wisén and Lindblom (2009), p. 163-180.

12 After Action Review

After the results of the exercise/project have been analyzed and presented, this information can be used to make suggestions for new education/exercise efforts, propose changes in the organization or certain processes, and so on.

Some ways to follow up these results include:

- education efforts (within certain subject areas, for the exercise management, etc.)
- new projects (new technologies, new organization, new processes, etc.)
- new exercises
- networking for exercise enthusiasts and people with a good knowledge of exercises.

13 Practical Advice and Suggestions

This handbook for information technology and cyber security exercises was written largely based on the Swedish Civil Contingencies Agency's (MSB) exercise handbook "Crisis management exercises – A handbook for planning, implementing and feedback." Furthermore, the current handbook even builds upon the experiences of previous information technology and cyber security exercises.

Among the handbook's recommendations are the following practical advice and suggestions:

- Start with the exercise's mission statement and develop feasible and measureable objectives for the exercise. Do not have too many objectives! Use the directives to see if the allocated resources are sufficient for the purpose of the exercise. If not, the ambition level or the scale of the exercise should be adjusted accordingly. Otherwise, additional resources need to be obtained.

- Keep in mind the legal aspects with respect to information management and exercise documentation (such as security and confidentiality) throughout the entire project management and exercise process (from planning, implementation, evaluation, processing feedback, and following up). Make time to formulate appropriate contracts and agreements between the involved parties in planning the exercise.

- Make a risk and impact assessment and continually update it. This can be used to illustrate the expected and unexpected risks with the exercise. Information technology and cyber security exercises are often complex in structure and therefore often require relatively large resources of time, people and capital (including purchase of hardware and software, etc.).

- Be sure to include the technical management for support and communications (i.e., those responsible for the infrastructure used in information and cyber security exercises) as well as the evaluation management in planning the exercise and defining the purpose and objectives.
- The foundation for a well-structured implementation can be laid with good planning and a project management that provides adequate staff and establishes clear responsibilities and roles for the planning and implementing organization and for the evaluation organization and regularly makes follow ups.
- Remember to assign coordinators for managing information on the exercise project as well as appoint a media and communications manager for visitors.
- Communication and information management as well as exercise documentation should be traceable.
- Technical exercises require the ability to update situation awareness, and therefore the exercise environment and its systems should be thoroughly tested before the exercise is launched.
- Last but not least, remember that information technology and cyber security exercises are about people! If possible, maintain regular meetings and conferences with the involved participants and give them the opportunity to meet during the planning, implementation and following up phases of the exercise.

14 References and Suggested Readings

Baltic Cyber Shield Cyber Defence Exercise 2010, After Action Report. For Public Use. Available at: https://www.fhs.se/sv/forskning/centrumbildningar-och-forskningsprogram/cats/nyheter-och-artiklar/2010/ (published 2010-10-06).

European Commission (2009) "Communication from the Commission to the European Parliament, the Council, European Economic and Social Committee as well as the Committee of Regions on the Protection of Critical Information Infrastructure, 'Protection against Large-scale IT Attacks and Disruptions: Enhancing Preparedness, Security and Resilience in Europe'." EC Commission, COM (2009) 149 final. Brussels. March 30, 2009.

Karlsson, J. (2010) "Rapport efter CCD COE – Swedish CDX 2010" [Report after CCD COE- Swedish CDX 2010] Internal report to MSB. Stockholm: Center for Asymmetric Threat Studies, Swedish National Defence College. May 2010.

Lag (1990:409) om skydd för företagshemligheter. [Swedish Act on the Protection of Trade Secrets].

Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH). [Swedish Act on municipal and county council measures prior to and during extraordinary events in peacetime and during periods of heightened alert (2006:544)].

Lag. Offentlighets- och sekretesslagen (2009:400). [The Public Access to Information and Secrecy Act of Sweden] Swedish Code of Statutes – SFS 2009:400.

Merriam Webster. Available at: http://www.merriam-webster.com/

MSB (2011) Ett fungerande samhället i en föränderlig värld, Nationell strategi för skydd av samhällsviktig verksamhet. [A functioning society in a changing world: The MSB´s report on a unified national strategy for the protection of vital societal functions] Publication number: MSB266. English version available at: www.msb.se/RibData/Filer/pdf/26084.pdf

MSB (2011-03-01) Nationell hanterandeplan för allvarliga IT-incidenter, Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap [National plan for handling serious IT incidents. Response to the Government’s task given to the Swedish Civil Contingencies Agency]. (Fö2010/701/SSK, Government decision 12, 2010-04-14). Case nr 2010-4545.

