Exercitium



EUROPEAN HANDBOOK OF MARITIME SECURITY EXERCISES AND DRILLS

Foreword 2
Legal Framework 5

PART 1
THEORY 9

Theoretical structure makes practical exercises 11

The basics 12
General aspects of exercises: plans, objectives and resources

1 Background 12
Definitions 12
Aim and philosophy of exercises 13
The advantages of an exercise 13
Equivalent Security Arrangement 14
Restrictions 14
Experience with exercises in the port of Antwerp 14

2 Before the exercise 15
Be real 15
Exercise schedule 15
Time line 15
Graphic and other resources 15
Communication and discretion 16
Checklist 16
The Deming circle 17

3 During the exercise 18
Organising and holding a major exercise 18
The scenario 18

4 After the exercise 20
Evaluation 20
Documenting and reporting 20
Feasibility of procedures and measures 21
Practicing at exercising 21

Typology 22

1 Types of exercise 22
Monodisciplinary exercises 22
Multidisciplinary exercises 22
Alarm exercises 22
Virtual exercises 22
Tabletop exercises 23
Exercises on the ground (CPX – FTX) 23
Seminars/info sessions 24

2 Types of security plans 25

Participants 26
Who takes part in the exercise

Collaboration 27

Organising a port security exercise 28

Introduction 28
How to organise a port security exercise 29

12 steps towards a successful exercise 32

PART 2
PRACTICE 39

Practice makes perfect 41

Drills 42
1-5: Organisation and performance of port facility security duties 43
6-12: Communication and raising alarm 48
13-24: Access to the port facility 55
25-27 : Restricted areas within the port facility 67
28-33 : Monitoring the security of the port facility 70
34-37 : Handling of cargo 76
38-40 : Delivery of ship's stores 80
41-42 : Handling unaccompanied baggage 83
43-44 : Training, drills and excercises on port facility security 85
45-49 : Ferry Services 87

Annual exercises 92
1-12 : Annual exercise 94

Example:
Cooperative Shield, an Antwerp port security exercise 106

PART 3

TOOLS 113

Tips & Tricks 115
- 1. Put up barriers by dismantling 115
- 2. Set up barriers with big bags 116
- 3. Set up barriers with containers 116
- 4. Tailgating 117
- 5. Deploy additional personnel 117
- 6. Use of visual means to announce a heightened security level 118
- 7. Watch out for inconsistencies 118
- 8. Identification procedure 119
- 9. Identity swap 119
- 10. Watch out for unattended vehicles or packages 120
- 11. Getting a lift in a vehicle 120
- 12. Gain unauthorised access to the facility 121
- 13. Use the wide-angle mirror to check for objects 121
- 14. Use available resources to close gates 122
- 15. Create lock gates 122
- 16. This is a breach 122
- 17. Advance notice of arrival of persons with vehicle 123
- 18. Keep your perimeter fence unobscured 123

Tests in the field 124

Security Questionnaire 126

Breaches of Security 128

Port Security Awareness Handbook 130

Suspect behaviour 144

Cargo inspection 146
- Seal inspection 146
- Container inspection 147
- Truck & trailer inspection 147

Port Security Exercise 148
- Mind-map 149
- COOP-MEL 150
- Exercise convention 150

Audit Questionnaire 152

Pamphlet (example) 156

Declaration Of Security 157

Bomb Threat Form 158

Alarm Signals 159

Evacuation Signalisation 160

Safety first! 162

PART 4

BACKGROUND

Bibliography 166

Abbreviations 167

CONTENTS

Never be too sure about security

Mr Dimitrios Theologitis and his successor Mr Robert Missen from the European Commission, DG Move, Unit A4, Land and Transport security, have been instrumental in writing out a Grant for the European Handbook of Maritime Security Exercises and Drills.
We owe them, and their supporting team of Unit A4, thanks for having taken this initiative and for having supported us during the whole project period.
Furthermore, I want to thank Mr E. Bruyninckx, CEO of the Port of Antwerp and Capt. Jan Verbist, Harbour Master/Commander for allowing me to apply for the grant and consequently supporting the endeavors of the editorial team.
I am very much obliged to the people from several European authorities who have corresponded, provided useful information and have given feedback on proposals. Special thanks to Winnie Venstergard (Danish Coastal Authority), Stephen Hilton (TRANSEC, UK), Christian Schlüter (Hamburg Port Authority), Ralf-Udo Lemke (Landespolizeiamt Schleswig-Holstein), Kim Pettens (Harbour Master Port of Zeebrugge) and Erik Noor (Estonian Maritime Administration)
For sharing the basics of exercising, and allowing to actually witness all the steps of a major exercise, I want to thank Mr Bart Bruelemans, the City of Antwerp Contingency planning Manager, and Mss Ilse Van Mechelen, Attaché Contingency planning Province of Antwerp.
Without the continuing efforts from the Harbour Master's Safety & security team and the Port Facility Security Officers in the Port of Antwerp, this handbook would not be the practical "users guide" we aimed it to become.
A sincere thanks is on order for Tine Vandendriessche who taught us about the existence of a copywriter and lay-out specialists.
I am thankful to Mr Geerdt Magiels for properly structuring our thoughts and writings and to Mr Edward Cuypers who taught us that lay-out is much more than text and pictures.
Finally, my gratitude goes to Kathy Dua, for her continuous dedication to this project.

COLOPHON
Responsible editor
Tine Vandendriessche
Design
Pi-design, Antwerp
Photography
© Antwerp Port Authority
Paper
FSC-certified

Port of Antwerp

> **The importance of security in ports and on board ships has grown during the past decade along with the growing awareness of the dangers posed by terrorist attacks or activities. The need for this manual has arisen from this concern.**

foreword

Ports are complex places, covering a wide area with many kilometres of quays and involving hundreds of companies and thousands of people. There are just as many points and times when security may be compromised, either through human error or through malicious intent.

We cannot afford not to be thoroughly prepared for such occasions. We can do this only by having detailed Security Plans and by exercising these plans in realistic settings. While theoretical knowledge is important, we have to practice the relevant skills so that we know they will work in an emergency.

It is therefore no coincidence that European Regulation 725/2004 requires under ISPS Code Part B para. 18.5 and 18.6 that drills and exercises should be held on a regular basis. Drills have to be conducted at least every three months, testing individual elements of the Security Plan. Exercises should be carried out at least once each calendar year. They test communication, coordination, resource availability and response of the several services involved in security. These exercises may be full-scale or live, tabletop simulations and seminars or combined with other exercises, such as emergency response or other state authority exercises.

This Regulation points the way for ports and port facilities to learn the necessary practical skills, to test the feasibility of their plans and to be ready for the moment that the plan actually has to be put into operation.
These security drills are extremely important because they enable us to gain live experience of the importance of networks between people collaborating across the boundaries between levels and organisations.

This manual is intended to give Security Officers of ports and port facilities a full package of drills and exercises, in all possible forms and for every imaginable purpose. It has grown out of the long years of experience gained by the Port of Antwerp security services. It first describes the legal framework and then sketches the theory of security and safety and how it is put into practice. This is followed by ready-made, practical scenarios, then another section describing available tools for easily setting up such scenarios, and finally a collection of background information.

This manual is a practical guide. Each port is different, and each situation demands its own particular approach. Only one thing is sure: the greatest threat to security is complacency. Therefore, practice is essential.
Be safe, never be too sure!

The conclusions of this Handbook and the examples of drills and exercises provided therein are in no way binding for the European Commission or for the Commission inspectors during the Commission inspections. This Handbook gives only examples and suggestions for carrying out drills and exercises.

TERRORISM

"Terror" is Latin for fear. Terrorism is the use of extreme violence or threat of violence against civilians to create an atmosphere of fear, panic and uncertainty. It targets not specific victims but the general public. Terrorist acts can be viewed as planned campaigns of violence carried out against various types of group in order to achieve political or ideological objectives.

All forms of terrorism have five basic characteristics, irrespective of the type of organisation that carries them out:

1. Terrorist actions are planned and carried out with prior intent.
2. Terrorist actions are targeted against the general public, rather than particular victims.
3. Terrorism does not make any distinction between its victims.
4. Terrorism goes beyond the bound of acceptable moral behaviour.
5. The aim of terrorism is to put pressure on the political system.

Terrorism has become a worldwide problem, although its root causes are frequently to be found in a particular local conflict.

Technological solutions (both hardware and software) can be used to detect and combat terrorism, but even these solutions are uselesswithout vigilant people.

THE MOST IMPORTANT AND EFFECTIVE MEASURE AGAINST TERRORISM IS TRAINED HUMAN ALERTNESS.



Legal framework

Summary of the relevant articles
from the EU Regulation and Directive that relate
directly or indirectly to drills and exercises.

REGULATION 725/2004

The aim of the regulation is to protect ships and port facilities against terrorist activities, by providing an international framework for collaboration between local and federal authorities and the shipping industry, in which each participant has their own tasks and responsibilities. This framework is aimed at detecting threats to security and taking measures to prevent security incidents occurring, at the direct interface between quay and ship. The regulation requires security measures to be taken both for the port facilities and for ships, and for these measures to be practiced.
The main aim of this regulation is to introduce EU-wide measures to improve security from terrorism against international trade, shipping and associated port facilities.

The ISPS code (reg. 725/2004) requires port facilities to conduct security drills at least once every quarter (i.e. four times per year). In practice these drills are fairly small-scale and should not have any impact on the commercial activity of the port facility. Their purpose is to test the separate parts of the Port Facility Security Plan (PFSP).

In addition, at least one large-scale exercise should be carried out at least once every year (with not more than 18 months between two exercises). The aim should be to combine several procedures from the plan within the exercise, and if possible, to involve local authorities who have a port security responsibility (the competent authority, the police, shipping police, fire department,...), the Company Security Officer (CSO) or the Ship Security Officer (SSO).

All the drills and exercises can be carried out live or may take the form of a computer simulation or seminar. It is also possible to combine the security drills or exercises with other exercises, for example the disaster plan.

Compulsory

A 1.3 Functional requirements
.7 requiring training, drills and exercises to ensure familiarity with Security Plans and procedures.

A 17.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the Port Facility Security Officer shall include, but are not limited to:
.3 implementing and exercising the Port Facility Security Plan
.8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility

A 18.3 To ensure the effective implementation of the Port Facility Security Plan, drills shall be carried out at appropriate intervals, taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in part B of this Code.

A 18.4 The Port Facility Security Officer shall ensure the effective coordination and implementation of the Port Facility Security Plan by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

B 16.3 All PFSPs should (section B that has been made obligatory):
.6 detail reporting procedures to the appropriate Contracting Government's contact points.

B 18.5 To ensure the effective implementation of the provisions of the Port Facility Security Plan, drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan such as those security threats listed in paragraph 15.11.

B 18.6 Various types of exercises, which may include participation of Port Facility Security Officers, in conjunction with relevant authorities of Contracting Governments, Company Security Officers, or Ship Security Officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of Company Security Officers or Ship Security Officers in joint exercises should be made, bearing in mind the security and work implications for the ship. These exercises should test communication, coordination, resource availability and response. These exercises may be:

1. full-scale or live;
2. tabletop simulation or seminar; or
3. combined with other exercises held, such as emergency response or other port State authority exercises.

Section B art. 15.11:

Types of security incidents:

1 damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism;
2 hijacking or seizure of the ship or of persons on board;
3 tampering with cargo, essential ship equipment or systems or ship's stores;
4 unauthorised access or use, including presence of stowaways;
5 smuggling weapons or equipment, including weapons of mass destruction;
6 use of the ship to carry those intending to cause a security incident and their equipment;
7 use of the ship itself as a weapon or as a means to cause damage or destruction;
8 blockage of port entrances, locks, approaches, etc.; and
9 nuclear, biological or chemical attack.

Art. 14
Sanctions
Member States shall ensure that effective, proportionate and dissuasive sanctions for breaching the provisions of this Regulation are introduced.

Recommendations

B 16.5 Contracting Governments should approve the PFSPs of the port facilities under their jurisdiction. Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval. The PFSP should make provision for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.

B 18.4 The objective of drills and exercises is to ensure that port facility personnel are proficient in all assigned security duties, at all security levels, and to identify any security-related deficiencies which need to be addressed.

DIRECTIVE 2005/65

The regulation is supplemented by the European Directive. The objective of this Directive is to introduce EU-wide measures for raising port security in relation to the threat of security incidents.

Directive 2005/65 makes it obligatory for port authorities to carry out various types of exercises in order to test the Port Security Plan. These exercises must be held at least once per calendar year, with not more than 18 months between exercises.

(7) Member States should approve Port Security Plans which incorporate the findings of the port security evaluation. The effectiveness of security measures also requires the clear division of tasks between all parties involved as well as regular exercises. This clear division of tasks and the recording of exercise procedures in the format of the Port Security Plan is considered to contribute strongly to the effectiveness of both preventive and remedial port security measures.

Art. 7
Port Security Plan
7. Member States shall ensure that adequate exercises are performed, taking into account the basic security training exercise requirements listed in Annex III.

Art. 17
Penalties
Member States shall ensure that effective, proportionate and dissuasive penalties are introduced for infringements of the national provisions adopted pursuant to this Directive.

Annex II
Port Security Plan
On the basis of these general aspects, the Port Security Plan assigns tasks and specifies work schedules in the following areas:
- training and exercise requirements

Annex III
Basic security training exercise requirements
Various types of training exercises which may involve participation of Port Facility Security Officers, in conjunction with the relevant authorities of Member States, Company Security Officers, or Ship Security Officers, if available, will be carried out at least once each calendar year with no more than 18 months elapsing between the training exercises. Requests for the participation of Company Security Officers or Ship Security Officers in joint training exercises will be made bearing in mind the security and work implications for the ship. These exercises will test communication, coordination, resource availability and response. These exercises may be:
1. full-scale or live;
2. tabletop simulation or seminar; or
3. combined with other exercises held, such as emergency response or other port State authority exercises.

NATIONAL LEGISLATION

Each country has its own specific legislation, with the necessary local restrictions. This national legislative framework must of course be taken into account when carrying out the security exercises.





part 1

THEORY



EXERCISE OF THE PORT SECURITY – REACT AS FORESEEN.

OEFENING VAN DE HAVENVEILIGHEID – HANDEL ZOALS VOORZIEN.

EXERCICE DE LA SECURITE DU PORT – REAGIR COMME PREVU.

Port of Antwerp

PORT SECURITY
HAVENBEDRIJF
SECURITE DU PORT

Theoretical structure makes practical exercises

In life-threatening situations we have to depend on experience, and that can only be acquired by practice. Situations in which normal routines are disturbed quickly lead to mistakes which can have disastrous consequences. Only by constant practice can we properly prepare ourselves for possible attacks and their aftermath. Regular practice is the key to greater security.

Exercises are the best way to keep our know-how and skills up to the proper level and even to improve them. However, an exercise is not a spontaneous occurrence; we have to prepare for it. It also demands expert knowledge in order for the necessary elements in the Security Plan to be included in the exercise, and to decide which steps have to be gone through. When carrying out an exercise great attention must be paid to collaboration and to sharing of information.

Security plans for ports and port facilities are drawn up in accordance with the EU Directive and Regulation. However, the measures laid down in the plan must never be allowed to become set in stone. Plans must be revised as foreseen in the Regulation and Directive. Exercising the procedures and measures laid out in the plan ensures their effectiveness both in a day-to-day routine as well as in a high-tension situation.

The Directive and Regulation also make it compulsory to organise exercises that test the Security Plan. However, they do not prescribe how the exercises should be carried out and evaluated, nor the way in which their quality can be improved.
The why, how and what of maritime drills and exercises will be found in this manual.

THE BASICS

general aspects of exercises: plans, objectives and resources

The core tasks of a Port Facility Security Plan (PFSP) and port security in general are to ensure preventive security against terrorism, and to be ready to respond appropriately if a terrorist act is actually committed.
For this purpose an international framework of intelligence sharing has been set up within the maritime sector, and a minimum of security measures laid down. All aspects of this framework must be tested at set times.
Only in this way can the security organisation be ready to respond. The precondition for this is that everyone must have the required knowledge and resources, together with all the essential, updated information. The best way of testing and maintaining this is by means of exercises.
While carrying out exercises, the flow of information between the various parties (ship, port facility, local and national authorities) can be practised and evaluated.

WHY CARRY OUT EXERCISES?

- **Exercises test security plans, policy and procedures, and enable them to be assessed.**
- **Exercises reveal weaknesses in your Security Plan.**
- **Exercises improve individual performance, and streamline communication and organisation.**
- **Exercises train personnel, and make tasks and responsibilities clear.**
- **Exercises are required by law.**
- **Exercises prepare us for reality.**
- **Exercises heighten our sense of responsibility.**
- **Exercises teach us to accept responsibility.**

1/BACKGROUND

Definitions

DRILL – A drill is a small, coordinated practice that tests at least one part of the Port Facility Security Plan (PFSP). A drill is used to test a procedure or a particular function. It serves to maintain a high level of preparedness.
Small drills concentrating on a single aspect of the plan are important in training specifically for that aspect.

EXERCISE – An exercise is an annual activity involving extensive training in which various aspects of the Port Facility Security Plan or Port Security Plan (PSP) are practised. Communication, coordination, availability, resources and reactions are all rehearsed and tested.
Large-scale exercises are important for training and testing the coordination between the various components of the PFSP and/or PSP.

> Mistakes are an opportunity to learn and do better next time

3 LEVELS OF SECURITY

Security level 1
The level at which the ship, port facility and/or port normally operates.

Security level 2
The level that applies whenever there is a heightened risk, or when a security incident occurs.

Security level 3
The level that applies during the period in which there is a probable or imminent risk of a security incident.

Aim and philosophy of exercises

The aims and methodology of an exercise are more important than the scenario that it is meant to represent. This means an exercise is drawn up on the basis of the objectives laid down for it, not on the basis of the scenario. In other words, first the objectives, then the scenario.

One way of formulating objectives is to hold a meeting of various people in positions of authority within your organisation, in order to gather their opinions. The objectives can help to determine the type of exercise and the scenario.

Exercising people

The most important aspect of any exercise is to keep skills and know-how up to date, and to improve them. Particular operations have to be regularly repeated, so that people with security responsibilities acquire the necessary skills and keep them up to the proper level. Exercises can also be used to test out new work procedures and so to further expand skills.
People can be exercised in two ways: through an evaluation (i.e. by assessing the tasks carried out by them) or through training (i.e. teaching people new tasks and coaching them).

Practicing procedures

Practicing procedures enables weaknesses in the security system to be identified. It also tests whether the procedures are workable and effective at the three security levels.

Types of exercise objectives

In general terms we distinguish three types of objectives:

1. Main objective
   Example: testing the general communication and alarms within the facility

2. Specific objectives
   Example: specific tests for security personnel or the Assistant PFSO

3. Indirect objectives
   Example: enabling participants to gain knowledge, experience and self-confidence

IT IS IMPOSSIBLE TO PRACTICE EVERYTHING IN ONE EXERCISE. THE OBJECTIVES MUST THEREFORE BE PROPERLY DEFINED BEFOREHAND.

The characteristics of an exercise

The objectives must be **SMART**: Specific, Measurable, Acceptable, Realistic and Time-bound.

Specific: the objective must be clear and unambiguous.
Measurable: there must be a clear definition of what has to be achieved or done, and whether it has been done in the proper way, so that the success or failure can be measured. However, this can be difficult for some exercises.
Acceptable: the objectives must be acceptable to everyone.
Realistic: the objectives must be attainable.
Time-bound: it must be possible to attain the objective by the end of the exercise. However, there should be a certain amount of flexibility in the schedule, in order to deal with unexpected situations.

How to draw up the objectives

1. Define key objectives
2. Examine which objectives can be attained
3. Select only objectives that are mutually compatible
4. Set objectives that are realistic for your organisation
5. Don't be too ambitious
6. Spread the objectives over a reasonably long schedule
7. Allow for weaknesses that have been found in the past

The objectives described in the scenarios in this manual can always be adapted by the person leading the exercise (Port Facility Security Officer or Port Security Officer).

The advantages of an exercise

Simulating a threat enables people to gain experience in dealing with unfamiliar situations. This can reveal aspects of an organisation's operations that could be improved. These can then be specifically practiced.
Exercises also form a reality check for the system: they make it easier to identify weak points in the organisation.

ESA – equivalent security arrangements

Port facilities with "equivalent security arrangements" are e.g. port facilities that receive calls by fewer than 10 seagoing ships per year, or seasonal facilities, as decided by the government that is party to the Treaty ("the Contracting Government").
For such facilities it may be agreed that (for example) they only need to organise an exercise whenever there is a seagoing ship in the port. If there has not been a port call by a seagoing ship for a full three months, this is noted on the exercise form at the end of the quarter.

Reg. 725/2004 Regulation 12 - Equivalent security arrangements.

When implementing this chapter and part A of the ISPS Code, a Contracting Government may allow a particular port facility or a group of port facilities located within its territory, other than those covered by an agreement concluded under regulation 11, to implement security measures equivalent to those prescribed in this chapter or in Part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Contracting Government, which allows such security measures, shall communicate to the Organisation particulars thereof.

RESTRICTIONS

The same exercise should not be carried out twice in the same calendar year.
However, inspections by the EU or by competent authorities are not counted as exercises.
Similarly, revising and modifying the Port Facility Security Plan is a separate task of the Port Facility Security Officer and so is not an exercise.
Port facilities in the same group located at different sites have to carry out separate exercises for each site.

BEWARE OF PRACTICING THE WRONG WAY!

In some exercises, a change in the order of steps or missing out one or more steps can result in incorrect patterns of behaviour being learned.
This may happen e.g. with an exercise such as an evacuation for which people are not prepared and which is incorrectly carried out: people train the wrong behaviour or attitude.
IT IS MORE DIFFICULT TO GET RID OF BAD HABITS OR TO CORRECT FAULTY PROCEDURES THAN IT IS TO LEARN A NEW PROCEDURE.
So, get it right the first time!

Experience with exercises in the port of Antwerp

Most port companies do not have a culture of security and exercises, unlike petrochemical (Seveso) companies or ships. Until recently they were frequently vague about how to set up an exercise. They were also worried about the negative impact that exercises might have on their commercial activities. A survey by the responsible departments of Antwerp Port Authority also revealed that while the facilities in fact did carry out exercises they did not report them.

Nevertheless, exercise reporting is compulsory in Belgium. The local committee on maritime security has set the objective of 100% of exercises being reported. So far the task of encouraging port facilities to comply with this reporting obligation has always been done through consultation, without threats and without penalties having to be imposed.

The following resources and methods have been used by the local committee:
- Provided general info to the PFSOs with tips about the quarterly exercises.
- Keeping the agenda and reminding PFSOs by mail or telephone.
- The topic "drills & exercises" is an integral part of an inspection.
- The local committee has drawn up a syllabus describing the possible exercises for each part of the security plan.
- Drills & exercises are a frequent subject during meetings of local working groups (such as: port security think tank).
- Drills & exercises are a fixed subject during the annual information session for PFSOs.
- Facilities having difficulty in fulfilling their obligation were targetted and actively assisted.
- The local committee participates actively in the preparation and the execution of the drills and exercises whenever asked by the facility.

After receipt of the reports, the quality of the exercise is examined and graded as one of the following:
- Positive
- With recommendations
- Not acceptable or not relevant to the ISPS

The description of the exercises and their evaluation give a rough indication of the degree to which the principles used can be carried out in practice.

2/BEFORE THE EXERCISE

Be real

You have to make the exercise as realistic as possible. It has to be an exercise, not a "demonstration." The people taking part should therefore keep to what would actually be available when it comes to resources and manpower.

There is a great temptation – especially for large-scale exercises with outside attention focused on them – to double the manning levels and to order extra equipment beforehand or transfer it from other locations.
If you give in to this temptation you will miss the point of the exercise. The intention is not for everything to go perfectly. If you don't make any mistakes, you won't learn anything!

Exercise schedule

Draw up a schedule of exercises. That way you'll avoid forgetting an exercise or letting it slip by. A quarter passes quickly, and work schedules are soon full!
An exercise schedule enables everyone to make themselves available at the right time.

The quarters are defined as follows:
- Quarter 1: January – March
- Quarter 2: April – June
- Quarter 3: July – September
- Quarter 4: October – December

Time line

Each exercise has a time line specifying the planned events and where and when the necessary equipment has to be available.
It is possible to draw up a dual time line: one real and one fictitious. This makes it possible for e.g. a scenario that would unfold over three days in real time to be completed in one day.

You have to be fairly flexible in following the time line, in order to deal with unexpected situations. For example, you may call "time out" in order to correct a wrong situation or fill a shortage that is found in the course of the exercise. In this way you can avoid having to wait for the next exercise in order to deal with the situation.

It must be clear to everyone when the exercise begins and ends.
Make clear agreements with the participants about the start and end of the exercise.

GIVE PARTICIPANTS THE TIME TO PRACTICE

ADDITIONAL TIPS

- You can exercise for a new system while the old one is still operational. In this way there does not have to be a gap in the exercises or in production.
- You can deliberately give different information to two departments, in order to see how long it takes them to notice the differences.
- Start with small-scale exercises and progress to larger ones as experience is gained.

> **Practice creates routine through repetition**

Graphic and other resources

Make sure the participants are kept constantly up to date throughout the course of the exercise. Keep them constantly informed, and use a clear text for the description of the scenario.

Make the exercise interesting for all participants. There are various ways of involving everyone in your security organisation and putting them to work. Give them exercising materials that encourage them to keep practicing.

This can be done using:
- PowerPoint presentations to describe the scenario
- Photographs to help them visualise the situation
- Flash cards with additional events to feed into the exercise
- Maps showing the evacuation routes and areas (specifying the way in/way out, or setting the perimeters).
  Use www.googlemaps.com, www.msn.com (maps)
- Media simulations. For example, set up a blog with video messages, or a twitter feed. This enables you to judge reactions within the organisation.
  Use www.yammer.com to create a simulation.

Communication and discretion

Communication is a crucial part of any security organisation or plan, and so is also essential to any exercise.
Who communicates with whom, about what, and how? Particular attention must be paid to this in exercises, with clear agreements being made beforehand.

The exercise director determines who has to be notified about the planned exercise. Information about the scenario is on a strict "need to know" basis. Players should not have any advance knowledge of the scenario.

However with major exercises, if notifying or calling the emergency services forms part of the scenario, it is necessary to communicate the exact date and time to the coordinator of the emergency centre that takes emergency calls.

Precautionary measures

Neighbouring companies and people living in the vicinity must be informed if it is a large-scale exercise that may have an external impact. The appropriate communication channels should be used for this. Bystanders on the site should be informed immediately and if necessary asked to leave.

Safety regulations

It is essential for all announcements to mention that it is an exercise, so as to avoid any misunderstanding.
It is a good idea to have the contact details of the exercise director, organisers and participants to hand during the exercise, so that they can intervene whenever necessary.
Code words or abbreviations that have been agreed in advance can be used in communication, but keep to the known jargon.
If the situation becomes unsafe, then call off the exercise.

> **Practice breeds alertness**

CODE WORDS

STRIKE
One of the participants is no longer able to act further. For example, if someone feels unwell or is actually injured, then this is made known with the code word strike.

LOCK OUT
If the exercise director or one of the observers decides for safety reasons that a participant should no longer continue acting, this is made known with the code word lock-out.

NO PLAY NO PLAY NO PLAY
If one of the emergency services is no longer available, for example because it is called out for a real emergency, this is made known with the code word noplay-noplay-noplay.

