BS ISO 22398:2013

BSI Standards Publication

Societal security — Guidelines for exercises

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO 22398:2013.

The UK participation in its preparation was entrusted to Technical Committee SSM/1, Societal security management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013. Published by BSI Standards Limited 2013

ISBN 978 0 580 74562 1

ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2013.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 22398:2013

INTERNATIONAL STANDARD

ISO 22398

First edition
2013-09-15

Societal security — Guidelines for exercises

Sécurité sociétale — Lignes directrices pour exercice

Reference number
ISO 22398:2013(E)

Documents
Document Sharing Hub

© ISO 2013

Full document details: BS ISO 22398:2013

COPYRIGHT PROTECTED DOCUMENT

© ISO 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO 2013 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 22398:2013

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Planning, conducting and improving an exercise programme **4**
4.1 General 4
4.2 Planning 4
4.3 Conducting 6
4.4 Reviewing and improving the exercise programme 7
5 Planning, conducting and improving exercise projects **7**
5.1 General 7
5.2 Planning 8
5.3 Conducting 19
5.4 Improving 21
6 Continual improvement **21**
6.1 General 21
6.2 Evaluation 21
6.3 Management review and corrective action 23
Annex A (informative) **Exercises within a management system description** **24**
Annex B (informative) **Needs analysis** **27**
Annex C (informative) **National strategic exercises** **29**
Annex D (informative) **Exercise enhancement** **32**
Annex E (informative) **Creating scenarios through experience** **33**
Bibliography **35**

© ISO 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 223, *Societal security*.

© ISO 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

Introduction

This International Standard describes the elements of a generic approach to planning, conducting and improving exercise programmes and projects. The purpose of this International Standard is to:

— provide a basis for understanding, developing and implementing an effective exercise programme within an organization;

— provide guidelines for planning and conducting an exercise project;

— enhance the organization's ability to conduct exercises with internal and external involved parties;

— assist the organization with developing and assessing its exercising capability in a consistent and risk-assessed manner that reflects good practice; and,

— enable continual improvement in exercise programmes and projects within an organization.

It is applicable to all organizations, regardless of type, size and nature, whether private or public. The guidance can be adapted to the needs, objectives, resources, and constraints of the organization.

Exercises are an important management tool intended to identify gaps and areas for improvement as well as to determine the effectiveness of response and recovery strategies. In addition to measuring the competence of the organization and its personnel, exercises are excellent tools to assess revised plans and changed programmes for completeness, relevancy and accuracy.

Exercises can be used for validating policies, plans, procedures, training, equipment, and inter-organizational agreements; testing information and communication technology (ICT) disaster recovery systems; clarifying and training personnel in roles and responsibilities; improving inter-organizational coordination and communications; identifying gaps in resources; improving individual performance; identifying opportunities for improvement; and, providing a controlled opportunity to practice improvisation.

Exercise projects usually have performance objectives such as:

— *orientation/demonstration*: simulating experience of an expected situation to increase awareness of vulnerabilities and the importance of effective action in response to the simulated conditions;

— *learning*: enhancing knowledge, skills, or abilities by individuals or groups with the goal of mastering specific competencies;

— *cooperation*: providing an opportunity for people to work together to achieve a common end result;

— *experimenting*: trying new methods and/or procedures with the intent of refinement; and,

— *testing*: evaluating a method and/or procedure to assess which components are sufficiently developed.

See Figure 1.