MSB (2010a) Strategi för samhällets informationssäkerhet, 2010-2015. [Strategies for society’s information security]. Karlstad. Available only in Swedish at: https://www.msb.se/RibData/Filer/pdf/25482.pdf

MSB (2010b) *Utvärdering av* övningar [Handbook – Evaluation of Exercises]. Publication No. MSB244. English version available at: https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Evaluation-of-Exercises/

MSB (2009) *Öva Krishantering – Handbok i att planera, genomföra och återkoppla övningar”* [Crisis management exercises – A handbook on planning, implementing and processing feedback]. Available only in Swedish at: http://www.msb.se/RibData/Filer/pdf/25608.pdf

Nationalencyklopedin [The National Encyclopedia]. Available only in Swedish at: http://www.ne.se/

OTRS (Open-source Ticket Request System). Available at: http://www.otrs.org

SIS (Swedish Standards Institute) (2007) *Terminologi för informationssäkerhet* [Information security terminology].SIS HB 550, 3rd edition. SIS Förlag AB.

Wikipedia. Available at: http://sv.wikipedia.org/wiki/

Wisén, J. and Lindblom, B. (2009) *Effektivt projektarbete* [Effective project management]. Sweden: Norstedts Juridik AB.

15 Appendix

Below are examples of content that should be included in templates and on checklists for documenting the project management and the exercise planning process.

- **Mission statement**
  The mission statement should include the following elements:
  1. A comprehensive title
  2. Background to the project's origins
  3. Description of the mission in the terms of reference (what should be achieved?)
  4. Purpose, vision and objectives
  5. Explanation of the project's limitations
  6. Necessary resources (rough estimate)
  7. Preliminary time table (with at least the final deadline)
  8. Instructions regarding who should be consulted and informed throughout the project.

- **Consulting agreements and project employment terms**
  Consulting agreements and project employment terms should contain the following elements:
  - The commissioning organization (or the organization representing it)
  - Service providers/contractors
  - The mission (what it involves and where)

  - Period of agreement (times for launching, completing, and debriefing)
  - Compensation/fees
  - Vacation pay
  - Social security fees/costs

- **Agreements and contracts between the parties involved in the exercise project**

  Agreements and contracts may include the following:
  1. The involved parties' names, contact information, and, perhaps even, organization registration numbers
  2. Background and purpose
  3. Insurance policy
  4. The parties' commitments in the project
  5. The commitments of the project (financial, funding)
  6. Terms of reference for delays
  7. Terms of payment
  8. Duration of the agreement and terms regarding interventions or transfers
  9. Rights to the final product
  10. The designated contact people
  11. Terms regarding a breach of the agreement
  12. Force majeure – unavoidable circumstances beyond the control of the involved parties
  13. Amendments and supplementary information

- **Project plan**
  1. The project plan (with the appropriate version number) should contain:
  2. The objectives, focus and limitations
  3. Strategy and methodology
  4. General activity plan and time table
  5. Project budget
  6. Project organization (people, roles, and responsibilities)
  7. Internal and external information and communication
  8. Expected outcome/end product
  9. Anticipated effects

- **Description of activities[30] and activity plan**

  Every activity (with its respective version number) that is included in the exercise project can be described with the following:

  1. Name of the activity
  2. The cost units/carriers
  3. When the activity should be carried out and by whom
  4. Description of activity: aim, objectives, methodology, etc.
  5. Activity's desired effect
  6. Timeline for the activity (planned and actual start date, completion date, and resource needs)

  Often, an action plan is made (for example, in the form of a Gantt bar chart), where activities are described and placed on a timeline. This way activities and timings are combined and illustrated in one document.

- **Project budget[31]**

  The project budget should include:

  1. The date when it was proposed and the date when a decision was made to accept it
  2. Name/Title
  3. Budget year (applicable for every year included in the exercise)
     a. The number of working days
     b. Wages
     c. Consultant expenses
     d. Travel costs
     e. Other issues
  4. Total and estimated costs per quarter
  5. Additional information

- **Time table**

  1. The time table can be neatly illustrated using a Gantt bar chart with the following information:
  2. Dates covered by the time table
  3. Time line with month/quarter and year
  4. Each activity is added to the chart under the time period when it is expected to be carried out.

[30] Wisén and Lindblom (2009), p. 312.

[31] Wisén and Lindblom (2009), p. 311.

5. Different symbols or colors can be used on the chart to indicate when the steering committee, reference group, or similar have meetings to highlight fixed times in the exercise planning.

- **Project deviations**[32]
  This reflects the project budget and contains the following:
  1. The date when the activity was proposed and the date when the decision was made to accept it
  2. Name/Title
  3. Budget year (applicable for every year included in the exercise)
     a. The number of working days
     b. Wages
     c. Consultant expenses
     d. Travel costs
     e. Other issues
  4. Total and estimated costs per quarter
  5. Reasons for why deviations appeared as well as proposed measures for resolving them.

- **Terms of reference for the exercise participants**
  The terms of reference for the exercise participants should include the following information:
  1. Exercise times (e.g., when the exercise will start and end)
  2. Exercise form and methodology
  3. Roles and responsibilities
  4. Purpose as well as overall and intermediate objectives
  5. Information about the organization, participants, and exercise management
  6. Information about the scenario, including previous developments and background information about the scenario, and the starting point
  7. Times for reviews and such
  8. Technology and communications issues
  9. Security issues
  10. Practical matters – the conditions necessary for people to be able to work (food, drink, restrooms, etc.)