Checklist

- Meeting room
- Phones
- Fax
- Computer with internet connection
- Printer
- Extension cable
- Digital maps or street directory
- Spare maps, documents and equipment
- Whiteboard & markers
- Paper
- Ball-point pens
- Notification lists
- Presence lists
- Plans & procedures
  (USB stick with recent update)
- Lighting
- Soft drinks, coffee or other catering

HELP WITH SETTING UP AN EXERCISE

THE DEMING CIRCLE OR PDCA CYCLE

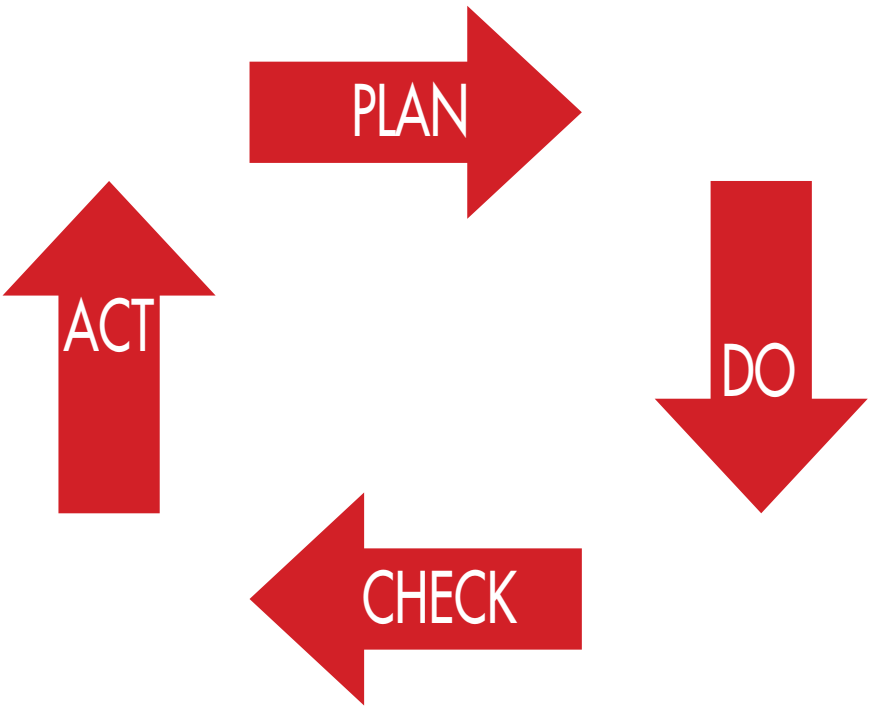
The "Deming quality circle" developed by William Edwards Deming describes four activities that must be applied successively when organising an exercise. This continuous, cyclic process also illustrates the constant striving for quality by an organisation.

- **PLAN:** draw up a plan and define the objectives of the exercise.
- **DO:** carry out the plan (exercise).
- **CHECK:** verify how the plan (the exercise) was carried out, and assess the efforts and results on the basis of the pre-defined objectives.
- **ACT**: modify the procedures if the results are not satisfactory and/or adopt the procedures that have led to good results.

Organising and carrying out an exercise is part of a process of continuous improvement.

Observations are recorded and conclusions are subsequently drawn from them. In this way concrete improvements are made, so as to prevent the errors or omissions re-occurring in a subsequent exercise (or worse, a real incident).

A correction can be very simple, such as updating a telephone number. However, it can also be radical, such as revising a procedure that turns out to be unworkable in practice, so that the PFSP/PSP in turn has to be revised. This can also lead to modified exercises being organised, or new equipment being purchased.



3/DURING THE EXERCISE

Organising and holding a major exercise

When organising a large-scale or tabletop exercise it is recommended to first draw up a scenario. This describes in practical terms how the exercise is organised and how it unfolds. It serves as a guide throughout the process of the exercise.

A scenario contains the following elements:

- The name of the organisation
- The name of the exercise
- Participants
  When drawing up the basic scenario it is necessary to consider who the possible participants are. It is also possible to invite participants who at first sight are not involved but who can nevertheless contribute added value. The organisation is responsible for this.
- Objectives
  It is impossible to practice everything in one exercise. It is therefore important to specify the aims of the exercise beforehand. These objectives are made known to everyone, so that all the participants are aware of them. The exercise marshals play an important role in achieving the objectives, and make adjustments to them where necessary.
- The scenario
  The various events are listed in the form of a time line. However, the time line has to be flexible, in order to allow for unforeseen circumstances. It is also possible to make a distinction between exercise time and real time. The simplest approach is to draw up a realistic scenario, but a tabletop approach affords the possibility to make the scenario wider and more complex.
- Information about the exercise
  - Date
  - Place
  - Start time
  - End time
  - Debriefing: place and date
- Preparation and practical aspects
  - The exercise director
  - The participants
  - Observers (if any)
  - Find a suitable location
  - Make the exercise known
  - Necessary resources/equipment
- Remarks and questions

The exercise can then start, following the scenario.
The progress of the exercise is as follows:

Start of the exercise:

The exercise starts with a clear description of the incident. An internal incident can be specified, but it is also possible to have an external incident in which the company is also involved (for example, a gas leak in a nearby pipeline).

Various examples of scenarios that can be developed in greater detail as a tabletop exercise can also be found

Annual exercises 3,6, 7 and 10 are (partly) "table top" exercises. Other drills and exercises in this manual may be converted to a (partly) table top.

During the exercise, the participants may be provided with additional information in order to achieve the objectives which have been set out. Photographs, geographic plans or powerpoint presentations can be used to make the situation more realistic.

Achieving the objectives

If the objectives are reached, or if the exercise goes according to plan, the exercise marshals bring it to an end.

Debriefing and evaluation

A debriefing is held immediately after the exercise, with evaluations being made by each participant. You want to find out: what is the situation? What are the dilemmas? What are the positive and negative points of the chosen approach? The results of the debriefing are included in the more detailed evaluation.
If debriefing forms filled in by participants and/or participants are used, then these should be combined into a summary in the period between the exercise and the evaluation. This in turn is distilled into an action report that is presented at the subsequent evaluation meeting.
The points for action are further developed and put into practice.

Examples of points for evaluation:
- Was the incident correctly assessed?
- Were the correct resources used?
- Were all the necessary external services contacted?
- Were all the necessary internal services contacted?
- Were tasks properly divided?
- How was the collaboration?
- Did the participants contribute the correct information?
- What are the consequences of the decisions that were taken?
- Do you know your own job and the tasks of others?
- Was the stress kept under control?
- Are the decisions that were taken clear to everyone?
- Was sufficient information asked and obtained?
- Were the correct priorities set?
- Were the right security measures taken?


RESTRICTED AREA
STOP
PORT FACILITY UNDER REGULATION (EC) n° 725/2004 ON ENHANCING SHIP AND PORT FACILITY SECURITY
IN THE INTERESTS OF PUBLIC SAFETY AND SECURITY :
- Access can only be authorized on verification of the AlfaPass or a full registration at security lodge
- Admittance will be denied to all unauthorized persons and vehicles
- All areas of this Port Facility are under continuous Closed Circuit Television Control - CCTV
Entry into this area without authorisation is a violation of security regulations and will be reported to the Federal Committee for the Protection of Port Facilities – FCBH.
IN CASE OF ABSENCE OR EMERGENCY PLEASE CONTACT
' NAME COMPANY ' SECURITY SERVICES :
TELEPHONE : +32 ...
GIVE PRIORITY TO TERMINAL VEHICLES !
KEEP OUT
NOTICE
NOTICE
NOTICE
CAUTION WEAR SAFETY EQUIPMENT
SPEED LIMIT 30

4/AFTER THE EXERCISE

Evaluation

An exercise is an opportunity to learn, and this must be encouraged. It should have a positive impact. An evaluation with positive reinforcement is a valuable instrument to this. Evaluation is not a witch-hunt for guilty persons. Criticism should be aimed at deeds and actions, never at people.

EVALUATION IS A TOOL FOR IMPROVEMENT, NOT A WITCH-HUNT

The evaluation is carried out after the exercise. If there are several evaluation forms, then a summary is drawn up to as to give an overall picture for each department or discipline. On the basis of the evaluation, a list is drawn up with positive points and points for improvement. On the basis of the latter, recommendations are made.
This can be included in a summary table with points for improvement, current projects and projects to be planned. The final result is an action plan.

Assessing an annual exercise

If the exercise is a large one in which various parties are involved, a "Lessons learned" is drawn up not only for the participants but also for the exercise director/marshals.
A large exercise demands more preparation than an intermediate drill. The best way to go about it is in three steps:

1/ **Dry run:** before the exercise is carried out, each person gives his or her input, and the possible consequences are discussed.

2/ **Hot wash up:** immediately after the exercise the exercise marshals can get together and discuss a couple of positive and a couple of negative points, as an initial debriefing.

3/ **General debriefing:** all the comments from the exercise marshals and participants are gathered together and discussed at a general debriefing three weeks or so after the exercise.

> **Evaluation is essential if you want to learn from an exercise**

THE KIRKPATRICK EVALUATION MODEL

In the Kirkpatrick model, evaluation is done in four steps.

LEVEL 1 – REACTION:
the reactions of the participants immediately after the exercise.

LEVEL 2 – LEARNING:
what have the participants learned from the exercise?

LEVEL 3 – BEHAVIOUR:
do the participants adapt their behaviour to what has been learned from the exercise?

LEVEL 4 – RESULT:
is there a difference noticeable in the work of the participants?

Documenting and reporting

We refer in this connection to Reg. 725/2004 Article 9 – Implementation and conformity checking.

- Member States shall carry out the administrative and control tasks required pursuant to the provisions of the special measures to enhance maritime security of the SOLAS Convention and of the ISPS Code. They shall ensure that all necessary means are allocated and effectively provided for the implementation of the provisions of this Regulation.

- Member States shall designate a focal point for maritime security by 1 July 2004

- Each Member State shall adopt a national programme for the implementation of this Regulation.

The Member States and inspectors from the European Commission check the ISPS facilities for compliance with the Regulation.
Carrying out quarterly and annual exercises is obligatory in order to assure that the provisions of the Security Plan are actually implemented. For the inspection, the exercise must be documented in order to be able to show that it was carried in conformity.

In Belgium, for instance, the national authority for maritime security has drawn up a procedure for ISPS facilities within its territory. This procedure includes a standard form which asks for a description of the exercise and the points for

action. It also lays down a procedure for the completed reports to be sent to the chairman of the local committees for maritime security or the PSO. The form also allows for feedback concerning the exercise, so that the local authority can give recommendations to the port facility.

In this way the national authority for maritime security assures checking of the conformity with the Regulation, at least as regards the "exercise" part, while the port facilities for their part assure that they meet their responsibilities in this regard.

For the purpose of reporting on exercises, the form contains at least the following elements:

- Facility and PFSO
- Date, time and location
- Level of security
- Quarterly or annual exercise
- Description of the exercise
- Participants
- Evaluation and points for action
- Feedback from the competent authority

The report should contain a brief summary, with the detailed information on the exercise being attached.
DON'T FORGET TO KEEP A LIST OF PARTICIPANTS.
For example, checklists that have to be signed by people attending can be kept.

It is possible to work with a standard document for all port facilities (perhaps based on the recommendations of the competent authority) so that the whole port follow a uniform procedure.

Based on the forms, the competent authority is able to keep an overall situation summary with a number of reports on exercises carried out by port facilities on its territory. This can help it to remind port facilities that have not yet submitted a report.

Feasibility of procedures and measures

It is essential to ask the following questions: are the procedures and measures feasible in practice?
Are they effective?

It is up to the competent authorities to check that the Regulation is applied. The facilities in turn are answerable to the competent authorities, submitting their reports to them. These reports describe:

- The content of the exercise that has been carried out = the obligatory exercises give an indication of the feasibility
- The regularity of the exercises carried out = compliance with the Regulation

The exercise reporting is both a quantitative and a qualitative indicator.

Practicing at exercising

Exercises form part of an exercise policy. The next step in developing this exercise policy is to concentrate on improving the quality of the exercises. This implies systematically looking into formulating the exercise objectives, policy provisions, planning, organisation, involving members of personnel and process control (by means of evaluation and feedback), and how this all leads to achieving the set objective.

As objectives are achieved and new ones are made more and more demanding, the participating organisations will improve; they will become "learning organisations" that constantly strive for improvement, defining all the relevant information, experience and lessons learned. In this way new decisions can be taken on the basis of what has been learned from the past.

Improving yourself by means of quality control

The European Interreg IIIC AWARE project (completed in 2007) has set up various project groups including the "Quality" workgroup. This workgroup drew up a questionnaire for use in carrying out audits of exercises and disasters. This very comprehensive questionnaire goes through the exercise process step by step, looking successively at the preparation, attendance by participants, the start of the exercise, the decision-making, the information provided beforehand and the measures taken afterwards.
The results of the questionnaire can be used to improve the quality of the exercise.

The questionnaire is attached to this manual as a tool in part 3 entitled **Audit Questionnaire**. The list is adapted specifically for use in maritime port security exercises.


SECURITY
LEVEL
1



TYPOLOGY 1
types of exercise

Various types of exercise can be distinguished, according to the participants, the objectives or the purpose.

A general distinction is between mono-disciplinary and multi-disciplinary exercises.

Mono-disciplinary exercises

In a mono-disciplinary exercise, a single discipline practices one or more parts of the tasks assigned to it.

\+
Such exercises are attractive, since you can set the objectives yourself, you can make adjustments to the exercise, and it demands only short preparation.

\-
The weakness of such exercises is that they only cover your own discipline, and do not test communication between different departments or services.

Multi-disciplinary exercises

In a multi-disciplinary exercise, several disciplines practice one or more parts of the tasks assigned to them. The emphasis is on collaboration between them. The exercise can be both operational and managerial.

\+
The strength of such exercises is that interaction is promoted and measured, and that gaps in the security or emergency plans are discovered sooner.

\-
The weakness is that they demand more preparation and are more expensive.

Exercises can be further broken down according to the activities that they are meant to practice.

Alarm exercises
Communication exercises

In these exercises the notification and alarm procedures in the PFSP, PSP and emergency plans are tested and trained. The communication data and lines are tested, as are the availability and speed of reaction of key persons.
This exercise can be carried out at the level of a company or at the level that includes emergency services, with the collaboration of the latter.
In an alarm exercise the actual equipment should also be tested, such as the sirens.

\+
This exercise demands minimum personnel, time and cost. Communication is always a difficulty, both during real incidents and during exercises. It is therefore useful to practice the communication lines regularly.

\-
This exercise covers only a limited (but not unimportant) part of the plan.

Virtual exercises

There are virtual reality simulation programmes available, as a support for training and exercises. A 3D application enables participants to practise in a realistic (yet safe) environment.
In virtual scenarios a threat is simulated by the computer in a realistic way. One or more participants use a joystick to navigate around the virtual world of a simulated threat or incident, and decide which actions to perform.
The instructor determines the structure of the scenario, and can make changes to the threat or incident in order to take it in a different direction.
Thanks to modern technology such techniques are very realistic.

\+
A virtual exercise is much more dynamic than a sandbox exercise. It can be used to simulate places that are normally inaccessible. They also make it possible to train many people in a relatively short time.

\-
Virtual exercises are more suitable for operational leaders, and are expensive.

Tabletop exercises

Tabletop exercises are used to gain understanding of the tasks, responsibilities and competencies of the various departments or services involved. A group of people carries out an analysis and evaluation of a security threat or emergency situation, in an informal, stress-free environment; there is no real action on the ground.
In such exercises the emphasis is on thinking about the knowledge available and testing it. The various departments concerned study a situation together, and look for a way of dealing with the incident as quickly and appropriately as possible.
Tabletop exercises are intended for examining operational plans so as to identify difficulties and solve underlying problems.

The exercise starts on the basis of a possible threat or incident, and is illustrated by a model, plan or powerpoint presentation. Various persons in positions of authority sit around the table, with the exercise marshals feeding in information and constantly making changes. In this way the participants have to deal with an unfolding series of situations.
An important role is played by the exercise marshals, who direct the sequence of events. The participants for their part need to have good powers of imagination.
Tabletop exercises therefore demand very good preparation and expert knowledge on the part of the exercise marshals.

There are two ways of holding a tabletop exercise.
- Either it can be an exercise in which a scenario is presented and the exercise marshals constantly ask questions.
- Or it can be an exercise in which a scenario is presented and the participants then "play" it by themselves.

In both cases, however, changes to the exercise can only be made by the exercise marshals: they ask the questions, and the teams provide new information. The participants relate the steps/decisions taken by them as part of the exercise.

+
An advantage of this type of exercise is that there are few practical limitations: almost any scenario can be played out. It is also inexpensive, as well as being independent of weather conditions.
The team has to take the challenge seriously, and the importance of preparation and practice are made obvious. On the other hand a great deal of input is required in order for the tabletop exercise to be successful.

–
Not all aspects can be tested; there are no operations on the ground, and there is little interaction. A great deal of imagination is required from participants.

Exercises on the ground: CPX and FTX

An exercise on the ground offers a high degree of realism. The difference between a limited and a general exercise on the ground is the number of participants. This type of exercise tests the different objectives of all departments, disciplines and authorities.

On the basis of a predetermined scenario, the threat or incident is escalated to the point where the competent authority takes over the coordination. At this point the authority's crisis committee is activated.
An example of an exercise on the ground is a large-scale evacuation exercise, with all emergency services and the press also being involved.

Limited scale exercise
CPX Command Post Exercise
Without involving personnel on the ground:
management exercise

This is a fully simulated, interactive exercise that tests the ability of the organisation to react to a simulated event.
It focuses on the coordination of several functions or organisations.
This exercise strives for realism, and aims to assess the actual use of equipment and personnel.

+
The exercise is relatively simple to organise.

–
It is a limited exercise. Furthermore, because the people are frequently busy at other jobs it is sometimes difficult to convince them of the usefulness of holding a management exercise.

FULL SCALE EXERCISE
FTX or Field Training Exercise
With deployment of people on the ground:
operational exercise

The exercise is based on a simulated event, emergency situation or threat, designed to be as close to reality as possible. It involves full commitment of equipment and people concerned with security tasks, together with the external services involved as detailed in the scenario.

+
The exercise tests many aspects, including communication and collaboration. As a result of the exercise the participants get to know one another better, which is very useful in case of an actual threat or escalation.
The exercise is apparent to local residents.

–
It demands a great deal of preparation, is difficult to plan fully (including the budget and the number of people involved), and is very expensive. Holding such exercises too often can lead to "exercise fatigue."

Seminars/info sessions

A seminar serves to provide information and enable people to become acquainted with the organisation, measures and procedures concerning security.

The Port Facility Security Officer can hold an info session for the security organisation and members of personnel within the company, in order to explain the how and why of security. This also raises the security consciousness of everyone in the facility.

See also Part 2 - Practice drill n° 43 and drill n° 44

The competent authority, for instance, can also organise an annual info session for the Port Facility Security Officers, for which participation counts as a quarterly exercise. This is an opportunity for authorities and PFSOs to network and exchange information. It improves the supportive dynamics between authorities and industry.

In fact, info sessions can be held for a very wide range of people, from labour workers to company managers. The presentation should, of course, be tailored to the particular target audience.

Possible subjects include:

- Updates to the Regulation and the Directive during the past year
  - Exercises
  - Incidents
  - Inspections
  - Work points
- Emergency planning
- Local legislation
- Presentations by the authorities
  - Police
  - Customs
  - Port Authority
  - State Security
  - Military command
  - Government crisis centre
- Terrorism
- Awareness
- Security methods
- Security companies
- The impact of a bomb



TYPOLOGY 2
Types of Security Plan

Different types of plans require different types of exercises. But as these plans should be aligned with each other, exercises need to test the consistency of the alignment.

PFSP (Reg. 725/2004)

A Port Facility Security Plan is intended to ensure that measures are taken to protect the port facility, ships, people, freight, freight transport units and ship's stores against the dangers of a security incident.

SSP (Reg. 725/2004)

A Ship Security Plan describes the security measures on board a ship to protect passengers and crew, freight, freight transport units, ship's stores and the ship itself against the threat of a security incident.

PSP (Dir. 2005/65)

A Port Security Plan deals with the security of the port and/or specific parts of the port.
The Port Security Plan should take account of, or refer to, the PFSP of the facilities within the port area.

Internal emergency plan (safety)

Reg. 725/2004 A.16.3
Such a plan shall be developed taking into account the guidance given in part B of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

5. Procedures for evacuation in case of security threats or breaches of security.

The internal emergency plan contains evacuation procedures which may be referred to in the PFSP. It is drawn up at the level of the facility. Its aim is to ensure the most appropriate possible reaction to an emergency situation; the situation may internal within the facility, or it may be external if the situation has consequences for the safety of the facility.
The internal emergency plan covers a number of organisational measures that are to be taken internally, either to meet the greatest possible risk or a specific risk. The internal emergency plan also provides for alarming procedures, notifying emergency services (fire brigade, health care, ...). The plan also contains arrangements for escorting these services on the site.
Consultation with the emergency services during the compilation of the plan provides for practical procedures and arrangements.
In the case of petrochemical and nuclear sites, internal emergency plans are required by law; for other ISPS facilities it is sufficient to have an alarm and evacuation procedure.
Internal emergency plans must coordinate perfectly with the PFSP, PSP and with eventual government's contingency planning.

TESTING THE CONNECTIONS BETWEEN THE DIFFERENT PLANS IS A GOOD SUBJECT FOR EXERCISES.

PARTICIPANTS

Who takes part in the exercise?

Exercise director

The exercise director is someone with powers of oversight, who sees the big picture.

Marshals

For large-scale exercises, a marshal is appointed for each participating discipline or part of the organisation, ideally the marshals were member of the scenario team as described further.
The main task of the marshals is to keep an eye on the time schedule: they ensure that everything keeps to schedule. If an operation or procedure is missed out, they make adjustments to the exercise.

Observers

The job of the observers is to judge whether the objectives of the exercise have been attained. These people play an important role in the evaluation, as they note the good and bad points.They don't evaluate the exercise as such; rather, they act as the "eyes and ears" of the exercise director, to whom they will report.
Observers must have the necessary technical expertise. They must also be aware of the exercise objectives and the relevant evaluation criteria. Observers must be able to form an objective judgement. It is also useful to give observers specific tasks, such as assessing a particular part of the exercise.

Roll players/simulants

These people can be deployed to make parts of the exercise more realistic. However, it is essential to assure their safety. Especially since roll players are most probably volunteer who are not familiar with the exercise surroundings.

Press/media

If the press is present at (or simulated in) the exercise, a communication officer has to be appointed. The press should certainly not be given complete freedom: they must always be briefed, and must be accompanied. They should be given a press folder. They may take photographs and hold interviews, provided there is permission from the organisation. It is advisable to make members of the press easily identifiable, in order to prevent misunderstandings. It is also important to make a distinction between members of the press taking part in the exercise and those who come along to report.

Communications officer

This is the person appointed to deal with the press. Other participants must be told to refer all questions to this person.
Remember that as soon as the press is involved, news of any incident soon becomes public and spreads very quickly, e.g. via the internet and social media.

Logistics support personnel

All the people responsible for radio communication, documents, invitations, evaluation forms, exercise rules, catering, high-vis jackets, meeting rooms, car parks etc.

Port facility security officer

The person responsible for development, implementation, review and maintenance of the Port Facility Security Plan. He or she also maintains contacts with the ship security officer and the Company Security Officer of the shipping company.

Security guards

Port facilities may use subcontracted security guards to carry out tasks as described in the PFSP (for example: access control, supervising the facility). As such they belong to the port facility security organisation.

Personnel with security tasks

Certain security tasks will be carried out by port facility personnel, thus forming part of the security organisation of the port facility (for example: supervising cargo).

Reception personnel

Personnel who meet visitors at the entrance to the facility (security personnel or own personnel). They provide access to the facility, and therefore are part of the security organisation of the port facility.

Facility personnel

Other members of personnel of the facility who do not have security responsibilities.

Technical department

Port facility personnel (own personnel or subcontractors) responsible for tasks such as maintenance of equipment.

SSO

A person on board a ship, answering to the master, appointed by the company as being responsible for the security of the ship, including implementation and maintenance of the ship's Security Plan, who also stays in contact with the Company Security Officer and the Port Facility Security Officer.

CSO

A person appointed by the shipping company, responsible for assessing the ship security and the ship Security Plan (which must be submitted for approval and then implemented and maintained); he or she also keeps in contact with the Port Facility Security Officer and the Ship Security Officer.

Ships' suppliers

Specialised companies providing equipment and stores to the ships in port.

Visitors

Visitors may be for the port facility or the ship. (For example: truck drivers, ship's agent, social services, subcontractors,...)

Competent authority (local/national)

This refers to the organisation(s) or administrative body/bodies appointed by the Contracting Government (Regulation 725/2004) as being responsible for implementing the provisions of the Regulation with regard to the security of port facilities, ship/port interfaces and ports.
The port security authority is responsible for security matters in a particular port (Directive 2005/65).

Authorities and emergency services include:

- Police
- Fire brigade
- Medical services
- Military command
- Customs

When emergency services take part in large-scale exercises, they should not be blue light driving (since it is only an exercise). If this results in unrealistic transfer times, they can be asked to wait at an agreed place until their expected arrival time.

Making participants conspicuous

For the sake of safety, all participants must be clearly recognisable during an exercise. One practical way of doing this, is providing high-visibility jackets in different colours identifying the particular tasks.

COLLABORATION

Security and security exercises are joint efforts.

Teamwork from the various involved organisations is essential for achieving good port and port facility security.

Exercising improves professionalism and refines existing procedures. In reality, the greater the threat the more organisations are involved in the security measures, and the more collaboration is required between them.

Within the port facility

Within the port facility, exercises can be held on the operational level and on the management level.
A combination of both has the great advantage that security gaps are recognised throughout all levels of the organisation, thus receiving wide support for improvement.
Whenever a ship (as described in Reg. 725/2004) is alongside, it is good practise to invite the SSO to be involved with the exercise.

**SEE PART 2 - PRACTICE:
DRILL 10, DRILL 11, DRILL 32,
DRILL 38, DRILL 39, DRILL 40**

Exercises with neighbouring port facilities

Joint exercises with neighbouring port facilities (as defined in Reg. 725/2004), and preferably involving local authorities, improves coordinating skills of all parties.

Authorities

Seminars or information sessions can be organised by the competent authority, in order to improve relations between the authority and the companies.
Companies in turn can strengthen relations with the authorities by inviting them to attend exercises.

