
Roadmap to provide more proactive and efficient Computer Emergency Response Team training



SECURITY

Roadmap to provide more proactive and efficient Computer Emergency Response Team training

Follow ENISA on

 [Facebook](#)  [Twitter](#)  [LinkedIn](#)
 [YouTube](#) and  [RSS feeds](#)

Contact details

To contact ENISA for this report please use the following details:

Email: opsec@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent the state of the art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2012

Disclaimer: The views and opinions expressed in this document are from experts from the CERT Community and other relevant stakeholders. The document does not necessarily reflect the position of ENISA.

Contributors to this report

This roadmap was originally written under contract, by the following authors:

Mirosław Maj, ComCERT, Poland

Don Stikvoort MSc(Hons) CTNLP, S-CURE, The Netherlands.

They were supported within their team by the following experts:

Dr. Tomasz Chlebowski, ComCERT, Poland

Dr. Klaus-Peter Kossakowski, PRESECURE Consulting, Germany

Michael Potter BA, S-CURE, USA

Mirko Wollenberg CISSP, PRESECURE Consulting, Germany.

Alan Thomas Robinson BSc (Hons) MIET, Northern Ireland.

Agreements or Acknowledgements

During the first half of 2012, the following experts contributed to the ideas and concepts which led to creation of this roadmap:

Dr. Wim Biemolt, SURFnet

Jim Buddin, TERENA

Dr. Serge Droz, SWITCH

Sven Gabriel, GRID community, Nikhef

Chris Gibson, CITIbank

Jaap van Ginkel, University of Amsterdam

Peter Haag, SWITCH

Tilman Haak, DFN-CERT

Christian van Heurck, CERT.be

Xander Jansen, SURFnet

Przemek Jaroszewski, CERT Polska

Mark Koek, FOX-IT

Adrian Leuenberger, SWITCH

Prof. Manel Medina, ENISA

Kevin Meynell, TERENA

Dr. Claudia Natanson, Global Corporate Executive Program

André Oosterwijk, NCSC-NL

Martin Peterka, CZ.NIC

Peter Peters, University of Twente

Wayne Routley, DANTE

Aidan Ryan, CSIRT-IE

JP Velders, University of Amsterdam.

The following expert acted as an external reviewer of this roadmap:

Alan Thomas Robinson BSc (Hons) MIET, Northern Ireland.

The target audience of this report is:

ENISA;

the European CERT community as assembled in TF-CSIRT and the Trusted Introducer; interested members of FIRST, the worldwide CERT forum;

professors/lecturers in the field of Information Security working for European universities;

companies/institutions specialising in training and

courses in the area of Information Security;

ENISA Permanent Stakeholders' Group;

ENISA Management Board, composed of representatives of the Member States, the Commission and of the Stakeholders;

all other interested audiences.

Contents

| | | |
|-----------|--|-----------|
| 1. | Executive summary | 8 |
| 2. | Introduction and background | 12 |
| 2.1. | Objectives of the report and description of work | 12 |
| 2.2. | Methodology used | 13 |
| 3. | Legal and policy basis | 16 |
| 4. | Proposals: how ENISA can provide more proactive and efficient CERT training | 20 |
| 4.1. | ENISA support to the TRANSITS Framework and other suitable training programmes | 20 |
| 4.2. | CERT Exercises at universities | 23 |
| 4.3. | ENISA as co-provider of CERT trainings and trainers | 27 |
| 4.4. | CERT Training Information Desk | 30 |
| 4.5. | Video material by ENISA – how to organise the exercises? | 32 |
| 4.6. | ‘Fire Drills’ for the CERT community | 34 |
| 4.7. | ENISA CERT Training Hubs (ECTH) | 37 |
| 4.8. | ENISA CERT Exercises Certified Provider (ECTCP) | 41 |
| 4.9. | Recommendations for public administration organisations (national exercises) | 44 |
| 4.10. | Certification Paths | 47 |
| 5. | Implementation strategy | 54 |
| 5.1. | Evaluation metrics | 54 |
| 5.2. | Benefit versus effort | 55 |
| 5.3. | Implementation timeline | 57 |
| 6. | Summary of proposals | 60 |
| 7. | Conclusion | 64 |
| 8. | Annex I: Abbreviations | 66 |
| | Annex II: Survey questions (overview) | 68 |

List of Graphs & Tables

| | |
|---|----|
| Graph 1: Average perceived value of various trainings..... | 22 |
| Graph 2: Percentage of respondents desiring specific scopes of fire drills..... | 46 |
| Graph 3: Certification path 1 – existing exercises..... | 48 |
| Graph 4: Certification path 1 – new exercises..... | 48 |
| Graph 5: Certification path 2 – existing exercises..... | 49 |
| Graph 6: Certification path 2 – new exercises..... | 49 |
| Graph 7: Certification path 3 – existing & new exercises..... | 50 |
| Table 1: Evaluation metrics for various proposals..... | 55 |
| Graph 8: Benefit versus effort for various proposals..... | 56 |
| Graph 9: Overall timeline for implementing proposals..... | 57 |

1

Executive summary

1

Executive summary

Until 2012, the efforts of ENISA, with regard to the *training* of Computer Emergency Response Teams (CERTs), were mostly focused on supporting the TRANSITS training framework,¹ organising various workshops² and on providing the ENISA CERT Exercise material.³ While these efforts were widely used and appreciated by the CERTs and other communities, the challenges and circumstances have now changed. Since ENISA started its training and support activities, the importance of managing information security incidents has grown to become a top priority for companies, government institutions, universities, schools, and EU Member States. CERTs have emerged in all sectors and countries, and the number of national and governmental CERTs is continuing to grow. This trend is expected to continue worldwide for the foreseeable future.



1 <http://www.enisa.europa.eu/activities/cert/events/transits-training>

2 <https://www.enisa.europa.eu/activities/cert/events>

3 <http://www.enisa.europa.eu/activities/cert/support/exercise>

Executive summary

At the same time, the *maturity* of the CERT community has been increasing. The community itself is only 23 years old, and insiders compare its maturity with that of a 'teenager': adulthood is in sight, but there is still much to be done to get there. To name just a few examples of what has been happening over the last few years:

- European CERTs have intensified their cooperation across the board from national levels to companies and educational institutions, and also internationally, with ENISA, CERT-EU and others, and also outside Europe
- supplementing the already existing European *accreditation* of CERTs, a formal *certification* has been defined and implemented⁴
- Many CERTs are working on the development and implementation of automated incident related tools

To adapt to this constantly evolving environment, there is a growing need for specific training and exercises for CERT members and teams, and a need to define education profiles and demands for CERT professionals.

So that CERTs could have access to the necessary support, ENISA included in its Work Programme 2012 an activity related to the further development of capabilities to provide training and exercises for CERTs. ENISA aimed at procuring services in order to create an updated and extended collection of CERT exercise material, and a roadmap on how to prepare ENISA for the more (pro)active provision of training and exercises for both new and mature CERTs, leveraging the available good practice material produced since 2005.

This report presents the outcome of this work and the roadmap for more effective training and exercises. The proposals, which will benefit most of the European CERT community, are as follows:

1. ENISA support to the TRANSITS Framework and other suitable training programmes;
2. ENISA CERT Exercises at universities;
3. ENISA as co-provider of CERT trainers and training;
4. CERT Training Information Desk;
5. Video material by ENISA – how to organise the exercises?;
6. 'Fire Drills' for the CERT community;
7. ENISA CERT Training Hubs (ECTH);
8. ENISA CERT Exercises Certified Provider (ECTCP);
9. Recommendations for public administration organisations (national exercises);
10. Certification paths.

4 https://www.trusted-introducer.org/ti_process/certify.html

Executive summary

It is important to note that the results of the report originate not only from the knowledge and experience of the authors and reviewers, but that both bilateral talks with stakeholders and an online survey among CERTs were used to substantiate, prioritise and fine-tune the ideas presented here.

The roadmap identifies 10 proposals on how ENISA could improve CERT training and exercises, and therefore its effectiveness in Europe, and places them on a suggested timeline of implementation spanning 2013 to 2017. Each of the 10 is examined in more depth in Chapter 5, featuring content, timing, impact, finance, risks, community support, legal environment and mandate support.

The maturity of the CERT community in Europe has indeed reached such a stage where the need for good training and exercises is very strong. Unfortunately, the existing offerings no longer match the need, and urgently require expansion, quality improvement, and organisational embedding. These actions are most clearly in the interest of the CERT community of Europe and its whole constituency: the EU citizens.



2

Introduction and background

2 Introduction and background

This document, 'Roadmap for ENISA to provide more proactive and efficient CERT training', is based on an effort conducted between March and September 2012. The study is aimed at preparing ENISA for a more (pro)active provision of training and exercises for CERTs, leveraging the available good practice material produced since 2005.

The document is structured as follows.

Chapter 2 describes the methodology used to obtain results.

Chapter 3 gives an overview of the legal environment and mandate support relevant for the subject here.

Chapter 4 presents the core of the report – proposals on how ENISA can provide more proactive and efficient CERT training.

Chapter 5 proposes an implementation strategy for the various suggested proposals, and supports this with evaluation metrics and a benefit versus cost assessment.

Chapter 6 summarises the suggested proposals.

Chapter 7 presents the overall conclusion.

Finally, **Annex I** explains the abbreviations used and **Annex II** lays out the questions of the online survey used to gauge the stakeholders' needs, the results of which provided part of the momentum and prioritisation in this report.

2.1 Objectives of the report and description of work

The major objectives of this study were to produce:

- an updated and extended Collection of the CERT exercise material
- a Roadmap on how to prepare ENISA for a more (pro)active provision of training and exercises for both newly established and mature CERTs, leveraging the available good practice material produced since 2005

The latter is laid out in this report.

The ENISA CERT Exercises is a separate deliverable consisting of a **Handbook** for teachers, a **Toolset** for trainees and a **Virtual Image** to support hands-on exercises.

2.2 Methodology used

This section describes the methodology used in this study and the creation of the final report.

Desktop research and initial analysis of information

The online ENISA CERT Exercise materials were reviewed in depth, together with other ENISA support measures for CERT training – supporting TRANSITS framework, organising annual workshops etc. Also an online review was done of other available training schemes in the same field.



2.2 Methodology used

Identifying stakeholder needs (online survey and live consultations)

At various occasions (TRANSITS courses,⁵ TF-CSIRT⁶ and TI⁷ meetings, FIRST conference,⁸ GLOBAL CEP meeting⁹) live consultations with stakeholders were conducted on the topic of CERT training and how ENISA could continue to offer effective support in the future. Stakeholders were mostly from European CERTs, plus from TERENA,¹⁰ the organiser of TF-CSIRT, TI and TRANSITS.

Additionally, a web-based survey was conducted in May–June 2012. There were 24 respondents. The questions asked can be found in Annex II of this report. The results and conclusions relevant to this report are in the base of the sections devoted to 'Community Support' – where applicable, there is reference to the *Stakeholder Needs Survey*.

Identifying possible future models to prepare ENISA for a more proactive provision of training and exercises

This was based on the results of the desktop research and analysis, the live consultations and the *Stakeholder Needs Survey*, plus subsequent brainstorming and discussions inside the project team. The models identified are presented in this report.

Evaluating identified models

Three approaches were used to evaluate the models identified:

1. logical approach based on all information available (see above) – this is the result of the discussions in the project team;
2. evaluation metrics – subjective metrics based on experience;
3. benefit versus cost approximation.

Preparation of the roadmap

The proposed implementation timeline is based on a consideration of the proposed training material together with information available to the project team about ENISA timelines, programmes and available resources.

5 <http://www.terena.org/activities/transits/>

6 <http://www.terena.org/activities/tf-csirt/>

7 <https://www.trusted-introducer.org/>

8 <http://www.first.org/>

9 <http://www.globalcep.com/>

10 <http://www.terena.org>

3

Legal and policy basis

3

Legal and policy basis

The following legal and mandate-related documents are especially relevant for the work undertaken for this project and for the proposals that are presented in this report. What is provided in this section is the overview of these documents – specifically relevant passages are cited in the various proposals where appropriate.



3. Legal and policy basis

1. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)¹¹



‘Ensuring confidence in networks and information systems requires that individuals, businesses and public administrations are sufficiently informed, educated and trained in the field of network and information security. Public authorities have a role in increasing awareness by informing the general

public, small and medium-sized enterprises, corporate companies, public administrations, schools and universities. These measures need to be further developed. An increased information exchange between Member States will facilitate such awareness raising actions.’

Thus: *‘The Agency should provide advice on best practices in awareness-raising, training and courses’.*

2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the European Network and Information Security Agency (ENISA) (COM(2010) 521 final 30.9.2010)¹²

There are metrics in this document that should be used to measure and monitor the Agency’s activity in the field of prevention, detection and response to security incidents. One of them is the ‘number of network security trainings organised’. It is clear that many of the ideas for facilitating CERT trainings/exercises by the Agency are in line with this task and indicator.

