EISAS – European Information Sharing and Alerting System

Deployment Feasibility Study

December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (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.

Authors

- Bence Birkás, security expert
- ENISA (main editor, Romain Bourgue)

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquiries about this document, please use press@enisa.europa.eu

ISBN 978-92-79-00077-5 doi:10.2788/14231

Executive summary

EISAS – European Information Sharing and Alerting – has proven to be a great opportunity to enhance collaboration and foster awareness-raising actions across Europe. ENISA helped design EISAS, but now EISAS has to run by itself.

The deployment plan presented in this document defines an information sharing concept and infrastructure and an accompanying organisational structure, where ENISA can support the Member States involved, but not drive the initiative. The study touches upon the main components of a deployment plan, such as organisational, financial, technical, legal and operational issues. By consideration of these elements, interested entities should be able to evaluate their own involvement and specific roles in the network of EISAS.

The deployment plan takes into consideration the results of the accomplished steps defined in the EISAS Roadmap so far, highlighting the main features and perspectives of information sharing. It also includes a stocktaking of relevant entities that may have an incentive to take part in the implementation part of the network. The concept of a complementary project – NISHA, that built a technical infrastructure as an interpretation of the EISAS concept, is described. Financial considerations resulted in the realisation that a successful pan-European network cannot be run on the basis of voluntary involvement and that funding will need to be secured to support different maturity phases of the network. Funding alternatives are proposed that allow flexibility fo finance based on different metrics or functions.

The deployment plan concludes with an action plan that provides a step-by-step checklist for any entity that is considering taking on the driving role for EISAS.

Table of Contents

Acronyms

AR – Awareness raising

CERT – Computer Emergency Response Team

CIIP – Critical Information Infrastructure Protection

EC – European Commission

EISAS – European Information Sharing and Alert System

ENISA – European Network and Information Security Agency

FISHA – Framework for Information Sharing and Alerting

ISAS – Information Sharing and Alert System

ISP – Internet Service Provider

NISHA – Network of Information Sharing and Alerting

NREN – National Research and Education Network

SIC – Safer Internet Centre

SME – Small and Medium Enterprises

1 Introduction

1.1 Background

The main goal of an EISAS would be to raise awareness about IT security issues among citizens and SMEs across Europe. A secondary objective is to assess the benefits of enhancing cooperation among existing activities and the added value which would be achieved by these activities as a result.

EISAS has been a long-running project driven by the European Commission that has come to its final stage with this deployment feasibility study. A lot of effort has been invested into the EISAS Roadmap, from the initial feasibility study in 2007 to the first large-scale pilot in 2012. The support, and thus the expectations of EU policy making have been driving the EISAS project and its complementary developments.

This deployment feasibility study has a double objective:

1. On one hand, this study summarises and pinpoints the basic features of a pan-European IT security information sharing system that aims to target EU citizens and SMEs as the weakest link in European CIIP. This is done by characterising the main features of the aforementioned target groups, their main user preferences, the risks and threats they face, and a brief, non-inclusive analysis of current technological trends.

2. On the other hand, this deployment plan suggests a possible method and infrastructure to reach the target groups with the aim of raising their level of understanding and awareness of cyber-related issues. The focus with this objective is to find entities in Europe willing to take the driving force over from ENISA and implement a network capable of running on its own. This is done by a brief stocktaking of relevant European entities based on the nature of their activity, partly to manage, partly to participate in such a future European network.

So far, a number of stakeholders have taken part in the previous stages established in the EISAS Roadmap[1]. Expert groups have given their views on the feasibility of such a network, with emphasis on the types of information valuable to the target groups, the legal, technical and organisational prerequisites of taking part in such a network, and the long-term viability of such a network. Furthermore, a basic EISAS toolkit[2] was developed with the intention of showing the outreach capacity of IT security awareness raising among subgroups of the general target groups, and a large-scale pilot was conducted with the participation of several Member States, validating the findings of the basic EISAS toolset.

All these antecedents lead to the approach followed by the EISAS deployment study.

[1] Ref: https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap
[2] Ref: https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-basic-toolset

2 Previous achievements

To highlight the importance of global awareness-raising actions, the European Commission has identified the key role for Member States in keeping home users and SMEs properly informed so that they can contribute to their own safety and security[3]. Subsequently, in 2006, the Commission introduced, in its communication 'A Strategy for a Secure Information Society',[4] the notion of a European Information Sharing and Alert System (EISAS) in order to improve the European capability to respond to network security threats.