© ISO 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

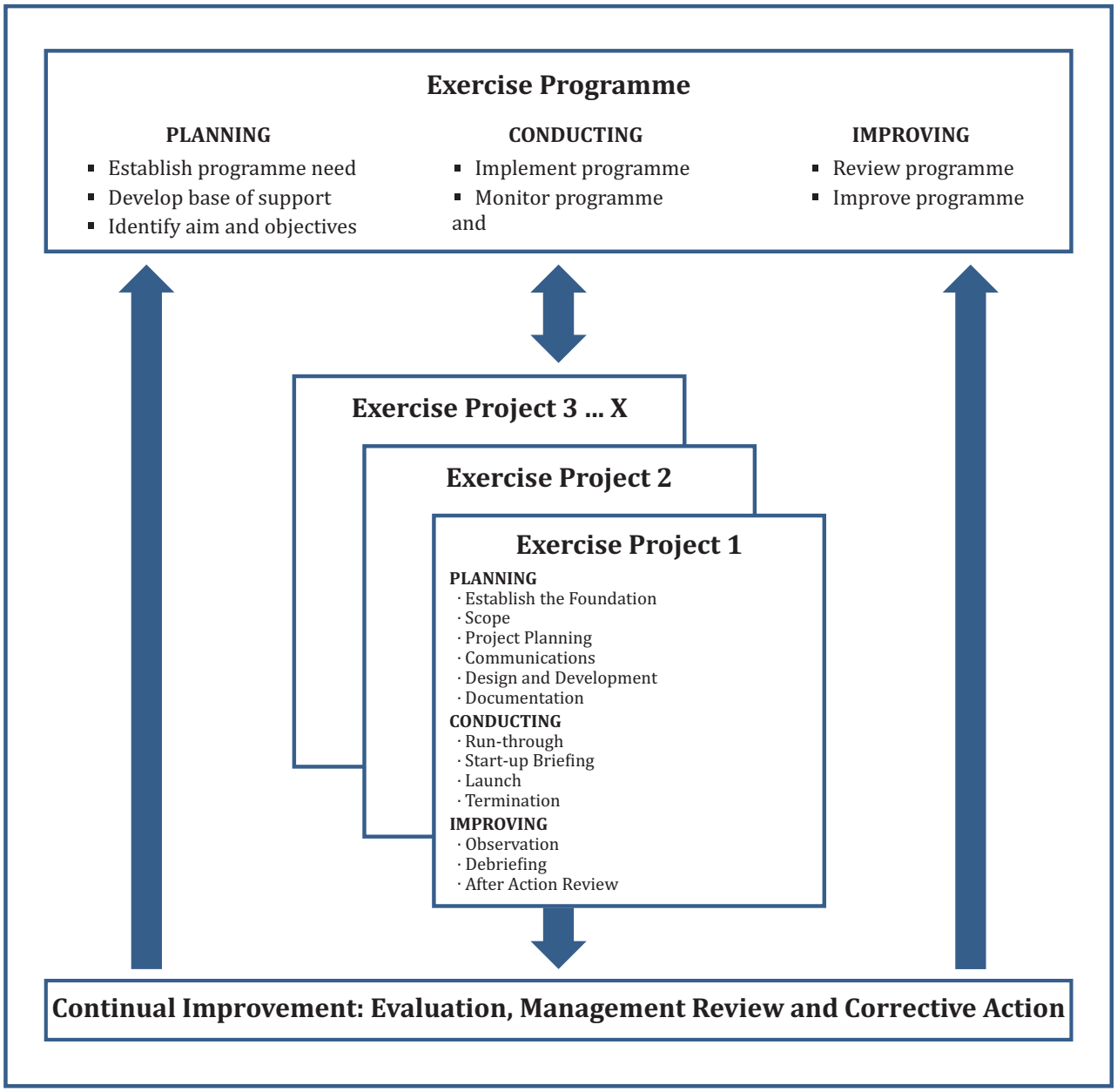

Figure 1 — Relation between exercise programme, exercise projects and continual improvement

© ISO 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

INTERNATIONAL STANDARD ISO 22398:2013(E)

Societal security — Guidelines for exercises

1 Scope

This International Standard recommends good practice and guidelines for an organization to plan, conduct, and improve its exercise projects which may be organized within an exercise programme.

It is applicable to all organizations regardless of type, size or nature, whether private or public. The guidance can be adapted to the needs, objectives, resources, and constraints of the organization.

It is intended for use by anyone with responsibility for ensuring the competence of the organization's personnel, particularly the leadership of the organization, and those responsible for managing exercise programmes and exercise projects.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

3.1
after-action report
document which records, describes and analyses the exercise, drawing on debriefs and reports from observers, and derives lessons from it

Note 1 to entry: The after-action report documents the results from the after-action review.

Note 2 to entry: An after-action report is also called a final exercise report.

3.2
competence
demonstrated ability to apply knowledge and skills to achieve intended results

3.3
drill
activity which practices a particular skill and often involves repeating the same thing several times

EXAMPLE A fire drill to practice safely evacuating a building on fire.

3.4
evaluation
systematic process that compares the result of measurement to recognised criteria to determine the discrepancies between intended and actual performance

Note 1 to entry: The gaps are inputs into the continual improvement process.