> **The safety of participants must never be endangered**

ORGANISING
a port security exercise

EU Directive 2005/65 EC

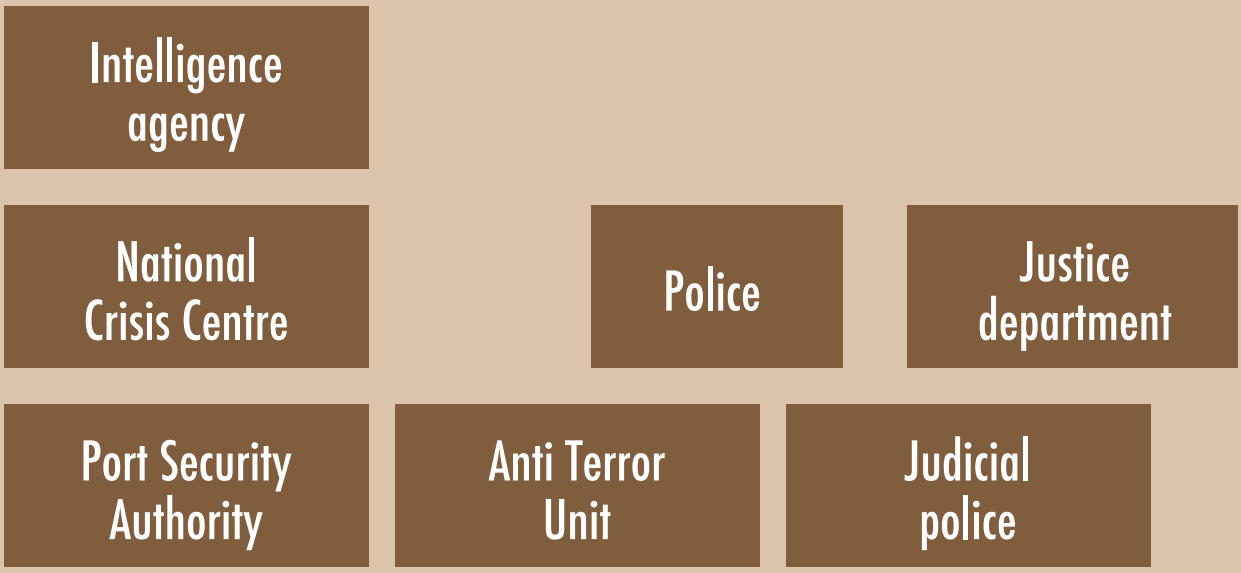
INTRODUCTION

EU Directive 2005/65 EC specifies that the authorities responsible for port security must organise an exercise at least once every calendar year, with not more than 18 months between exercises.
A port security exercise requires considerably more effort and especially more preparation than an ISPS exercise, because it requires the coordination of various services and disciplines.

The Port Security Plan defines the procedures and measures taken to ensure a heightened level of security against terrorism (among other threats). In case of a heightened threat the local authority will be given the necessary instructions by the national authority. It is quite possible that the alarm will also be raised with other authorities (police, Ministry of Justice etc.) whom will initiate their own procedures.

It is therefore very important to review your own security organisation, and it is also useful for you to know all the other stakeholders.
Dialogue with the other stakeholders can lead to collaborative arrangements for setting up exercises, ultimately creating added value for the exercise, and above all better security for the port.

EXAMPLE (FICTIONAL)



The exercise is organised by the "Port Security Authority". The PSA can opt for a minimalistic approach and only test its own procedures, or it can also seek to obtain input from higher authorities, which in turn raise the alarm with other bodies. The latter can also be involved, testing their own procedures on the basis of a joint scenario. Based on the results of the evaluation, this can lead to improved coordination among all stakeholders, and ultimately better security for the port.

> It is very important that non-participating authorities are duly informed about the exercise.
> This avoids situations where a communication during the exercise may lead to confusion or even or to the idea that a real incident is acutally happening.

HOW TO ORGANISE A PORT SECURITY EXERCISE

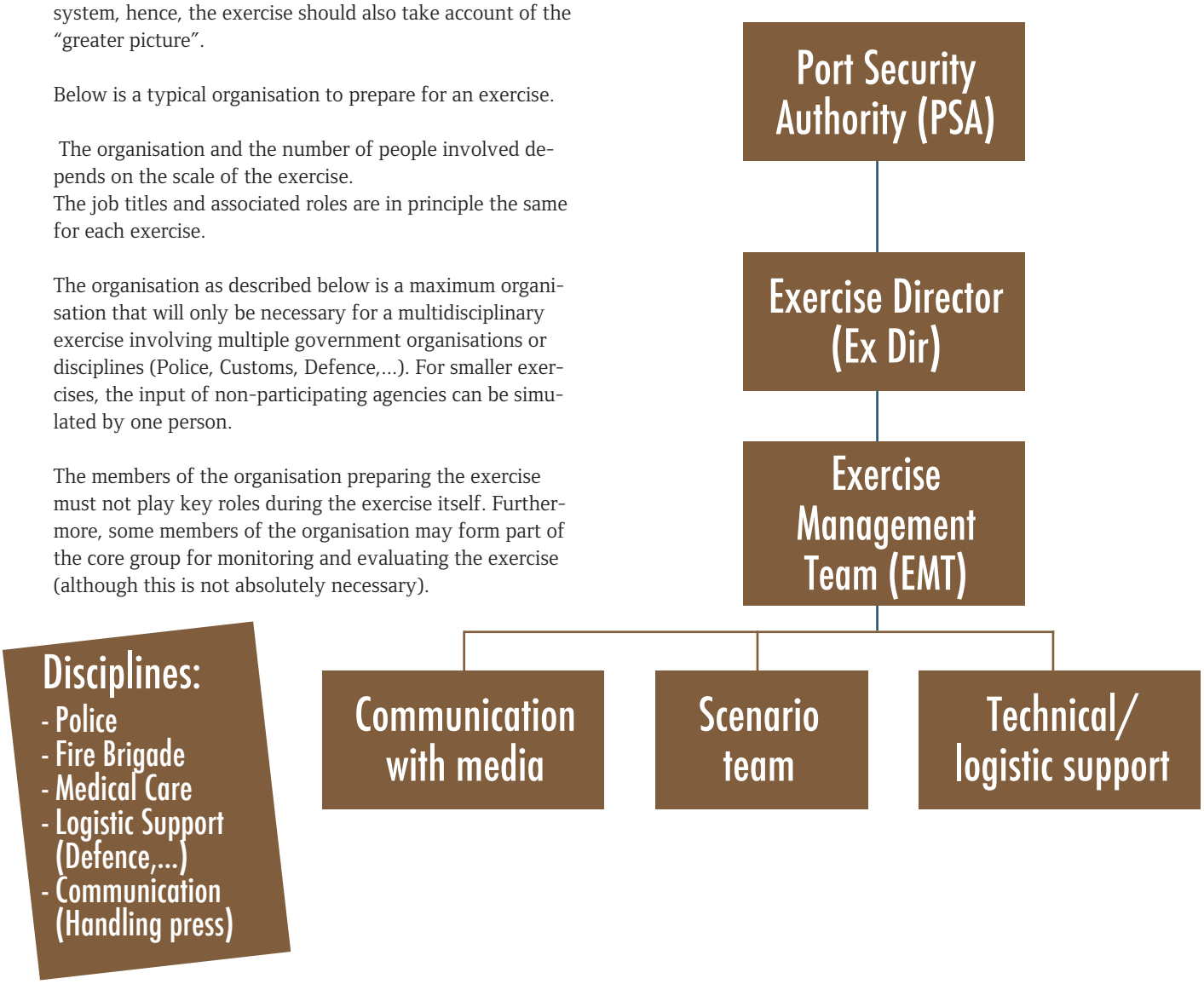
The port security authority fits into a national security system, hence, the exercise should also take account of the "greater picture".

Below is a typical organisation to prepare for an exercise.

The organisation and the number of people involved depends on the scale of the exercise.
The job titles and associated roles are in principle the same for each exercise.

The organisation as described below is a maximum organisation that will only be necessary for a multidisciplinary exercise involving multiple government organisations or disciplines (Police, Customs, Defence,...). For smaller exercises, the input of non-participating agencies can be simulated by one person.

The members of the organisation preparing the exercise must not play key roles during the exercise itself. Furthermore, some members of the organisation may form part of the core group for monitoring and evaluating the exercise (although this is not absolutely necessary).



Port Security Authority

It is up to the Port Security Authority (PSA) to reach a consensus about the type, scale and general themes of the exercise, and to mobilise the necessary resources both for the preparation and for the actual exercise.

It is the task of the PSA to approve the "Exercise Convention." This is a document laying down a clear description of the boundaries of the exercise, together with the commitment expected from each participating organisation/ discipline.

The PSA works in three stages:
1. It defines the scale, resources and general themes for the exercise
2. It approves the Exercise Convention
3. It discusses the conclusions of the exercise

The Exercise Director

The Exercise Director (Ex Dir) ensures that responsibilities are clearly assigned.
He/she ensures that good, clear agreements are made with the non-participating authorities concerning calls and alarms.

The exercise management team

For the purpose of preparation, various people within the participating organisations and disciplines are appointed to draw up the detailed objectives and accompanying scenarios. Participants in the organisation do not take part in the exercise.
On the other hand they are very well placed to act as marshalls.

The exercise management team is responsible for:

- Drawing up the specifications for the exercise.
- Giving the exercise a code name.
- Assigning responsibilities among the organisations that prepare for the exercise.
- Controlling and modifying the scenario to keep it in line with the set objectives and expectations of the exercise.
- Drawing up the Major Event List or MEL (see below).
- Drawing up the criteria for evaluation of the exercise.
- Drawing up the guide for evaluators and observers.
- Drawing up the guide for players.
- Managing the process.
- Approving the presence of observers and spectators.
- The use of roll players/simulants.

The scenario team

Depending on the agreed scale of the exercise, a scenario team is formed. It's good practise to involve a member of each participating discipline. The composition of the team should match the size of the exercise. Ideally team members will become marshalls during the exercise.

One person should take charge. This person must have detailed knowledge of the environment in which the exercise will take place, as well as the applicable procedures and measures. If one or more port facilities are involved in the exercise, it is necessary to know the security procedures of the participating facilities. The team member, contributes input for the scenario, based on their specific role.
However, it is up to the person in charge to coordinate the input, and to ensure that the exercise meets the objectives set by the port security authority.
The scenario team will also provide for the necessary timing, including the data of the exercise.

The support team

The technical and logistical support is the specific support for holding the exercise, not the normal support for the day-to-day functioning of the various disciplines and organisations.
The logistical and/or technical support function is provided by the Ex Dir.
The latter can carry out this task by him/herself, or can delegate it to other persons, depending on the scale of the exercise.
If it is delegated, the logistical and technical preparations are carried out by a team or assigned to an individual member of the support team or a member of the support personnel, depending on the area which the exercise covers.
Logistical and technical preparations include:

- Reserving a meeting room to be used by the full evaluation and observation team for the exercise, and by the evaluators who monitor the exercise.
- Organising the communication resources for the evaluators and observers.
- Providing safety equipment.
- Providing easily recognisable identification for all participants.
- Catering for all participants.
- Arranging suitable transport.
- Producing and distributing copies of the scenario, guidelines etc.

The communication team

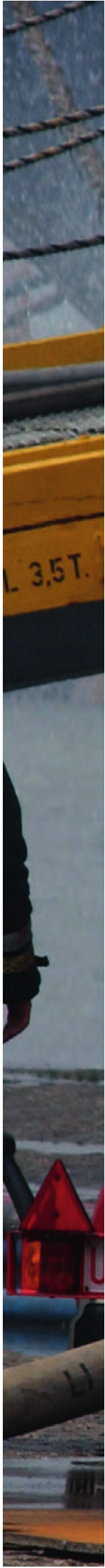
This team is responsible for all relations with the outside world, such as:

- Deciding which strategy to use for dealing with the real media, before and during the exercise.
- Acting as official spokesperson on behalf of the Ex Dir.
- Making preparations for a media simulation unit, if this corresponds to the objectives of the exercise.

This team will usually consist of a communication officer from the port company concerned, together with communication officers from the other disciplines involved. The team may also include media specialists or a real journalist.

CHECKLIST EXERCISE

- **Transport to and from the locations in the port must be arranged. This is particularly important for the team members who have to move around with the players, and for any roll players/simulants used.**
- **The observers/evaluators must have a clear view of everything. Measures must be taken to ensure that they can keep in contact with each other at all times.**
- **Take account of "dead areas" with poor reception or insufficient coverage. Specify the correct radio channels for the players to avoid interference. Before starting the exercise, all observers and evaluators should be given a list with all telephone numbers and/or radio frequencies. These numbers and frequencies must be tested before the exercise begins.**
- **It is necessary to determine who will need special protective equipment (such as safety goggles or helmet) in order to gain access to areas where safety regulations apply.**
- **All evaluators and observers must be identifiable. This can be by means of an armband, badge or coloured jacket.**




rosenbauer
rosenbauer
GIELEN

12 STEPS
to a successful exercise

The consecutive steps required for preparing an exercise and subsequent reporting are described below.
See part 3 - Tools: Schematic list.
During this process the documentation for the exercise is also built up. Including the joint reports of all meetings, to-do lists and draft versions of documents. Combined with the reports from observers and marshalls and feedback from the "players", this forms the documentation for later analysis.

FIRST THINGS FIRST: THE ROLE OF THE "PORT SECURITY AUTHORITY"

The PSA must reach a consensus on the type, scale and overall themes of the exercise.
The PSA determines the scale of commitment, as regards time, manpower and resources. The PSA is responsible for providing support, including all necessary and appropriate resources. This applies to all aspects of the exercise (including e.g. logistic resources or catering).
The PSA does not play any role in actually working out the exercise. During the preparations the PSA is only involved in approving the Exercise Convention, mainly to ensure that the objectives and commitments of each discipline during the exercise are specified in detail, in practical terms.
After the exercise the action plan drawn up by the exercise management team is submitted to the PSA for approval.

THE FIRST STEPS IN PREPARING THE EXERCISE ARE CRUCIAL FOR A SUCCESSFUL EXERCISE. STEPS 1 TO 3 ARE PRIOR TO DRAWING UP THE SCENARIO.

	What needs to be done?		Who has to do it?
STEP 1	Commitment by the heads of the participating disciplines	PSA determines the type, scale and overall themes of the exercise	PSA
STEP 2	Type, date, duration, deployment on the ground (if any), degree of detail, deviations and limitations	Appoint an Ex Dir and an exercise management team	PSA PSA + Ex Dir
STEP 3	Based on detailed, existing plans	Draw up the objectives for all the departments concerned	EMT Ex Dir

STEP 1:

Define the type and scale of the exercise

The PSA defines **the scale of the exercise**. The preparations for this can already be made at the debriefing of the previous exercise.

Defining the scale of the exercise means:
- Specifying which disciplines will take part in the exercise, and to which degree.
- Specifying the extent of the actions that will be taken during the exercise.

Define the **type of exercise** and **general themes** for the exercise.

Example: "practice the flow of communication between the different stakeholders during a level 2 situation: communication as laid down in the plan."

Define the **time and duration** of the exercise (period: exact date is not necessary).

Define the **scope of collaboration and deployment on the ground** and the **degree of detail** with which the themes will be dealt with.

Example: actual deployment of police services on the perimeters (no/yes); involvement of Customs service (no/yes); use of all communication resources exercised in full detail, etc.

Define the **limitations** and **deviations**, both with regards to the themes to be dealt with and the limitations on the use of resources, as well as to the availability of the different players/actors.

Example: "port facilities not actually involved, so no alarm given to PFSOs." This also includes limitations on the use of people and resources, as well as other practical limitations (e.g. "not during the weekend").

Define (in outline) the **actual media policy**, i.e. the method of dealing with the actual media in the context of the exercise (not what the role of the media will be within the exercise scenario; the two aspects are dealt with separately).

Step 2:

Appoint the Exercise Director and Exercise Management Team

The PSA appoints an exercise director, and consecutively, with participation of the exercise director establishes an exercise management team.
Members of the team belong to the involved disciplines and have the necessary experience.

STEP 3:

Define the overall and detailed objectives

The **objectives of the exercise** must be **formulated in such a way that the expected result is clear**. Concrete, detailed objectives ensure that more lessons can be drawn from the exercise.
The Ex Dir, assisted by the members of the exercise management team, is responsible for drawing up the objectives. Sufficient time must be allowed for this.

Consult all the participating disciplines (within the limitations defined by the port security authority), and allow them to put forward their own objectives. If future players are involved in the consultation, care must be taken not to divulge any information about the scenario.

Consider whether the objectives are attainable: it may happen that objectives are proposed which cannot be included within the type, scale and overall themes as initially determined by the port security authority.

Add objectives demanding coordination among various participants.
The coordination and how the objectives fit together should be discussed with people who have an overall view of the exercise.

One of the purposes of exercising is to discover gaps in the existing procedures, in order to remedy and improve. The objectives must be formulated with this in mind, taking into account the shortcomings found during previous exercises.

The Ex Dir ensures that the detailed objectives are in line with the proposed theme, and that the exercise remains within the scale and resources laid down for it by the PSA. For this purpose it is desirable to have a regular consultation with the members of the PSA.

Already at this stage in the preparations shortcomings may be found and can be taken care of.

When setting objectives there is a temptation to test as many things as possible. Try to avoid this. It is better to test a number of key objectives in detail, and possibly also some objectives that were not attained during the previous exercise.

Having a limited number of objectives makes it easier to draw lessons from the exercise, and the plans for improvement can be kept under better control.

TIPS

- **Select objectives that are compatible with one another**
- **Avoid being too ambitious**
- **Avoid trying to do everything at once**
- **Spread the objectives over several exercises**

Step 4:
Develop a coherent, consistent scenario

Determine who will be part of the scenario team. If port facilities are involved in the port security exercise, input of the PFSO is required. However, the actual players do not take part in drawing up nor in validating the scenario.

First draw up **a general outline or list** of the important and desired events, possible consequences and situations that take into account the various objectives set for the exercise.

The scenario should be built up through dialogue between the **on-site** and **off-site team** (on-site = actions on the ground, including preparatory acts to produce a plausible threat; off-site = crisis centre and management).
The on-site technical scenario should be as realistic as possible and should include a series of events leading to a situation that also enables the off-site part of the exercise to be played.
Discuss the concept of the scenario with specialists in the relevant areas (such as intelligence, law enforcement or Customs). These specialists are not players in the exercise. The details of the scenario should be further refined and events added so as to create situations in which all the objectives of the exercise can be played. Inputs should be prepared to create the threat situation and to keep the players informed about the scenario events during the exercise.

Some examples of inputs:
- Intelligence received from friendly countries
- A series of events at home and abroad
- Suspicious situations in the port (persons making observations or challenging the security, etc.)

The scenario should simulate a real threat as faithfully as possible.

A fully developed scenario contains the following elements:
- The initial situation
- Important events, with a critical time line
- The technical scenario
- The detailed series of events
- The description
- The Major Event List (MEL)
- Input, information and data

In parallel, the media unit formulates the strategy for dealing with the real media, both in the preparation stage and during the exercise.

Step 5:
Develop the simulation data

Except for the fact that they are simulated, the data for the exercise should not be any different from real data. They **provide information** that is used to assess the seriousness or potential impact of the threat. They also **determine which actions must be taken** in order to limit the consequences of the situation.
The types of data required are represented by:
- Messages
- Tables
- Graphics
- Figures or illustrations
- Maps

Step 6:
Draft the Major Event List (MEL)

The MEL is the **list of main events in the scenario**, in chronological order. It is the **most important tool for managing the exercise** and keeping it under control. The list is very extensive, but can be managed in the form of a spreadsheet.

The actions by the various disciplines are listed in full detail:
- scenario events
- inputs
- actions by participating disciplines
- recommendations
- decisions
- consultation and other communication between players
- consultation with simulated workgroups; communication with the outside world (press and other communication).

If working with time windows, the time scale must be very specific. By contrast, for "free play" and exercises with operations in the field it may be better to work with periods. Once the MEL has been worked out, further development of the exercise is relatively simple; the complexity that is typical of setting up a large-scale exercise is relatively under control after this step.

As of this point the various documents are drawn up and the practical/logistical side of the exercise can be tackled:
- Identify all the evaluators and observers by name.
- Start to draw up the guidelines for the evaluators and observers, starting with the evaluation criteria.
- Specify the policy for observers and spectators, and take measures to deal with them.
- Identify logistical requirements and start to make arrangements.
- Arrange transport.
- Arrange for extras or bit players (if any are required).

At this stage, the communication team makes a media action plan:
- Decide on the policy for dealing with the media.
- Prepare a briefing package for the media.
- Decide on the media broadcasts for the real media.
- Draw up guidelines for all participants about how to deal with the media before and during the exercise.

MEL
is for:
- Ex Dir
- Marshalls
- Evaluators
- Observers

EXERCISE CONVENTION
is for:
- players
- evaluators
- observers

Step 7:
Draft the Exercise Convention

The convention must include **all the information about the exercise that the players need to have** in order to prepare them for the exercise. The scenario is **not** revealed (of course!).
This guide for players (known as the "Exercise Convention") contains general information about the exercise, the general objectives of the exercise, which groups are taking part and what is expected of them, the timing of the exercise (and the way it is split up, if applicable), the limitations of the exercise and the way it deviates from a real threat, and all particular arrangements concerning the exercise.

The Exercise Convention additionally contains all information on practical arrangements for the exercise:
- What the objectives of the exercise are.
- Who is expected to take part.
- Whether it is a full play or a table-top consultation, and to what extent actions are actually carried out.
- Which communication channels are used, and which arrangements apply during the exercise
  Example: will normal telephone and fax numbers be used? Clearly mention in all communication "This communication is part of a security exercise. It is not a real threat".
- How participations will know when the exercise starts.
- Who is responsible for each group of participants.
- Which participants are simulated, and how they are contacted.
- Which assumptions apply to the exercise
  Example: weather conditions
- What the particular time windows are, and how they influence the play by the participants.
- Guidelines for dealing with the media.

Other aspects included in the Exercise Convention can be:
- Safety: this section lays down clear guidelines, in order to guarantee safety throughout the exercise. It specifies the responsibility of players to follow the safety procedures, and the obligation to stop the exercise if the safety of the facility or personnel is endangered.
- Logistics: practical arrangements for transport, accommodation and catering.
- The Exercise Convention should not contain information that might impose unnecessary restrictions on the normal operation of the participating entities.

The Exercise Convention is approved by the PSA and is then distributed to the participants in good time before the exercise.

It is therefore necessary that the Ex Dir gives feedback during the preparation process to the members of the PSA.

Step 8:
Draft the manuals for the evaluators and observers

The manual for evaluators and observers is based on the MEL. All observers have access to the MEL. This enables them to use all aspects of the exercise and to filter out what is (or could be) important for the discipline or the company. Together with the inputs this makes up the manual for the observers.

The observers' manual can consist of:
- The Exercise Convention(s)
- Conclusions and agreements emerging from briefings
- The MEL
- General instructions and specific instructions for each observer
- The time schedule
- The contact details of all observers and all possible ways of interacting
- Supplements (for each observer) with technical or specific information

The evaluators' manual can consist of:
- The Exercise Convention(s)
- Conclusions and agreements emerging from briefings
- The MEL
- General instructions and specific instructions for each evaluator
- The time schedule for the exercise
- The contact details of all evaluators and all possible ways of interacting

The evaluators assess whether the set objectives have been reached. They do this using evaluation criteria drawn up by themselves, on the basis of the objectives.
The objectives are attained if the actions laid down in the MEL are performed in a correct way. The evaluators have full access to the MEL for the purpose of making their quantitative or qualitative assessments.

Step 9:
Organise the support for the exercise

- Make sure all the logistics are arranged
- Accompany the media
- Organise information or training sessions for all players in the exercise
- Train the evaluators and observers for the exercise
- Also accompany any observers or spectators
- Make practical arrangements with roll players and simulants

Step 10:
Play the exercise

During the play it is important to keep to certain guidelines:
- Always **stick to the scenario**
- **Follow the agreements** that have been made
- Make sure that confidential information is **kept confidential**

Step 11:
Debriefing

The aim of the debriefing is to **draw lessons from the exercise**. The first step is to identify the lessons. At the various debriefing sessions, feedback is asked from participants, evaluators and observers. The exercise management team and marshalls then discusses the different feedback, suggests solutions, sets priorities and finally draws up an action plan. This action plan is presented to the PSA for approval.

The emphasis is always on positive feedback: this means that points of attention must be clearly identified.
Negative feedback example: "This was a bad exercise..." does not generate any added value.
When gathering feedback, a clear distinction needs to be made between comments about how exercise objectives were reached (or not reached) and comments about the organisation of the exercise.

Immediately after the exercise it is recommended that the Ex Dir organises a "hot wash-up" lasting about half an hour, asking people for their impressions and noting these down. Experience shows that this is a good way to list the aspects that will come up later at the debriefing, for each discipline. In the 2 or 3 weeks after the exercise, each discipline draws up a more extensive report about the exercise, with the emphasis on the lessons learned from it, both in the positive sense and as regards identifying possible points for improvement.

The observers similarly draw up a report of their impressions and their conclusions from the exercise, and submit a copy to the Ex Dir.
The evaluators produce a comprehensive report and document their findings too.
The Ex Dir organises a separate debriefing session for the evaluators and observers.
Afterwards a separate debriefing is organised with all the representatives of the various disciplines and the support team (Ex Dir, evaluators and observers) at which all the points are discussed.
At the debriefing it is necessary to ensure that the exercise is looked at both from the point of view of the players and from the point of view of the EMT, specifically those who were marshall during the exercise.
It is important for the complete set of documentation to be archived, as it can be useful for further analysis afterwards, especially in preparation for other exercises.

Step 12:
Draw up the action plan

The purpose of an exercise is to test procedures and measures, and to draw the necessary lessons. But beyond that the necessary initiatives must be taken to improve the various aspects.
After the evaluation the support team lists the points for improvement and translates them into action plans. These action plans are submitted to the PSA for approval, and are then implemented.

Each action plan must state at least the following:

- **The things to be done**
- **The persons responsible**
- **The deadline for doing them**




Police
G-10
GEseaco
HLL




CARU
MAX. GR.
TARE
NET
CU. CAP.

part 2
PRACTICE



Practice makes perfect

The proof of the pudding is in the eating, and that also applies to practicing security protocols and situations. In this part you will find lots of practical examples for small-scale practice (drills) and large-scale practice (annual exercises). This is followed by various Port Security Exercises, along with some Tips & Tricks. Finally, as an attachment, there is an example of a brochure to help raise security awareness.

This is a workbook: at the end of each drill or exercise sheet there is space under *Remarks* for you to enter your own observations, notes and to-do or not-to-forget lists.

DRILL _____

QUARTER: 1 ❑ 2 ❑ 3 ❑ 4 ❑

SECURITY LEVEL: _____

PFSO/DEPUTY: _____

DATE: _____ TIME: _____

EVALUATION: _____

_____

_____

_____

_____

_____

ACTIONS TO BE TAKEN:

_____

_____

_____

_____

_____

_____

❑ FEEDBACK DESIGNATED AUTHORITY

You find the word-document on the USB-stick

DRILL 1 } Organisation and performance of port facility security duties

Regulation 725/2004: A/14.2.1 A/18.2 B/16.8.1 B/18.2.6

SCENARIO:

Test the role and structure of the security organisation, by asking various people within this structure who in the hierarchic line they report to concerning security procedures and subjects.
Test whether the correct procedures and forms are readily available, e.g.:

- Bomb warning form
- Incident report form
- Telephone list with contact persons
- Procedure for escalating to a higher level
- Handbook with security procedures
- …

LOCATION:

- Facility – offices – security guardhouse – reception

PARTICIPANTS:

- PFSO
- Security guards
- Personnel with security responsibilities

OBJECTIVES:

- Ensure that everyone in the security organisation is aware of the alarm and notification procedures
- Assure correct and quick exchange of information concerning security
- Respect confidentiality and ensure that the right people are briefed
- Create an efficient security organisation
- Make sure the key figures in the security organisation are known to all members of personnel
- Find out whether the security documents are sufficiently well known
- Find out whether the security documents are readily available and up to date

DRILL 2 } Organisation and performance of port facility security duties

Regulation 725/2004: A/16.3.6 B/16.8.2

SCENARIO:

Port facility personnel with specific security tasks and responsibilities must have good understanding of these tasks and responsibilities.