CERT trainings/exercises can be used as components or backbone material of cyber exercises, inside teams, on a national level or internationally. This is also one of the most important expectations from ENISA coming from the mentioned document: *‘Facilitating EU-wide cyber security preparedness exercises with the support of the Commission and the contribution of ENISA, with a view to extending such exercises at a later stage at international level’.*

3. REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))¹³

According to this report ENISA should: *‘support capability-building by the Member States and Union institutions and bodies. It shall (a) offer network and information security training, including to Member State officials engaged in the fight against cybercrime, if appropriate in cooperation with stakeholders, in fields including network, information and application security, forensics and audit’.*

11 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

12 <http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf>

13 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>



4. CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)¹⁴

In this report, one of the conclusions and recommendations is to provide specialised training. The report argues that this recommendation has strong community acceptance and that ENISA's mandate allows acting on this recommendation. A few concrete actions are mentioned, like:

- supporting TRANSITS training
- facilitating pan-European incident response exercises
- investigating further technical training opportunities
- creating a training matrix for various groups of users

¹⁴ <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4

**Proposals:
how ENISA can provide
more proactive and
efficient CERT training**

4

Proposals: how ENISA can provide more proactive and efficient CERT training

ENISA should consider implementation and further research of the 10 proposals presented in this chapter, in the sections 4.1 to 4.10. These proposals are **arranged in the proposed chronological order of implementation**.¹⁵ The ENISA work programme planning cycle has been taken into account.

4.1

ENISA support to the TRANSITS Framework and other suitable training programmes

Implementation proposal: First half of 2013 (continue as required and needed)¹⁶

Duration: 3 years, then re-assessment

Description

ENISA continues to support TERENA¹⁷ in the provisioning of TRANSITS I, TRANSITS II and TRANSITS Train-the-Trainer courses¹⁸. Additionally it should identify relevant new training courses to support, for example, cooperation with CEPOL,¹⁹ EUROPOL,^{20,21} EU Fi-ISAC and INTERPOL.²²

Implementation strategy

The implementation strategy should include the following steps.

1. Identify forms of support:
 - financial (limit per course, limit in number of courses per year);
 - content (use of ENISA training materials);
 - PR (promotion of TRANSITS through EU and EU Member States);
 - trainers (ENISA will provide trainers to TRANSITS and other selected training courses).
2. Identify and respect constraints linked to the ENISA mandate (no involvement in operational work).
3. Implement the various forms of support as identified: financial, content, PR and trainers.

¹⁵ An overview of the implementation timeline is presented in section 5.3, and a summary of proposals in Chapter 6.

¹⁶ ENISA Work Programs 2011 and 2012.

¹⁷ TERENA, European society for national educational & research networks, see <http://www.terena.org/>

¹⁸ <http://www.terena.org/activities/transits/>

¹⁹ <http://www.cepola.europa.eu/index.php?id=home0>

²⁰ <https://www.europol.europa.eu/>

²¹ The focus of ENISA workshop was on cooperation between national/governmental CERTs in Europe and their national Law Enforcement counterparts: <https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-partII>

²² <http://www.interpol.int/>

4.1 ENISA support to the TRANSITS Framework and other suitable training programmes

4. Monitor the TRANSITS courses continuously, evaluate with TERENA annually and re-assess the ENISA support after three years.

Financial aspects

Potential budget for implementation could include:

- contribution per course times the number of courses per year
- overhead costs like a suitable training venue
- contributions for on-going improvements and updates to the course materials
- management of recurring costs that would need to be set aside for training each year; these costs would have to come out of the ENISA operational budget

Potential impact

- Improvement of the ENISA image
- Fostering of the continuity of the (non-commercial!) TRANSITS framework
- Helping to keep TRANSITS costs low, which would allow more CERTs to attend more courses
- Possibility of creating a training course tailored to meet the exact needs of CERT community

Risks

- Quality of courses must be very high or there may be a negative effect on the community and on ENISA's image
- TRANSITS courses might not attract enough audience to be economically justified
- There is currently no mechanism to guarantee the provision of a fixed budget for training for future work programmes after the year under consideration

Community support

From the *Stakeholder Needs Survey* it transpires that on a scale of 1 to 10, the average perceived value of the TRANSITS courses was 8.7 for *TRANSITS I*, 9.5 for *TRANSITS II* and 8.0 for *TRANSITS Train the Trainer*. SANS trainings scored 6.5²³ – and 100% use TRANSITS, less than 40% use SANS. CERT/CC courses score even lower, but if that is restricted to the typical CERT trainings, the score is around 7. See the following graph:

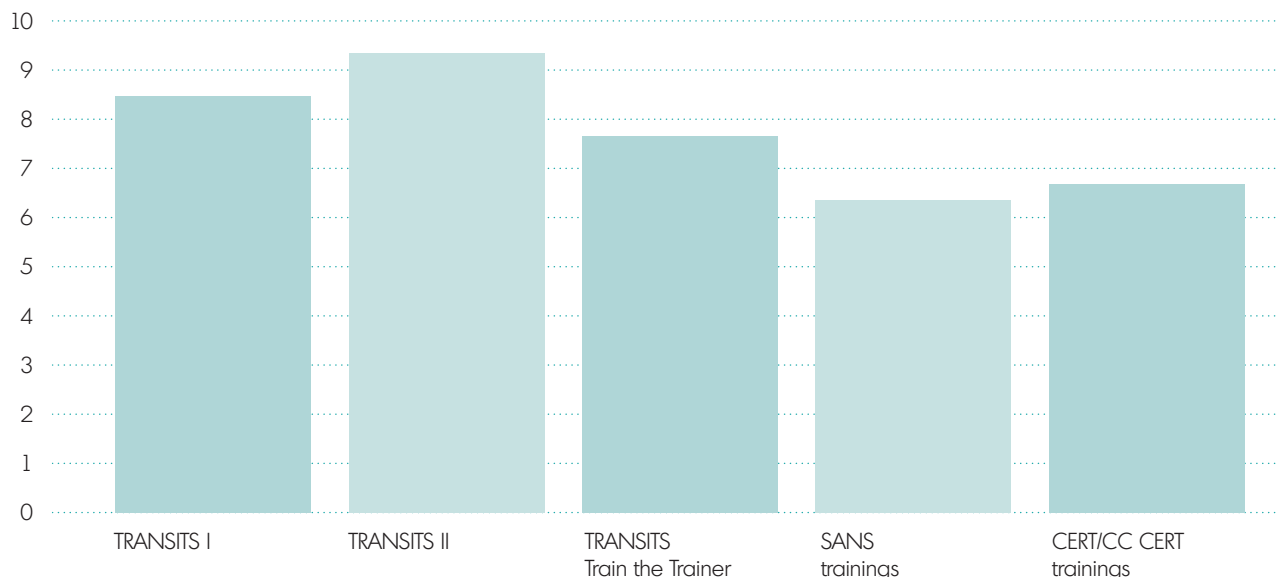


23 This 6.5 score for SANS was lower than expected from one-to-one interviews – the reason for this is unknown.

4.1 ENISA support to the TRANSITS Framework and other suitable training programmes

Graph 1:

Trainings average perceived value of various trainings on a scale of 1-10 (10 = best)



This data shows that *TRANSITS* courses are very popular and score very highly. ENISA has been supporting *TRANSITS I* and *II* all along, and the survey result justifies the fact that ENISA should continue and possibly expand support, also including the *Train the Trainers*.

This conclusion is further supported by five relevant observations from the *Stakeholder Needs Survey*.

- *TRANSITS I* – very useful; continue; keep renewing and pay for that when needed; maybe make 2.5 days; ENISA continue support; *FIRST* support would be welcome; legal module could be made more useable on national levels; role play exercise could be made more lifelike; *TERENA* – continue trend to professionalise but do not lose the character of ‘voluntary contribution’ as that will be counter-productive.
- *TRANSITS II* – excellent; continue; not much experience with it yet, so evaluate well; ENISA continue support; maybe additional modules could be added; maybe *TRANSITS II* modules could be piggybacked to *TF-CSIRT* meetings on occasion; keep ‘human communication skills’ in there even if not a security topic: ‘it’s all about communication’ (Robert Schischka); as for *TRANSITS I*, *TERENA*, continue trend to professionalise but do not lose the character of ‘voluntary contribution’ as that will be counter-productive.
- *TRANSITS Train the Trainer (T4)* – especially useful when the trainers are trained, like partially happened in Rome early 2012; continue that thread with good presentation and communication training; use T4 less to discuss *TRANSITS* modules, do that in separate sessions with module experts; if ENISA can facilitate, then very welcome; *FIND NEW TRAINERS* and not only from *NRENs*.

4.2 CERT Exercises at universities

- SANS trainings are expensive (especially due to travel cost) and less valued than TRANSITS: on a scale of 1–10 SANS scores an average 6.5, whereas TRANSITS does 8.7 (and even 9.5 for TRANSITS III). 100% use TRANSITS, less than 40% use SANS.
- For CERT trainings more or less the same applies. On average they score even lower (5.1), but the traditional CSIRT courses of CERT/CC actually score higher than SANS (but lower than TRANSITS) – it is the more focused trainings of CERT/CC that score dramatically low. Less than 30% use CERT/CC for this.

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the European Network and Information Security Agency (ENISA)²⁴
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)²⁵

4.2

CERT Exercises at universities

Implementation proposal: First half of 2013

Duration: to be decided

Description

ENISA CERT Exercises provide useful materials to be used not only at CERTs or training providers that provide security training, but also in the educational centres, in the academic sector.

At universities, especially technical universities, there are a number of courses that provide IT-security oriented exercises.²⁶ Lecturers are required to prepare detailed plans and exercises for students. The ENISA CERT Exercises are very interesting material for them as it could help them to prepare their own sets of exercises. However, at the moment lecturers do not use them, or they only use them sporadically, probably because they are mostly unaware they exist.

The aim is to make lecturers aware of this material and to provide them with help if needed, e.g. by means of the CERT Training Info Desk (see 4.4 below).

²⁴ <http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf>

²⁵ <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

²⁶ Arbitrary examples, by no means complete or indicating any preference, are:
 Tallinn University of Technology (Estonia): Masters course 'Cyber Security' – http://www.ttu.ee/studying/masters/masters_programmes/cyber-security/
 University of Amsterdam (The Netherlands): Masters course 'Security of Systems and Network' – <http://studiegids.uva.nl/web/sgs/en/c/12225.html>
 The University of Warwick (UK): Master course 'Cyber Security and Management (CSM)' – <http://www2.warwick.ac.uk/fac/sci/wmg/education/wmgmasters/courses/csm/>

4.2 CERT Exercises at universities

To convince lecturers at universities to use the Exercises, it would be useful to carry out a limited number of case studies of how ENISA CERT Exercises could be used to teach students. Such case studies would begin by reviewing the relevant educational programmes at a few chosen universities – preferably those that are well recognised in chosen countries – and establishing the parts of those programmes that would benefit most from adding ENISA CERT Exercises. Next, working together with lecturers from those universities would lead to concrete implementation examples. A video could well be added to support that action (see 4.5 below).

Implementation strategy

The implementation strategy should include the following steps.

1. Market concept and case studies towards the academic sector:
 - a. work together with CERT communities to reach academic sector in the EU Member States;
 - b. work together with governments in the Member States (especially with academic/education sector ministries) to reach academia;
 - c. explore the option if there is any programme at the EU level that could spread the information about ENISA Exercises horizontally across countries.
2. Identify potential, well-recognised universities where the IT security courses could benefit from addition of CERT ENISA Exercises.²⁷
3. Review the relevant education programmes and find the ones where the Exercises would be of most use.
4. Propose implementation ideas and work with universities' staff to assess feasibility.
5. Complete the case studies, add video material (optional), and make all of this available via the CERT Training Info Desk and market it towards the CERT community.
6. Work with a pilot of between three and five universities to test the concept.
7. With proven success, allow other universities to join in.
8. Promote new case studies of the use of ENISA CERT Exercises in universities.
9. Keep the academic sector and other stakeholders (CERT community, governments) informed all along.

²⁷ This could potentially be done together with the CERT community, as many CERTs have academic background or have a good relationship with academia.