© ISO 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

3.5
exercise
process to train for, assess, practice, and improve performance in an organization

Note 1 to entry: Exercises can be used for validating policies, plans, procedures, training, equipment, and inter-organizational agreements; clarifying and training personnel in roles and responsibilities; improving inter-organizational coordination and communications; identifying gaps in resources; improving individual performance and identifying opportunities for improvement; and a controlled opportunity to practice improvisation.

Note 2 to entry: A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

3.6
exercise coordinator
person responsible for planning, conducting, and evaluating exercise activities

Note 1 to entry: In larger exercises, this function may include several persons/staff and may be called "exercise control".

Note 2 to entry: Some countries use a term such as "exercise director" instead of "exercise coordinator" (or similar text).

Note 3 to entry: The exercise coordinator role is also responsible for the cooperation among internal and external entities.

3.7
exercise programme
series of exercise activities designed to meet an overall objective or goal

3.8
exercise programme manager
person responsible for planning and improving the exercise programme

3.9
exercise project team
persons planning, conducting and evaluating an exercise project

3.10
exercise safety officer
person tasked with ensuring that any actions during the exercise are performed safely

Note 1 to entry: In larger exercises, involving multiple functions, more than one safety officer may be assigned.

3.11
hazard
source of potential harm

Note 1 to entry: A hazard can be a source of risk.

3.12
interested party
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: A decision maker can be an interested party.

3.13
inject
scripted piece of information inserted into an exercise designed to elicit a response and facilitate the flow of the exercise

Note 1 to entry: Injects can be written, oral, televised, and/or transmitted via any means (e.g. fax, phone, e-mail, voice, radio, or sign).

© ISO 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

3.14
management
coordinated activities to direct and control an organization

3.15
observer
exercise participant who witnesses the exercise while remaining separate from exercise activities

Note 1 to entry: Observers may be part of the evaluation process.

3.16
participant
person or organization who performs a function related to an exercise

3.17
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected - positive and/or negative.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

Note 3 to entry: Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated likelihood of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

3.18
scenario
pre-planned storyline that drives an exercise, as well as the stimuli used to achieve exercise project performance objectives

3.19
scope of exercise
magnitude, resources, and extent which reflects the needs and objectives

3.20
script
story of the exercise as it develops which allows directing staff to understand how events should develop during exercise play as the various elements of the master events list are introduced

Note 1 to entry: The script is often written as a narrative of simulated events.

3.21
target group
individuals and/or organizations subject to exercise

3.22
test
exercise with an aim to obtain an expected measureable pass/fail outcome

Note 1 to entry: A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned.

Note 2 to entry: The terms “test” and “testing” are not the same as “exercise” and “exercising”.

© ISO 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

3.23
training
activities designed to facilitate the learning and development of knowledge, skills, and abilities, and to improve the performance of specific tasks or roles

4 Planning, conducting and improving an exercise programme

4.1 General

An organization conducting exercises should establish an exercise programme. Establishing an exercise programme allows for a coordinated approach to building and maturing the organization's capabilities by allowing the exercising of the individual plans, people, capabilities and/or resources that contribute to the organization's strategic objectives.

Top management should ensure that the exercise programme objectives are established and assign a competent person to manage the exercise programme. The scope of an exercise programme should be based on the size and nature of the organization undertaking exercising, as well as on the scope, functionality, complexity and the level of maturity of the plans and capabilities being exercised.

The exercise programme should include the information and resources necessary to organize and conduct its exercises effectively and efficiently within the specified time frames. It should also include the following:

— needs analysis;

— base of support;

— exercise programme aim and objectives;

— extent/number/types/duration/locations/schedule of the exercise projects;

— selection of exercise project teams;

— necessary resources and budget; and,

— processes for handling confidentiality, information security, health and safety, and other similar matters.

The organization should monitor and measure the implementation of the exercise programme to ensure the established objectives have been achieved. The exercise programme should be reviewed in order to identify possible improvements.

4.2 Planning

4.2.1 Establishing the need for an exercise programme

The organization should perform a needs analysis to identify or establish the following:

— the organization's strategic objectives;

— the risks to the organization;

— legislative and regulatory requirements;

— the organization's maturity to respond and/or recover compared to desired objectives, noting gaps in capability and plans;

— the plans, procedures, capabilities or resources that require exercising;

— the period in which a defined level of response and/or recovery capability (programme scope) should be met; and,

© ISO 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013

— the base of support and guide the content of the exercise programme.