Test their theoretical knowledge using a questionnaire drawn up in-house, for example:

- What is ISPS?
- What is the PFSP?
- Who is the PFSO?
- Which is the competent authority?
- What is the difference between the CSO and the SSO?
- What is the difference between security levels 1, 2 and 3?
- What is the escalation procedure?
- …

TOOLS:

- Security Questionnaire

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Personnel with security responsibilities

OBJECTIVES:

- Ensure that personnel with security responsibilities are aware of their related tasks
- Minimise weaknesses by ensuring good basic knowledge of ISPS
- Ensure good security organisation in which each person knows what he/she has to do

DRILL 3 } Organisation and performance of port facility security duties

Regulation 725/2004: A/17.1-2-3 B/18.1-2-3

SCENARIO:

Test whether the PFSO (and/or the deputy) complies correctly with his/her obligatory tasks and responsibilities.

CHECKLIST – FOR THE PFSO:

- Have a comprehensive security survey of the facility?
  Yes/no. If yes, look up the documents.
- Assure development and maintenance of the PFSP? Make changes to the plan so as to correct deficiencies and update it to reflect significant changes in the facility?
  Yes/no. If yes, show the modifications made.
- Implement the PFSP and carry out the related exercises?
  Yes/no. If yes, is there a folder available with the exercises carried out?
- Carry out regular security inspections to ensure that appropriate security measures are taken?
  Yes/no. If yes, show what has been inspected, and when.
- Raise security awareness and alertness among port facility personnel?
  Yes/no. If yes, show what efforts have been made in this area.
- Ensure that personnel responsible for facility security are sufficiently trained?
  Yes/no. If yes, show exercises in which members of personnel have been tested.
- Report to the competent authority concerning security incidents?
  Yes/no. If yes, look up some reported incidents, or check the procedure.
- Coordinate and carry out the plan with the SSO/CSO concerned?
  Yes/no. If yes, how do you exchange contact details with the SSO, and which means of communication do you use to reach him/her?
- Coordinate with the security services?
  Yes/no. If yes, look up the list with the contact details of the security services.
- Assure compliance with the standards that apply to personnel responsible for security of the facility?
  Yes/no. If yes, what are these standards? Show that members of personnel comply with them.
- Ensure that the security equipment available is used, tested, calibrated and maintained in the correct way?
  Yes/no. If yes, show the last tests and maintenance carried out.
- Help the SSO in checking the identity of people allowed on board, if the SSO so requests?
  Yes/no. If yes, look up the procedure for this.

LOCATION:

- Facility

PARTICIPANTS:

- PFSO and/or deputy PFSO

OBJECTIVES:

- Ensure that the PFSO complies with his/her obligations under Regulation 725/2004
- Check that the PSFO is aware of his/her tasks and responsibilities

DRILL 4 } Organisation and performance of port facility security duties

Regulation 725/2004: B/18.2.6

SCENARIO:

Test whether personnel know when they are faced with a security incident, and that they know how to report it. For this drill you can create various scenarios or use photographic material.
Get people to draw up a report of the situation, paying attention to clarity, summing up facts, etc.

TOOLS:

- Breaches of security
- Photos of Tips & Tricks

EXAMPLES OF SCENARIOS:

- A visitor refuses to provide identification
- Somebody photographs/observes access to the facility
- Somebody asks questions about the organisation of security, shifts etc.
- Somebody is seen walking around the perimeter of the facility

LOCATION:

- Facility – offices – security guardhouse – reception

PARTICIPANTS:

- PFSO
- Security personnel
- Personnel with security responsibilities
- Facility personnel

OBJECTIVES:

- Check the presence and availability of the incident report procedure
- Awareness: recognition of incidents
- Clear, correct reporting of incidents
- Efficient reporting of all incidents

DRILL 5 } Organisation and performance of port facility security duties

Regulation 725/2004: A/14.3 A/14.4 B/16.19.1 B/16.20.4

SCENARIO:

On escalation to security level 2 or 3, can additional personnel be called from the subcontracting security company to guard access points and perimeter, and to mount extra security patrols inside the facility?

CHECKLIST IF SECURITY COMPANIES ARE CALLED UPON:

- Name of contact person in the security firm
- Are the contact details still up to date?
- Is the previous contact person still in the same job, or do the details have to be updated?
- How many people can be made available by the security firm?
- Have these people received ISPS training?
- How quickly are these additional security personnel available?

CHECKLIST IF FACILITY PERSONNEL ARE CALLED UPON:

- What is the current number of personnel?
- Which people can be assigned to which tasks?
- Who can additionally be called by phone?

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security firm
- Facility personnel

OBJECTIVES:

- Assure the possibility of extending the security organisation on escalation (availability of personnel)
- Assure maximum control and awareness
- Assure good communication, division of tasks, supervision and carrying out of instructions for "extra" personnel
- Ensure that this task is carried out efficiently

DRILL 6 } Communication and raising the alarm

Regulation 725/2004: A/16.3.10

SCENARIO:

Test how easily the PFSO can be reached during office hours, evenings, weekends, public holidays, or when he/she is travelling abroad, etc.
Does the PFSO know who he/she additionally needs to contact in case of escalation? Does he/she have these contact details, and does he/she have them immediately to hand?

LOCATION:

- Outside the facility

PARTICIPANTS:

- PFSO
- Deputy PFSO

OBJECTIVES:

- Is the availability of the PFSO and his/her deputy as good as it needs to be in a crisis situation?
- Can the PFSO notify the necessary people immediately, if he/she is not at the facility?

DRILL 7 } Communication and raising the alarm

Regulation 725/2004: B/18.2.2

SCENARIO:
Simulate an exercise in which a suspicious object/package has been left at the security guard-house/reception.

TOOLS:
- Tips & Tricks (10)

LOCATION:
- Security guardhouse - reception

PARTICIPANTS:
- PFSO
- Security guards
- Personnel at reception

OBJECTIVES:
- Check the level of awareness
- Check knowledge of procedure for handling suspicious objects by security guards/reception personnel

DRILL 8 } Communication and raising the alarm

Regulation 725/2004: B/18.2.1

SCENARIO:

Simulate a bomb warning. For this purpose, appoint an observer to be present alongside the person who receives the bomb warning.

TOOLS:

- Bomb threat form

EXAMPLE OF SCRIPT:

Hello,
Listen to what I say and don't interrupt.
The Clowns Liberation Organisation considers the attitude of your facility to be very negative.
An explosive device has been placed in your terminal and will go off in 45 minutes.

- Background noises may be added, for additional realism
- The person receiving the bomb warning may be allowed to use forms and ask questions, but not too long

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Personnel with security responsibilities
- Reception
- Observer

OBJECTIVES:

- Find out whether the bomb warning form is used
- Find out whether the procedure for a bomb warning is followed
- Ensure that the situation is dealt with calmly and as much information as possible is gathered

DRILL 9 } Communication and raising the alarm

Regulation 725/2004: A/18.2 B/18.2.7

SCENARIO:

Check how familiar security personnel are with the communication equipment. Find out what communication equipment they have: e.g. telephone, mobile phone, PC, walkie-talkies, marine VHF, etc.

CHECKLIST:

- Communication equipment works and is used correctly
- Is there a maintenance contract?
- Check operation and condition of accessories (e.g. batteries) and backup equipment
- Test the knowledge of alarm-raising codes

LOCATION:

- Facility – offices – security guardhouse – technical department

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Assure optimum communication possibilities and skills of personnel
- Assure correct operation of the communication equipment
- Assure correct repair/replacement of defective equipment

DRILL 10 } Communication and raising the alarm

Regulation 725/2004: A/13.1 A/17.2.6 B/16.8.4

SCENARIO:

Contact the SSO to examine various aspects of the security procedures with him/her.

TOOLS:

- Declaration Of Security

CHECKLIST:

- Jointly draw up a Declaration of Security (DOS)
- In consultation with the SSO, check who does what in case of escalation to a higher level of security for the ship
- Test the communication and coordination between port facility and ship

LOCATION:

- Facility – on board the ship

PARTICIPANTS:

- PFSO
- SSO
- Facility personnel
- Security guards

OBJECTIVES:

- Give SSO and PFSO experience in assuring the security of the facility and ship
- Assure collaboration and contact between SSO and PFSO
- Ensure that SSO and PFSO have each other's contact details in case of emergency
- Ensure that SSO and PFSO have the necessary documents and communication equipment in case of emergency

DRILL 11 } Communication and raising the alarm

Regulation 725/2004: B/18.1.16 B/18.2.7

SCENARIO:
Test the port facility's alarms and/or sirens. Inform neighbouring companies, ships alongside, authorities, emergency services etc. beforehand, telling them that it is an exercise.

TOOLS:
- Alarm Signals

CHECKLIST:
- Do the alarms and/or sirens work correctly?
- Are they tested periodically?
- Are the maintenance diagrams present?
- Is there a maintenance contract for any repairs that might be necessary?
- Are there backup systems available, e.g. in case of a power failure?
- Can the alarms and/or sirens be heard everywhere: throughout the facility, inside buildings (including offices and toilets), on board ships, in noisy workplaces etc.?
- Do all members of personnel know the different signals?

LOCATION:
- Facility – offices – security guardhouse – technical department – on board ships – neighbouring companies

PARTICIPANTS:
- PFSO
- SSO
- Facility personnel
- Security guards

OBJECTIVES:
- Assure correct operation of the alarm/siren whenever it is really needed
- Assure correct internal and external communication concerning the signal
- Ensure that the signal can be properly heard everywhere, so as to assure the safety of personnel in an emergency

DRILL 12 } Communication and raising the alarm

Regulation 725/2004:

SCENARIO:

At different locations inside the facility, leave pamphlets with the following brief message:

- This is a security exercise
- Follow the usual procedure

TOOLS:

- Pamphlet (example)

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Personnel with security responsibilities
- Facility personnel

OBJECTIVES:

- Create awareness among members of personnel
- Apply the incident reporting procedure
- Ensure that information is passed on quickly to the PFSO

DRILL 13 } Access to the port facility

Regulation 725/2004: A/16.3.2 B/16.12

SCENARIO:

Check the identification systems.

CHECKLIST:

- Does the system work correctly?
- Is the system updated regularly?
- What are the various means of identification used?
- Are these known at the facility access points? Check examples
- Is proper action taken in case of misuse?
- What is the procedure for lost passes?

LOCATION:

- Facility access points

PARTICIPANTS:

- PFSO
- Security personnel
- Facility personnel

OBJECTIVES:

- Assure proper access rights
- Ensure that unauthorised persons do not gain access
- Assure good, efficient communication with local and national authorities
- Assure good, efficient identification

DRILL 14 } Access to the port facility

Regulation 725/2004: A/14.2 A/14.2.2 A/14.3 A/14.4 B/16.16

SCENARIO:

At regular intervals, check the security enclosure (perimeter), entrances and access points for effectiveness and possible damage. Carry out a round of inspection covering not only the main entrance but also access points that are seldomly used or permantly closed, emergency exits, restricted areas etc.
A key plan must be available so that if the level of security is raised the facility can be completely locked quickly and efficiently.

CHECKLIST:

- Do barriers, gates, rail gates, turnstiles etc. operate correctly?
- Is the security guard present at the access point?
- Check any remote controls for gates etc.
- Check the security enclosure for possible damage
- Check for obstacles or objects close to the security perimeter that could be used to climb over it or compromise its effectiveness
- Check that gates are properly locked. Also check the key plan and register
- Check that all restricted areas are sufficiently well closed off
- Check that access points that are not regularly used are properly locked
- Document all deficiencies: take photographs of all damage, objects etc., and check that damage is repaired, compromising objects removed, etc.
- Draw up a report for the technical department, if necessary

LOCATION:

- Facility – security perimeter – barriers – gates – turnstiles

PARTICIPANTS:

- PFSO
- Security personnel
- Facility personnel
- Technical department personnel

OBJECTIVES:

- Assure correct operation of the access points/systems
- Assure correct operation of access points that are not used, or not used often
- Assure emergency exits
- Create a good "enclosure" mentality among personnel
- Assure perfect condition of the security enclosure (perimeter) so that unauthorised persons are effectively kept out by it (detect holes, evidence of breaches etc.)
- Periodically inspect the perimeter (security) of your facility
- Also keep a watch for situations just outside the facility
- Assure correct management of keys

DRILL 15 } Access to the port facility

Regulation 725/2004: A/14.2.2 A/14.3 A/14.4 B/16.13

SCENARIO:

A truck from a ship chandler service arrives at the facility. It is carrying a suspicious, unknown load not listed on the manifest.
Appoint an observer for this drill.

LOCATION:

- Facility – security guardhouse – reception

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel
- Observer

OBJECTIVES:

- Check whether the correct procedure for access to the facility is used
- Check whether an incident report is drawn up
- Give personnel experience with "suspicious situations"
- Give personnel training in awareness and recognition

DRILL 16 } Access to the port facility

Regulation 725/2004: A/14.2 A/14.3 A/14.4 B/16.10

SCENARIO:

Check the different procedures for access control.

CHECKLIST:

- Is the access procedure followed as laid down in the PFSP for: passengers, crew members, visitors, personnel, vehicles and vehicle occupants?
- Check the procedure for visitors with prior notification
- Check the procedure for change of crew (check the current crew lists)
- Check the procedure for visitors to ships
- Check the logbook and the way information is recorded in it: surname, forename, ID number, vehicle, licence plate etc.

LOCATION:

- Facility – access control point and/or security guardhouse – reception

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Assure an efficient access control system for each type of visitor
- Prevent unauthorised persons gaining access
- Ensure that existing procedures are fully described

DRILL 17 } Access to the port facility

Regulation 725/2004: A/14.2 A/14.3 A/14.4 B/16.12 B/16.13

SCENARIO:

An unknown person tries to gain access to the facility using a pass that has been "lost" by one of the facility members of personnel.

TOOLS:

- Tips & Tricks (9)

CHECKLIST:

- Is the impersonation noticed?
- Has the port security authority been warned?
- Is the pass withheld?
- Is this recorded in an internal system?
- Are the circumstances of the pass being lost investigated?
- Is the person asked the reason for the visit?

LOCATION:

- Facility – security guardhouse – porter's lodge – reception

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Check whether the correct procedure for access to the facility was used
- Prevent unauthorised persons gaining access
- Prevent incorrect persons being recorded as present
- Assure correct pass policy
- Assure awareness by access control/reception

DRILL 18 } Access to the port facility

Regulation 725/2004: A/14.2 A/14.3 A/14.4 B/16.10

SCENARIO:

Check the register of visitors present. Are the lists complete and up to date?

LOCATION:

- Facility – security guardhouse – porter's lodge – reception

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Assure an exact (manual) system
- Check that people logged in are actually in the facility, and that those leaving are logged out, so as to prevent misunderstanding in case of emergency/evacuation

DRILL 19 } Access to the port facility

Regulation 725/2004: A/14.2.2 A/14.3 A/14.4 B/16.13

SCENARIO:

The security personnel inform you that they have just checked a car entering the facility, and have discovered goods for which no documentation can be produced. The vehicle is blocking the entrance and the driver is making a row.

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Ensure that the incident is dealt with in a disciplined manner, and that personnel keep their self-control (despite the row)
- Test communication with the authorities

DRILL 20 } Access to the port facility

Regulation 725/2004: A/14.2.2 A/14.3 A/14.4 B/16.19 B/16.20

SCENARIO:

Close off all access points, as laid down for escalation to level 2 or level 3..

TOOLS:

- Tips & Tricks (1) (2) (3) (14) (15)

CHECKLIST:

- Check the time necessary to close off all access points
- Is the closing off adequate?
- Are the points to be closed laid down beforehand, or are they closed on an ad hoc basis according to the situation?

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Check correct closing, with the number of access points being minimised
- Centralise intensified identity control at 1 point
- Check that access points are closed off by the authorised persons within the time laid down, or as quickly as possible
- Assure a fully closed perimeter

DRILL 21 } Access to the port facility

Regulation 725/2004: A/14.2 A/14.3 A/14.4 B/18.2 B/18.3

SCENARIO:

Get someone to try to gain access to the facility without being noticed, or without the proper authority.

TOOLS:

- Tips & Tricks (4) (9) (11) (12)
- Tests in the field

CHECKLIST:

- Alertness: is the attempt noticed, and what action is taken?
- The method by which the person is challenged
- Is there a number to call or a point of contact to report irregularities?
- Does the facility have CCTV? Check whether recorded images can be called up. Test using the CCTV to search for unauthorised persons within the facility
- Is a report drawn up?

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Awareness
- Prevent unauthorised access
- Create discipline among personnel, so that “unknown” persons are challenged
- Assure correct subsequent action and reporting of the incident

DRILL 22 } Access to the port facility

Regulation 725/2004: A/14.2.1 B/18.2

SCENARIO:

Get someone to try to obtain as much sensitive information as possible from the porter or the security guard by asking questions such as the following:

- What times do the guards change shift?
- Are you always by yourself?
- Is there always someone here?
- Are there other entrances where I can meet someone?
- Is there someone who can help me at the other entrance?
- Are you satisfied with the camera system?
- Can recorded camera images be called up, because I had an accident here a couple of days ago?
- Are there any dangerous goods in the facility?

TOOLS:

- Tips & Tricks (8)

LOCATION:

- Facility – security guardhouse – porter's lodge

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards
- Porter

OBJECTIVES:

- Check that people are asked for identification
- Check that sensitive information is dealt with correctly
- Limit the amount of information provided
- Check awareness and recognition of unusual situations
- Assure confidentiality
- Check whether a report is drawn up with a description of the person(s) in question plus details of the vehicle (licence number, make, colour)

DRILL 23 } Access to the port facility

Regulation 725/2004: A/14.2.2 B/15.3

SCENARIO:

Check how long unmanned, remote-controlled gates remain open, e.g. rail gates, second entrances, suppliers' entrances etc.

For this drill the PFSO can also have the gate opened.

LOCATION:

- Facility – security guardhouse – porter's lodge – control room

PARTICIPANTS:

- PFSO
- Security guards
- Porter
- Facility personnel

OBJECTIVES:

- Avoid these gates standing open for too long
- Prevent unauthorised persons gaining access through them
- Assure correct monitoring of the way these gates are operated by all parties involved (including external people, e.g. rail/road operators)
- Create awareness concerning these gates among personnel

DRILL 24 } Access to the port facility

Regulation 725/2004: A/16.3.1 A/16.3.2 B/16.19.2 B/16.19.3 B/16.20

SCENARIO:

When the security level is escalated, the competent authority imposes a time limit for setting up a security perimeter around the ship. Access control must be imposed, and a record kept of persons and vehicles entering and leaving.

TOOLS:

- Tips & Tricks (2) (3) (6)

CHECKLIST:

- Is the temporary enclosure (necessary for levels 2 and 3) available?
- How long does it take to set up a perimeter around the ship?
- If fencing is kept in stock: check and simulate (how many metres can be set up in 1/2 hour: extrapolate)
- If contract: check delivery time, contact person and contact details for external company
- Is there a register available to record vehicles and persons?
- How many people are affectively needed for the access control and recording at the perimeter?

LOCATION:

- Facility – quayside

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Comply with time for setting up perimeter
- Check that the perimeter is adequate
- Assure security of the ship and facility by means of the perimeter
- Assure correct organisation of setting up the perimeter and carrying out access control
- Check whether procedures described in the plan are realistic, or need improvement.

REMARKS:

Extrapolate = take the results and use them to work out how much time/material/manpower would be required for a greater area

DRILL 25 } Restricted areas within the port facility

Regulation 725/2004: A/14.2.4 A/14.3 A/14.4 B/16.22 B/16.27 B/16.28 B/16.29

SCENARIO:

Test the measures and examine the procedures for all areas to which restrictions apply:

- Partially enclosed areas or closed places for suspicious or damaged cargo
- Storage facilities for flammable or explosive materials
- Computer server rooms and communication centres.
- PFSO office
- Security guardhouse

CHECKLIST:

- Check the access procedure: number of authorised persons, who has a key or badge, is there a list of authorised persons, is a record kept of who accesses the restricted area, and when?
- Check the restricted area for suspicious items: belongings and luggage
- Check for damage: evidence of break-in attempts on doors, windows and security fence
- Check the register of rounds and reports
- Check protection equipment and hardware installations, including sprinklers, fire extinguishers etc.

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Ensure that there is absolutely no access to Restricted areas within the port facility by unauthorised persons
- Assure good supervision, surveillance and security of Restricted areas within the port facility
- Ensure that Restricted areas within the port facility get extra protection

DRILL 26 } Restricted areas within the port facility

Regulation 725/2004: A/14.2.4 A/14.3 A/14.4 B/16.24

SCENARIO:

If there are automatic access points with detection equipment, test them for correct operation and check that the alarm actually reaches the control room. Check how the person in the control room reacts to the alarm.

LOCATION:

- Facility – access points with detection equipment

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Assure correct operation of the detection equipment and electronic alarms
- Assure correct reaction and compliance with the procedure by the person receiving the alarm

DRILL 27 } Restricted areas within the port facility

Regulation 725/2004: A/14.2.4 A/14.3 A/14.4 B/16.21.4

SCENARIO:

Check that all Restricted areas within the port facility are clearly marked with signs saying "No access to unauthorised person," or "Restricted access area" or similar prohibition.

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Ensure that Restricted areas within the port facility are clearly indicated, with a warning that strict security measures apply

DRILL 28 } Monitoring the security of the port facility

Regulation 725/2004: A/14.2 B/16.49.2

SCENARIO:

Check that patrol rounds are carried out as indicated in the PFSP.

CHECKLIST:

- Check the patrol plan of the facility
- Check that all important points are included in the plan (up to date)
- Is the security patrol well organised?
- Are the instructions for security personnel clear and well understood?
- Check: authority, equipment, procedures, patrol reports

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Assure effectiveness of the patrol plan
- Assure correct carrying out of patrol rounds
- Assure correct reporting of the rounds carried out

DRILL 29 } Monitoring the security of the port facility

Regulation 725/2004: A/14.2 A/14.3 A/14.4 B/16.49.3

SCENARIO:

Use the CCTV to see whether someone inside the facility is acting suspiciously.

TOOLS:

- Port security awareness handbook
- Tests in the field
- Suspect behaviour

CHECKLIST:

- Test the ability of the CCTV operator: zoom, tilt, tracking etc.
- Test communication and coordination
- Check the reaction to the situation
- Check which points are noted (description)
- Check that images are recorded and can be called up

LOCATION:

- Facility – security guardhouse – porter's lodge – control room

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel
- Roll players

OBJECTIVES:

- Assure correct operation of the camera by personnel
- Assure good quality, usability and positioning of the cameras
- Awareness: detailed reporting of the images
- Assure correct response to the incident
- Ensure that the right persons are notified and sent to the location

DRILL 30 } Monitoring the security of the port facility

Regulation 725/2004: A/18.1 A/18.2 B/18.1.14 B/18.2.3 B/18.2.6 B/18.3.3

SCENARIO:

There is a suspicious vehicle on the facility. Someone is taking photographs of the facility.

TOOLS:

- Tests in the field

CHECKLIST:

- Check whether the security guards follow the correct procedure: reporting, description, acting correctly (who, what, where) etc.
- Check whether the facility members of personnel have the necessary "security awareness" and act according to a set procedure: do they have someone they can report to within their own management, do they know the contact number of the security department?

LOCATION:

- Facility – security guardhouse – porter's lodge

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards
- Roll players

OBJECTIVES:

- Improve awareness: notice suspicious behaviour
- Give a detailed description
- Assure good communication, ensure that the right persons are notified
- Assure full, correct reporting

DRILL 31 } Monitoring the security of the port facility

Regulation 725/2004: A/14.3 A/14.4 B/16.53.1 B/16.54.2, A/17.2.12 A/18.2 B/18.1.16 B/18.2.7

SCENARIO:

The security level is escalated and there needs to be extra vigilance. Instruct the security guards to pay extra attention to the CCTV images.

CHECKLIST:

- Check that the most important areas are covered: ISPS area, access routes by land and water, Restricted areas within the port facility, the ship, area around the ship
- Check the surveillance equipment after dark, with the facility lighting. Check for blinding of cameras, check quality of images. Reposition cameras if necessary
- Test the ability of the CCTV operator: locating people, vehicles, objects etc.
- Test the capability of the CCTV system: zoom, pan, tilt, split screen etc.
- Test calling up recorded images (where possible)
- Does the CCTV system meet expectations?
- Are security personnel familiar with the operation and possibilities of the CCTV system?

LOCATION:

- Facility – security guardhouse – porter's lodge – control room

PARTICIPANTS:

- PFSO
- Facility personnel
- Security personnel

OBJECTIVES:

- Assure correct use of the camera and knowledge of the equipment on the part of personnel
- Ensure that personnel can call up images
- Assure good quality, usability and positioning of the cameras

DRILL 32 } Monitoring the security of the port facility

Regulation 725/2004: A/14.2 A/14.3 A/14.4 B/16.54.1

SCENARIO:
Test the fixed or mobile lighting necessary for escalating the security level.
In consultation with the SSO, all the ship's lighting may be switched on as well.

CHECKLIST:

- Do all the lights work?
- Check for dark areas: in the facility, in and around Restricted areas within the port facility, around the ships, along access routes
- Check the operation of fixed and mobile lighting
- Check maintenance and repair
- If there is a contract: check the contact details and contact persons for the external company
- Check that a logbook of vehicles and personnel is kept

LOCATION:

- Facility – quayside

PARTICIPANTS:

- PFSO
- Facility personnel
- Security personnel
- Where applicable, SSO

OBJECTIVES:

- Assure sufficient lighting for visibility in all conditions (at night, in bad weather etc.)
- Assure correct operation of all equipment

DRILL 33 } Monitoring the security of the port facility

Regulation 725/2004: A/14.2.7(?) B16.8.4-5

SCENARIO:

You discover an equipment defect or incorrect operation:

- Communication equipment: mobile phone, fixed telephone, walkie-talkie, siren etc.
- Gates, barriers etc.
- Camera or CCTV

CHECKLIST:

- Are there repair procedures for the different items of equipment?
- Are there spare parts or replacement equipment available?
- Can the repair service come quickly, at any time?
- Are the contact details of the company still up to date?

LOCATION:

- Facility – offices – security guardhouse – reception – technical department

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel
- Technical department personnel

OBJECTIVES:

- Assure correct operation and management of all equipment
- Reduce repair times to the minimum

DRILL 34 } Handling of cargo

Regulation 725/2004: A/14.2.5 B/16.32 B/16.33

SCENARIO:

Check that cargo inspections are carried out correctly and that all points are attended to.

TOOLS:

- Cargo Inspection
- Seal inspection
- Container inspection
- Truck & trailer inspection

CHECKLIST:

- Is the shipment date checked?
- Do the goods correspond to the waybill?
- Are the goods and/or vehicles properly inspected?
- Is the seal checked?
- Is visual or physical inspection, scanning or sampling carried out each time?
- Is there a check for stowaways?

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Ensure that goods are inspected correctly, so that no incorrect, contaminated or suspicious goods enter or leave the ship
- Ensure that members of personnel carry out their tasks correctly and know the procedure for suspicious goods
- Assure correct operation of all inspection equipment
- Assure security of cargo

DRILL 35 } Handling of cargo

Regulation 725/2004: A/14.2.5 A/16.3.1 B/16.31 B/16.33

SCENARIO:

Check the inventory and location of dangerous goods/substances stored within the facility.