4.2 CERT Exercises at universities

Financial aspects

The budget for making ENISA CERT Exercises be adopted by universities could include:

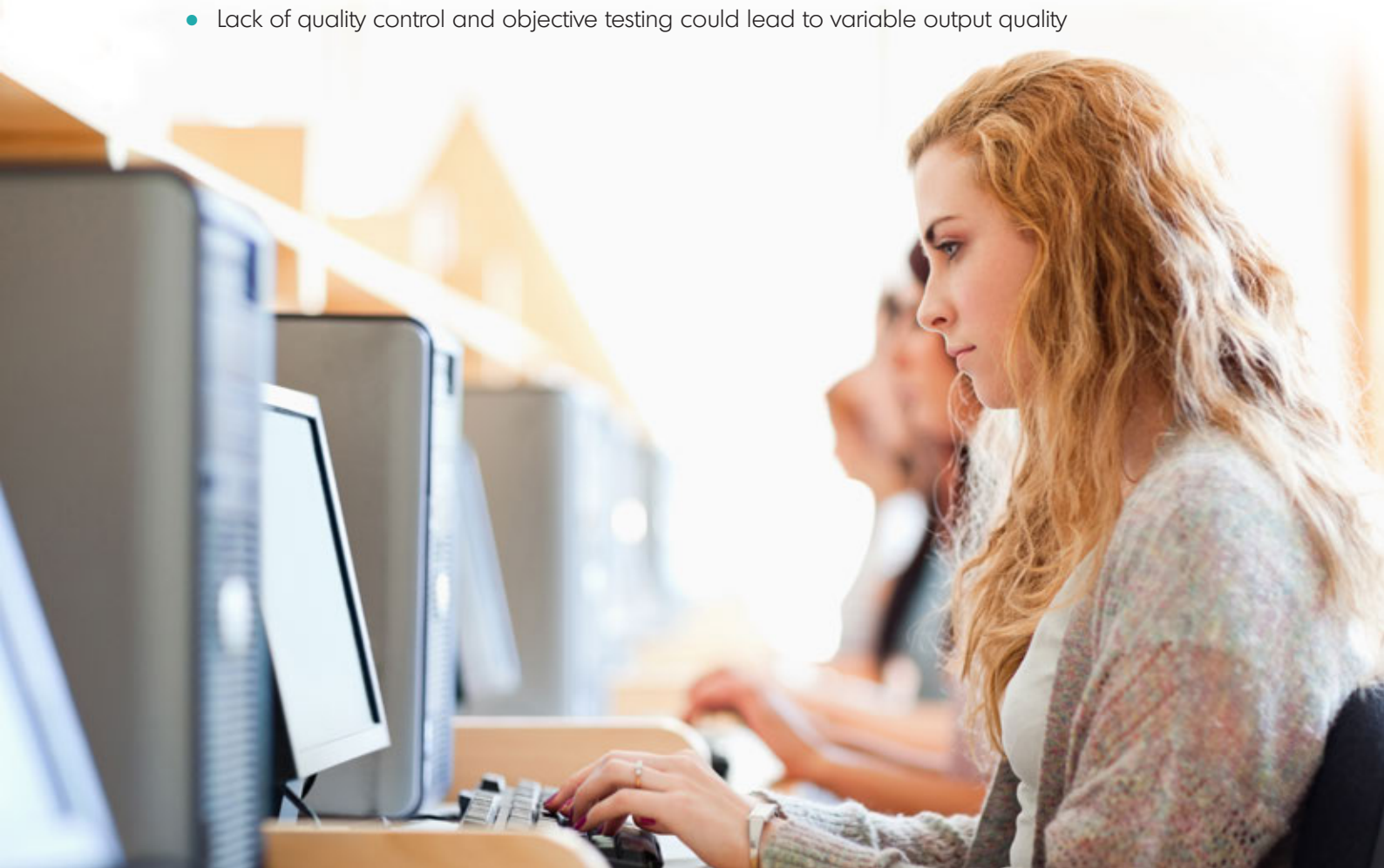
- the cost of preparing a final, detailed concept of the adoption of ENISA CERT Exercises at universities
- the cost of working with universities to develop case studies and 'success stories' (e.g. travelling to chosen universities or organising a seminar related to the concept idea)
- cost of promoting the concept:
 - conference presentations
 - marketing materials (including – optionally – videos)

Potential impact

- Potentially more CERT knowledge among graduates: potential future members of CERTs
- Greater interest in providing CERT-oriented courses by delivering ready-to-use materials for academic teachers
- Better knowledge at universities about ENISA and their work

Risks

- Lack of interest within the academic sector
- Bad implementations of Exercises could damage the reputation of the community and of ENISA
- Lack of quality control and objective testing could lead to variable output quality



4.2 CERT Exercises at universities

Community support

Community support for this idea has not been tested in the *Stakeholder Needs Survey*. However, from the authors' inside experience of the CERT community, spanning the period of 1993 until today, it can safely be concluded that CERTs will applaud any effort that will help to increase the influx of well-trained CERT professionals, as well as increase the maturity of the CERT 'profession' in general.

From the *Stakeholder Needs Survey* it is apparent that a variety of courses is of great interest to them – and it is easy to understand the advantages for CERTs when several such courses would already be given at universities. The relevant conclusion from the *Report* is as follows:

The top 10 of popular topics for training for CSIRTs is as follows:

1. *Incident Detection & Early Warning*
2. *Advanced Internet Security & Attack Scenarios*
3. *Advanced Incident Handling/Management*
4. *Netflow Analysis and Use*
5. *Improving the Maturity Level of your CERT*
6. *Advanced Forensics and Application*
7. *Human Communication skills*
8. *Vulnerability & Malware Analysis*
9. *Basic Legal Issues for CERTs (country specific)*
10. *Cooperating with Law Enforcement*²⁸

To meet the stakeholder needs, ENISA has been organising annual workshops on topics that are required at the given time based on bilateral communication with trainees.^{26, 30}

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)²⁹
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)³⁰

28 The focus of the ENISA workshop was on cooperation between national/governmental CERTs in Europe and their national law enforcement counterparts <https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-partII>

29 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

30 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.3 ENISA as co-provider of CERT trainings and trainers

4.3 ENISA as co-provider of CERT trainings and trainers

Implementation proposal: 2nd half of 2013

Duration: Three years initially, then re-assessment

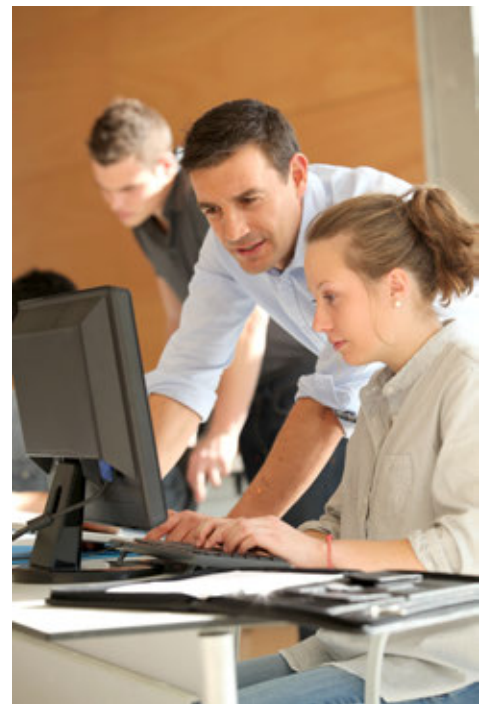
Description

ENISA would work together with existing CERTs³¹ to host trainings at CERT premises by offering support with trainers and funding. The use of suitable ENISA materials would be promoted for such courses. Additionally ENISA could host trainings and use ENISA staff as a base for trainers. ENISA has already organised several workshops to support and provide training and communication on several relevant topics – for example a hands-on workshop to technical CERT specialists,³² in addition, a workshop to improve cooperation between national/governmental CERTs in Europe and their national law enforcement counterparts was organised in 2012.³³ Therefore, ENISA has already in-house experience of organising various events and has the required contacts to ensure that both the quality and the means that training would reach the intended target audience.

Implementation strategy

The implementation strategy should include the following steps.

1. Identify the list of training sessions and exercises where ENISA could provide trainers (from inside ENISA and from existing CERTs, trained with the support of ENISA) in cooperation with existing CERTs.
2. Identify the training sessions that could be organised by ENISA.
3. Prepare pilot training sessions to ensure the quality of the trainers and the materials presented.
4. Allocate resources to attend to training sessions as trainers.



31 When ENISA CERT Training Hubs (ECTHs) are implemented, these are obvious candidates for such action.

32 The seventh annual CERT workshop focused on hands-on technical training <https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop>

33 The focus of ENISA workshop was on cooperation between national/governmental CERTs in Europe and their national law enforcement counterparts <https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-part1>

4.3 ENISA as co-provider of CERT trainings and trainers

Financial aspects

Potential budget for implementing the concept can include:

- the cost of launching a pilot training session
- the cost of training the trainers
- the cost of sending trainers to the location of the training session
- the cost of the venue
- management of recurring costs that would need to be set aside for training each year; these costs would have to come out of the ENISA operational budget

Potential impact

- Direct contact with CERT community and other target audiences will improve the image of ENISA
- Creation of new image of ENISA as a recognised partner of CERT training provider
- The communication and presentation skills of trainers will improve during the training session
- The overall level of expertise will improve both the trainers and the target audience



4.3 ENISA as co-provider of CERT trainings and trainers

Risks

- The training may require more resources than ENISA could make available at a given time
- The quality of trainers may not be satisfactory, which could have a negative effect on the ENISA image
- There is currently no mechanism to guarantee the provision of a fixed budget for training for future work programmes after the year under consideration

Community Support

As per the previous section, it follows from the *Stakeholder Needs Survey* that there is a very high appreciation of the various trainings. However, though it has not been a problem yet to find volunteer trainers for example for TRANSITS trainings (with only expenses covered), the base from which these trainers are drawn is fairly small, and mostly dependent on experts from NRENs.³⁴

One conclusion from the *Stakeholder Needs Survey* deserves to be repeated here:

TRANSITS Train the Trainers (T4) – especially useful when the trainers are trained, like partially happened in Rome early 2012; continue that thread with good presentation and communication training; use T4 less to discuss TRANSITS modules, do that in separate sessions with module experts; if ENISA can facilitate then very welcome; FIND NEW TRAINERS and not only from NRENs.

When other training courses are identified that will be supported by ENISA (see next section), the same reasoning will hold – that co-providing experienced trainers would be most welcome, when feasible.

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the European Network and Information Security Agency (ENISA)³⁵
- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))³⁶
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)³⁷

34 NREN: National Research & Educational Network – like SURFnet, GRNET, DFN, NASK, GARR, RedIRIS, SWITCH etc.

35 <http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf>

36 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

37 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.4 CERT Training Information Desk

Implementation proposal: First half of 2014

Duration: Three years initially, then re-assessment

Description

Establishing a CERT Training Information Desk would provide the CERT community with the needed basic information about existing trainings that are useful for CERTs, how to use them, who can provide them, etc. This information would be mostly available via the ENISA web site, but additionally the Information Desk should answer to questions coming in by e-mail or web form. This Info Desk would be an opportunity to provide the CERT community with quality information about available trainings, for example trainings provided by SANS, CERT/CC, (ISC)², ISACA, EC-Council, ISC etc. Of course, this will also be a good vehicle for making the ENISA CERT Exercises more widely used by introducing them into the training curricula. Additionally, ENISA together with TI/TF-CSIRT, might liaise with SANS, CERT/CC, FIRST, APCERT and with other similar institutes, to be able to offer certain popular trainings at a reduced cost in Europe.

Implementation strategy

The implementation of the CERT Training Information Desk does not require advanced actions. Rather, the concept assumes that, after a research and liaison phase, followed by making the collected information available via the web, marketing activities will be undertaken, such as announcing the launch of the Information Desk, putting the Information Desk banner on the ENISA front webpage, mentioning the Info Desk during ENISA presentations etc. Of course, the e-mail response function needs to be ensured³⁸ and bound to a quality level – such as answering e-mail within three business days.³⁹

Financial aspects

Implementing and running the CERT Training Info Desk will not require a significant budget. As the concept has a promotional/informational goal rather than an operational one, it is expected that the concept would be realised inside ENISA as a joint effort between CERT/security experts and communication staff. When ENISA CERT Training Hubs (see section 5.6) take off, the Info Desk would co-operate with these and refer to them.

Potential impact

- A well-recognised single point of contact for all parties interested in trainings will be useful/good for the CERT community in Europe
- Positive effect on the reputation of the ENISA CERT community support programme
- Focal point for liaison activities in regard CERT/security trainings
- Good vehicle to market ENISA CERT activities, including the CERT Exercises

38 Currently a similar e-mail support already functions as cert-relations@enisa.europa.eu - this can simply be adapted to the Info Desk label.

39 As this kind of question is generally not time-critical, answering within three business days is entirely reasonable. Answering within one business day requires substantially more effort, whereas answering in 5 days or later gives the perception of being 'slow'.

4.4 CERT Training Information Desk

Risks

- The incoming requests for information could require more staff resources than expected
- If continuous quality of service is not ensured, damage to ENISA's reputation may occur
- The selection procedure to decide what kind of information about which trainings to offer is complicated and may cause conflicts of interest

Community Support

A number of three conclusions from the *Stakeholder Needs Survey* support the case of the CERT Training Info Desk:

- *There are various other parties like (ISC)², ISACA, EC-Council and ISC who offer trainings also worthwhile for CSIRTs. They are listed above. It would prove worthwhile if ENISA together with TI/TF-CSIRT take a closer look at those and possibly list them for the community's sake.*
- *ENISA together with TI/TF-CSIRT might liaise with SANS, CERT/CC and/or one or more of the other institutes, to be able to offer certain popular trainings at a reduced cost in Europe*
- *TI/TF-CSIRT and ENISA work together with FIRST, APCERT and similar bodies in Africa and Latin America (e.g. LACNIC, CERT.br) to help ourselves and them as well – we have shared interests and need to work together on trainings and exercises*
- *ENISA exercises have been badly marketed thus far: 60% of the **active** respondents to our survey know about them, whereas 100% know about TRANSITS! There are not that many suggestions for improvement/expansion of the materials (they are listed above and have been used in our roadmap planning), but what is really in need is better marketing – the project team are of the opinion that ENISA marketing in general is below average in the CERT community: everyone knows and respects people like Marco Thorbruegge, Andrea Dufkova, Manel Medina et al., but the ENISA products (Exercises but also other CERT materials) are too little known, and absolutely deserve better according to those who do know them!*

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)⁴⁰
- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))⁴¹
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)⁴²

40 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

41 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

42 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.5 Video material by ENISA – how to organise the exercises?

This is an accompanying measure of the other elements in this roadmap and can be adopted whenever video materials would significantly benefit in addition to the set goals. To be organised in conjunction with the CERT Training Info Desk.