In view of its role in fostering a culture of network and information security in Europe, the European Commission asked ENISA to 'examine the feasibility of a European multilingual Information Sharing and Alert System'.[5] EISAS would build upon and link together existing or planned national public and private initiatives. The EISAS feasibility study was published in 2007. It analyses the current state of affairs with regard to existing systems and initiatives in the public and the private sectors in the EU Member States, and identifies possible sources of security information that could potentially contribute to a Europe-wide information sharing and alert system. The study concludes that the most effective level of involvement for the European Union in the establishment and operation of an information sharing system for its home users and SMEs would be that of **a facilitator, moderator of discussion and a 'keeper of good practice'**. The report closes with proposals for the next steps to be taken and a **'proof of concept' scenario**.

The importance of functioning information and alert sharing systems targeting citizens and SMEs was further emphasised in 2009 by the European Commission in its Communication on Critical Information Infrastructure Protection:[6]

> *The Commission supports the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects. ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS.*

One of the complementary projects funded by the European Commission was the FISHA (Framework for Information Sharing and Alerting) project[7]. The FISHA project has initiated a network of IT security teams, among them national/ governmental CERTs, which have agreed to put into a standard format the relevant security information that they usually process to inform and alert end-users. The result of the project was a prototype model whereby they share these 'information objects' and publish them in the native languages of targeted citizens and SMEs. The follow-up to the project is NISHA, with the objective of further developing the existing prototype of EISAS achieved under FISHA into a pilot version of the system. The network will function based on an organisational model proposed within the project frames. The project will include a study of organisational and legal aspects concerning functioning of the system as well as technical development and implementation

[3] http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679
[4] http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766
[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:EN:NOT
[6] COM (2009)1493, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[7] http://fisha-project.eu/the-project

encountered while establishing the pilot, with a focus on lessons learned and suggestions for improvement.

In response to the 2009 EC communication, which called upon ENISA to produce a roadmap to further the development and deployment of EISAS, ENISA delivered the EISAS Roadmap (published in February 2011) which introduced a step-by-step approach to develop EISAS with the final objective being to fully deploy EISAS by 2013.

According to this roadmap, the basic functionalities and services of EISAS were to be developed and integrated in a regional prototype in 2011: the EISAS Basic Toolset. This prototype was to be extended to larger communities in 2012 in the EISAS Large-scale Pilot project. In 2011, ENISA furthered the EISAS approach by developing dissemination methods and testing this approach in a pilot project on awareness-raising information towards citizens and SMEs within one Member State. The EISAS Basic Toolset methodology followed a three-step approach as follows:

This approach and experiment formed a Basic Toolset that defined the basis of a larger experimental deployment involving several Member States, which was delivered in the form of an EISAS Large-Scale Pilot, implemented in 2012, as defined in the EISAS Roadmap. The large-scale deployment pilot focused on two main aspects: collaboration among the relevant key players, and sharing and distributing good practice information. Stakeholders from six Member States took part in the large-scale pilot, testing the roles of information production, information processing and information dissemination. High quality, pre-produced information was used for dissemination purposes that dealt with the topics of a) botnets, b) identity theft, and c) social engineering.

The results and findings of the large-scale pilot list a number of factors that need to be taken into consideration for the EISAS deployment plan. The large-scale pilot was conducted in an artificial environment, meaning that the content to be shared was limited, focused, and pre-produced. While the materials used were all high quality in information and production, the role of the participating disseminators only extended to a one-time translation and dissemination through their direct outreach channels. The large-scale pilot ran for a relatively short time; however, the results were measurable.

The EISAS Pilot clearly shows that participants willing to provide information have to be supported by some entity that takes over the task of information post-processing (from the point of view of the information provider) and the task of information pre-processing (from the point of view of the information disseminator). The issue of further support for a start-up phase of a pan-European EISAS needs to be solved. Some central administration or management entity should be in place that helps

- with advice for original information producers on how to produce internationally distributable materials;
- in building up an incentive system that makes it worthwhile for original information producers to become information providers (e.g., fostering PPPs);

- in bringing information providing and information disseminating partners together into teams;
- in providing services that help with professional translation and localisation of materials;
- in providing services that help overcome technical obstacles;
- in collecting best practices over time, thus making the information-brokering entity possibly unnecessary in the end.

The outcomes of the EISAS Pilot show that a situation in which dissemination and consumption of IT security information runs by itself is highly improbable, at least in the early phases of community building.

The EISAS deployment plan needs to take these findings into account and propose recommendations that solve these issues.