CHECKLIST:

- Are the inventories of the dangerous goods/substances immediately available?
- Compare the inventory with the actual situation

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Ensure that an up-to-date inventory is available as necessary
- Ensure that the location of dangerous goods is monitored correctly, so that action can be taken rapidly if necessary
- Assure constant monitoring of dangerous goods, so as to prevent sabotage, contamination or misuse of these goods

DRILL 36 } Handling of cargo

Regulation 725/2004: A/14.2.5 A/14.3 A/14.4 B/16.31 B/16.35.2 B16.37.2

SCENARIO:

Simulate SL2 and apply the control procedure for goods at the access points.

TOOLS:

- Cargo Inspection
- Seal inspection
- Container inspection
- Truck & trailer inspection

CHECKLIST:

- Can the consignment/container be identified?
- Has the consignment been inspected? Has the container seal been checked, or have the contents been compared with the waybill?
- Has the consignment/container been accepted?
- Has all information been provided?
- If scanning or detection equipment is available, check that it works correctly.

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Porter
- Facility personnel

OBJECTIVES:

- Assure efficient, speedy inspection of goods despite the higher security level
- Assure appropriate inspection of goods entering the facility

DRILL 37 } Handling of cargo

Regulation 725/2004: A/14.2.5 A/14.3 A/14.4 B/16.31 B/16.35.2 B16.37.2

SCENARIO:

Check the freight storage areas and apply procedures for when the security level is raised.

CHECKLIST:

- Can the warehouses and storage areas be closed off?
- Who has access to these warehouses and storage areas?
- Check the Restricted areas within the port facility in these warehouses or storage spaces for dangerous or suspicious materials
- Check for suspicious objects in the warehouses and storage areas

LOCATION:

- Facility – warehouses – storage areas

PARTICIPANTS:

- PFSO
- Security guards
- Porter
- Facility personnel

OBJECTIVES:

- Ensure that no unauthorised persons gain access to warehouses or storage areas
- Ensure that goods can be stored there safely

DRILL 38 } Delivery of ship's stores

Regulation 725/2004: A/14.2.6 B/16.8.10 B/16.41 B/16.42 B/16.43

SCENARIO:

Test the procedure for delivering supplies to ships as laid down in the PFSP.

CHECKLIST:

- Check the details of the ship's supplier
- Check the advance notice of deliveries
- Check the actual composition of the goods delivered
- Check the delivery driver's details
- Check the vehicle registration
- Check the Delivery of ship's stores
- Search the vehicle

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security personnel
- Facility personnel/reception
- Ship's supplier
- SSO, where applicable

OBJECTIVES:

- Ensure that no supplies get on board without being inspected
- Ensure that no ship's supplies get into the facility without advance notice
- Ensure that there are no suspicious packages among the ship's supplies
- Ensure correct checking of the information
- Check knowledge of the procedure to be followed by security personnel or facility personnel
- Assure correct identification and recording of the identity of suppliers and visitors

DRILL 39 } Delivery of ship's stores

Regulation 725/2004: A/14.1 A/14.2.6 A/14.3 A/14.4 B/16.8.10 B/16.42 B/16.43 B/16.44

SCENARIO:

If supplies have to be escorted for level 2 or up, apply this measure as laid down in the PFSP. This drill can also be carried out in combination with Delivery of ship's stores drill 38.

LOCATION:

- Facility – security guardhouse – porter's lodge

PARTICIPANTS:

- PFSO
- Security guards
- Porter
- Facility personnel
- SSO, where applicable

OBJECTIVES:

- Assure good organisation for escorting supplies on board the ship (shortest and safest way)
- Ensure that Delivery of ship's stores are not left unattended on the facility

DRILL 40 } Delivery of ship's stores

Regulation 725/2004:

SCENARIO:

When the security level is escalated, the Delivery of ship's stores must be handled according to the ISPS procedure. Time this procedure: how long does it take for the complete Delivery of ship's stores to be fully inspected?

LOCATION:

- Facility – Gate-in

PARTICIPANTS:

- PFSO as observer
- Where applicable, SSO
- Security personnel
- Ship's supplier

OBJECTIVES:

- Test the procedures laid down in the PFSP
- Ensure that the procedure is known to security guards
- Carry out spot checks of goods supplied / ordered
- Check what happens to Delivery of ship's stores that arrive without advance notice (what does the security guard do?)

DRILL 41 } Handling unaccompanied baggage

Regulation 725/2004: A/14.1 B/16.45 B/16.46 B/16.47 B/16.48

SCENARIO:

PAX

If Handling unaccompanied baggage is permitted, handle and screen it correctly. Bring the luggage safely to the ship.

CHECKLIST:

- Test the procedure for screening luggage
- Test the scanner used
- Test the security guards' knowledge of the procedure
- Check communication with the ship

LOCATION:

- Facility

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel

OBJECTIVES:

- Assure correct compliance with the procedure for Handling unaccompanied baggage
- Identify Handling unaccompanied baggage as safe
- Assure communication with the ship

DRILL 42 } Handling unaccompanied baggage

Regulation 725/2004: B/16.45 B/16.46 B/16.47 B/16.48

SCENARIO:

CARGO

Get someone to deliver a package to the security guardhouse or porter's lodge, with a request for it to be taken to a ship at berth. (Invent a believable explanation.)

CHECKLIST:

- Check that security personnel follow the procedure and report the incident correctly
- Measure the response time (for application of the procedure)
- Check how the threat level is assessed: how suspicious is the package considered?
- Check compliance with the procedure: drawing up the incident report form
- If necessary, update the details of the external bodies to be contacted

LOCATION:

- Facility – gate or security guardhouse/porter's lodge

PARTICIPANTS:

- PFSO
- Security guards
- Facility personnel/reception

OBJECTIVES:

- Ensure that personnel know the procedure for Handling unaccompanied baggage
- Test the feasibility of the procedure
- Prevent bomb packages being taken onto the facility or ship

DRILL 43 } Training, drills and exercises on port facility security

Regulation 725/2004: A/17.2.7 A/18.1 B/18.1

SCENARIO:
Attend the information session held by the local authority or some other maritime security-related seminar.

LOCATION:
- See invitation

PARTICIPANTS:
- The competent authority
- PFSO
- Security guards
- Facility personnel

OBJECTIVES:
- Provide information about ISPS and security: current situation, legislation, developments, projects etc.
- Exchange know-how and information

PART 1
- Theory: Types of exercise
  Seminar / info sessions

DRILL 44 } Training, drills and exercises on port facility security

Regulation 725/2004: A/17.2.7 A/18.1 B/18.2

SCENARIO:

As PFSO, organise a training course or information session on "improving the security of ships and port facilities" for the personnel of the facility.

- Target groups to be informed: facility personnel, personnel working in the secured area
- Subjects: security awareness, effective communication (top-down and bottom-up), "What is a security incident?"

LOCATION:

- Facility

Participants:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Provide information about ISPS and security
- Improve awareness

PART 1

- Theory: Types of exercise
  Seminar / info sessions

DRILL 45 } Ferry services

Regulation 725/2004:

SCENARIO:

A passenger has booked and presents a valid ticket, but turns out to be carrying a permissible weapon (e.g. a hunting weapon).

CHECKLIST:

- What is the procedure to be followed?
- Is the procedure followed correctly?
- What route does the weapon follow to get on board?

LOCATION:

- Facility entrance

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Assure correct application of the procedure by personnel responsible for access control
- Ensure that weapons are not left unattended
- Ensure communication with the SSO

DRILL 46 } Ferry services

Regulation 725/2004:

SCENARIO:

Once all the passengers are on board, a suitcase is found after the check-in desk, in the transit zone (i.e. not yet on board). What do you do?

LOCATION:

- Facility transit zone

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Ensure that the procedure is followed correctly by security and other personnel
- Ensure that the suitcase is brought safely on board, with security check, without causing unnecessary delay (if owner is identified and suitcase is harmless)

DRILL 47 } Ferry services

Regulation 725/2004:

SCENARIO:

A passenger has booked a return ticket with cabin. He does not show up for the return trip. What do you do?

LOCATION:

- Facility entrance

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Ensure that the passenger manifest/check-in list is correctly checked
- Ensure that the proper information channels are informed

DRILL 48 } Ferry services

Regulation 725/2004: A16.3.1

SCENARIO:

Somebody turns up at the check-in desk and asks for a birthday present to be brought to her daughter in the other port. She explains that the girl's aunt will collect the present at the gate-in on the other side.

LOCATION:

- Facility entrance

PARTICIPANTS:

- PFSO
- Facility personnel
- Security guards

OBJECTIVES:

- Assure correct application of the procedure by personnel responsible for access control
- Assure correct application of the procedure for Handling unaccompanied luggage,packages
- Make sure the right questions are asked
- Ensure that the incident report is used

DRILL 49 } Ferry services

Regulation 725/2004: A16.3.2

SCENARIO:
A man in the pax transit zone asks to be allowed to go to his car (in the transit zone car park) to fetch baby food. What do you do?

LOCATION:
- Facility transit zone

PARTICIPANTS:
- PFSO
- Facility personnel
- Security guards

OBJECTIVES:
- Ensure that the procedure is followed correctly by security and other personnel
- Make sure the right questions are asked.

ANNUAL EXERCISES



ANNUAL EXERCISE _____

SECURITY LEVEL: _____

PFSO/DEPUTY: _____

DATE: _____ TIME: _____

EVALUATION: _____

_____

_____

_____

_____

_____

ACTIONS TO BE TAKEN:

_____

_____

_____

_____

_____

_____

❏ FEEDBACK DESIGNATED AUTHORITY

You find the word-document on the USB-stick

ANNUAL EXERCISE 1}

Regulation 725/2004:

CONDITIONS:

Initiate the emergency plan: carry out the evacuation exercise with the facility actually being evacuated. This can be done in combination with a safety scenario, with e.g. the Fire Department or other emergency services attending.

SCENARIO:

The following disasters can be included in this exercise:

- Bomb alert
- Fire of unknown origin
- Leak of a dangerous product
- Truck incident with dangerous goods
- Incident on board of a ship alongside

ACTION:

The facility is expected to do the following:

- Test all internal and external communication
- Test evacuation procedures (assembly point, access routes for emergency services, etc.)
- Test emergency generators
- Test safety and security procedures (instructions to visitors, drivers, subcontractors etc.)
- Test warning procedures (alarm signal, sirens etc.)
- Close off access points, call up and check register/list of persons present
- Test procedures for ships (notification, common guidelines etc.)

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO, SSO, CSO
- Security
- Own personnel
- External personnel: visitors, drivers, contractors
- Assistance from competent authority (optional)
- Observer(s)

TOOLS:

- Evacuation Signalisation
- Alarm Signals
- Bomb Threat form
- Tips & Tricks (7)

OBJECTIVES:

- Assure correct operation of the alarm system, so that everybody (internal members of personnel, ships, authorities, neighbouring companies) immediately take the correct action. Make sure the signal can be heard everywhere and is recognised
- Ensure that the list of persons present and/or crew lists are complete and can be used efficiently in case of evacuation
- Use checklists to ensure that no steps in the procedure are forgotten
- Time the evacuation, to find out how long it takes to complete
- Assure efficient collaboration between different facilities
- Assure efficient internal and external communication
- Crowd control
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action

ANNUAL EXERCISE 2}

Regulation 725/2004:

CONDITIONS:

SL2 cluster exercise

This exercise is carried out with other ISPS facilities in the vicinity

The exercise can be directed by the competent authority or by the different ISPS facilities in collaboration

The exercise starts with a simulated message to escalate to security level 2 for the whole cluster

SCENARIO:

Various facilities are being targeted by a small terrorist cell seeking to deal with personnel inside the facility in order to smuggle materials, steal data or make other preparations for a terrorist attack

ACTION:

The facilities are expected to do the following:

- Test all internal communication necessary to raise the security level
- Assure increased alertness among personnel present, until the security level is lowered
- Check that personnel with security responsibilities know the procedures they have to follow for SL2 (this can be done using a checklist)
- Designated people attempt to infiltrate the facilities in order to check the robustness of the level 2 procedures.

LOCATION:

- Entire facility

TOOLS:

- Security Questionnaire
- Tests in the field
- Tips & Tricks
- Port security awareness handbook

PARTICIPANTS:

- PFSO
- Security
- Own personnel
- Assistance from competent authority (recommended)

OBJECTIVES:

- Assure the effectiveness of security level 2 procedures
- Ensure that members of personnel are alert and apply the procedures
- Assure the internal and external communication
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 3}

Regulation 725/2004:

CONDITIONS:

This exercise can be carried out in combination with the port security exercise of the competent authority

SL3 cluster exercise – table top

This exercise can be carried out if there are other ISPS facilities in the vicinity

The exercise can be directed by the competent authority or by the different ISPS facilities in collaboration. But active participation by the authority is required, in whichever case!

The exercise starts with a simulated message to escalate to security level 3 for the whole cluster

ACTION

The representative(s) of the competent authority and the various PFSOs in the cluster meet at one location. Each PFSO has a map of his/her facility. A map of the surrounding area for the whole group is provided.

The evacuation assembly points of the different facilities are compared in order to determine whether they might interfere with one another or the escape routes. Also discuss each other's alarm signals and check each other's contact details.

Discuss whether there are any factors in the vicinity that could make such a combined evacuation necessary. Possibilities include:

- Incident with a rail car carrying dangerous goods in the vicinity of the facilities
- Incident with a pipeline near the facilities
- Incident with a truck near the facilities
- Incident involving dangerous goods in one of the facilities
- etc.

LOCATION:

- Various facilities

PARTICIPANTS:

- PFSO
- Security
- Own personnel
- Competent authority

OBJECTIVES:

- Assure awareness of possible dangers in the vicinity of the facility
- Assure efficient internal and external communication and collaboration
- Coordinate the procedures among the different port facilities and the competent authority
- Prevent each other's escape routes interfering with one another, and/or ensure the most efficient evacuation for the entire area
- Coordinate simultaneous evacuation of the different port facilities
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 4}

Regulation 725/2004:

CONDITIONS:

Full escalation of the facility to SL2, with all procedures in the PFSP being applied. Examples include:

- Set up mobile barriers
- Illuminate the security zones
- Set up additional access control
- Test the CCTV systems
- Allow only essential vehicles and persons to enter
- Keep an access register
- Test the internal and external communication systems
- Put on additional security guards/own personnel, etc.

Any seagoing ships alongside may also be asked to simulate escalation. Test the communication with the ship, and check the security measures with the SSO. A DOS may also be set up
Various simulations can be produced. Examples include:

- A website for a fictitious company is set up, using this as a pretext to gain access to the facility
- People who are refused access to the facility start to cause trouble. Simulate this and test the reaction of personnel. To make it more difficult, get people speaking different languages
- Someone claiming to be from the press phones reception/security, saying he/she has heard about an escalation and asking for information
- Someone starts acting suspiciously in front of one of the surveillance cameras; check whether the person monitoring the cameras notices
- Someone leaves behind a briefcase in the reception area
- Someone tries to gain access using somebody else's ID card or access card
- Somebody tries to gain access using a strange excuse
- Somebody shows unusual interest in the facility: taking photographs, using binoculars, hanging around, asking questions etc
- Somebody leaves their ID card lying around at reception

Depending on the particular tests, the "Security incident report" procedure for reporting to the PFSO and the competent authorities may be tested.
De-escalate the facilities (and any ships involved) to SL1. Check which actions are involved and how long it takes until all procedures are going entirely according to SL1

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO, SSO, CSO (optional)
- Security
- Own personnel
- Assistance from competent authority (optional)

TOOLS:

- Tips & Tricks
- Security Questionnaire
- Tests in the field
- Port security awareness handbook

OBJECTIVES:

- Determine the time necessary to deploy mobile barriers or perimeter
- Assure correct operation of CCTV system, if there is one
- Assure correct use of presence lists, crew lists and registers
- Assure good operation of lighting around the facility and on board the seagoing ship
- Assure efficient internal and external communication
- Check the general knowledge of ISPS and of important documents, on the part of security guards
- Check that all procedures for level 2 are practical
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 5}

Regulation 725/2004:

SCENARIO:
Blackout caused by sabotage, affecting the entire facility

ACTION:
Check the following action points for level 1 and 2:

- What effect does this have on the various processes?
- Which processes are covered by an emergency generator, and for how long?
- How are the other processes dealt with?
- Check also what security equipment no longer works. Determine how continuity of the various security operations can be ensured, so that unauthorised persons are not able to take advantage of the situation to create further mischief. Discuss the situation with agents on the ground

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO
- Security
- Own personnel
- Assistance from competent authority (optional)

OBJECTIVES:

- Ensure that security operations continue to be carried out, despite the reduced technological support
- Assure good communication
- Assure alertness and awareness in exceptional circumstances
- Ensure that the important processes continue to operate, and find out which other processes are degraded or no longer operate
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 6}

Regulation 725/2004:

CONDITIONS:

Table top - Participation by the competent authority is required!

The security alarm system of a ship moored at your quay is activated. The competent authority instructs the PFSO to assemble the company's crisis team at an external location and to continue directing the facility from there. The other members of personnel are not allowed to leave the facility, and no indication of an emergency must be given.

It is advised to actually carry out the tabletop exercise at the external location: this will make the exercise more effective, since the resources available there will be inventoried and tested. It will also allow to determine the time necessary for the full team to assemble at the external location and begin operation

ACTION:

Examine the following:

- Who is in the company's crisis team?
- Which location does the crisis team move to?
- Which resources do they need in order to operate from there?
- Who are the contact persons who remain inside the facility? What are the "secure" lines for communicating?

The security guards/reception must not allow anyone to enter the facility, except members of the authorities. How do the security guards/reception accomplish this? How do they identify authorised members of the emergency services?

A possible scenario is that the ship's crew have been taken hostage after the ship has moored: the hostage-takers must not notice that the facility is aware of the situation, and the terminal should appear to continue operating normally. A short while later a hijacker contacts the CEO, saying that a huge explosive charge is hidden among freight that has just been unloaded, and that he will detonate it. The facility has to be evacuated immediately: how will the crisis team deal with this from the external location?

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO, Security, Own personnel
- Representative(s) of the competent authority

OBJECTIVES:

- Assure good coordination between the competent authority and the terminal
- Assure awareness on the part of personnel present
- Test the bomb alarm/alert procedures
- Coordinate operation of the terminal from a remote location
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 7}

Regulation 725/2004:

SCENARIO:

Table top and simulation. Participation by the competent authority is required!
During a cargo spot check, security finds tampered cargo. They find a suspect item, which may well be a WMD. The entire cargo that has been unloaded from the ship has to be inspected in detail.

ACTION:

Examine the following:

- How is the inspection carried out?
- Which resources are used for this?
- How can space be made available on the facility where the ship's cargo can be set apart, and where freight that has been inspected can be distinguished from freight that has not been inspected?
- Which government authorities have to be involved?

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO
- Security
- Own personnel
- Representative(s) of the competent authority

OBJECTIVES:

- Evaluate the inspection resources available within the port facility, and determine which resources can be contributed by the competent authority
- Evaluate the possible locations for the inspection available within the facility, which can be set apart as separate areas
- Assure good coordination between the competent authority and the terminal
- Assure correct inspection of the cargo
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 8}

Regulation 725/2004:

CONDITIONS:

Carrying out ship supply operations at SL2.
Simulate escalating the facility to SL2. Determine how ship supply operations can be carried out under SL2 conditions. Apply the relevant procedures.
Involve the competent authority.

SCENARIO:

The facility is escalated to SL2 in response to a threat of an unknown type.
The procedure for supplying ships under SL2 has to be applied

ACTION:

The facility is expected to do the following, as per the PFSP:

- Check the details of the supplier and the ship
- Check the advance notice of arrival
- Check the composition of the goods supplied
- Check the details of the driver supplying the goods
- Check the vehicle registration
- Inspect the ship's supplies
- Search the vehicle
- Accompany the supplies to the ship

LOCATION:

- Facility: gate-in – security guards' lodge – porter's lodge – quayside

PARTICIPANTS:

- PFSO
- SSO
- CSO (optional)
- Own personnel
- Security guards
- Person delivering the ship's supplies
- Representative(s) of the competent authority

TOOLS:

- Tips & Tricks (15)

OBJECTIVES:

- Test procedures for supplying ships, with security guards or own personnel at SL2
- Prevent ship's supplies getting into the facility without advance notice
- Check that there are no suspicious packages among the ship's supplies
- Ensure correct checking of the information
- Assure correct identification and recording of the identity of suppliers and visitors
- Ensure that no ship's supplies get on board without being inspected
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 9

Regulation 725/2004:

CONDITIONS:

Training in personal descriptions, for security personnel and security guards whenever SL2 procedures have to be applied. All facility personnel with security responsibilities are given instruction in how to maintain higher vigilance at SL2.

SCENARIO:

The facility is thought to be targeted by a group of people wishing to gather sensitive information about the facility and finding weak points in the organisation

ACTION:

Members of personnel with security responsibilities must be able to:

- Recognise breaches of SL2
- Maintain heightened vigilance for suspicious people/behaviour
- Operate any CCTV systems present
- Be familiar with communication systems (means of communication, code words, important telephone numbers, contact persons etc.)
- Report incidents clearly

Get various types of people (chosen by the facility or the authorities) to try and gain access to the facilities in different ways (on foot and by vehicle), look for weak points or obtain sensitive information. Actions may be repeated by the same persons, but make sure that external appearances are different each time (e.g. with/without glasses, with a different colour of jacket, with/without briefcase, with/without hat, etc.)

- The security guards must recognise and note the suspects and the suspicious behaviour.
- In their communication and in their reporting to the PFSO, the security guards must practice giving very detailed descriptions of the persons and vehicles

Give the security guards a clear description of one or more suspects who may be present on the terminal. Get one guard to look for the suspect(s) using the CCTV system; once found, the guard should use the communication system to give a clear description and send a colleague to the suspect(s). If there is no CCTV system, a patrol can be sent out to look for the suspect(s)

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO, Security guards, Own personnel
- Assistance from competent authority (optional)

TOOLS:

- Tips & Tricks (9) (10)
- Security Questionnaire
- Tests in the field
- Port security awareness handbook

OBJECTIVES:

- Ensure that good use is made of the CCTV system
- Assure correct use of presence lists, crew lists and registers
- Assure good internal and external exchange of information
- Carry out a debriefing with all parties involved
- Test the professionalism and ISPS knowledge on the part of security guards and people with security responsibilities
- Improve awareness and give training in detailed personal descriptions
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 10}

Regulation 725/2004:

CONDITIONS:

Specifically for cruise/passenger vessels and ferry services

Table top exercise – in collaboration with the competent authority and SSO

SCENARIO:

Simulating bomb alarm/evacuation.

An unknown person contacts the facility by telephone with the following message:

"There are bombs set to explode in the next four hours placed in the terminal of your port."

The caller was female, with a northern accent and spoke quietly without any trace of emotion or panic and she said this only once

ACTION

Think of the various ways in which bombs could be brought in (in hand luggage, in a vehicle, carried on the person, in accompanied luggage etc.)

Discuss with the competent authorities and SSO which actions you have to take, the division of tasks and how you will organise the evacuation

Call for the registration list and passenger manifest to determine the number of people on the terminal and on the vessel, and plan accordingly

Use the layout plan of the facility and of the vessel during the exercise in order to discuss the situation

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO
- SSO
- Security supervisor
- The competent authority

OBJECTIVES:

- Discuss how to organise the evacuation as efficiently as possible
- Agree on conventions for communication between the vessel, port facility and competent authorities
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 11}

Regulation 725/2004:

SCENARIO:
Specifically for passenger vessels and ferry services

ACTION 1: search for persons
On the news you hear a report about two wanted persons. The description seems to match two men you saw earlier on the facility. A check of the passenger manifest confirms the names of the people, and you immediately inform the police. In the meantime your security guards try to recognise the men among the crowd. The exercise can be carried out in collaboration with the vessel, with one of the men on the facility and one on board

ACTION 2: due to sabotage/power failure the entire scanning system goes down (table top)

- Determine how you will carry on inspecting the luggage
- Determine how you will carry on checking the passengers
- Determine whether there is an additional location that will enable you to split up the inspection/checking
- Determine how much additional surveillance is needed to carry out the task
- Estimate the probable delay, etc.

ACTION 3: search for suspicious packages
Leave a package lying on the terminal. Test the awareness of the security guards: do they notice the package? Do they follow the correct procedure, according to plan?

ACTION 4: While scanning the luggage, parts of weapons are found in four different bags. Each bag belongs to a different person. There are two vessels at berth and there are 280 people on the port facility, including 208 passengers
What steps do you take?

LOCATION:

- Entire facility

TOOLS:

- Tips & Tricks (9) (10)

PARTICIPANTS:

- PFSO, SSO, CSO (optional)
- Security guards
- Personnel with security tasks
- Person in charge of each department of the facility
- Assistance from the competent authority (optional)

OBJECTIVES:

- Create awareness
- Assure good collaboration and communication between terminal, vessel and competent authorities
- Provide adequate backup procedures
- Ensure that all procedures continue to operate without inconvenience for passengers
- Deal with unusual situations
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action.