Implementation and Duration: in parallel with CERT Training Info Desk

Description

Video material that would present ideas on how to use the ENISA CERT Exercises could be a useful promotional tool. It could introduce users from the CERT community to various training related concepts, such as the following.

- How to prepare and run ENISA CERT Exercises
- How to establish and run an ENISA CERT Training Hub (ECTH) (see 4.6 below)
- How to become an ENISA CERT Training Certified Provider (ECTCP) (see 4.7 below)
- How to use ENISA CERT Exercises at universities (see 4.9 below)
- What the ENISA Certification Paths for CERT members are (see 4.9 below)

These materials could be made available via the CERT Training Info Desk webpages and could be used while presenting/promoting ENISA activities focused on of CERT trainings.

Video materials should be short and they should present the most important part of a particular topic. The basic idea of a video scenario is to prepare an animated graphic representation of the process in question and then to add to that interviews with ENISA CERT experts as well as with experts from the CERT community, offering opinions and 'success stories'.

Implementation strategy

The implementation strategy should include the following steps.

1. Decide which ideas should be presented and promoted by video material.
2. Prepare the scenario for presenting the chosen topics (including a tender process if needed).
3. Video production (including a tender process if needed).
4. Promotion activities:
 - by means of the ENISA website, specifically the pages for the CERT Training Info Desk;
 - by adding video fragments to ENISA presentations.

4.5 Video material by ENISA – how to organise the exercises?

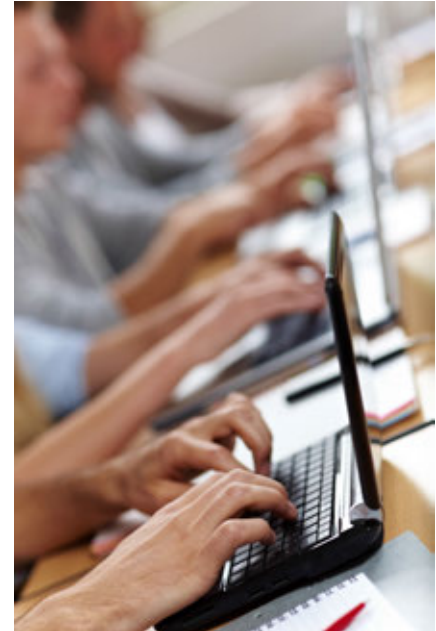
Financial aspects

Potential budget for implementing Video material by ENISA concept can include:

- the cost of preparation of video scenarios
- the cost of preparation for video production
- the cost of the promotion
- the need to keep such material up to date, which would result in a recurring cost

Potential impact

- Better recognition and promotion of ENISA's activities concerning CERT training, **explicitly including the ENISA CERT Exercises**
- Increased interest in joining the concepts proposed in this report, like ENISA CERT Training Hubs (ECTH, see 4.6 below) or ENISA CERT Training Certified Provider (ECTCP, see 4.7 below)
- Increased awareness of how to become and set-up an ECTH or ECTCP



Risks

- Creating good videos, and managing such a project is a resource-intensive effort that could take resources away from where they are most needed – at implementation and support. Therefore there is a need to limit the scope and application of videos to those cases where there is a very clearly positive benefit/cost balance.
- Low benefit-effort ratio
- Desired impact is lower than expected
- May result in significant workload to maintain previous material

Community Support

As said, this element is supportive of the CERT Training Info Desk, and thus it also derives its community support from the support for that element. However, one conclusion from the *Stakeholder Needs Survey* deserves to be explicitly repeated here:

*ENISA exercises have been badly marketed thus far: 60% of the **active** respondents to our survey know about them, whereas 100% know about TRANSITS! There are not that many suggestions for improvement/expansion of the materials (they are listed above and have been used in our roadmap planning), but what is really in need is better marketing – the project team are of the opinion that ENISA marketing in general is below average in the CERT community: everyone knows and respects people like Marco Thorbruegge, Andrea Dufkova, Manel Medina et al., but the ENISA products (Exercises but also other CERT materials) are too little known, and absolutely deserve better according to those who do know them!*

4.6 'Fire Drills' for the CERT community

Legal environment and mandate support

The following legal and mandate-related document, covered in section 3, is especially relevant to this proposal:

- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))⁴³

4.6

'Fire Drills' for the CERT community

Implementation: pilot autumn 2014 together with TF-CSIRT using the Trusted Introducer subgroup (focal point: autumn TF-CSIRT/TI meetings)

Duration: turn into annual event for CERT community, ENISA should go back to advisory role after first two 'fire drills'.

Description

ENISA CERT Exercises could easily become a part of scenarios of periodic 'fire drills',⁴⁴ organised by the CERT community in Europe. This is similar to exercises inside a team, or between teams on a national level – only this time the scope is wider, and involves international cooperation.

The CERT community in Europe is united in TF-CSIRT/TI. The TI already provides a proven 'trust' mechanism, which would be a good starting point for such 'fire drills'.

However, to develop and organise 'fire drills' involves a significant amount of work. This needs an enabler, and ENISA could play an important role in that. Also, organisers of national exercises could in turn help realise international 'fire drills' to run inside the CERT community.



⁴³ <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

⁴⁴ The word 'fire drill' is used here as an analogy with a 'fire drill' for a fire brigade – meaning an exercise in which a real or simulated fire is used to test and train various aspects of the work of the fire brigade. This analogy is easily applicable to CERTs, where the 'fire' will be a security breach or threat, or a series of those, making it necessary to 'extinguish the fire', i.e. handle the incident and related threats, and make sure that the 'fire' is contained, meaning that the threat is neutralized or removed. 'Fire drills' potentially simulate a real-life incident. Various skills and competencies are tested and trained in the course of a 'fire drill', and various parties are involved.

4.6 'Fire Drills' for the CERT community

Implementation strategy

The implementation strategy should include the following steps.

1. Determine suitable ENISA CERT Exercises to be used as parts of a new, bigger scenario, which could serve as the basis for 'fire drills'.
2. Prepare the good practice guide on how to use ECTHs (see 4.6 below) for this situation.
3. Promote the concept within the CERT community using for example TF-CSIRT/TI as a partner.
4. Build the community in a structured manner.
5. Assist (if needed and requested) in providing suitable training.⁴⁵

Financial aspects

- Cost of adjusting training/exercise materials to suit the 'fire drill' scenario
- Costs associated with building the community
- Cost of assistance in providing suitable training
- Management of recurring costs that would need to be set aside for training each year; these costs would have to come out of the ENISA operational budget

Potential impact

- Better cooperation between CERTs in Europe
- Good assessment of existing international cooperation between CERTs in Europe
- Popularising ENISA CERT Exercises by incorporating them into CERT 'fire drill' scenarios

Risks

- Significant cost for ENISA involved in set-up process of 'fire drills'
- Risk of sensitive information leakage during 'fire drills'
- There is currently no mechanism to guarantee the provision of a fixed budget for training for future work programmes after the year under consideration

⁴⁵ This could be done by the CERT Training Info Desk working together with ENISA CERT Training Hubs

4.6 'Fire Drills' for the CERT community

Community Support

When asked, in the *Stakeholder Needs Survey*, if teams participate in 'fire drills', about one half answers 'no / not right now', but three quarters do perform drills or are planning to engage in them. When asked about the scope of such drills, more than 70% would like to do 'fire drills' inside their team and at a national level. Between 30% and 40% would like to engage in sectoral and/or European drills, and just over 20% even on a global scale.

Unmistakable support for the European 'fire drill' idea emerges in the same survey when the question is asked: *Would you consider it useful if such fire drills were enabled and organised with support of such parties as ENISA, TF-CSIRT, Trusted Introducer?* A full 100% answers YES, and, when asked for more detail, the TI emerges as the most suitable community, because there the teams have already invested in 'trust' through the accreditation/certification processes and community building. Finally, it turns out that once per year is a good compromise for the frequency of such 'fire drills'.

The following conclusion from the *Stakeholder Needs Survey* summarises it well:

More complicated exercises, in fact, 'fire drills' are in need of using inside teams and with other teams. 100% of respondents are in favour of doing a 'fire drill' roughly once every year in the context of the Trusted Introducer trusted environment, under auspices of ENISA and TF-CSIRT. Developing and leading such drills is time consuming (expensive); support from ENISA and other partners is essential to make this succeed.

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the European Network and Information Security Agency (ENISA)⁴⁶
- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))⁴⁷
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)⁴⁸

46 <http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf>

47 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

48 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.7 ENISA CERT Training Hubs (ECTH)

Implementation proposal: Second half of 2014 in parallel with ENISA CERT Training Certified Provider (ECTCP): two sides of the same coin

Duration: undefined; proposed are three-year cycles and then re-assessment

Description

An ENISA CERT Training Hub (ECTH), as branded by ENISA, would be an existing well-known CERT entity that promotes CERT exercises and trainings recognised by ENISA. Such entities, CERT teams and security competence centres that are well recognised and known by the communities do exist in almost all countries or other specific regions.⁴⁹ These teams or centres are potentially the best candidates for playing the role of ENISA CERT Training Hub (ECTH), which in close cooperation with ENISA will promote ENISA CERT Exercises, and other trainings recognised and promoted by ENISA. The assumption is that ECTHs have a significant influence in their regions as the security competence centres and can promote ENISA CERT Exercises and other relevant trainings as one of the best methods of acquiring or improving the level of security knowledge, especially that related to building and running CERTs.

Setting up an ECTH would be based on a preparation workshop of between two and three days for CTH staff by ENISA, during which ENISA experts (ENISA employees or hired external consultants) would explain the idea of ECTH in detail and would teach how to organise and run ECTH. During such workshops, ENISA experts/consultants would provide the best practice for potential ECTH candidates, which could be used in providing CERT trainings. Additionally, they could analyse, on-site, the organisational and logistic capabilities of ECTH candidates and whether they would be able to meet the ENISA expectations.

Potential activities of ECTH:

- organising 'Train the Trainers' sessions for other security and CERT teams that might be interested in provisioning ENISA supported exercises/trainings in their environments (e.g. in the academic sector)
- supporting a constituency by providing answers to questions related to CERT exercises/trainings asked by the ECTH constituency members
- actively working on implementing ENISA supported exercises/trainings in various security trainings
- providing recommendations and input to improve the content and add new scenarios to the ENISA CERT Exercises set, and other ENISA-supported trainings

49 Arbitrary examples, holding no recommendation of whatever kind: NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE); NCSC, National Cyber Security Centre of The Netherlands (including the national and governmental CERT); DFN-CERT, NREN CERT of Germany; CERT-POLSKA, NREN CERT of Poland; SWITCH CERT, NREN CERT of Switzerland (not EU, but EEA).

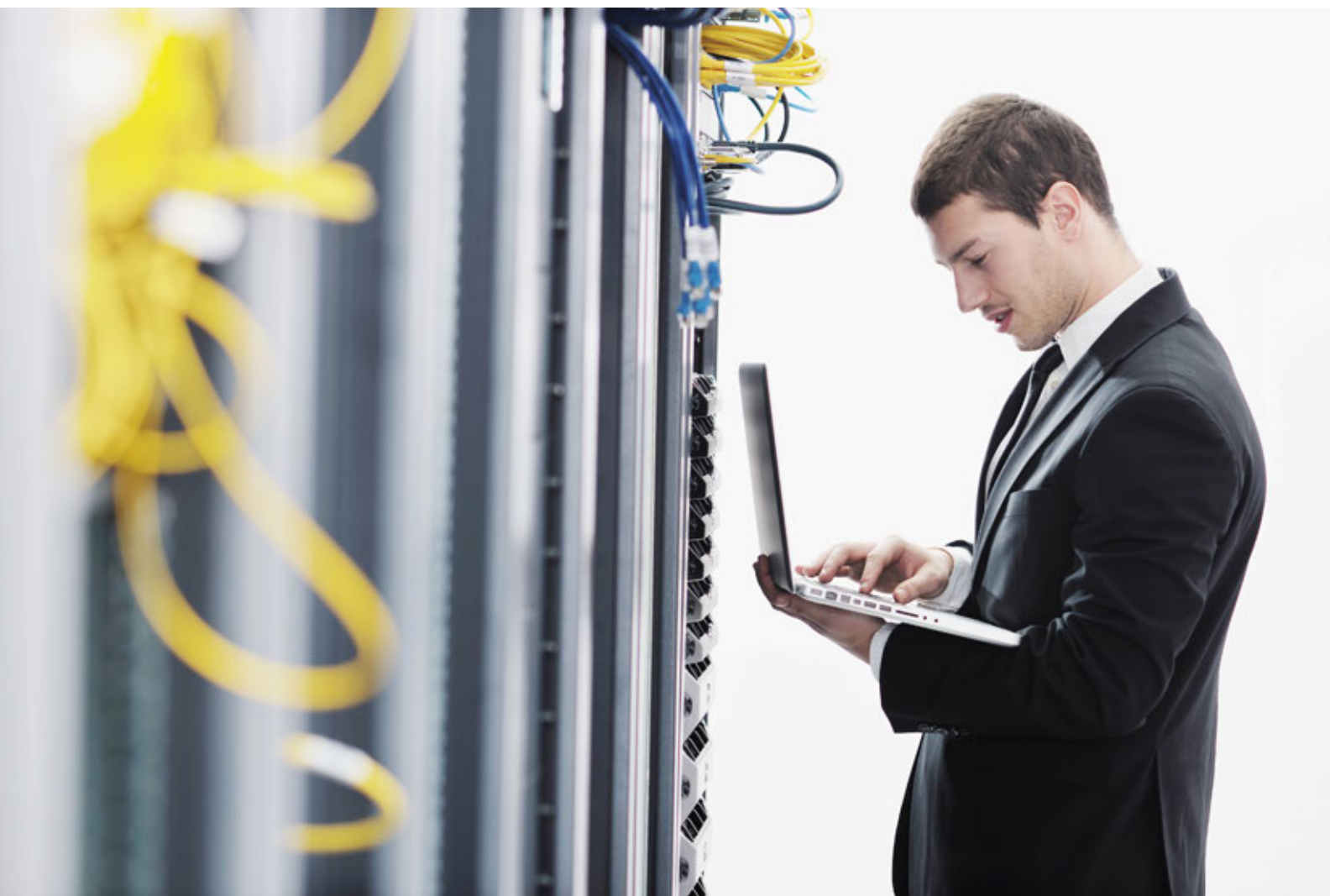
4.7 ENISA CERT Training Hubs (ECTH)

If more than one centre in a specific region/country would be interested in being an ECTH, ENISA could organise a 'Call for ECTH'. Which candidate to choose would depend on the following factors:

- availability of training facilities
- availability of experts ready to provide trainings
- their level of competence in running a security training centre
- experience in cooperation with ENISA and understanding ENISA training framework
- membership in the CERT trust network – for example, in Trusted Introducer

From the perspective of ENISA, ECTHs would be important partners in spreading the ENISA-supported exercises/trainings and making them popular, as well as significant partners in the further development of the ENISA CERT support programme.