[32] Wisén and Lindblom (2009), p. 313.

11. Financial matters and considerations
12. Evaluation and feedback
13. Presence of visitors, if there will be any
14. Related attachments.

- **Terms of reference for the exercise management**

  The terms of reference for the exercise management should include the following information:

  1. The organization
  2. Instructions about documentation and reporting for exercise controllers and evaluators
  3. Technology and communication (that is above and beyond that stipulated in the terms of reference for the exercise participants)
  4. The scenario including the planned development of events
  5. Any special directions for evaluation
  6. Any special directions for the counterplay organization
  7. Any additional necessary information concerning the exercise

- **Security and safety regulations**

  Ordinary employment insurance and occupational safety rules should apply during the exercise. The exercise controller is required to inform all exercise participants of the relevant security and safety regulations before the exercise begins. This can be done by including them in the terms of reference for the exercise participants.

  In addition to the participants' physical safety, the terms of reference should also touch upon issues related to data, IT, and administrative security (i.e., policies, continuity plans, regulations, etc.) so that the exercise not only addresses such issues but also actively applies and trains information and cyber security.

- **Terms of reference for privacy/confidential issues**

  These terms of reference should take into account the following issues:

  1. How information and documents are expected to be used and archived during the information and cyber security exercise.
  2. Whether the data from the exercise should be considered a public document under the Freedom of Press Act, or if there are exceptions regarding the issue of confidentiality according to the Public Access to Information and Secrecy Act (2009:400).

3. Confidentiality issues applicable to private organizations in accordance to the law on the protection of trade secrets (1990:409).
4. Are there employment contracts binding employees to professional secrecy?

- **Terms of reference for communications**
  The terms of reference for communications should ideally be included in terms of reference for the exercise participants and exercise management.

- **Contact list for the exercise organization**
  This should include the following information:
  1. Name
  2. Organization/company and department
  3. Role/function in the exercise
  4. Email address
  5. Telephone number
  6. If available, information about Skype accounts, MSN, video conferencing, Jabber, Web, etc

- **Exercise documentation**
  Evaluation documentation on the planning organization and the participants collected via technical/automatic data collection during information technology and cyber security exercises should include:
  1. The purpose of collecting certain data for the evaluation
  2. Confidentiality, security and privacy concerns with respect to the management of collected data and using this data to evaluate the exercise.
  3. What is to be collected and how should it be collected before, during and after the exercise.

- **Project report** [33]
  After the project is completed, it should be documented for future follow-up. The project report should include:
  1. Date, title and total cost
  2. The commissioning organization, the project leader, and the other organizations/departments

[33] Wisén and Lindblom (2009), p. 314.

3. Reports and other documentation from the project
4. Someone who is responsible for following up:
   - How well were the objectives fulfilled?
   - How well was the time table kept?
   - Did the project stay within the budget?
   - Organization and staffing issues
   - Any other effects of the exercise that were expected, and proposals for future work in another exercise form.
5. Organization and staffing
6. Explanation for uunexpected effects and proposals for future work on another exercise.

- **Evaluation report (of the participants as well as of the exercise project)**

  An evaluation report generally contains the following items:
  1. Summary
  2. Background to the exercise
  3. Purpose and objectives of the exercise
  4. Exercise Form – why this method was selected and its pros and cons
  5. The scenario – the major events in the exercise
  6. Follow-up of the purpose and objectives – an illumination of the actions and any deviating events
  7. Lessons
  8. Proposals for using the results
  9. The next step in the exercise process.

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

Cyber Defence Exercise (CDX) is a tool for raising cyber security awareness and train people to handle different situations in a controlled cyber environment. To exercise is a way of enhancing Tools, Techniques and Procedures, TTP. It's also a way of building trust between the participants, as cooperation is needed to solve problems under stress. Failures give lessons learned and not any drastic consequences.

In this handbook by the Swedish National Defence College's Center for Asymmetric Threat Studies (CATS), Nina Wilhelmson and Thomas Svensson describes different types of exercises and in particular Red versus Blue Team Exercise. It covers the process from the first idea to the after action analysis. Thomas Svensson has been represented CATS in Baltic Cyber Shield 2010 and Locked Shields 2012 – 2014 as a member of the exercise control team (White Team). The base for the handbook has been Swedish Civil Contingencies Agency (MSB) Exercise Handbook with additions and lessons learned from Cyber Defence Exercises held in cooperation between Sweden and Estonia.

ISBN 978-91-86137-36-6

NATIONAL DEFENCE COLLEGE

CATS
Center for Asymmetric Threat Studies

National Defence College
Box 27805
SE-115 93 Stockholm
www.fhs.se