ANNUAL EXERCISE 12}

Regulation 725/2004:

Specifically for passenger vessels and ferry services
All facility personnel with security responsibilities are instructed how to maintain higher vigilance at SL2 without worrying the passengers

SCENARIO

After a series of terrorist attacks against passenger/cruise terminals or ferry services in Europe, there are indications that the series of attacks will continue. For this reason all passenger, cruise and ferry services are advised to escalate to SL2

ACTION

The facility is expected to:

- Test all internal and external communication necessary for escalating the security level
- Test internal and external communications systems for communication with seagoing ships
- Test evacuation procedures
- Test emergency generators
- Test safety and security procedures
- Test how well personnel with security responsibilities are aware of the SL2 procedures to be applied by them
- Provide additional security guards / own personnel
- Use scanners + any backups
- Set up mobile barriers or perimeter as a security perimeter, if necessary
- Assure heightened vigilance for suspicious persons / actions
- Inspect ship's supplies and accompany them to the ship
- Access control: check vehicle registrations and/or personal details
- For passenger/cruise terminals: only permit essential vehicles to enter
- Test the CCTV system, if there is one
- Test the incident reporting procedure

Certain persons (appointed by the facility or by the authorities) must try to enter/infiltrate the facility in various ways and to look for weak points while SL2 procedures apply

LOCATION:

- Entire facility

PARTICIPANTS:

- PFSO, SSO, CSO (optional)
- Security guards
- Personnel with security tasks
- Person in charge of each department of the facility
- Assistance from competent authority (optional)

TOOLS:

- Security Questionnaire
- Port security awareness handbook
- Tips & Tricks
- Tests in the field

OBJECTIVES:

- Assure good internal and external communication between the various parties
- Assure good collaboration between the various parties
- Assure correct use of presence lists, crew lists and registers
- Check the time necessary for evacuation
- Check the time necessary for setting up mobile barriers or perimeter
- Assure correct operation of CCTV system, if there is one
- Assure awareness on the part of personnel
- Assure heightened security consciousness
- Check the procedures for security guards
- Check procedures at SL2
- Assure heightened collaboration
- Carry out a debriefing afterwards with all parties involved; draw up a list of points for action


HOME TERMINAL
MSC HOME TERMIN
MSC ELÂ

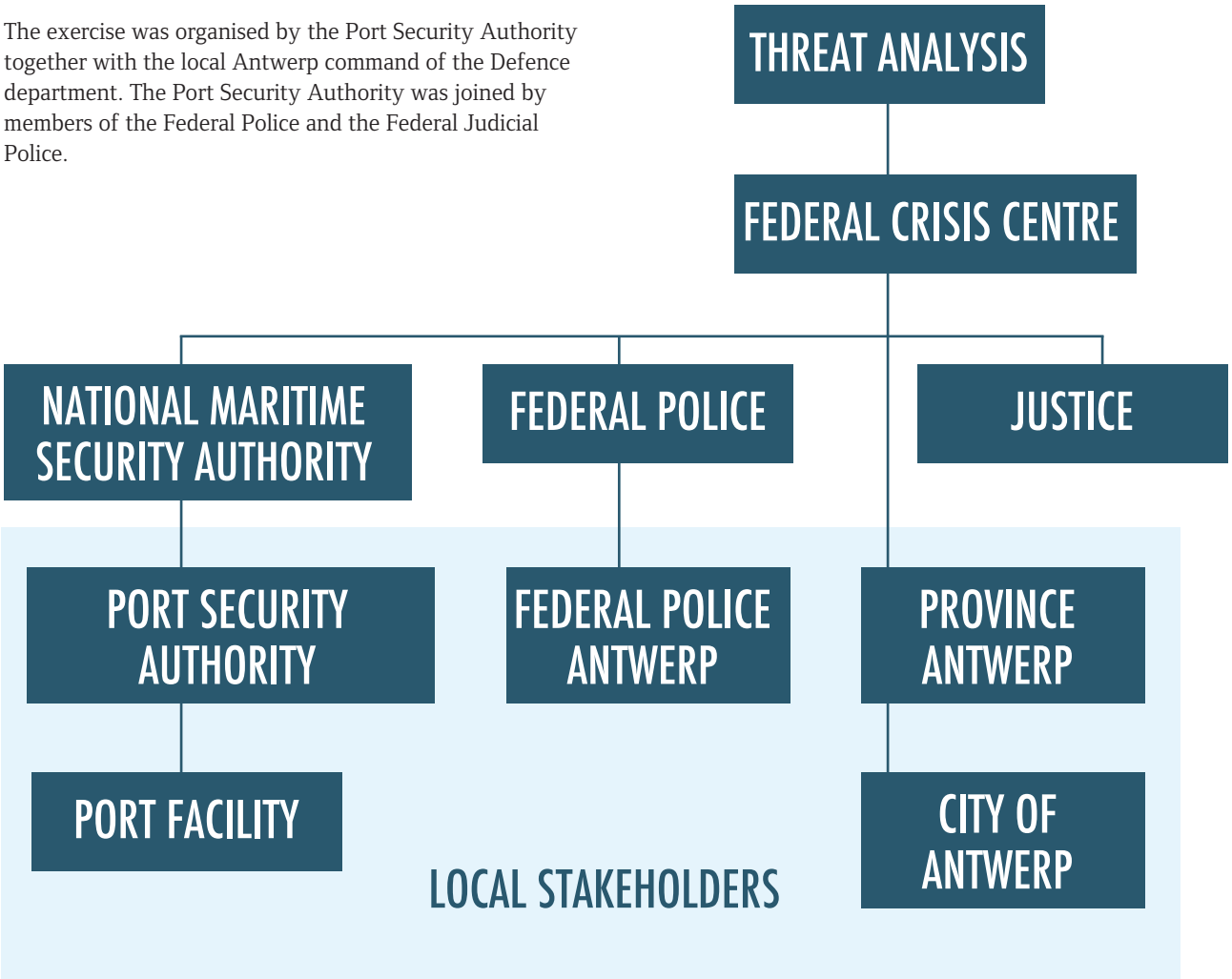


PSA
- Port Authority
- Maritime Police
- Local Police
- Customs
- Provincial Command (Defense)
- Sûreté de l' état

EXAMPLE:
COOPERATIVE SHIELD
an Antwerp port security exercise

INTRODUCTION

The exercise was organised by the Port Security Authority together with the local Antwerp command of the Defence department. The Port Security Authority was joined by members of the Federal Police and the Federal Judicial Police.



12 STEPS

At T-7 months the initiative was taken to organise a port security organisation with the support of Defence. It soon became clear that in reality a terrorist threat would lead to the alarm being raised with various authorities, each of which would play a role in dealing with a security incident.

It was therefore considered appropriate to at least take into account the input from these authorities and if possible to involve them in the exercise.
The authorities involved reacted positively, which led to the scope of the exercise being considerably expanded.
The general themes and the scale of the exercise were discussed at a kick-off meeting.

STEP 1

(In the following historical description of steps 1-12 a "narrative present tense" is used)

Define type and scale of the exercise

- Participating authorities:
  - PSA
  - Federal Police (Antwerp)
  - Province of Antwerp
  - City of Antwerp

- General themes
  - Testing the communication structure
  - Testing the protocols between various services
  - The security procedures of the various authorities oriented towards a maritime environment (test?)

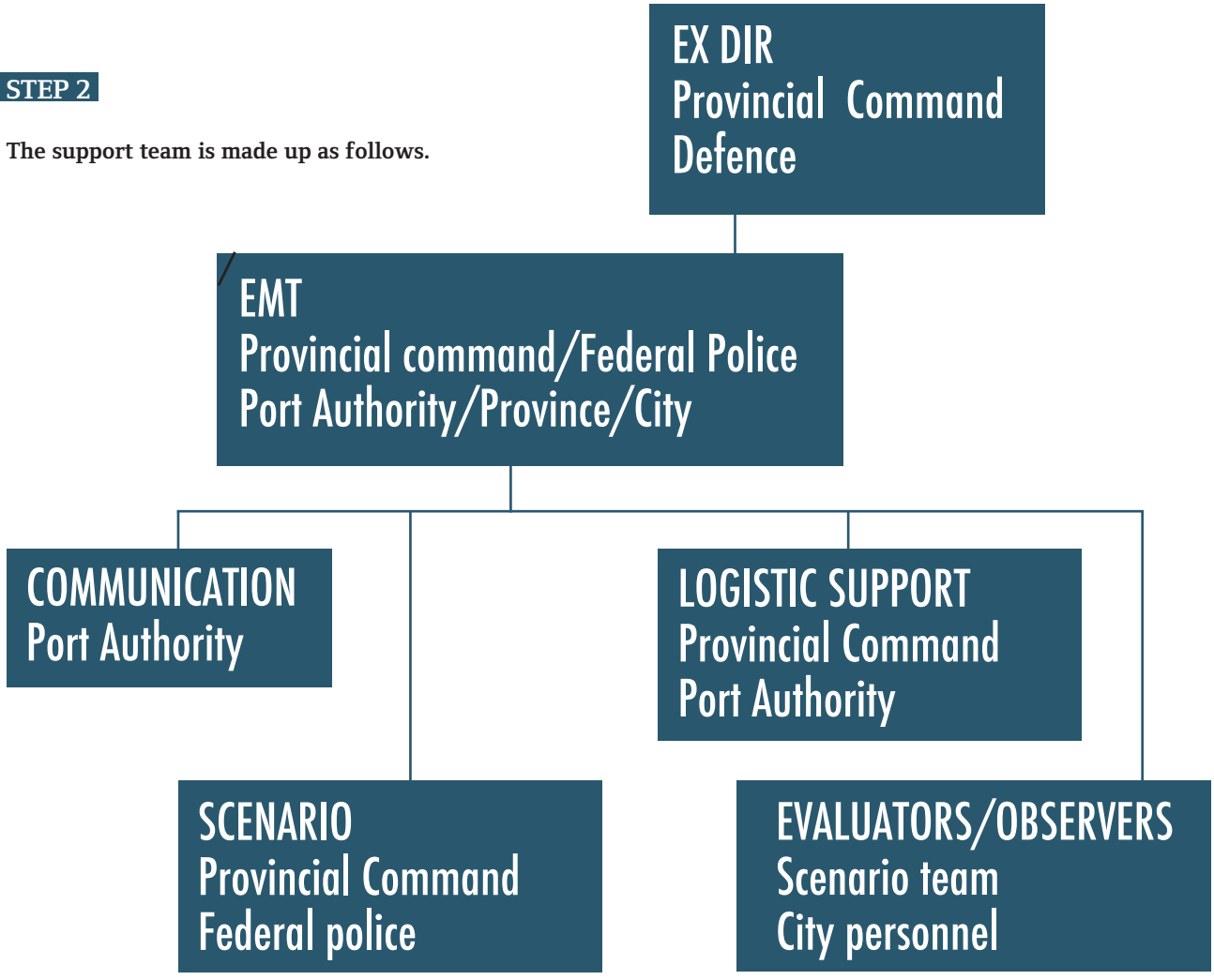
- Scope of the activities:
  - Table top + limited deployment on the ground
  - The focus is to lie on consultation between the various authorities. It is decided that Defence will carry out a reconnaissance of possible targets.
  - The exercise is to be played locally, with the central authority being simulated.

- Indicative period and time needed
  - It is agreed to hold the exercise in the autumn of that same year, over a period of 3 days, in order to deal with the objectives of the various participants. Since it is the first exercise of this type, it is also assumed that it will be necessary to hold the exercise without any pressure of time.

- Media
  - The initial guidelines are drawn up for media policy, with the communication officers of the various participating organisations being approached. The Port Authority communication officer is to act as contact point and coordinator.

STEP 2

The support team is made up as follows.



STEP 3

General and detailed description of the objectives

In this stage the exercise objectives of the different participants are outlined and compared with each other so as to arrive at a single corresponding list.

- PSA:
  1. Test the communication structure for port security
  2. Test the interaction with other services and evaluate the feasibility of the existing procedures
  3. Escalating the lock complexes (ISPS facilities):
     - Test communication
     - Test the feasibility of the security procedures
     - Investigate the impact on commercial operations

- FED. POLICE + MARITIME POLICE:
  1. Escalating the security level: communication
  2. Test support by "central support"
  3. Determine the feasibility/effectiveness of deployment on the ground

- FED. POL + DEFENCE:
  1. Test communication between the two
  2. Test the protocol for support by Defence
  3. Test the feasibility/effectiveness of deployment on the ground

- PROVINCE:
  1. Test communication
  2. Coordinating role

STEP 4

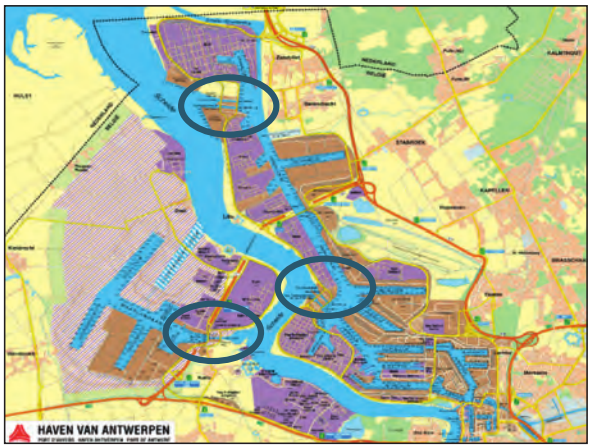
Develop a consistent scenario.

Based on information from international intelligence services, a report has been issued from which it is clear that a terrorist group has concrete plans to hit the Western economy and international trade through attacks on major ports and airports. Certain sources also state that the port of Antwerp could present a further strategic objective.

STEP 5

Simulation data

- A large quantity of explosive (400 kg of Semtex) disappears from a munitions depot in another country.
- A known, dangerous terrorist organisation calls for attacks against European port cities, in particular Antwerp.
- Plans are discovered mentioning lock complexes. (There are locks at three locations in the port of Antwerp: Zandvliet/Berendrecht lock complex, Boudewijn/Van Cauwelaert lock complex, Kallo lock.)



STEP 6

Draw up the MEL

The exercise is largely "free play."

- Draw up a situation with sufficient indications of a serious terrorist threat against the port, specially the locks:
  1. Munitions stolen in another European country (400 kg Semtex).
  2. Call by a known, dangerous terrorist organisation for strikes against European economic and logistics centres.
  3. Plans discovered in a house search, specifically targeting locks.

- Directives from ADCC (government crisis centre) => escalate to Level 3 (simulated).
- Port security plan activated for the threatened area
- Security mechanism activated by police + request sent to Defence
- Security mechanism further developed by police + support requested from Defence
- Support confirmed by Defence. Joint command structure outlined: rules for commitment
- Orders drawn up for police and Defence
- Command structure started up and tested, including demonstration and testing of technical assets
- Resources deployed on the ground (command element)
- Demonstration + press conference
- Hot wash-up

Example: Part 3 - Tools MEL

STEP 7

The Exercise Convention is drawn up and passed on to the various authorities.
Example: Part 3 - Tools Exercise Convention

STEPS 8 & 9

The evaluators are all member of the scenario team and are thus informed about the objectives.

STEP 10

The exercise

Security level 2 (day 1)

The Federal Service providing threat analysis, gives a report to the Federal Crisis Centre, indicating that the Port of Antwerp is threatened by an International Terrorist Organisation.
The Federal Crisis Centre decides to increase the port security and the security of the Antwerp Port Locks (ISPS facilities) to level 2.

Above mentioned is simulated "Provincial Command".
- The PSA meets at the indicated location (Port Authority Offices) and issues the escalation order to the port facilities.
- The procedures as described in the Port Security Plan for level 2 are initiated.
    - Extra patrols by the Maritime Police (Table top)
    - Extra checks by the Customs (Table top)
    - Close contact with PFSO

! IN TABLE TOP:
Check whether decisions taken can be carried out in reality!

- Keep National Maritime Security Authority informed (simulated).

Within the Port Security Authority, the Port Authority provides the necessary specific port related data:
Shipping information:
- ships in port
- ships underway (with previous ports)
- ships expected (with previous ports)
- follow-up traffic with harbour radar
- providing data supported by the geographical information system

Security level 3 (days 2 & 3)

Further information transmitted to the Federal Crisis Centre indicates that the threat has become imminent, consequently the threat level is raised to level 3.
(Simulated by "Provincial Command")

Day 2:
The PSA takes following actions:

- Instruct the port facility (the locks) accordingly.
- Escalate port security measures as described in the port authority plan. (tabel top)
    - Road blocks
    - Diversion of traffic
    - Access restriction of certain types of ships to the locks

The Federal Police and Defense agree a joint set of procedures, based on existing protocols, enabling defense to support the police efforts.

2 main actions are taken:

1. Reconnaissance of the 3 lock complexes by "Defense team"
    a. Identification of weak points
    b. Threat assessment
    c. Resources required

2. Inventarisation of required resources, provided by defense and police

Day 3:
Actual deployment of resources as planned on day 2.
A "Command Post Operation" is organised on the site of the "Zandvliet/Berendrecht Complex" and specific resources are demonstrated, such as:
- Remus sidescan sonar
- Infantry
- B-Hunter UAV (Unmanned Aerial Vehicle)

A press conference is incorporated in this stage of the exercise in order to give a general outline on port security and to emphases the cooperation between the several disciplines and authorities (province, city, port, port security authority)

At 11:15 am on day 3 the threat level is lowered to 1 and all parties are informed that the exercise has ended.

FROM: EX DIR
TO: ALL CONCERNED PARTIES
SUBJECT: END EXERCISE COOPERATIVE SHIELD
EXERCISE – EXERCISE – EXERCISE
11:15 AM: END OF EXERCISE
"SCENERY TO BE CLEARED, ALL UNITS BACK TO NORMAL DUTIES"
EXERCISE – EXERCISE – EXERCISE

STEP 11

The first debriefing (hot wash-up) is held on day 3, immediately upon conclusion of the exercise. This is essential to record first impressions. The information received is bundled with the subsequent reports from the evaluators or players. The final debriefing has been given on 13 November 2008 including a list of defined action points.

Conclusion of the exercise

There was no doubt that the exercise was a success. It is necessary to have regular consultation with the other police services involved, and to provide them with information. This exercise was a simulation; the question remains, how will the judicial system act in case of a real threat?

During the exercise it became clear that certain preventive measures (such as using side-scan to inspect ships) would have a serious impact on activities within the port. Data provided by the port authority can be used to screen out vessels which do not present a significant risk.

The GIS maps of the port contain a great deal of information that is of crucial importance for deciding the further course of events in case of a security problem.

The Port Authority has a state-of-the-art radar system which is an added value for security on the water side.

AN ORGANISATION CANNOT BE CRITICISED FOR A CRISIS HAVING OCCURRED, ONLY FOR THE WAY IN WHICH THE CRISIS IS DEALT WITH.

This exercise showed that Antwerp Port Authority can play a unique role in port security.

Furthermore, the Port Authority has invested in systems that can be of considerable use for security, namely the port radar and the camera surveillance in the docks.

The overall concept of port security is based on information; escalation to a higher level is imposed by the federal crisis centre on the basis of information received by the threat analysis. All decisions that were taken during the exercise were based on information obtained.
The port is a provider of information to the authorities in charge, during a crisis, by making the radar and camera images available and sharing the data from the APICS system.




tie
Poli




GEEN TOEGANG
VOOR
ONBEVOEGDEN
ZEER GEVAARLIJKE
ZONE
Bij werkzaamheden:
veiligheidshandschoenen
Gemeentelijk Havenbedrijf
Antwerpen
Over de blauwe streep: zwemvest

part 3
TOOLS



TIPS & TRICKS
to improve your security





1/Put up barriers by dismantling

During drills and exercises you can simulate particular situations by issuing a message an alternative to implementing the security measures in reality.

When raising the security level it is possible to be creative by "dismantling" certain accesses to the facility.

Set up barriers ...

By being creative and using materials available on the site – such as goods and vehicles – it is possible to quickly set up a physical barrier and deploy a perimeter in a simple and effective way.

By using large, heavy objects – such as big bags or containers – it is possible to close off the front end of the quay, thus raising a physical barrier so as to create a marked-off area when the security level is raised.

2/... with big bags





3/... with containers





Vehicles that happen to be available can also be used as a gate. In this way the marked-off area can still be kept available for movements of persons – by vehicle or otherwise – who are essential for the operation of the facility.







5/Deploy additional personnel

During drills and exercises it is possible to use your own members of personnel and/or extra personnel to carry out additional checks when the security level is raised.

Make sure that these extra people have the necessary resources such as mobile phones, walkie-talkies, contact lists, important telephone numbers, cameras, extra batteries etc. so that they can keep in contact at all times with the right person(s) without having to leave the place where they are told to be operational.

4/TAILGATING

One way of gaining access to a facility is by driving very close behind another vehicle which is permitted to enter. In this way it is possible to get inside the facility with an unauthorised vehicle.





This operation may be part of an exercise. It will check whether security personnel are keeping a proper watch.

6/Use visual means to announce a heightened security level

By being creative and using the resources available within the facility it is possible to make the security level known visually.





Use an electronic message board to announce the heightened security level.

When the security level is raised, use an electronic message board to announce that additional checks are being carried out. This will help to make the security operations at the entrance go more smoothly.

7/Watch out for inconsistencies

Always be on the lookout for inconsistent or contradictory situations on the workfloor! The members of personnel are the most familiar with the work environment, so they are the ones who are most likely to notice if something is out of place. You should therefore give them a contact point or contact person to whom they can report the situation.



8/Identification procedure

Try to obtain confidential information about access procedures by talking to security guards or members of personnel, either personally or on the phone. Claim to be from some organisation and ask questions about the company, guards etc.
Ask for various security documents, e.g. the security manual, the security incident form, list of contact persons, bomb alarm report form etc.

Do they know about these documents? Can they find them quickly? Are the available documents up to date?

In this way it is possible to check whether security guards and/or members of personnel react in an alert way when people who do not belong to the facility/company ask for confidential information and try to obtain documents.



9/IDENTITY SWAP

Be alert and on the lookout at all times!

Y ≠ X and X ≠ Y

Person X registers at the gate according to the access procedure, showing some form of identity. Pay attention to the person's physical appearance, and make sure they resemble the ID photograph.
It is quite possible for people to swap identities, and for person Y to take the place of X, because they resemble one another.





10/WATCH OUT FOR UNATTENDED VEHICLES OR PACKAGES

Be alert and on the lookout! If you notice an object or vehicle that seems to be out of place in your workplace or work environment, report it to the security staff or your immediate superior! In most cases the object or vehicle will not pose any threat, but a healthy dose of awareness – without being paranoid – is always a good thing.





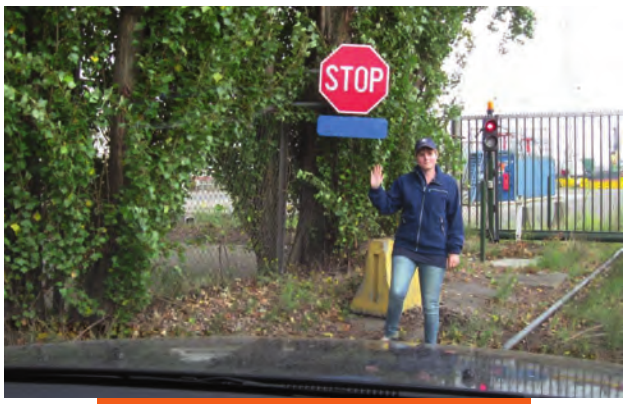


11/Getting a lift in a vehicle

One of way of gaining access in an unorthodox way and at the same time testing the alertness of the security personnel is to do the following during a drill or annual exercise.

Stop a truck on the way to the facility, a few hundred meters away from the gate.

Try to convince the driver that you want to test the alertness of the security personnel as part of an ISPS exercise, and ask him to drive you through the gate.



This is one way of checking whether the security guards know the procedures and follow them correctly.

12/Gain unauthorised access to the facility







It's only a "window of opportunity," but by using the cover of a large vehicle it can sometimes be very easy to evade the security and so gain unauthorised entry to the facility.

13/USE A WIDE-ANGLE MIRROR TO CHECK FOR OBJECTS

People reporting at the gate when entering the facility sometimes leave objects behind, out of absent-mindedness. But in some cases objects may be left behind deliberately! It should be second nature for the security guard or porter to check for such objects.

A wide-angle mirror is a very useful tool for detecting objects that may or may not be suspicious.



14/Use available resources to close gates

By being creative and using materials available on the site – such as goods and vehicles – it is possible to quickly set up a physical barrier and deploy a perimeter in a simple and effective way when the security level is raised.

Large, heavy objects such as big bags as well as handling equipment, pallets etc. can be used to close off gates and doors.





15/Create lock gates

To maintain maximum control of people and vehicles when the security level is escalated, a vehicle or vehicles can be used to create a set of lock gates, with only one person or vehicle being allowed through at a time.

In this case the vehicle is used both as a gate and as a physical barrier, so as to keep a security zone accessible for people or vehicles that are essential for operation of the facility.

16/This is a breach

During drills and exercises you can simulate particular situations by posting a message to represent an abnormal situation.

Existing damage can be marked with text, so that it can be visualised as part of a drill or exercise!



17/Advance notice of arrival of persons with vehicle

Advance notice may be given of the arrival of persons in a vehicle, but that doesn't mean they should be allowed in without any check! There must always be some form of visual check when they arrive at the gate, before they are allowed to enter the facility.





18/Keep your perimeter fence unobscured

Don't let nature compromise your security! Always keep your perimeter fence free of weeds and growth. That way you can always spot weak points or damage, not to mention unauthorised persons trying to gain access





TESTS
in the field

1/ Try to gain access to the facility by getting a lift with a truck driver.

2/ Look for places where the perimeter fence is damaged, in order to get in.

3/ Try to impersonate somebody at the reception.
Try to use someone else's identity card/access pass.
Plant a dummy access pass at the reception area.

4/ Use some sort of excuse to gain access to the facility. For example:

- Use the internet to find out the name of someone who works there. Say that you have a present for him or her.
- Set up a website for a fake company, giving yourself a false identity as a member of the company. Use this to arrange a visit to the facility, and try to gain access this way.

5/ Try to drive in by tailgating another vehicle.

6/ Try to gain access at the reception, knowing perfectly well that you will be refused. Act upset and challenge security, eventually simulate that you are speaking another language.

7/ Leave a briefcase, package or other object behind at the reception area.

8/ Show undue interest in the facility: take photographs, use binoculars, hang around, ask specific questions about the working of the facility, etc.

9/ With one or more other people, get someone to start a conversation with the security guards/reception in order to divert attention, while another person tries to get in without registering, e.g. by slipping under the barrier.

10/ "Infiltrate backwards": try to get in by working your way against the flow of people coming out, during an evacuation or when a shift is coming off duty.

11/ At security level 2: get one person to drive in, registering normally, but with another person hiding behind the seats or in the boot.

12/ At a smaller entrance or turnstile (not the main entrance/, try to get someone to badge you in, with the excuse that you have lost or forgotten your own badge.

13/ Observe the rail entrance to the facility. Use the time between the train entering and the gate closing behind it in order to nip into the facility.

14/ Try to get more than one person into the facility (on foot or by vehicle/ by badging in with only one access pass. For example, use the blind angle of the camera, if there is one.

15/ Observe the facility and try to discover which barge is moored there. Claim to have some relationship with the bargee or the barge company: family member / insurance agent / surveyor or whatever, in order to gain access.

SECURITY QUESTIONNAIRE

Facility: _____

Name of security firm: _____

N° of personnel: _____

Presence: _____

Tick "yes" or "no" according to whether the question is answered correctly or not.