Being an ECTH would require continuous quality assurance. For instance, every two years, ENISA would have to evaluate the quality of service provided by an ECTH. Perhaps only these high-quality ECTHs would continue to be allowed to use the ECTH branding and participate in the related ENISA programme. These ECTHs would be in the first wave of new ideas, content and development.



4.7 ENISA CERT Training Hubs (ECTH)

Implementation Strategy

The implementation strategy should include the following steps.

1. Define the final 'ENISA CERT Training Hub' concept in detail including financial and organisational aspects.
2. Present the ECTH idea to the CERT community (TERENA TF-CSIRT, Trusted Introducer, FIRST).
3. Build the network of ECTHs (including a selection process, if needed).
4. Organise a workshop on how to establish and operate an ECTH for the chosen ECTH candidates.
5. Actively work with ECTH to achieve and maintain a high quality of service.

Financial aspects

Potential budget for implementing the ECTH concept should include:

- the Cost of preparing the final, detailed concept of ECTH
- the cost of promoting the ECTH concept:
 - conference presentations
 - marketing materials
- the cost of the quality assurance process

Potential impact

- Creating an effective network of centres of competence ready to provide CERT trainings would improve the both the availability and the quality of trainings
- Promotion of ENISA educational materials would increase overall awareness about the ENISA CERT support programme
- Promotion of usage of the ENISA CERT Exercise set (and potentially other ENISA-supported trainings) by incorporating them into other CERT training oriented materials
- Growth of the body of experts ready to train CERT staff
- Closer cooperation between ENISA and CERTs which run an ECTH – to mutual benefit
- Maintaining the ENISA supported CERT exercises/trainings on a high quality level

Risks

- Lack of interest from CERTs of being ECTH – especially due to lack of human and financial resources
- Lack of interest from other CERT training owners in incorporating ENISA CERT Exercises into their programmes
- Poor quality of trainings conducted by ECTH could negatively impact ENISA's reputation

4.7 ENISA CERT Training Hubs (ECTH)

Community Support

The following conclusions from the *Stakeholder Needs Survey* are relevant to the expected support for an ECTH concept:

- Work together with ‘centres of expertise’ like existing experienced CSIRTs who already offer various trainings to their constituents – and see if and how such trainings could be offered at a broader scale, for instance in smaller (language?) regions around such expert teams. Of course these teams can benefit from this too, as they on their turn could learn from others. ENISA together with TI/TF-CSIRT could play a leading role in this area. (Examples of such teams are JANET CSIRT, SWITCH CERT, SURFcert and NCSC-NL together with KPN-CERT: the latter two are working on a ‘CERT Academy’ programme).
- The top-10 of popular topics for trainings for CSIRTs is as follows:
 1. Incident Detection & Early Warning
 2. Advanced Internet Security & Attack Scenarios
 3. Advanced Incident Handling/Management
 4. Netflow Analysis and Use
 5. Improving the Maturity Level of your CERT
 6. Advanced Forensics and Application
 7. Human Communication skills
 8. Vulnerability & Malware Analysis
 9. Basic Legal Issues for CERTs (country specific)
 10. Cooperating with Law Enforcement⁵⁰

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))⁵¹
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)⁵²

50 The focus of workshop was on cooperation between national/governmental CERTs in Europe and their national Law Enforcement counterparts <https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-part1>

51 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

52 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.8 ENISA CERT Exercises Certified Provider (ECTCP)

Implementation proposal: Second half of 2014 in parallel with ENISA CERT Training Hub (ECTH)

Duration: undefined, proposed are three-year cycles and then re-assessment

Description

The goal here is to convince various (commercial) security training providers to implement ENISA-supported exercises/trainings into their training programmes. Those training providers that implement ENISA materials in their training programmes and have allocated and trained a sufficient number of trainers to handle ENISA supported exercises/trainings, would receive the certified status of ECTCP. Two levels of 'certification' are proposed initially here ('Gold' level to be defined later, if the concept proves to work):

- Level 1 – ECTCP Bronze
 - A training provider has implemented, for example, at least two ENISA-supported exercises/trainings in their training programme
 - A training provider has, for example, at least one trainer who has participated in the ENISA 'train the trainers' workshop
 - A training provider organises, for example, at least one training that includes ENISA supported exercises/trainings every 12 months
- Level 2 – ECTCP Silver
 - A training provider has implemented, for example, at least two ENISA-supported exercises/trainings in their training programme
 - A training provider has, for example, at least two trainers who have participated in the ENISA 'train the trainers' workshop
 - A training provider organises, for example, at least one training that includes ENISA-supported exercises/trainings every six months



4.8 ENISA CERT Exercises Certified Provider (ECTCP)

Implementation strategy

The implementation strategy should include the following steps

1. Define the final ENISA CERT Training Certified Provider concept in detail including financial aspects, organisational aspects, project plan, expectations, resources and timeframe.
2. Present the ECTCP idea to the CERT community (FIRST, TERENA TF-CSIRT, Trusted Introducer) and collect feedback.
3. Present the ECTCP idea to security training providers and collect feedback.
4. Build the network of ECTCPs.
5. Actively have ECTCPs work together with ECTHs and ENISA to ensure high quality of service.
6. Define and execute measurements to assess ECTCPs and see if they are worth their ECTCP certification.

It must be said here that, as CERT/security training is a fairly specialised activity, the potential ECTCPs are not necessarily big companies. Several smaller companies who provide trainings could be excellent candidates for ECTCP. To not lose such candidates in an ECTCP implementation, the ECTCP scheme should be set up so as to keep overheads low, especially since smaller companies can often not afford large overheads, or an expensive certification scheme.

Financial aspects

The budget for implementing the ECTCP concept could include:

- the cost of preparation of the final, detailed concept of ECTCP;
- the cost of promoting ECTCP:
 - conference presentations
 - marketing materials
- the cost of organising ECTCP/ECTH *Train the Trainers* workshops;
- the cost of support of maintaining the ECTCP network, which includes measurements to assess whether ECTCPs deserve their certified status;

Potential impact

- Higher interest from security training providers in implementing ENISA-supported exercises/trainings in their training programmes
- More CERT experts ready to train using the ENISA materials
- Introduction of competition between ECTCPs and even ECTHs leading to an increase of the quality/cost ratio
- Help from security training providers in upgrading the ENISA supported exercises/trainings

4.8 ENISA CERT Exercises Certified Provider (ECTCP)



Risks

- Lack of interest in being ECTCP, because of lack of visible (short-term) commercial gain
- Need to invest a significant amount of work in maintaining the certification schema
- It pre-supposes long term investment of ENISA in the CERT community/training support – without that, ECTCPs would soon lose interest, or not even being to be interested in investing in the ECTCP concept.

Community support

The ECTCP concept is very similar to the ECTH concept, only translated to the commercial environment of security training providers. Therefore, the community support that would exist for the ECTH concept would also exist for the ECTCP concept – providing the idea was worked out coherently and presented well to the community at large.

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))⁵³
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011) ⁵⁴

53 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

54 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.9

Recommendations for public administration organisations (national exercises)

Implementation proposal: pilot in first half of 2015 for the national exercises

Duration: creation of periodic events and creating synergies with existing exercises for EU Member States; ENISA should return to advisory role after pilot phase

Description

ENISA CERT Exercises (and potentially other ENISA-supported trainings) could easily become a part of scenarios of periodic national exercises, organised by the public administrations in the Member States. Periodic national exercises are becoming an increasingly important and popular method for testing the level of preparedness of a country to detect and mitigate Internet threat attacks, such as Distributed Denial-of-Service (DDoS) and Advanced Persistent Threats (APT). Additionally some legally oriented topics (e.g. data breach notification obligations) could be part of such exercises.

The idea is to propose possible potential usages of ENISA CERT Exercises to work with public administration representatives – preferably with governmental/national CERTs, to popularise them in the governmental constituencies of the Member States.

If CERT cooperation exists in a given country, involving them right from the beginning is a critical success factor: if possible, the national exercise should be developed inside or at least together with that community. To impose a national exercise top-down from a government level towards private companies will rarely succeed, or will at least meet with a lack of cooperation and enthusiasm. The idea is to make use of the existing forces – this applies much more widely than just here: to make any venture in incident management and CIP successful, public administrations should seek cooperation rather than imposition.⁵⁵

There are two main areas of potential use.

- **Area I – national cyber exercises** Public administration organisations could implement ENISA CERT Exercises as part of the scenarios.
- **Area II – fulfilling technical, organisational and legal obligations for public administration bodies** It is to be expected that the demands on incident management capabilities will become more formal inside public administration bodies – this is a natural consequence of the increasing maturity of the CERT environment and the increased importance of information security. This will gradually lead to certification-like obligations. It is to be expected that ENISA CERT Exercises will help such bodies prepare to meet those obligations.⁵⁶

⁵⁵ This cooperation model has worked well inside the CERT community in Europe since the very beginning back in 1993, when Don Stikvoort and Klaus-Peter Kossakowski organised the first meeting of European CERTs in the RARE (now TERENA) offices in Amsterdam; this marked the beginning of European cooperation in this area. The regular meetings that followed were the informal predecessor of TF-CSIRT, which was kicked off in the year 2000. This cooperative approach continues to work today. The majority of national and governmental CERTs in Europe have recognised and embraced this concept.

⁵⁶ If the match between such obligations and the Exercises will not be immediately obvious, then no doubt existing Exercises will be adapted and new ones designed to match and support the obligations

4.9 Recommendations for public administration organisations (national exercises)

Implementation strategy

The implementation strategy should include the following steps.

1. Determine the ENISA CERT Exercises suitable for Areas I and II.
2. Prepare a good practice guide on how to use the Exercises for Areas I and II.
3. Promote the concept within public administration institutions in the Member States (preferably working with governmental/national CERTs).
4. Assist (if needed and requested) in providing suitable ENISA CERT Exercises and potentially also other ENISA supported trainings.⁵⁷

Financial aspects

The budget to assist national exercises in including ENISA materials could include:

- the cost of preparation of a good practice guide on how to use relevant ENISA CERT Exercises (including a tender process if needed)
- the cost of workshops or seminars for public administration (e.g. governmental CERTs) to convince them and help them to implement ENISA CERT Exercises in their national exercises (for EU Member States)
- the cost of assistance in providing suitable ENISA CERT Exercises and potentially also other ENISA-supported trainings
- the cost of assistance for EU Member States in case they ask for more substantial assistance in this area
- the management of recurring costs that would need to be set aside for training each year; these costs would have to come out of the ENISA operational budget

Potential impact

- Widespread usage of ENISA materials within the public administration and CIP sector
- Better preparation for following EU level-legal obligations related to incident-handling practices
- Popularising ENISA supported exercises/trainings by incorporating them into national exercise scenarios

Risks

- Lack of interest within public administrations for using ENISA CERT Exercises
- A significant increase in requests for assistance in this area from EU Member States
- There is currently no mechanism to guarantee the provision of a fixed budget for training for future work programmes after the year under consideration