4.2.2 Establishing the base of support for an exercise programme

The organization should secure a base of support and commitment from top management to ensure the appropriate organizational involvement and commitment of resources. Securing a base of support ensures that the exercise aim and objectives correspond to the organization's strategic objectives and strategy.

Top management should give the organization a clear mandate and full authority to carry out the exercise programme. The benefits and advantages of the exercise programme, as determined by the needs analysis, should be clearly explained and presented to top management, and to those who have responsibility for the exercise programme.

4.2.3 Establishing the exercise programme aim and objectives

Top management should ensure that the aim and objectives of the exercise programme are established to direct the exercise planning, conducting and improving and should ensure the exercise programme is implemented effectively.

Based on the exercise programme aim, the objectives can be based on the following:

— the findings of the needs analysis;

— management priorities;

— management system requirements, as applicable;

— legal, regulatory and contractual requirements and other requirements to which the organization is committed;

— needs and expectations of interested parties;

— risks to the organization or interested parties;

— reports and results of previous exercises or actual incidents; and,

— the level of organization maturity and its resources being exercised.

NOTE Annex A provides additional information about exercises within a management system.

4.2.4 Roles and responsibilities of the exercise programme manager

The organization should establish the roles and responsibilities of the exercise programme manager who will be nominated by top management. These roles and responsibilities usually include:

— establishing the scope, aim and performance objectives of the exercise programme, and the scope, criteria and timeframe of the individual exercise projects based on the objectives;

— identifying, documenting and evaluating the exercise programme risks;

— determining the potential impacts of the exercise project upon the organization's operations, reputation and resources;

— estimating the impact of an actual incident occurring during the exercise project;

— establishing the exercise types and methods required to achieve the programme objectives;

— determining necessary resources, including the resources to plan and conduct the exercise;

— selecting the exercise project team;

— developing a procedure to complete documents, and managing and maintaining documentation;

AVA Documents
Document Sharing Hub

© ISO 2013 – All rights reserved

Full document details: BS ISO 22398:2013

— ensuring the implementation of the exercise programme; and,

— monitoring, reviewing and improving the exercise programme.

The exercise programme manager should inform top management of the activities and risks associated with the exercise programme and obtain approval to proceed with exercising.

The exercise programme manager should have the competence necessary to effectively and efficiently manage the exercise programme and the associated risks. The exercise programme manager is accountable to top management for the programme and top management should be responsible for the exercise programme. The exercise programme manager may form and select one or more teams to support the delivery of the programme, ensuring that team members are competent to meet their responsibilities effectively and efficiently.

4.3 Conducting

4.3.1 Implementing the exercise programme

The exercise programme manager should implement the exercise programme by:

— communicating the pertinent parts of the exercise programme to interested parties, and informing them periodically of its progress;

— coordinating and scheduling exercise projects and other activities relevant to the exercise programme;

— ensuring the selection of exercise project teams whose members have the necessary competence;

— providing necessary resources to the exercise project teams;

— conducting exercises in accordance with the exercise programme and within the agreed upon time frame;

— recording exercise activities and managing and maintaining documents; and,

— completing after-action reviews and following up on lessons learned and recommendations for improvement.

4.3.2 Monitoring exercise performance

The exercise programme manager should ensure the effective and efficient evaluation of individual exercise projects. Consideration should be given to the method used for comparison over the duration of the programme in order to implement an effective and efficient exercise programme.

Performance evaluation processes identify changing maturity, allow for comparison between teams, locations or capabilities and identify areas for development in future programmes. A consistent method of measuring the performance of participants, procedures and capabilities provides for effective evaluation of the performance of the exercise programme and should be included in the organization's evaluation process.

The exercise programme manager should ensure that the evaluation process and criteria assess the entire programme, inclusive of the individual exercise projects, based on programme aim and objectives. The exercise performance objectives should have predefined evaluation criteria and consistent measurement methods that compare exercise project results over time. A number of consistent objectives should be applied to individual exercise projects, and aligned to the exercise programme objectives. Examples of activities that could provide performance trends are the:

— time taken to respond to the information inserted into an exercise (specific injects);

— time taken to conduct a call cascade; and,

— number of resources mobilized in a given time or space.

© ISO 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 22398:2013