At what security level is the terminal operating?	☐ *Yes* ☐ *No*
Can you give us the name of the PFSO?	☐ *Yes* ☐ *No*
Do you have the details of the backup PFSO?	☐ *Yes* ☐ *No*
Do you have written procedures for ISPS security?	☐ *Yes* ☐ *No*
Can you demonstrate these procedures?	☐ *Yes* ☐ *No*
Do you have forms to report bomb warnings?	☐ *Yes* ☐ *No*
Which procedure do you follow in case of bomb warnings?	☐ *Yes* ☐ *No*
Which procedure do you follow whenever someone tries to gain access to the facility (on foot or by vehicle) without any form of identification (incident reporting)?	☐ *Yes* ☐ *No*
Which procedure do you use to report an incident?	☐ *Yes* ☐ *No*
Can you give some examples of incidents?	☐ *Yes* ☐ *No*
Can you explain the difference between security levels 2 and 3?	☐ *Yes* ☐ *No*
Are dangerous substances stored or handled in this facility? If so, do you have a list of these substances?	☐ *Yes* ☐ *No*
Can you show us a list of these dangerous substances?	☐ *Yes* ☐ *No*
Do you use a system of advance notice of arrival?	☐ *Yes* ☐ *No*

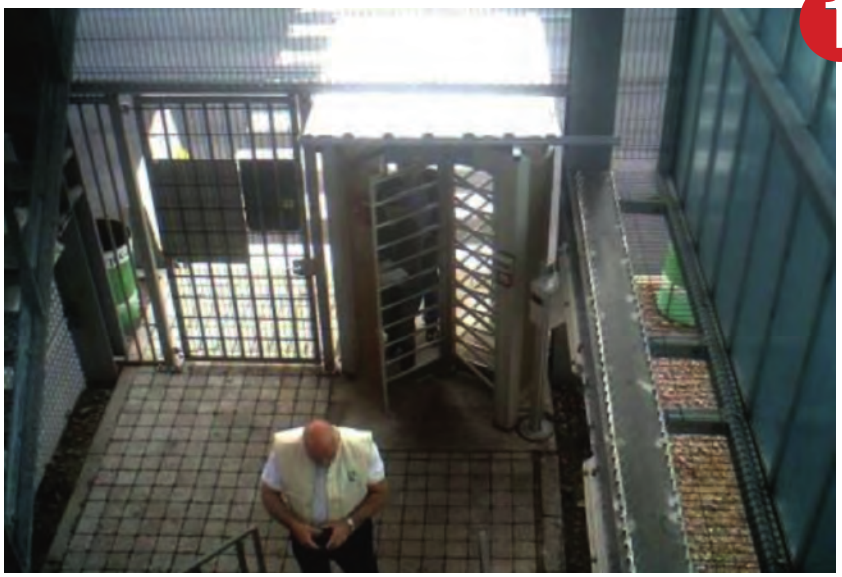
SECURITY QUESTIONNAIRE

Can you show us this procedure?	☐ *Yes* ☐ *No*
What procedure to follow if the cameras suddenly fail at night?	☐ *Yes* ☐ *No*
Can you demonstrate the possibilities of the CCTV system?	☐ *Yes* ☐ *No*
Have you followed specific training in ISPS and/or maritime security?	☐ *Yes* ☐ *No*
Where and when did you follow this training?	☐ *Yes* ☐ *No*
Did you take any exams?	☐ *Yes* ☐ *No*
Which procedure do you use for moving a suspicious package to a safe place?	☐ *Yes* ☐ *No*
If such a situation occurs, how do you react?	☐ *Yes* ☐ *No*
Do you have a procedure concerning shore leave for ship's crews?	☐ *Yes* ☐ *No*
Do you have crew lists of ships at berth?	☐ *Yes* ☐ *No*
Do you have a system for recording people and vehicles (PC, forms etc.)?	☐ *Yes* ☐ *No*

BREACHES OF SECURITY

Set up a report of your findings:

1



2



3

4

5

SOLUTIONS:

1. Two people entering together through the turnstile
2. The fence is holed
3. A suspicious package
4. A stranger is taking pictures of the terminal (note the licence plate of the car)
5. Gate blocked by a stone

"PORT SECURITY AWARENESS"

Handbook

Table of contents

Part 1 – Introduction
- The objective of this handbook
- How to use this handbook?

Part 2 – Threats to the maritime security
- Common threats within the maritime industry
- Why are ships and port facilities sensitive to criminal activities
- Techniques to circumvent security measures
- How can You, as a port employee, help to prevent illegal situations!

Part 3 – Dangerous goods, and products which may be used for illegal activities i.e. terrorism
- Recognise dangerous goods
- Recognise dangerous (illegal) items
  - Bombs and explosives
  - Weapons
- Which action can You, as a port employee, undertake!

Part 4 – The Port Facility Security Plan
- The definition of the threat levels and consequent the requirements.
- The objectives of the Port Facility Security Plan
- Means of communication
- What is your task, as a port employee

Part 2 – Fitting security measures
- Recognise suspect behaviour
- Recognise suspect containers
- Report suspect behaviour and/or suspect activities
- Fitting measures
- Access control
- Security rounds
- Illumination
- Evacuation, crowd control
- What is Your input, as a port employee

"Security Awareness Quiz"



PART 1/INTRODUCTION

What will You read in this part:
- The objective of this handbook
- How to use this handbook?

The objective of this handbook
This handbook has been created for all people legally active within the port and/or on a port facility.

This handbook aims to clarify the necessity of a proper port security as described within the regulation 725/2004 and the directive 2005/65 and to povide information to the reader about:

- Maritime security threats
- Recognise dangerous goods and dangerous products which may be used for terrorist activities
- Facts about the port facility security plan
- Fitting security measures
- Recognise persons and techniques who and which are aimed at circumventing security measures and might pose a threat.

How to use this handbook
Read it attentively at least once and subsequently answer the questions from the quiz. You may confirm having read and understood the handbook by entering name and date on the bottom of the quiz and sent the completed form to the Port Facility Officer.

When in doubt about certain aspects of this handbook, the Port Facility Officer can provide the necessary answers.

Coordinates PFSO

Name:
Tel:
Mob:
E-mail:

PART 2/THREATS TO THE MARITIME SECURITY

What will You read in this part:
- Common threats within the maritime industry
- Why are ships and port facilities sensitive to criminal activities
- Techniques to circumvent security measures
- How can You, as a port employee, help to prevent illegal situations!

Common threats within the maritime industry

Theft of cargo, pilferage and petty theft:

The yearly loss of revenue due to theft can amount up to several millions of Euro's. People, gaining illegal access to the port facility may well steal personal effects from the people active on the facility (dock labour, stevedores….). Money, mobile phones and other electronic devices, identity cards…etc., but also port facility equipment and documents. Cargo theft or pilferage has a negative influence on the reputation of Your port, which may have an impact on choices made for a specific port.
Petty theft an pilferage may also come from people actually having a legal job in the port.

Stowaways:

Stowaways try to get on board of a ship in order to reach the country "of their dreams". When a stowaway is found on board of a vessel, the shipping company operating that vessel will be held responsible.
It is essential that the port facility pays due vigilance during cargo operations with ships which are sensitive to such illegal actions.

Smuggling:

Your facility may eventually be used to ship/discharge illicit drugs, stolen goods, weapons… etc. It is a known fact that terrorist organisations use the vastness of the maritime industry to transport their goods.
For whatever final aim, smuggling is a dubious activity with a negative impact on the reputation of the port.

Sabotage:

Action carried out by one person or a group of persons with the purpose of damaging the port and/or a port facility.

Internally:
- sabotage by a disgruntled member of personnel
- Personnel from sub-contractors who gain access to systems and/or procedures which may be used for later illegal activity on the site.

Externally:
- Terrorists may use a port facility as a base to carry out a raid on a ship or on another (more sensitive) port facility.

Terrorism:

There are over a hundred definitions of "Terrorism", but this one is rather good:

> **"The use or intended use of violence against persons or material for ideological or political reasons, with the aim to reach its goal through terror, intimidation or threats."**

Terrorism is a potential threat to the maritime industry, because ships and/or port facilities may be used to:

- Hide explosives in the cargo
- Smuggle terrorists and/or weapons to the intended target
- Cause economic and/or environmental damage to the port
- Take hostages
- Serve as a diversion for a target at another location
- Steal dangerous goods for the production of explosives

All mentioned threats will additionally cause aggression, vandalism and intimidation.

There are at least four ways how a port facility may be affected by acts of terrorism:

1. The facility is the target of a terrorist or a terrorist organisation
2. The facility (dangerous goods, products) may be used as a tool for an attempt at another location.
3. The facility loses revenue through terrorist activity in the vicinity
4. The facility may be infiltrated by radicalised personnel.

Why are ships and port facilities sensitive to criminal activities?

The global playing field and the immense quantity of goods handled are an attraction pole for criminal activity and possible terrorism alike.

- Port facilities, even properly secured as defined by the regulation, are big surfaces in which a high quantity of goods and people move around.
- Port facilities and ships may be seen as "symbols" of a "higher" class or as instruments of "super powers" and as such, form a possible target.
- Not every single piece of cargo is checked, nor at departure nor at arrival.
- A port is a concentration of many people, but mainly a great amount of good (of which a respectable part id dangerous).

Techniques to circumvent security measures

Criminals and terrorists will try to circumvent the security measures by:

> Hang around in the vicinity of the facility in order to observe personnel movements and procedures.
> Gaining information about the facility. This can be done by taking pictures, drawing out plans and/or asking questions to personnel.
> Claiming to be personnel or a sub-contractor in order to gain access to the facility
> Sabotaging access points (gates, doors, fencing) at remote spots.
> Telephone and/or mail personnel in order to gain information about security procedures on the facility.
> Posing suspect packages in order to check the response of the personnel.
> Trying to drive along with trucks delivering cargo or sub-contractors….
> …



How can You, as a port employee, help to prevent illegal situations!

Actively participate within an operational port security, including regular drills.
A proper "security awareness" is essential to protect the facility and the personnel against criminal and/or terrorist activities

WHAT CAN YOU DO:

- Report security equipment failures (lightning, gates, fences, cctv…) The PFSO is responsible for properly maintaining and repairing this equipment.
- Recognise suspect and threatening situations and report to the PFSO
- Avoid illegal access to the facility by consequently keeping doors and gates which should be locked, that way.
- Do not hesitate to ask the PFSO for further guidance.

PART 3/DANGEROUS GOODS, AND PRODUCTS WHICH MAY BE USED FOR ILLEGAL ACTIVITIES I.E. TERRORISM

What will You read in this part:
- Recognise dangerous goods
- Recognise dangerous (illegal) items
- Bombs and explosives
- Weapons
- Which action can You, being active in the port, undertake!

Recognise dangerous goods

Certain dangerous goods, whether in bulk or packed (crates, barrels, pallets, containers) require extra vigilance for those handling these goods.

These dangerous goods may, in the wrong hands, be used as a weapon, either for making explosives, either to cause harm to people or to instigate environmental damage (which is also economic damage).

The maritime industry handles a huge amount of dangerous goods (HAZMAT= Hazardous Materials). These goods must be labelled.
For some more sensitive materials, a specific training is required.
When in doubt ask your superior to properly inform you whether there are any specific requirements.

Have due attention for strangers in the vicinity of these goods, and always wear the required protective clothing and equipment.
Always warn the PFSO when suspect people and/or situations are observed in the vicinity of dangerous goods. (see also part 5)



Class 1
Explosives



Class 2.1
Flammable Gas



Class 2.2
Nonflammable Gas



Class 2.3
Poisonous Gas



Class 3
Flammable Liquids



Class 4.1
Flammable Solids



Class 4.2
Spontaneously Combustible Solids



Class 4.3
Dangerous when Wet



Class 5.1
Oxidizing Agent



Class 5.2
Organic Peroxide Oxidizing Agent



Class 6.1
Poison



Class 6.2
Biohazard



Class 7
Radioactive



7
Fissile



Class 8
Corrosive



Class 9
Miscellaneous



P
Marine Pollutant

1. Explosives: may be fixed, liquid or gas. These products may explode through shock or friction, thus not only by ignition through fire or spark. Fireworks are a an example that is commonly transported by container.
2. Flammable gasses, such as LPG.
3. Flammable liquids, such as Petrol.
4. Fixed flammable products, some of which may ignite spontaneously or even through contact with water.
5. Oxidising goods, may combined with a flammable product, form an explosive mixture (Ammonium Nitrate is an oxidising product)
6. Poisonous goods, may cause bodily harm through oral intake, inhalation or skin contact.
7. Radioactive goods
8. Corrosive goods can affect other products and cause severe burns to humans. Inhalation of the fumes is also very dangerous.
9. Diverse goods, not classed in one of the above, but which constitute a risk.

Recognise dangerous (illegal) items:

Bombs, explosives IED
(Improvise explosive device)

Any item, package, luggage, which stands out or is located where it does not belong, should be considered as suspect.

These objects will be placed near :
- Public places, because they are easily accessible and disposing of the package has less chance of being noticed
- Places where a maximum of damage can be caused, near mess rooms, in the vicinity of dangerous goods

At the least doubt, contact the PFSO for further instructions.

What You shouldn't do:
> Stay near the object
> Use your cell phone, Walkie-Talkie or other transmitting device in the vicinity of the object.
> Touch or remove the object to another location

The PFSO will alert the authorities, who will take further action as appropriate.
Make sure that You are familiar with the facility's evacuation procedures.

Rule of thumb; If You cannot identify the item, report it.

Weapons

Within the EU, laws and regulations concerning the carriage of weapons is very strict.
For most weapons, a license is needed to own the weapon. Some (automatic) weapons are definitely forbidden.
In most EU countries only the police, the military and some private security (money transport) are allowed to carry a weapon.
Ask your PFSO which laws are applicable.
People, not belonging to one of the above, may be assumed to pose a threat.

Weapons include:
- Fire arms, automatic weapons, handguns…
- Knives, daggers, throwing stars…..
- Explosives (grenades..)

WHICH ACTION CAN YOU, AS A PORT EMPLOYEE, UNDERTAKE!

! Know which kind of cargo is a normal commodity in Your facility

! Immediately report suspect items

! Report people carrying forbidden weapons (almost everybody except the police)

PART 4/THE PORT FACILITY SECURITY PLAN

What will You read in this part:
- The definition of the threat levels and consequent the requirements.
- The objectives of the Port Facility Security Plan
- Means of communication
- What is your task, as a port employee, in the port.

The definition of the threat levels and consequent requirements:

- **Security level 1:** means the level for which minimum appropriate protective security measures shall be maintained at all times.

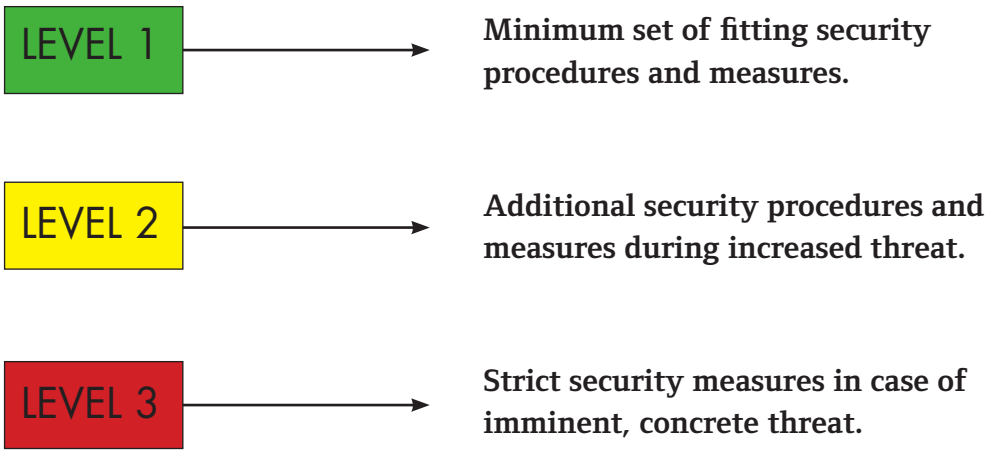
- **Security level 2**: means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

- **Security level 3:** means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Level1 is not intended to actually stop a terrorist, but it will turn the target (You port facility) into a harder target. A potential terrorist will have to prepare a lot more and eventually spend more in the process. This increases the exposure and the possibility of being notice by the intelligence community.

Level 1 is the everyday level. The decision to increase the level is taken by the National Authority responsible for port facility security and port security.
On threat levels 2 and 3, the security efforts are gradually increased and an active participation from the authorities is included.

The three threat levels are the common denominator throughout the port facility security plan.



The objectives of the port facility security plan

> Ensure fitting access control procedures
> Improve and follow-up security on the site
> Protect employees and visitors
> Protect the ships moored alongside
> Protect the port facility and the equipment
> Protect the cargo

It is important to be aware of the security level at which Your port facility is operating!

Means of communication

The port facility has the necessary means to alarm and communicate during an increased threat level.

Communication systems:
> Telephone
> Cell phone
> E-mail
> Signals
> Walkie-talkie
> Loudhailer (for smaller facilities)

WHAT IS YOUR TASK, AS A PORT EMPLOYEE

While carrying out Your normal tasks, You should be attentive for unusual (suspect) items and/or persons at your professional location.

Ensure that the material with which You are working is in a good condition, and that the necessary checks are being carried out.

! Know the security level of the facility

! Know your tasks at each security level

! If You are unsure about Your tasks or You have a question, contact the PFSO.

PART 5/FITTING SECURITY MEASURES

What will You read in this part:
- Recognise suspect behaviour
- Recognise suspect containers
- Report suspect behaviour and/or suspect activities
- Fitting measures
- Access control
- Security rounds
- Illumination
- Evacuation, crowd control
- What is Your input, being active in the port

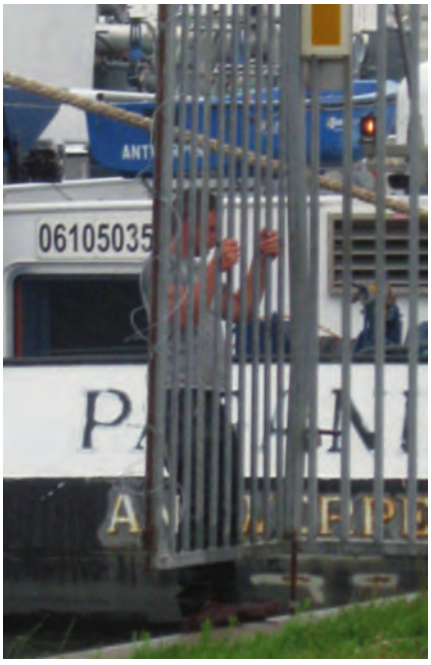
Recognise suspect behaviour

Following elements may be considered suspect behaviour

> Wide clothing not appropriate to the season/weather conditions
> purposefully adapting the clothes when being observed
> Suspect forms within the clothing (hidden weapon)
> taking pictures of the facility, drawing plans, observing
> Aiming to avoid the security system
> Aiming to get access to the facility
> Questioning people about the security measures
> Any activity which does not fit in the normal professional pattern of the area







Recognise suspect containers

There are already international initiatives in place to track suspect containers, but this does not mean that alertness is superfluous.

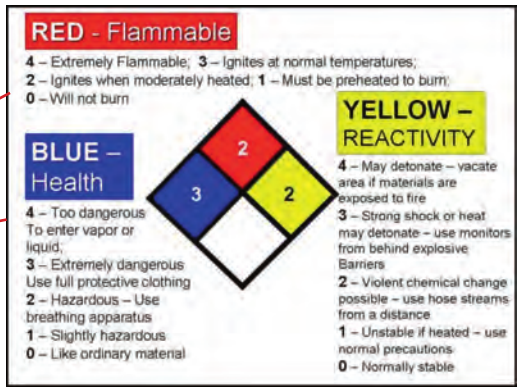
You can help by reporting suspect containers by watching for

> Unusual smell and/or sounds
> Traces of food and/or domestic rubbish in the vicinity of the container
> Holes in the container or adhesive tape on the container (hiding holes)
> Container numbers that does not match the manifest
> Wrong HAZMAT label for the declared cargo
> Seal missing or damaged



HAZMAT LABEL

AND/OR



Report suspect behaviour and/or suspect activities

Within port areas, the PFSO's should report security incidents to the authorities.
Suspect persons or cars noticed today, may already have been noticed before and give rise to establishing a pattern.
Proper and timely information by the port facilities is helping authorities to identify and prosecute illegal activities.

Whenever You are underway to or from the port facility, it may happen that you observe something suspect (even an abandoned car), report this to the authorities.

When in doubt while observing people behaving suspiciously, always think about Your own safety first. When the person does not belong

on the facility, alert the security guards and/or the PFSO.
When the situation is safe You may inquire about the person's business. At the least sign of unruliness refrain from insisting and take a distance.
When You have a colleague nearby, it is good practise to ask him/her to observe from some distance.

TIP

In case it is safe to inquire about the person's business, remain calm and ask open ended questions.

Example:

- **Good Question: Where do you come from?**
- **Bad Question: Are you coming from (name of ship)?**

In the bad question, the answer may simply be "yes", leaving no room for further questions without raising suspicion.

Fitting measures

Access control

> Supervision of doors and gates
> Identity checks
> Check of luggage, toolboxes, ...
> Report lost access identification cards

Security rounds

> Supervision on the key, warehousing and at ship's berth
> Check remote places on the facility which may be hiding places
> Be clearly present and alert

Lighting

> A proper lighting on the whole facility is a very good deterent for illegal activity.

Evacuation, crowd control

The port facility has evacuation procedures

> Know the emergency exits and an alternative route
> In case of alarm, proceed promptly to your allocated assembling point
> Remain calm, react promptly and helps your colleagues when required
> Do not return unless clearly allowed by the authorities and the facility's management.

WHAT IS YOUR INPUT AS A PORT EMPLOYEE

! Integrate safety and security into your daily activities

! Report suspect behaviour and/or suspect objects immediately

! Be alert!

"Security Awareness" Quiz

Right or wrong:

1. Stowaways, sabotage and terrorism are common threats in the maritime industry. Y/N
2. Port facilities are possible terrorist targets. Y/N
3. Some cargo may be harmful to people and/or the environment Y/N
4. Terrorism is a criminal offense with a political purpose. Y/N
5. All port facilities are well protected against acts of terrorism. Y/N
6. Criminals may gather information by asking questions and taking pictures. Y/N
7. Explosives and petroleum products are dangerous. Y/N
8. It is advisable that you remove any suspect package to a safe location. Y/N
9. The security levels are the common denominator for the Port Facility Security Plan. Y/N
10. The PFSP of your facility describes the security tasks and the responsibilities. Y/N
11. You need to be aware of the current security level. Y/N
12. In case of a bomb threat, search operations are only carried out by the employees. Y/N
13. Suspect situations may be, unadapted clothing, uncommon activities in the dock. Y/N
14. Container are always safe, as they are all inspected. Y/N
15. Your discreet presence is an added value for security. Y/N
16. You smell an unusual aroma, almost like almonds, do you call the PFSO? Y/N
17. Darkness scares thieves. Y/N

Describe:

18. Security Level 1: ....
    .....
    .....
19. Security Level 2: .....
    .....
    .....
20. Security Level 3: .....
    .....
    .....

CONFIRMATION "SECURITY AWARENESS"

I have read and understood the "security awareness handbook".
I have answered the 20 questions correctly.

Facility: .....

Signature employee: date: .....

PFSO: date: .....

SUSPECT BEHAVIOUR

Criminals, including terrorists, cannot be recognised by age, gender, colour of skin or religion. Selection based on these criteria is also illegal.
Criminals, including terrorists, may be recognised by their behaviour.

Organised crime such as terrorism, is based on preparation. Targets will be observed in order to find out the security procedures. When these actions are being noticed, compelling the criminal to suspend his actions, the relevant information will be an added value to proper law enforcement. Additionally it may well have averted the criminal's plans.

Suspect people can be recognised through the way they behave. In many cases, suspect people stand out, people tend to have a "feeling" about situations without being able to define why someone is suspect.
There are a number of behaviour patterns which may draw the attention, however, one should keep on using sound judgement.

- Appearance. Clothing may be not be in line with the actual weather conditions (baklava during summer, sunglasses while it is raining…) or with the environment (no proper safety clothing…). Very wide clothing, showing forms that indicate something is hidden. Persons equipped with tools which clearly do not belong in the environment (wire cutters, shovel, big bags..). People in the process of changing appearance (with a beret, sunglasses, coat, change of hair style…) without a proper reason.
- Conspicuous behaviour. This may include; taking pictures, drawing plans of the facility, observing the facility during an extended period (from a car), eventually with the use of binoculars. There is also a possibility that criminal observers will try to test the alertness of the security in place by attempting to enter the facility (bumper busting, using someone's badge, crawling under or dodging the barriers..). Unfamiliar people walking around on the facility are obviously to be considered suspect. People on the facility or in the vicinity ignoring safety requirements (such as telephoning near a chemical installation where it is clearly marked as forbidden). Any other activity which is out of line with the common activities.
- Implicit conspicuous behaviour. This may include; Nervousness, aggressive behaviour. This can be observed :
  - Looking around continuously
  - Slightly shaking
  - Avoiding eye contact
  - Sweating

It is obvious that not everybody who is acting nervously has to be considered a suspect. But when nervousness combined with the fact that the person is not familiar with the surroundings occurs, it is advisable to inquire about the purpose of the visit with some open questions, as indicated below.

> **Do not hesitate to report suspect situations to Your PFSO**

Address person:
When a person shows suspect behaviour, an employee can, when considered safe to do so, address the person. When two employees are in the vicinity, it is advisable that one of them stays at a distance and observes the conversation. If there are signs of aggressive behaviour, the observer should call for assistance and help his colleague.

A short conversation may clarify a suspect situation. It is good practice to calmly ask open ended questions.

NOT open ended: Are You coming from the ship alongside our quay ?

Open ended: Where do You come from?
Can I help You ?
Can You find Your way around ?
Do You have an appointment ?

Do not give an indication that you are suspecting something. When the situation during the conversation evolves towards aggression from the interviewed person (may start with person being irritated), remain friendly and calm, take a distance and warn the PFSO.
Avoid aggression and certainly don not respond to it.

Persons with legitimate reason for being on the Port facility will normally respond calmly and will remain polite.
During the conversation, some peculiarities may be observed, indicating a suspect situation :

- The person interviewed is not making eye contact, he/she may be looking around a lot or may be staring or looking at the interviewer but fixing on another part of the body (chin, arms , chest).
- The person does not give a clear answer, changes the subject, is absent minded.
- Takes with an abnormally high voice, is stammering or quivering. Loses the subject.
- The person makes a change of stance. This can be taking a step backward (may indicate fear) or a step forward (may indicate aggression) and or clenching and unclenching the fists.
- Some other indications from the person may be; breathing harder, sweating, changing facial colour (red or white), shaking, producing a "tick" and/or arteries in the throat region and/or the face which start to throb notably.
- The whole facial expression may indicate that the person interviewed is ill at ease with the situation.

In short, behaviour that clearly deviates from what is common during a normal conversation should be noticed, but also the context must be taken into account (if this is a candidate waiting for an application interview, it might be normal that he/she is nervous).
When in doubt, report to the PFSO. The information given to the PFSO should be as complete as possible ; colour of hair, stature, average age, eventual scars….
If a car can be linked to the person, it is important to not the license plate and the nationality of that plate.

Their main purpose is to protect the port facility, the ship and all legitimate people present on the premises, as well as the cargo and the personal effects from the people.