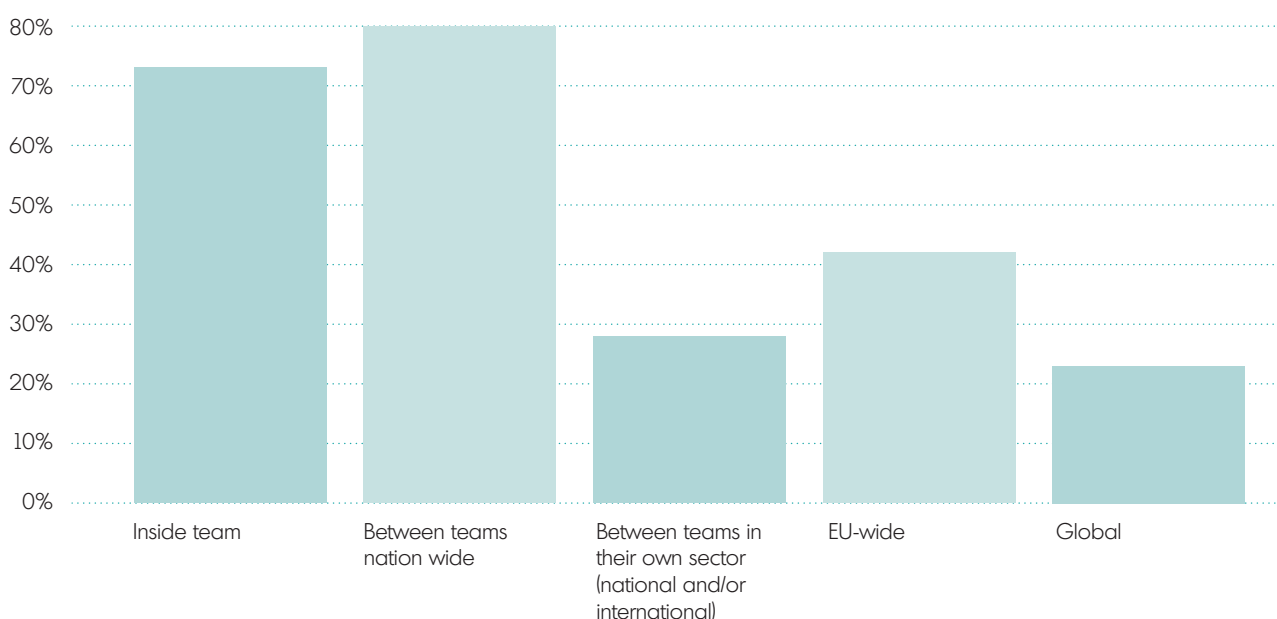
⁵⁷ This action could be done by working together with ENISA CERT Training Hubs

4.9 Recommendations for public administration organisations (national exercises)

Community Support

From the *Stakeholder Needs Survey*, it appears that there is a clear interest in exercises done at a national level. The following graph illustrates this.

Graph 2

Percentage of respondents desiring specific scopes of fire drills**Legal environment and mandate support**

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)⁵⁸
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the European Network and Information Security Agency (ENISA)⁵⁹
- REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)0521 – C7-0302/2010 – 2010/0275(COD))⁶⁰
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)⁶¹

58 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

59 <http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/Proposal%20new%20regulation%20ENISA.pdf>

60 <http://www.europarl.europa.eu/document/activities/cont/201202/20120215ATT38139/20120215ATT38139EN.pdf>

61 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

4.10

Certification Paths

Implementation proposal: Second half of 2015

Duration: to be decided

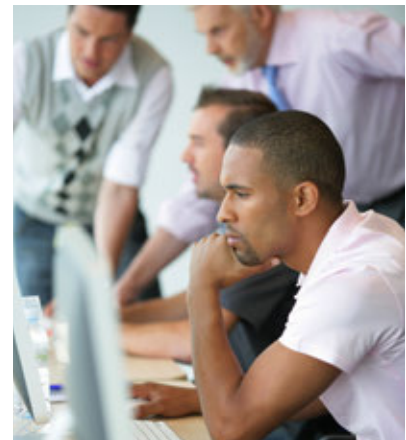
Description

After preparing the second, new set of ENISA CERT Exercises there will be a significant number (more than 20) of Exercises that will cover many IT security topics. Thus these exercises will be ready to be structured into particular thematic paths that have a potential to become Certification Paths.

Such Certification Paths could be offered to students (from universities) and trainees (from CERTs), who will have a clear understanding of which Exercises are for them. Such a scheme would help CERT managers to choose the best set of Exercises for their employees, and will likewise help lecturers at universities to choose the Exercises that best fit their education programme.

Another option is to deliver (e.g. through some other organisation) some form of certificate for those who complete a particular Path. If such a scheme were to be implemented, some more detailed rules would need to be developed for maintaining it, such as the following:

- requirements for receiving a certificate:
 - maximum time for completing a particular Path
 - training source – training centres or individuals who are eligible to provide trainings
 - examination and/or other completion demands
- requirements for keeping certified status:
 - obligations for refreshing knowledge included in exercises of particular Paths
 - obligations related to Exercises that are added to a Path⁶²




To gain recognition and to improve the potential success of these ideas, it is important to start working together. Parties such as FIRST, CERT/CC and (ISC)² could establish something like an *education points liaison system* so that trainings followed at such organisations also contribute to the certification path – and that trainings followed within the ENISA frameworks also contribute to any ‘education points’ systems of the others.

⁶² When ENISA updates Exercises and/or paths

4.10 Certification Paths

Three potential paths are described here:

Path 1: Operational CERT

 Following this Path, the student/trainee will learn the most important information about the methods and procedures used by CERTs. Exercises give an opportunity to learn in detail about the processes of CERT operational aspects and roles and positions in a CERT team.

Existing CERT Exercises for this Path:

- Triage & basic incident handling
- Incident handling procedure testing
- Vulnerability handling
- Writing security advisories
- Incident handling in live role playing

Graph 3:

Certification path 1 – existing Exercises



New CERT Exercises:

- CERT participation in incident handling related to the Article 4 obligations
- Advanced Persistent Threat incident handling
- Cost of ICT incident calculation


Graph 4:

Certification path 1 – new Exercises



4.10 Certification Paths

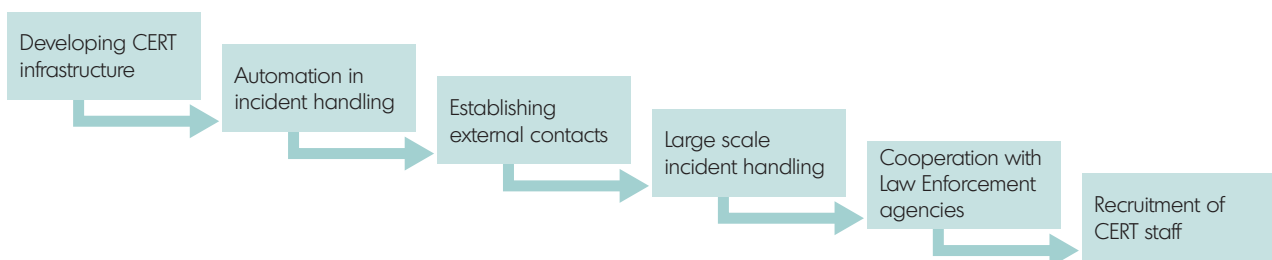
Path 2: Building CERT and Cooperation

 In this Path, the student/trainee will learn practical information on how to build a CERT in terms of its proper infrastructure preparation, tools implementation, acquiring human resources and establishing external contacts with the most significant parties and communities.

Existing CERT Exercises for this Path:

- Developing CERT infrastructure
- Automation in incident handling
- Establishing external contacts
- Large scale incident handling
- Cooperation with Law Enforcement agencies
- Recruitment of CERT staff

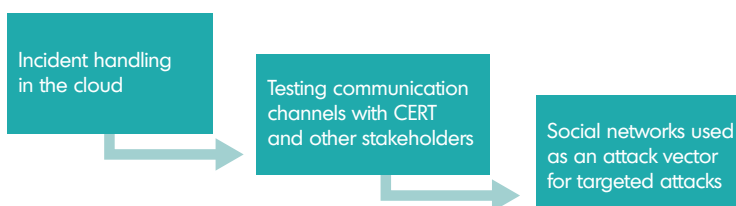
Graph 5:

Certification path 2 – existing Exercises

New CERT Exercises:


- Incident handling in the cloud
- Testing communication channels with CERTs and other stakeholders
- Social networks used as an attack vector for targeted attacks

Graph 6:

Certification path 2 – new Exercises

4.10 Certification Paths

Path 3: Technical CERT

 This Path consists of Exercises that have a technical nature. They are dedicated for CERT technical staff. Students/trainees can use them to improve their technical skills, especially those related to specific CERT operations.

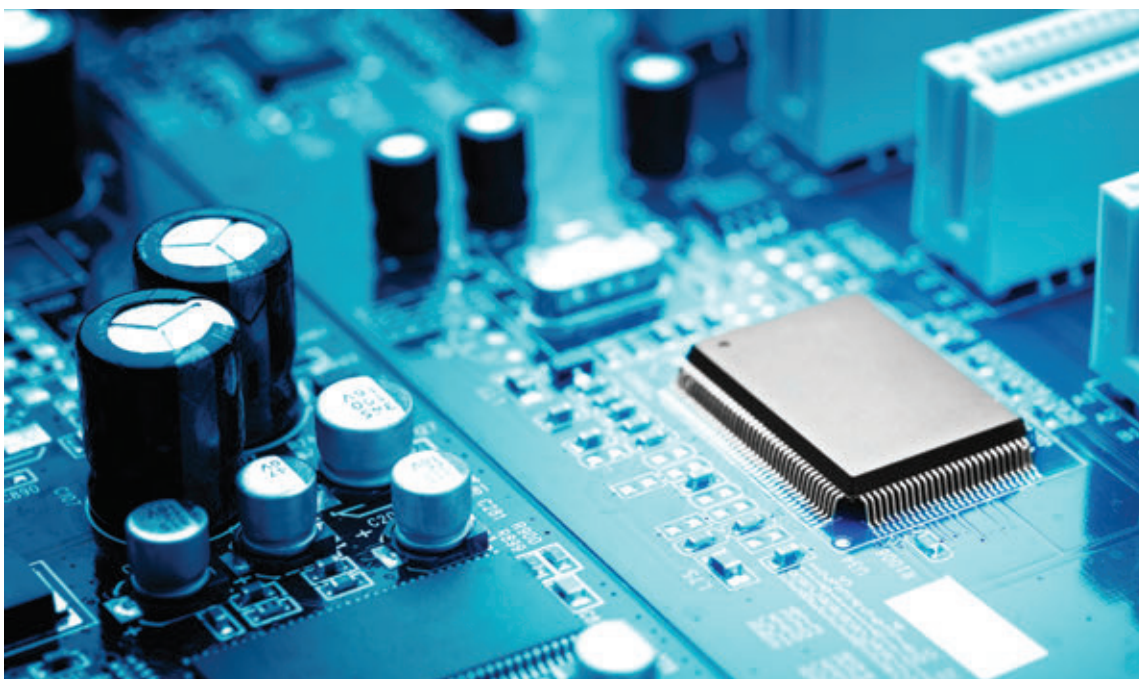
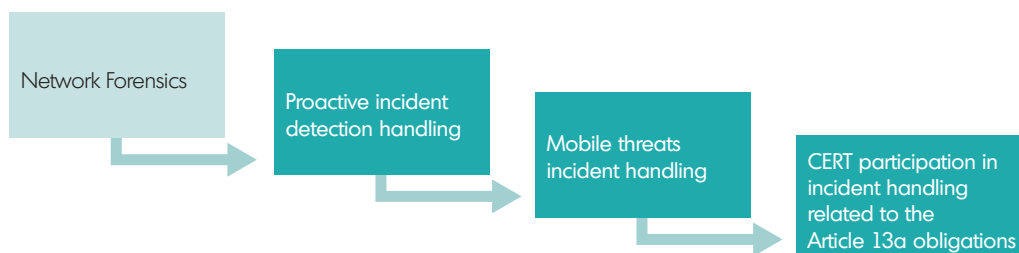
Existing CERT Exercises for this Path:

- Network Forensics

New CERT Exercises

- Proactive incident detection
- Mobile threats incident handling
- Incident handling during attack on SCADA
- CERT participation in incident handling related to the Article 13a obligations (contains hands-on investigation)

Graph 7:

Certification path 3 – existing & new Exercises

4.10 Certification Paths

Implementation strategy

The implementation strategy should include the following steps:

1. Announce the Certification Paths as a new concept of usage of the ENISA CERT Exercises.
2. Work together with ENISA CERT Training Hubs, ENISA CERT Training Certified Providers and universities to promote the concept.
3. Develop a detailed scheme of issuing certificates for students/trainees, who decide to follow any of the Paths.
4. Work together with other parties such as FIRST, CERT/CC and (ISC)² to establish something like an *education points liaison system*, which is designed to allow students/trainees to be more free in their choice of courses across Europe and even worldwide, and still follow an ENISA Certification Path.
5. Maintain the certification scheme and *education points liaison system*.