3 Deployment plan

To restate the concept of EISAS: citizens and small and medium enterprises (SMEs) constitute the largest group of Internet users in the EU. IT systems owned and operated by these users are more exposed to online risks, and the reason for this is that the computers of these end-users are generally less protected than those in large organisations and companies. Without proper security understanding, citizens' home computers will indirectly and unknowingly pose a threat to European critical information infrastructures.

In this context the overarching aim of an EISAS is to:

- empower all EU citizens and SMEs with the knowledge and skills necessary to protect their IT systems and information assets;
- build on national capabilities of EU Member States;
- enhance cooperation between dedicated entities in the EU Member States.

These aims are in line with high-level EU policy making. When it comes to implementation of the concept, a number of details need to be addressed. The previous EISAS activities pave the way for the EISAS deployment plan. The 'plan' itself should be treated as a collection of findings, as it is not possible to provide a single straightforward solution for deploying EISAS. A number of factors need to be considered before finding a solution that meets the expectations of the interested stakeholders. These factors should include technical/ organisational, political, and social/ cultural aspects.

Technical/organisational aspects must take into consideration the current state of affairs: the basic components of the ISAS have not gone under major upgrade since the initial feasibility study. Information production/ information gathering – information processing – information dissemination will need to be followed for all ISAS prospects. The workflow can be aided with an infrastructure dedicated to this purpose – the results of the NISHA project. However, this assumes a uniform solution for the EISAS.

There must be a strong commitment to any proposed way of running a local ISAS, whether it is public or private entities taking the driving role. There needs to be support, possibly in the form of financial recognition. It is beneficial if a newly established ISAS will not be competing with a well-established local model, but becomes a part of it, or operates in complementary areas. To map the complementary areas, it is suggested to assess the outreach capability to target groups of existing initiatives, and focus on the uncovered areas offered by the EISAS model, especially the European networking capacity.

The social/cultural aspects must take into consideration the current perception of IT security issues, user preferences of devices or applications, and their predictable needs in terms of usable information. This will play a vital role in being able to define which types of information dissemination should be focused on.

3.1 Setting the scene for possible actors of EISAS

The EISAS will be able to add most value to its users and operators if all roles of the system are taken care of by the most suitable entities. The deployment plan needs to clearly describe the functional and operational needs of the system. With regard to functionality, there are three key areas in a well-functioning EISAS, which are:

- information production
- information processing
- and information dissemination.

By operation, two main fields can be distinguished. These are:

- Community and Network supervision, where tasks include community governance, terms of reference and guidelines, secretariat functions for membership issues and technical/ operational aspects of maintaining the network for the benefit of the operators;
- Network Operation, where tasks include core activity from information gathering/ production to dissemination, and management of local IT systems. Enhanced network operation may involve assistance of the supervisor with network management activities. This applies, if a uniform infrastructure (e.g. NISHA) is preferred for deployment.

No less important is the need for a proper understanding of the current trends in IT security awareness raising and the comprehensive picture of user preferences. The EISAS Basic Toolset and the large-scale pilots already put emphasis on three currently valid online threats (botnets, identity theft, social engineering), which proved to be useful tools for the end-users based on perception and understanding. The contents disseminated through the local ISAS should focus on the following areas to provide full coverage of awareness raising and alerting types of information:

- description of main threats through exploitation (malware, ways of infection, targeted attack, vulnerabilities);
- description of main threats through using online services (online banking/shopping, cloud-based storage, ways of authentication);
- description of online social behaviour (social networking, cyberbullying, illegal and harmful contents);
- trends in most common hardware and software: desktop computers, laptop, mobile devices, untrusted applications, unpatched software, pirated software, wifi threats;
- cyber legal issues.

3.2 Potential actors of the EISAS

The challenge to deploying a successful EISAS is in finding the right types of entities that have the willingness to commit to the system, have the appropriate channels for outreach, and understand the topics of IT security awareness raising. Each area needs experts in their own profession. Based on the currently ongoing awareness-raising schemes, the following entities by nature can be defined as actors in the deployment process:

- **ISPs/communication companies**: these companies serve all users with Internet access, thus have an elemental interest in providing security-related information to their customers. ISPs/

communication operators are for-profit organisations and have a professional corporate structure including technical operation, marketing and PR. Their benefit is that they operate professional informational portals, where an ISAS could fit as a complementary element and they already have a good client base that would use this additional service. These companies often provide IT security tips on their own, and sometimes even produce quality AR material. Many of these companies have cross-border affiliations, so they can reach a number of EU citizens in several Member States. Since these companies are competing with each other, it is unlikely that they will jointly form an EISAS, but if enough incentives are available, one major player could be involved. These companies have a high potential of being information producers, processors and disseminators.