CARGO INSPECTIONS

SEAL INSPECTION

Seal verification and inspection process:

The **VVTT seal inspection** Process is a good example of one:

V – View seal & container locking mechanisms
V – Verify seal number for accurancy
T – Tug on seal to make sure it is affixed properly
T – Twist & Turn seal to make sure it does not unscrew



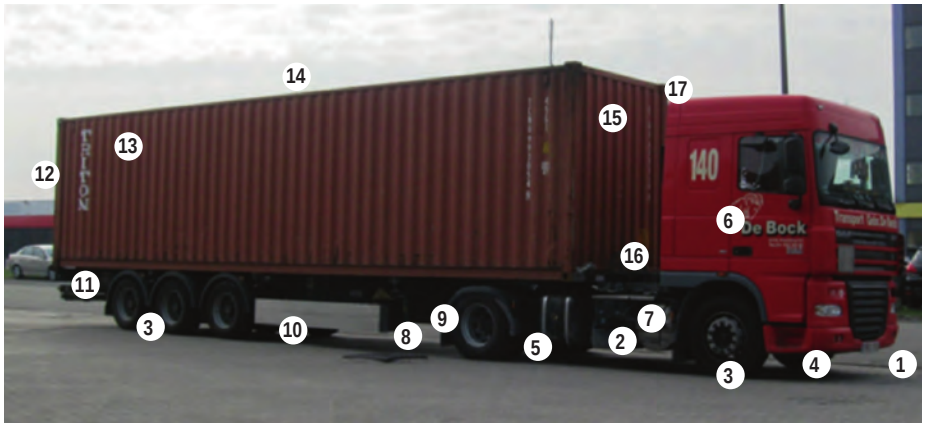
7-POINT CONTAINER INSPECTION

1. Outside/undercarriage (before entering facility)
2. Inside/outside doors
3. Right side
4. Left side
5. Front wall
6. Ceiling/roof
7. Floor (inside)



17-POINT TRUCK & TRAILER INSPECTION

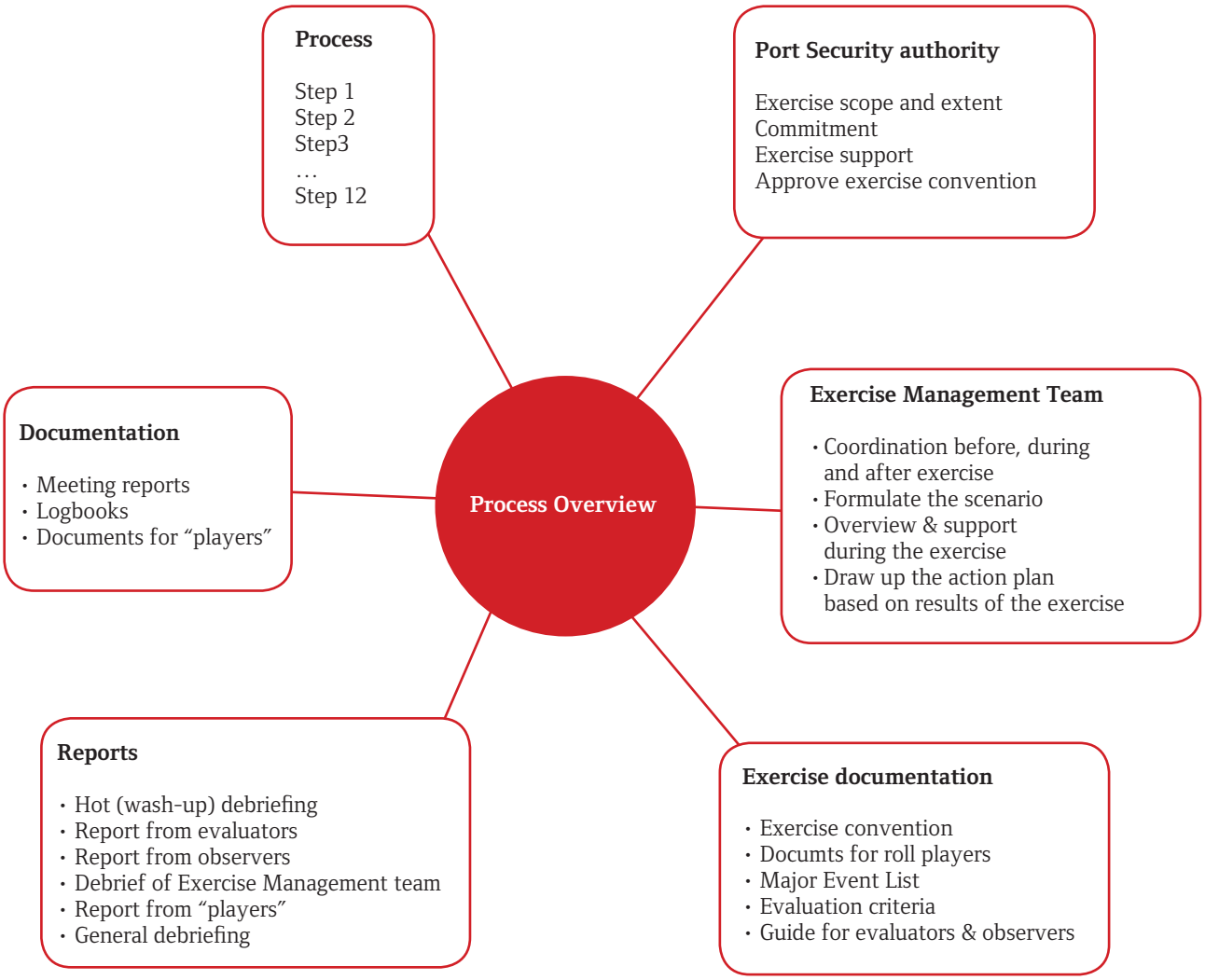
1. Bumper
2. Engine
3. Tires (truck & trailer)
4. Floor
5. Fuel tanks
6. Cab/storage compartments
7. Air tanks
8. Drive shafts
9. Fifth wheel
10. Outside/undercarriage
11. Floor
12. Inside/outside doors
13. Side walls
14. Ceiling roof
15. Front wall
16. Refrigerated unit (if present)
17. Exhaust



PORT SECURITY EXERCISE



MIND-MAP


Process
Step 1
Step 2
Step3
…
Step 12
Port Security authority
Exercise scope and extent
Commitment
Exercise support
Approve exercise convention
Documentation
• Meeting reports
• Logbooks
• Documents for "players"
Process Overview
Exercise Management Team
• Coordination before, during and after exercise
• Formulate the scenario
• Overview & support during the exercise
• Draw up the action plan based on results of the exercise
Reports
• Hot (wash-up) debriefing
• Report from evaluators
• Report from observers
• Debrief of Exercise Management team
• Report from "players"
• General debriefing
Exercise documentation
• Exercise convention
• Documts for roll players
• Major Event List
• Evaluation criteria
• Guide for evaluators & observers

COOP MEL

Nr	Timing	Event	Action	Results	Clarification
1	3 Oct08	message: explosives stolen	none	none	simulated message from intelligence agency
2	5 Oct08	message: motor yacht stolen	none	none	simulated message from intelligence agency
3	10 Oct08	message: writings of terrorist organisation found mentioning Port of antwerp	none	none	simulated message from intelligence agency, national threat
4	14 Oct08	message: plans of Port of Antwerp found with lock locations highlighted + added symbols	coördination between intelligence agency (threat analysis) and Federal Crisis Centre	decision to increase threat level to: 2	simulated situation. Situation only applicable to Port of Antwerp
				prepare warning cascade	only for Port of Antwerp and Provincial Administration
		coördinate with Federal Police HQ (FPHQ)	FPHQ sends instructions to Federal Police Antwerp (FPA)		
		warning Port Security Authority			
5	14 Oct08	message from National Crisis Centre to Federal Police HQ	FPHQ sends instructions to Federal Police Antwerp	actions from FPA	message regarding increased threat level, including messages from 03, 05, 10 and 14 Oct 08 (see 1, 2, 3, 4)
6	14 Oct08	message from FederalCrisis Centre to National Authority for Maritime Security and to Port Security Authority	members of the PSA warned and invited to meeting	instructions to affected port facilities.	message regarding increased threat level, including messages from 03, 05, 10 and 14 Oct 08 (see 1, 2, 3, 4)
7	14 Oct08	message from Federal Crisis Centre to Province of Antwerp	advice to city		message regarding increased threat level, including messages from 03, 05, 10 and 14 Oct 08 (see 1, 2, 3, 4)
			meeting at Provincial Crisis Centre		

EXERCISE CONVENTION

1. General outline
1.1. Mandate
1.2. General objectives
1.3. Exercise
1.3.1. Name
1.3.2. Period
1.3.3. Kind of exercise
1.3.4. Theme
1.4. Organisation
1.4.1. Exercise direction
- Ex Dir
- Exercise Management Team
1.4.2. Evaluation of exercise
- Evaluators
1.4.3. Observers (optional)
1.4.4. Participating disciplines
- On the field
- Table top
1.4.5. Non participating disciplines
1.4.6. Non participating, simulated disciplines
1.5. Communication
- Local community
- Media
- Bystanders

2. Course of the exercise
2.1. Scenario
(no detail, only general outline)
2.2. Timing
2.3. Location(s) of the exercise
2.4. Agreements
2.4.1. Use of messages
2.4.2. (…)
2.4.3. Identification of non players
2.5. Start of the exercise
2.5.1. Modalities (start signal)
2.5.2. Scenery at location
2.5.3. Set up of players: place, date and hour
2.6. Break-off exercise
2.6.1. Modalities/Break-off/re-start/
code words
2.6.2. Re oriëntactions (evt. to fit objectives)
2.6.3. Real incident
2.6.4. Real intervention
2.7. End of the exercise
2.7.1. Modalities (codeword/signa and
communication)
2.7.2. Action of participants
(debriefing “hot wash up”)
2.7.3. Clean up scenery, recondition to normal
2.8. Communication organisation
2.9. Measures taken to deal
with the (real) press

3. General information
3.1. Recommendations for participants
3.1.1. Conduct
- Motivation
- Respect for the infrastructure
3.1.2. Access restrictions, action restrictions
3.2. Logistics
3.2.1. Transport/Parking
3.2.2. Clothing
3.2.3. Equipment
3.2.4. Supplies, Catering
3.3. Safety
3.4. Insurrance

4. Specific information by discipline
4.1. Specific objectives (optional)
4.2. Means (personel and equipment)
deployed
4.3. Additional clarifications (optional)

QUESTIONNAIRE
on Audits for exercises



1/PREPARATION:

general questions concerning the period before the exercise

1. Keeping up knowledge and skills
   a. Have arrangements been made for personnel with security responsibilities to keep the necessary knowledge and skills up to date?
   b. To what extent are these arrangements followed?
   c. Are the staff concerned sufficiently aware of the applicable security procedures?
   d. Is everybody familiar with the role and tasks that may be assigned to him/her if the security level is escalated?
   e. If not, what are the reasons for this? (E.g. not selected for training or instruction, content of tasks forgotten due to the time between exercises being too long, etc.)
   f. To what extent has everybody received training specifically concerned with (maritime) security?
   g. Does the way in which the organisation makes use of its staff sufficiently stimulate them and give them recognition in achieving the maritime security objectives?

2. Degree of security practice of personnel
   a. What arrangements have been made for practising, and how are they put into practice?
   b. Do the staff concerned practice their own role and tasks separately?
   c. Have back-up personnel also practiced the tasks that may be assigned to them?

3. Version management of the Security Plan
   a. What arrangements have been made for managing the versions of the Security Plan?
   b. Is version management carried out in accordance with these arrangements?
   c. Have the arrangements proved sufficient?
   d. Are modifications to plans and procedures passed on to the competent authorities?

2/PRE-START:

questions concerning the moment at which the signal for the exercise if given, raising the alarm and escalation

1. Start signal
   a. Who gives the start signal for the exercise (internal or external signal)?
   b. If external: who receives the signal and takes action?
   c. What are the procedures? Are they laid down in writing? How are they made known?
   d. If in accordance with the procedures: to what extent do they work properly (or not)?
   e. If not in accordance with the procedures: how does that work out?

2. Availability and ability to be contacted
   a. Are the laid-down procedures followed?
   b. Is it clear who has to be immediately informed? Who is/are these persons? Looking back, were they the right persons?
   c. How long does it take for everybody to be informed?
   d. Can the necessary members of personnel be contacted easily? If not: where and how does it go wrong?
   e. Are the members of personnel available? (E.g. are they able to travel to the location where they are required?)
   f. Are there problems with employees travelling to the location where they are expected?

3. Accommodation and facilities for crisis team
   a. Is there a room directly accessible and fully equipped to house a crisis team?
   b. Does this room have the necessary facilities, such as e-mail, PC capacity, whiteboard, flap over, beamer, phone and fax (either in the room itself or directly accessible)?
   c. Can the crisis team communicate sufficiently well with the operations and -if necessary- with the competent authorities?
   d. Does everything function as desired? If not, what are the difficulties?

4. Transfer of information in the early stages
   a. How are all those concerned informed about the exercise?
   b. Do they all receive the correct information?
   c. Does the communication process go as planned?

3/START:

questions concerning the functioning of the security organisation

1. Composition of security organisation
   a. Is there immediate consultation within the security organisation about the procedures to be followed? Does everyone agree?
   b. Are there problems with the staffing of the security organisation (e.g. people absent, discussion about who takes charge of what, etc.)?
   c. Does everyone have a clear role within the security organisation?
   d. To what extent is the composition of the security organisation clearly laid down and fully described in the Security Plan?

2. The Port Facility Security Officer
   a. Does the PFSO update the security procedures as necessary?
   b. Is he/she satisfied with the team?
   c. Does he/she make corrections in good time if non-relevant facts/events/questions arise?
   d. Does the PFSO monitor the decision-making process? (Defining action to be taken, compliance with agreements, checking that the right procedures are followed, checking that the right people are informed?)
   e. Does the PFSO take over the final decision if the meeting or debriefing results in different options?

3. Personnel with security tasks
   a. Do members of personnel with security tasks also assume the responsibility that they have by virtue of their position?
   b. Are they sufficiently aware of their tasks and authority, and those of other people concerned?
   c. Do they take the initiative in carry out tasks in the course of the exercise?
   d. Do they have the correct attitude? Do they contribute to thinking about the situation?

4. Meeting discipline
   a. During meetings and/or debriefings concerning the exercise, do those taking part keep to a clear order?
   b. Is there an agenda? Who keeps it?
   c. Is attention paid to:
      i. Feedback concerning points for action previously defined
      ii. Determining the actual situation
      iii. Deciding and writing down points for action
      iv. Points for attention concerning communication and information

4/DECISION-MAKING:

questions concerning the decision-making process

1. Situation reporting
   a. Are members of personnel with security responsibilities adequately informed about the current situation, so as to draw the correct conclusions?
   b. Are they adequately informed about how the exercise went, so as to draw the correct conclusions?
   c. Are the conclusions drawn from how the exercise actually went sufficiently clear and relevant for decisions to be taken?
   d. Is the decision-taking sufficiently well supported by a standard situation report?

2. Vicinity management
   a. Are outside stakeholders and authorities informed in good time about the exercise, in case of evacuation or escalation?
   b. Is "in good time" experienced as such by these parties?
   c. Are stakeholders involved in the decision-making process?
   d. How is this achieved? What do the stakeholders think about it in practice?

3. Other aspects
   a. Given the specific circumstances of the exercise, is it possible to determine whether certain skills are lacking so as to be able to form a good judgement about the correct approach?
   b. How well does the support work? (E.g. shift timetable, back-up persons, availability of offices and other rooms, ability to reach key locations, etc.)

5/INFORMATION:

questions concerning information and communication

1. Information strategy
   a. Is there a strategy for how to deal with information and communication during the course of the exercise?
   b. Are there any gaps? If so, distinguish according to:
      i. Media information
      ii. Informing external parties: neighbours, visitors, contractors, collaboration partners etc.
      iii. Internal information

2. Media information
   a. Are press conferences held?
   b. How are they prepared?
   c. What is the attendance response?
   d. What is the result in terms of written/audiovisual journalism?
   e. What impression is given by the press conference approach?

3. External information
   a. Which external parties are informed?
   b. Is that sufficient, or do others need to be included?
   c. Which means are used to provide information to external parties?
   d. Does the organisation provide sufficient information for these external parties?
   e. What is the response to the information?

4. Internal communication
   a. Are the sections of the organisation that are not involved in the exercise informed of what is going on?
   b. What is done to tell these sections of the organisation to continue with normal business operations?
   c. Is the intranet site used for internal communication on the subject of security and exercises?

6/FOLLOW-UP:

questions concerning ending the exercise and follow-up

1. Ending the exercise
   a. Who decides when the exercise comes to an end?
   b. How does he/she make this known?
   c. Are particular steps required to return to the previous level of security?

2. Debriefing
   a. Is a debriefing held at which all those involved are given the opportunity to state their first-hand opinion of the approach followed during the exercise?
   b. Does the person responsible for the exercise take the initiative for a systematic evaluation of the approach taken and how the exercise went?
   c. Are arrangements in place for all those involved to see the results of the evaluation?
   d. Are arrangements in place to check how the agreements made are complied with some time later?

3. Follow-up
   a. To what extent is decided that provisional measures taken during the exercise should be included in the Security Plan?
   b. Are there aspects that require further follow-up? (E.g. further improvement measures, information etc.?)

PAMPHLET (example)



EXERCISE OF THE PORT SECURITY – REACT AS FORESEEN.

OEFENING VAN DE HAVENVEILIGHEID – HANDEL ZOALS VOORZIEN.

EXERCICE DE LA SECURITE DU PORT – REAGIR COMME PREVU.

Port of Antwerp

PORT SECURITY
HAVENBEDRIJF
SECURITE DU PORT

DECLARATION OF SECURITY

Name of ship _____

Port of registry _____

IMO number _____

Name of Port Facility _____

This declaration of security is valid from: _____ until : _____

for the following activities : _____

under the following security levels: Securitylevel(s) for the ship: _____

Securitylevel(s) for the port facility: _____

The port facility and the ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

The affixing initials of the SSO or PFSO underthese columns indicates that the activity will be done, in accordance with relevant approved plan, by:

ACTIVITY	PORT	SHIP
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily		
available between the ship and port facility		

The signatories to this agreement certify that the security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of the Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at _____ on the : _____

Signed for and on behalf of

The port facility : The Ship:

Name: _____ Name:_____

Title: _____ Title: _____

Contact details

Fort the port facility :

Address: _____

_____

_____

Tel : _____

Fax : _____

PFSO : _____

e-mail : _____

For the ship :

Master:

_____

Ship Security Officer:

_____

Company:

_____

Company Security Officer

_____

TELEPHONE BOMB THREAT FORM

INSTRUCTIONS:

STAY CALM. STAY COURTEOUS. LISTEN. DO NOT INTERRUPT THE CALLER.

NOTIFY SUPERVISOR / POLICE OFFICER OF THE SITUATION BY PREARRANGED SIGNAL WHILE CALLER IS ON THE LINE.

DATE: _____ / _____ / _____

INFORMATION ON CALL

Date: _____ Time: _____ Duration: _____

Phone number called: _____

Name of person receiving the call: _____

Phone number to call for follow up: _____

QUESTIONS FOR CALLER *(Try to ask these questions and document responses)*

When will the bomb explode? _____

What kind of bomb is it? _____

What will cause the bomb to explode? _____

Where is the bomb located? _____

What does the bomb look like? _____

Did you place the bomb? _____

Why did you place the bomb? _____

Where are you now? _____

What is your name? _____

Document exact wording of threat: _____

_____

INFORMATION ON CALLER

Gender of caller:

☐ Male ☐ Female

☐ Unknown

Approximate age of caller:

_____

Does the voice sound familiar:
If yes, who does it sound like?

_____

DESCRIPTION OF CALLER: *(Check all that apply)*

Voice

☐ Clean
☐ Distorted
☐ Hoarse
☐ Loud
☐ Muffled
☐ Nasal
☐ Pitch-High
☐ Pitch-Med
☐ Pitch-Low
☐ Pleasant
☐ Raspy
☐ Smooth
☐ Soft
☐ Squeaky
☐ Unclear
☐ Other

Speech

☐ Accented
☐ Deliberate
☐ Distinct
☐ Fast
☐ Hesitant
☐ Lisp
☐ Slow
☐ Slurred
☐ Stuttered
☐ Other:
☐ If Accented, Describe:

Language

☐ Educated
☐ Foreign
☐ Foul
☐ Intelligent
☐ Irrational
☐ Rational
☐ Slang
☐ Taped/Recorded
☐ Uneducated
☐ Unintelligible
☐ If Foreign, Describe:

Behavior

☐ Agitated
☐ Angry
☐ Blaming
☐ Calm
☐ Clearing Throat
☐ Crying
☐ Fearful
☐ Intoxicated
☐ Laughing
☐ Nervous
☐ Self-Righteous
☐ Other

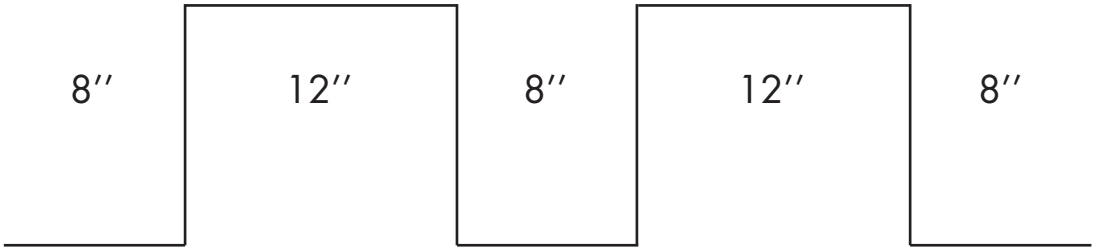
Background Noise

☐ Airport
☐ Animals
☐ Baby
☐ Birds
☐ General Noise
☐ Guns Firing
☐ Gymnasium
☐ Machinery
☐ Motor
☐ Music
☐ Party
☐ PA System
☐ Quiet
☐ Restaurant
☐ Static
☐ Street Noise
☐ Talking
☐ Tavern/Bar
☐ Television
☐ Traffic
☐ Train
☐ Typing
☐ Water/Wind
☐ Other

ALARM SIGNALS

WARNING SIGNAL

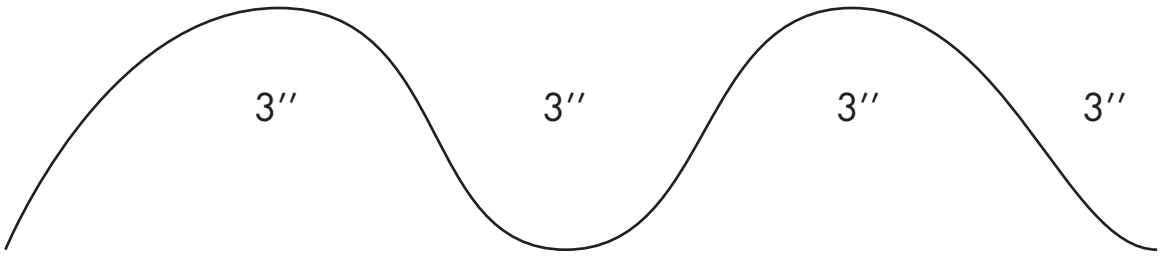
STOP WORKING, CLEAR PASSAGE!



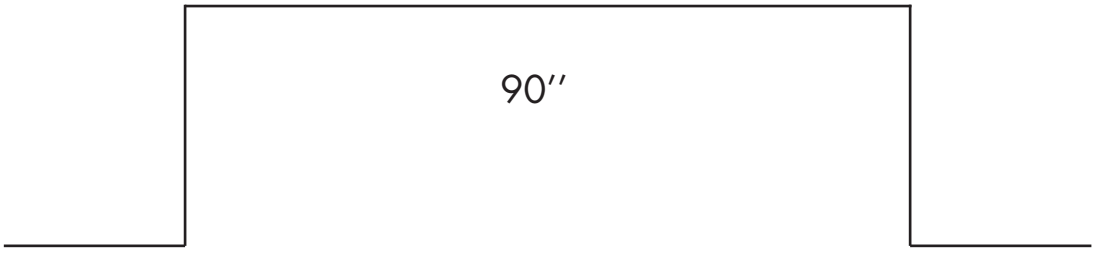
EVACUATION ALARM

GO TO YOUR ASSEMBLING POINT!





END OF DANGER



EVACUATION SIGNALISATION



EMERGENCY EXIT
RIGHT DIRECTION



EMERGENCY EXIT
LEFT DIRECTION



LOCATION
EMERGENCY EXIT



EMERGENCY EXIT RIGHT



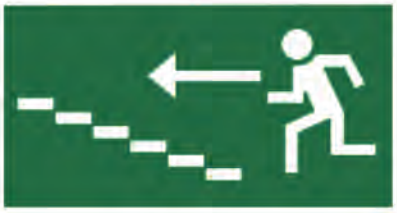
EMERGENCY EXIT LEFT



DIRECTION OF
EMERGENCY EXIT



EMERGENCY EXIT
STRAIGHT



ESCAPE STAIRS DOWN
TO THE LEFT



ESCAPE STAIRS DOWN
TO THE RIGHT



EMERGENCY EXIT
RIGHT DIRECTION



EMERGENCY EXIT
LEFT DIRECTION



LOCATION
EMERGENCY EXIT /
EMERGENCY EXIT

RESCUE FACILITIES



STRETCHER



EYEWASH



EMERGENCY SHOWER



PHONE FOR RESCUE AND FIRST AID



FIRST AID POST



DIRECTION INDICATION (RESCUE FACILITIES BOARD)



ASSEMBLAGE (FOR PERSONNEL)



POINT FOR RESCUE AND FIRST AID



RESCUE LADDER

SAFETY FIRST !!!

Watch out for the signs:

- Round signs (red) show what is prohibited ("You must not …").
- Round signs (blue) show what is obligatory ("You must …").
- Triangular signs are danger warnings ("Watch out for …").
- Square signs (green) indicate safety or emergency equipment.
- Square signs (red) indicate firefighting equipment.

The square signs (safety/firefighting) in particular are very important for preventing and reacting to accidents or disasters: they show where help is to be found.

prohibited





NO SMOKING



NO MP3 PLAYERS



NO MOBILE PHONES

obligatory





SAFETY BOOTS



HARD HAT



HI-VIS JACKET

danger





EXPLOSIVES



ACID OR CAUSTIC



BIO-HAZARD

safety equipment





DECONTAMINATION SHOWERS



FIRST AID



EMERGENCY PHONE

fire fighting





FIRE HOSE



EXTINGUISHER



EMERGENCY PHONE


LIBRA COPACABANA
MONROVIA
IMO 9326835
Seaco


CSAV
SPN 06

part 4
BACKGROUND

BIBLIOGRAPHY

Following publications have been consulted in order to complete this handbook:

- Antwerp Harbour Master's office, Isps Drill and exercise manual, Antwerp 2008
- Antwerp Harbour Master's office, Port Security Awareness handbook, Antwerp 2009
- Evelien Van Soest, Security Awareness in the Port of Antwerp (in dutch), Antwerp 2011
- European Parliament and Council, Directive 2005/65/EC on enhancing port security, 26 October 2005
- European Parliament and Council, Regulation EC 725/2004 on enhancing ship and port facility security, 31 March 2004
- Federal Police Belgium, Contingency exercises guide (in dutch), Brussels 2009
- Ilse Van Mechelen, Provincial Exercise policy, 2008
- UK, TRANSEC, Drills and exercises guidance, London 2008
- Collaboration on public safety for Zeeland, Questionnaire on audits for exercises and disasters, version 1.1, 28 August 2003
- University of St. Andrews, Certificate in Terrorism studies, August 2007
- Workgroup Exercise Policy Province of Antwerp, Training in organization exercises (in dutch), September 2011
- C-TPAT Supply Chain Security in a New Business Environment, Container and Seal Inspection Workshop (ppt.)

ABBREVIATIONS

Reg.	Regulation (EC) No 725/2004 of the european parliament and of the council of 31 March 2004 on enhancing ship and port facility security
Dir.	Directive 2005/65/EC of the european parliament and of the council of 26 October 2005 on enhancing port security
ADCC	Government/Federal Coordination and Crisic Center
APICS	Antwerp Port Information Control System
CCTV	Closed-Circuit Television
CPX	Command Post Exercise
CSO	Company Security Officer
DOS	Declaration Of Security
EMT	Exercise Management Team
ESA	Equivalent Security Arrangement
Ex Dir	Exercise Director
Fed Pol	Federal Police
FPA	Federal Police Antwerp
FPHQ	Federal Police Head Quarter
FTX	Field Training Exercise
GIS	Geographic Information System
HAZMAT	Hazardous Materials
ISPS	International Ship and Port facility Security
MEL	Major Event List
PAX	Passengers
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PSA	Port Security Authority
PSO	Port Security Officer
PSP	Port Security Plan
SEVESO	Seveso II Directive: Council Directive 96/82/EC, extended by the Directive 2003/105/EC
SL1	Security Level 1
SL2	Security Level 2
SL3	Security Level 3
SOLAS Convention	Safety Of Life At Sea Convention
SSO	Ship Security Officer
SSP	Ship Security Plan
UAV	Unmanned Aerial Vehicle
WMD	Weapon of Mass Destruction