Financial aspects

The potential budget for implementing the Certification Paths concept includes:

- the cost of developing a final and detailed concept
- the cost of promoting the concept
- the cost of liaising with other parties such as FIRST, CERT/CC and (ISC)² to establish an *education points liaison system*
- the cost of issuing certificates and maintaining the repository of certified students (including fulfilling requirements to refresh their knowledge)

Potential impact

- Higher prestige of the ENISA CERT Training programme because of the availability of Certification Paths provided by a European agency
- More experts becoming available for the CERT community and related suppliers
- Continuous interest in the usage of ENISA-supported exercises/trainings through the introduction of the requirement to keep a high level of knowledge related to the Certification Paths
- Increased understanding of the relationship between classic security techniques and CERT operations and procedures

4.10 Certification Paths

Risks

- High cost of setting up and maintaining the certification schema
- Cost of setting up and maintaining the *education points liaison system*
- Low interest in certification with a fairly narrow scope
- Has to be done very well or will result in damage to ENISA reputation

Community Support

Apart from the support already mentioned in the previous Section, the following conclusions from the *Stakeholder Needs Survey* are all of relevance here:

- Work together with 'centres of expertise' like existing experienced CSIRTs who already offer various trainings to their constituents – and see if and how such trainings could be offered at a broader scale, for instance in smaller (language?) regions around such expert teams. Of course these teams can benefit from this too, as they on their turn could learn from others. ENISA together with TI/TF-CSIRT could play a leading role in this area. (Examples of such teams are JANET CSIRT, SWITCH CERT, SURFcert and NCSC-NL together with KPN-CERT: the latter two are working on a 'CERT Academy' programme).
- Various accreditations (like CISSP, and CERT/CC Certified Incident Handler) come with 'points' earned for attending trainings, conferences etcetera. This model would prove useful for the CSIRT community too, e.g. as part of TI Accreditations/Certifications, or as part of a (still non-existent) professional accreditation for CSIRT members. E.g. one could gain such points by going to TRANSITS trainings, or TI/TFCSIRT and FIRST meetings. By working with organisations like FIRST, CERT/CC and (ISC)² we hope that it be possible in time to create a common understanding of what is useful for our professionals, so that e.g. going to one event could lead to 'points' which are valid for more accreditations. As part of this we need descriptions of skills and training options/requirements. ENISA could certainly play a bootstrapping role in this area.

Legal environment and mandate support

The following legal and mandate-related documents, covered in section 3, are especially relevant to this proposal:

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)⁶³
- CERT Operational Gaps and Overlaps (ENISA, 20 December 2011)⁶⁴

63 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

64 <http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps>

5

Implementation strategy

5 Implementation strategy

The proposals presented in the document come with recommendations about implementation time including start time and duration. In this section, additional evaluations (metrics and benefits versus effort) are introduced and, finally, an overall implementation timeline is presented.

5.1 Evaluation metrics

The evaluation is based on the following metrics.

- Difficulty – how difficult from the technical, organisational and logistical point of view would implementation of the suggested proposal be?
- Financial – how expensive would implementation of a suggested proposal be?
- Risk – how big are the risks to ENISA?
- Impact – how big an impact would the implementation of a suggested proposal have?
- Community support – how much would the particular suggested proposal be appreciated and supported by the CERT community (based on online survey results and interviews)?
- Legal environment and mandate support – how much is the particular element consistent with the ENISA mandate and other relevant documentation?

To avoid over-complication, each of the evaluation metrics was valued on a scale of one to three, with one being the lowest and three the highest. The ranking was done subjectively, based – however – on the long-time experience of the authors and reviewers, in a similar manner as they use when doing non-quantitative risk analysis.

The results of this evaluation are presented in the table below.



Table 1:
Evaluation metrics for various proposals

| Implementation element | Difficulty | Financial | Risk | Impact | Community support | Legal environment and mandate support |
|--|------------|-----------|------|--------|-------------------|---------------------------------------|
| ENISA support to the TRANSITS Framework and other suitable training programmes | 1 | 2 | 1 | 3 | 3 | 3 |
| ENISA CERT Exercises at universities | 1 | 2 | 1 | 2 | 2 | 2 |
| ENISA as co-provider of CERT trainings and trainers | 2 | 2 | 1 | 2 | 2 | 3 |
| CERT Training Information Desk | 1 | 1 | 1 | 2 | 2 | 2 |
| Video material by ENISA – how to organise the exercises? | 2 | 2 | 1 | 2 | 1 | 3 |
| 'Fire Drills' for the CERT community | 2 | 3 | 2 | 3 | 3 | 3 |
| ENISA CERT Training Hubs (ECTH) | 2 | 2 | 3 | 2 | 2 | 2 |
| ENISA CERT Exercises Certified Provider (ECTCP) | 2 | 2 | 3 | 1 | 1 | 2 |
| Recommendations for public administration organisations (national exercises) | 1 | 2 | 1 | 2 | 1 | 3 |
| Certification paths | 3 | 3 | 2 | 2 | 2 | 3 |

5.2

Benefit versus effort

The above evaluation can also be seen in terms of benefit versus effort: the potential benefit from the implementation versus the effort invested.

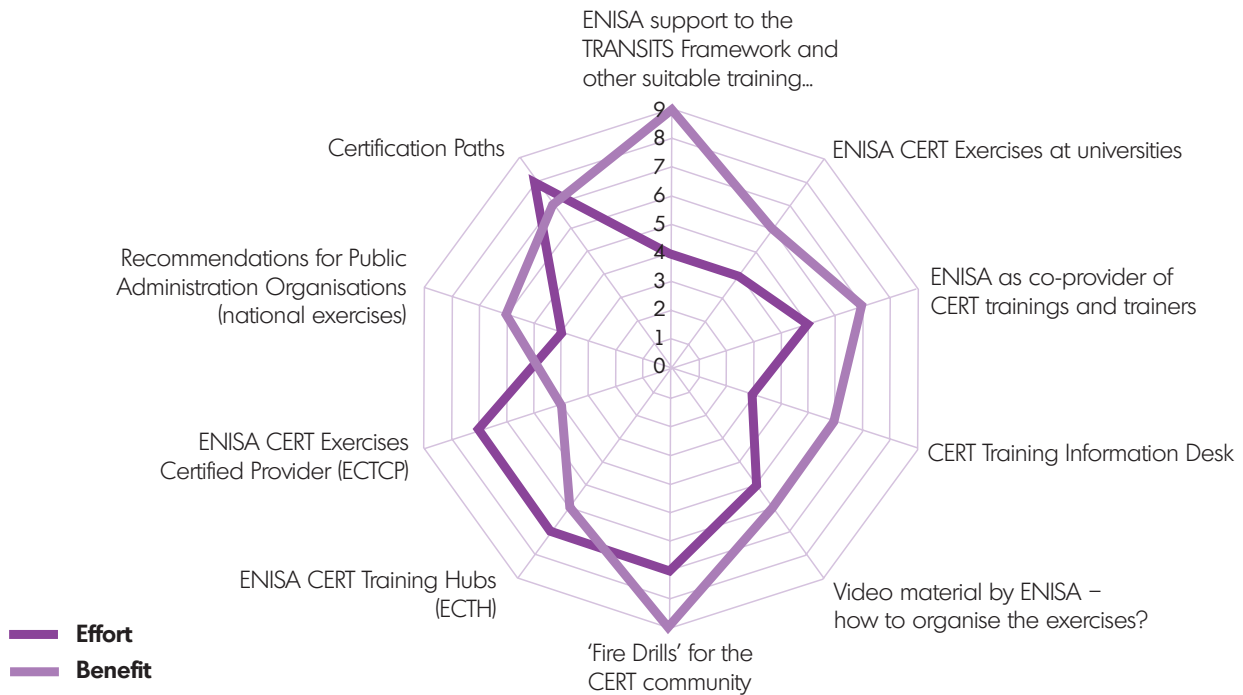
The benefits are calculated as the sum of those metrics that are related to added value and positive aspects reached by the element implementation. In this case, that means adding the values in the following columns in Table # 1: 'Impact'; 'Community support'; and 'Legal environment and mandate support'.

The efforts are calculated as the sum of those metrics that are related to the work needed to implement, the budget spent on implementation and the potential risk related to such action. In this case: adding the values in the following columns in Table # 1: 'Difficulty'; 'Financial'; and 'Risk'.

This benefit versus effort perspective is presented in the graph below.

5.2 Benefit versus effort

Graph 8:

Benefit versus effort for various proposals

When examining the graph, proposals for which the benefits are significantly higher than the efforts spent on their implementation, can easily be seen – for instance, Support to Transits Framework and other suitable trainings, ENISA as Trainings and Trainers Co-provider, and CERT Fire-Drills. Also visible is where the benefit-effort balance is less good, e.g. for ENISA CERT Training Hubs or ENISA CERT Exercises Certified Provider.

This graph helps us to visualise the benefit–effort balance more efficiently, and could therefore be useful in the overall evaluation of strategy and tactics in regard to CERT trainings. However, this graph should not be treated as 'absolute', as all judgements are subjective and based on the authors' and reviewers' experience. We recommend taking a very close look at the table in the previous paragraph: if the appreciations in the table change, the graph will change.

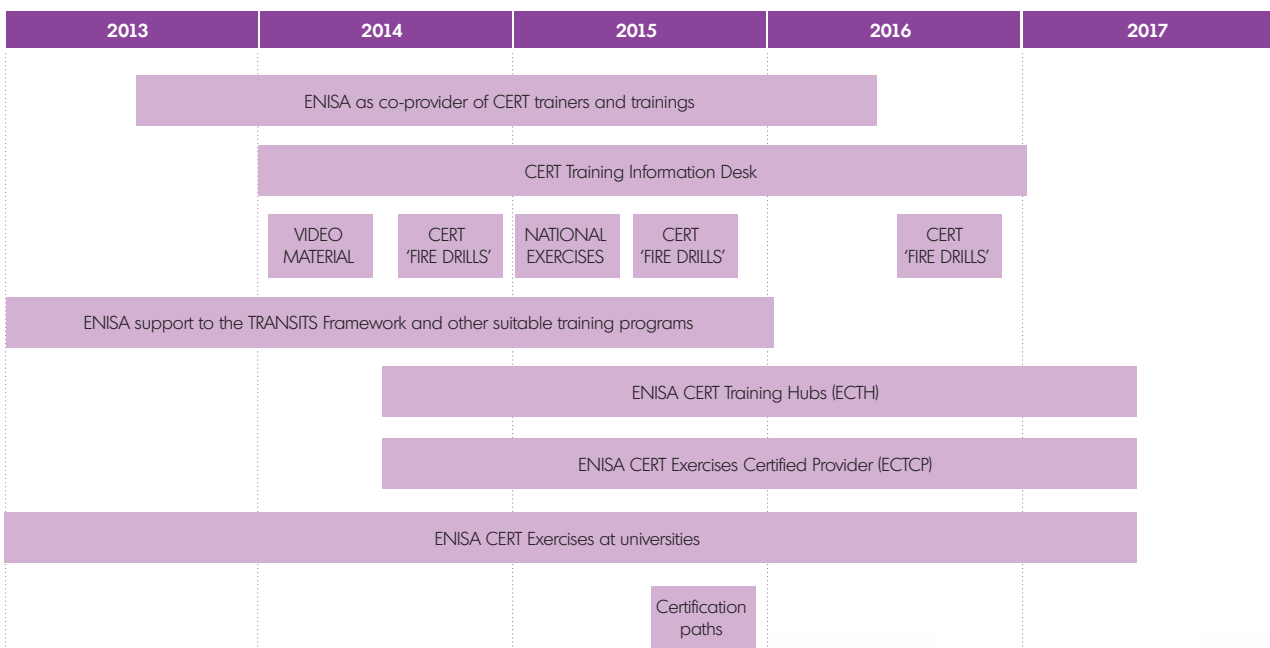
5.3 Implementation timeline

5.3 Implementation timeline

The proposals have been presented in the sections above, together with the proposed timeline details. In the below graph, all proposals are collected together with their timelines, to provide an overview.

Graph 9:

Overall timeline for implementing proposals





6

Summary of proposals

6 Summary of proposals

In Chapter 4, the various proposals that made up the core of the roadmap were presented in detail. Together, they propose how ENISA could improve the training and exercises landscape for the European CERT community. In the previous Chapter 5, these ideas were rated and presented together in one timeline. In this chapter, a summary of these 10 proposals is provided.

1. ENISA support to the TRANSITS Framework and other suitable training programmes

- ENISA continues to support TERENA⁶⁵ in the provisioning of TRANSITS I, TRANSITS II and TRANSITS Train-the-Trainer courses⁶⁶. Additionally it should identify relevant new training courses to support: for example, cooperation with CEPOL,⁶⁷ EUROPOL,^{68,69} EU Fi-ISAC and INTERPOL⁷⁰ has proven to be mutually beneficial.

2. ENISA CERT Exercises at universities

- ENISA CERT Exercises are very good materials to be used not only at CERTs or commercial training providers that provide security trainings, but also in educational centres in the academic sector. The aim is to make lecturers aware of this and provide them with help if needed e.g. by means of the CERT Training Info Desk.

3. ENISA as co-provider of CERT trainers and trainings

- ENISA would involve existing CERTs to host trainings at their premises by offering support with trainers and funding. The use of suitable ENISA materials will be promoted for such courses. Additionally ENISA could host trainings at its premises and use ENISA staff as a base for trainers.

4. CERT Training Information Desk

- The proposal is to establish a CERT Training Information Desk, which would provide such basic information as:
 - what trainings/exercises exist that are useful for CERTs;
 - how to adopt/implement these trainings/exercises;
 - who can provide them;
 - what is the perceived quality;
 - what is the best order to take them in.

65 TERENA, European society for national educational & research networks, see <http://www.terena.org/>

66 <http://www.terena.org/activities/transits/>

67 <http://www.cepoleuropa.eu/index.php?id=home0>

68 <https://www.europol.europa.eu/>

69 The focus of ENISA workshop was on cooperation between national/governmental CERTs in Europe and their national Law Enforcement counterparts <https://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-part1>

70 <http://www.interpol.int/>

6. Summary of proposals

- This information would be available via the ENISA web site under the banner of the CERT Training Information Desk, but additionally the Information Desk would answer questions coming in by e-mail or webform.

5. Video material by ENISA – how to organise the exercises?

- Video material that would present ideas on how to use the ENISA CERT Exercises could be a good promotional tool. It could introduce users from the CERT community to several of the ideas presented in this roadmap. The video material could be made available via the CERT Training Information Desk and could be used while presenting/promoting ENISA activities focused on CERT trainings.

6. 'Fire Drills' for the CERT community

- ENISA CERT Exercises could easily become a part of scenarios of periodic 'fire drills'⁷¹ organised by the CERT community in Europe. This is similar to the kind of exercises done inside a team, or indeed between teams on a national level; only in this 'fire drills' proposal, the scope is wider, and involves international cooperation.
- The CERT community in Europe is united in TF-CSIRT/ TI. The TI already provides a proven 'trust' mechanism, which would be a good starting point for such 'fire drills'.
- However, developing and organising 'fire drills' involves a significant amount of work. This needs an enabler, and ENISA could play an important role in this activity.

7. ENISA CERT Training Hubs (ECTH)

- There are CERT teams or security competence centres that are well recognised and known by communities existing in almost all countries or other specific regions. These teams or centres are potentially the best candidates for playing a role of ENISA CERT Training Hubs (ECTH), which in close cooperation with ENISA will promote ENISA CERT Exercises and other trainings recognised and promoted by ENISA.

8. ENISA CERT Exercises Certified Provider (ECTCP)

- The goal with its proposal is to convince various (commercial) security training providers to implement ENISA supported exercises/trainings in their training programmes . Those training providers that have implemented ENISA materials significantly in their training programmes and have allocated and trained a sufficient number of trainers to handle ENISA supported exercises/trainings would receive the status of ECTCP.

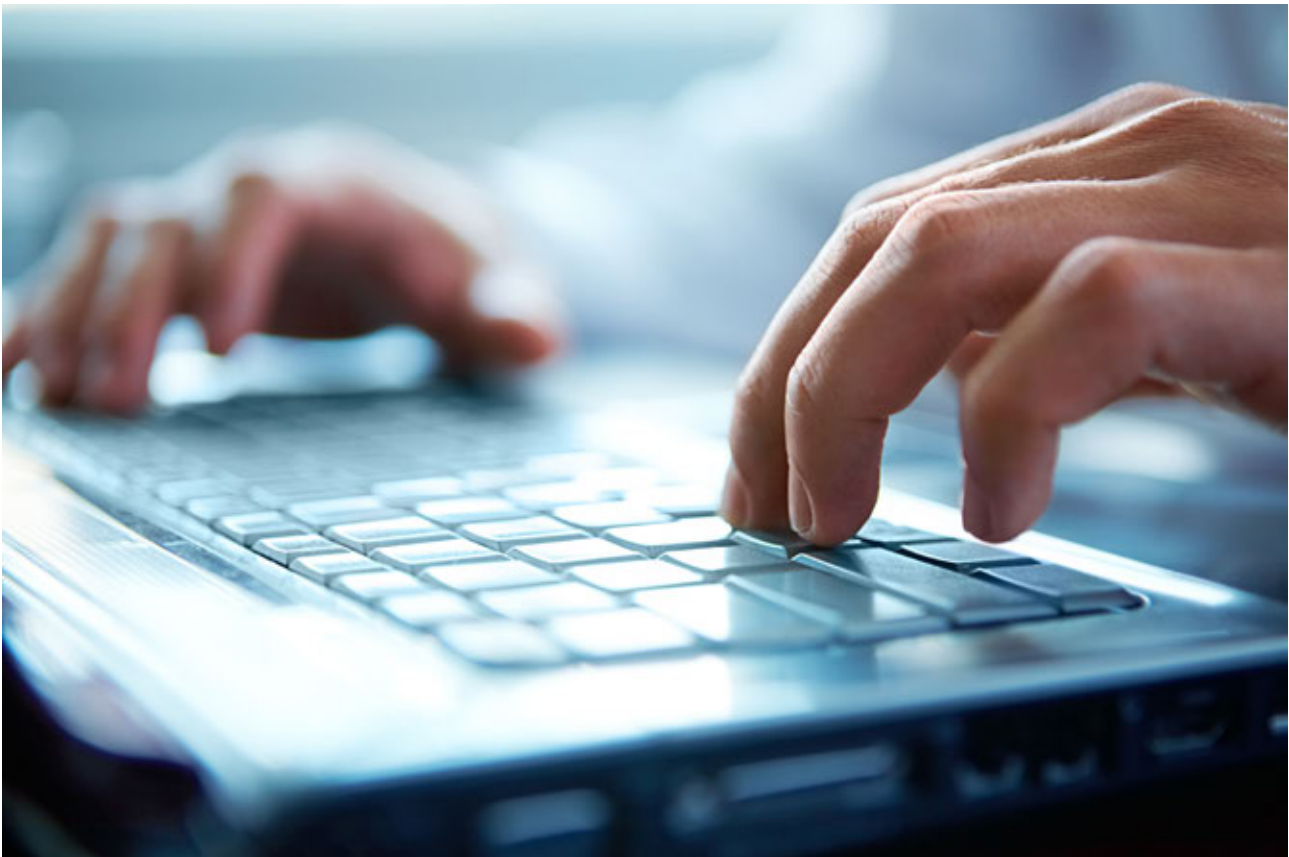
⁷¹ The word 'fire drill' is used here as an analogy with a 'fire drill' for a fire brigade – meaning an exercise in which a real or simulated fire is used to test and train various aspects of the work of the fire brigade. This analogy is easily applicable to CERTs, where the 'fire' will be a security breach or threat, or a series of those, making it necessary to 'extinguish the fire' i.e. handle the incident and related threats, and make sure that the 'fire' is contained, meaning that the threat is neutralized or removed. 'Fire drills' potentially are more complex exercises therefore, or existing of a variety of exercises, and simulate a real life incident situation. Various skills and competencies are tested and trained in the course of a 'fire drill', and various parties are involved.

9. Recommendations for public administration organisations

- ENISA CERT Exercises (and potentially other ENISA supported trainings) could easily become a part of scenarios of periodic national, organised by the public administration bodies in the Member States. Periodic national exercises are becoming an increasingly important and popular method of testing the level of preparedness of a country to detect and mitigate threats against information infrastructure and citizens' wellbeing in the electronic environment.
- The idea is to propose a few possible potential usages for ENISA CERT Exercises and work with public administration representatives – preferably with governmental/national CERTs – to popularise them in the governmental constituencies of the Member States.

10. Certification Paths

- After preparing the second, new set of ENISA CERT Exercises, there will be a significant number of Exercises. Thus these exercises will be ready to be structured into particular thematic paths that could become Certification Paths.
- Such Certification Paths could be offered to students (from universities) and trainees (from CERTs), who will have a clear understanding what Exercises are for them. Such a scheme would help CERT managers to choose the best set of Exercises for their employees, and will likewise help lecturers at universities to choose the Exercises that fit their education programme the best.



7

Conclusion

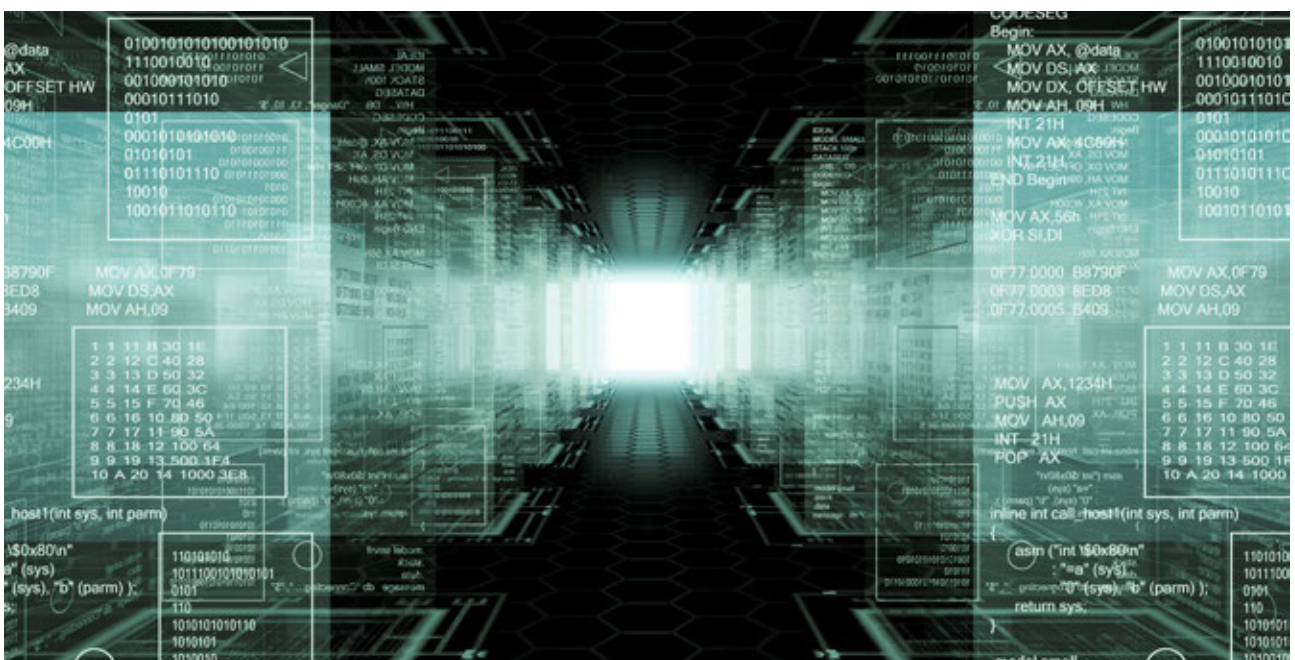
7 Conclusion

The views and opinions expressed in the document are from experts from the CERT Community and other relevant stakeholders. The document does not necessarily reflect the position of ENISA and there might be different options regarding how ENISA could provide more effective exercises and training besides those mentioned in this document. The ideas presented here are valuable, as they reflect the actual community needs and requirements and there could be mutual benefit from both CERT community and ENISA in this more active training and exercises approach.

To name just a few of the benefits of implementing these ideas, they would help to:

- set up more efficient and specialised trainings for the CERT community;
- ensure that enough CERT trainers are available;
- make sufficient and good quality information on trainings easily available;
- provide better content for trainings;
- stimulate 'fire drills' for the international CERT community;
- provide assistance for setting up national exercises.

The CERT community in Europe has reached a level of maturity where the demand for quality education is increasing, demands on the availability of existing training and exercises is high and there is a clear need for an intermediate party, who could encourage, guide and provide support to the CERT community in the aspects of exercises and trainings. That intermediate party could be ENISA. The proposals presented are analysed so as to be compliant with ENISA's current mandate and in the interests of the CERT community in Europe.



8

Annex I: Abbreviations

8

Annex I: Abbreviations

| | |
|----------|--|
| CERT | Computer Emergency Response Team |
| CSIRT | Computer Security Incident Response Team |
| ECTH | ENISA CERT Training Hub |
| ECTCP | ENISA CERT Exercises Certified Provider |
| FIRST | Forum of Incident Response and Security Teams: see http://www.first.org/ |
| NREN | National Research and Education Network (like SURFnet, NASK, GRNET) |
| TERENA | European society for NRENS: see http://www.terena.org/ |
| TF-CSIRT | Community and meeting place of European CERTs: see http://www.terena.org/activities/tf-csirt/ |
| TI | Trusted Introducer for CERTs in Europe : see https://www.trusted-introducer.org/ |
| TRANSITS | Training for CERT staff by CERT staff: partially volunteer set-up to enable high quality but affordable training for CERT staff in Europe and beyond: see http://www.terena.org/activities/transits/ |



**Annex II:
Survey questions
(overview)**

9

Annex II: Survey questions (overview)

- What type of constituency does your CERT serve?
- How many FTEs (full-time equivalents) do you have working in your CERT?
- What is your role in your CERT?
- What is the value of the following TRANSITS courses for members of your CERT?
- What is the value of the following SANS training courses for members of your CERT?
- What is the value of the following CERT/CC courses for members of your CERT?
- What training courses offered by other organisations have you found valuable?
- Does your CERT offer training courses which you might consider offering to other CERTs?
On what topics?
- What is the value of the ENISA exercises for your CERT?
- What ENISA exercises do you use in your CERT?
- What kind of training exercises would be really useful for your team?
- How could the ENISA Exercises be improved?
- Does your CERT organise or participate in incident handling fire drills i.e. small to large-scale exercises, with one or more teams, where incident handling, communication, escalation etc. are being put to the test? If you can, please briefly specify the name and the essence of the fire drill and what its scope is.
- What scope of fire drills do you find useful?
- Would you consider it useful if such fire drills were enabled and organised with support of such parties as ENISA, TF-CSIRT, and Trusted Introducer? Please explain your opinion 'yes' or 'no' and if 'yes', how often would you like such drills to be organised, and with what scope?
- What training topics would your team find most valuable?



SECURITY

Contact details

To contact ENISA for this report please use the following details:

Email: opsec@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>

PO Box 1309 71001 Heraklion
Greece
Tel: +30 2810 391 280 Fax: +30
2810 391 410
Email: info@enisa.europa.eu

www.enisa.europa.eu

Follow ENISA on

 [Facebook](#)  [Twitter](#)  [LinkedIn](#)
 [YouTube](#) and  [RSS feeds](#)