- **CERTs**: initially, CERTs/network security teams were considered to be the most suitable entities to participate in the EISAS, as they are managing early warning systems and have a high expertise in IT security issues. Previous EISAS involvement aroused mixed enthusiasm from national/ governmental CERTs due to the fact that engagement stretches as far as their national mandates. CERTs usually are small in staff and focus on core activities. In order to run the local ISAS, they need to build new dissemination channels, which are time and resource consuming. CERTs also operate in corporate environment or academia, and their possible involvement depends on their level of autonomy and interest. The great advantage of the CERTs is that they work in extensive networks and their activity is highly built on trust. CERTs also have a high potential of being information producers, processors and disseminators.
- **Safer Internet Centres**: the Safer Internet Programme[8] is funded by the EC, and it promotes a safe and secure online environment for children. The focus with the EC funding is on general training and awareness raising, providing helplines with prompt aid through telephone or chat services, and an online reporting point for the removal of illegal and harmful content found on the internet (hotlines). With these aims, information sharing fits very well into the activities of the SICs, but there is a limitation to their mandate. Taking up the role of a local ISAS would be a voluntary involvement, which is not among their core activity, therefore current funding would not be eligible for that. The benefit of the SIC, similarly to the CERTs, is that they cover Europe in an extensive network. The challenge for the SICs would be recruiting staff with enough IT security expertise to handle information gathering and processing. SICs produce quality resources in awareness raising and have a high potential of disseminating information.
- **Child welfare organisations**: in terms of interest and involvement, these organisations would represent a subset of the SIC entities. Many of the child welfare organisations (e.g. Save the Children[9], eNACSO[10], etc.) are running helplines or hotlines. These services assume some dedication to IT security related topics, mostly focusing on cyber bullying or privacy or removal of illegal content. Participating in an ISAS would be a relatively new field for these organisations, but they could have a role in either information dissemination or multiplication. Challenges to their involvement would be similar to the SICs. Child welfare organisations have a good potential for outreach capacities.
- **Media/content industry**: this set of entities covers a huge industry, and their involvement needs to be considered with the caveat that news channels and positive online content providers could have an active part in the EISAS. As ISPs/ communication providers, these entities are for-profit organisations. If involvement in an ISAS will provide better market value or more viewers, these companies could be convinced to participate. Their benefit is having multiple channels of distribution, from traditional broadcast and print media to online

[8] http://www.saferinternet.org/
[9] http://www.savethechildren.org/
[10] http://www.enacso.eu/

channels, so they are capable of influencing public opinion. In case of urgent need for quick outreach, the media/content industry is the best option. These companies have a high potential of being information producers, processors and disseminators. A special subgroup of the content industry is the governmental gateway for electronic services, which in each Member State is regarded as a trusted source of information, and a vast group of citizens and SMEs use the services provided by these gateways. However, special care is needed here as these for-profit company could use EISAS only to serve their commercial interest.

- **Public authorities**: national telecommunication regulatory authorities (NRAs) and national consumer protection authorities have are the best prospects for taking part in EU-wide cooperation in information sharing, inclusive of IT security. These authorities are in direct contact with industry players – those who provide services – and consumers. The benefit for public authorities taking the driving role in running the EISAS is that a supplementary legal mandate can make a good basis for this activity among their other activities. Such a mandate also presupposes the allocation of funding sources for participation. These organisations have a good potential of being information producers and disseminators.
- **Academia**: educational institutions take the lead in innovative services, therefore they can be regarded as a good option for running local ISAS as well as playing an important role in driving the whole network. Universities are known for research and collaborative work, and this asset could be exploited to guarantee that development and support is in place for the EISAS. Another advantage of academia is the resource in terms of workforce, as voluntary involvement could be worked out among students and researchers. Incentives can be worked out for participation within the interested organisations, if academic involvement seems feasible. Also, the academic sector is connected via a common network (NRENs), which already supposes a wide European network. The operators of the NRENs possess a high expertise in IT security issues, and many of these teams also have CERTs in place to oversee secure network operation. A further advantage of the academic involvement is that they can share first-hand information for the EISAS network based on the research activities of the institutions. Academia has a high potential of being information producers, processors and disseminators.
- **Consulting companies**: the private sector may find added value in running an ISAS for the local community, if this service will add a higher public recognition, thus better market value for the companies. The benefit of these specialised SMEs is that they are flexible and have a rather quick decision making processes. The condition for a successful privately run ISAS is that they can deploy a functioning mechanism (including the infrastructure) and focus on the information production cycle. Outsourcing an ISAS activity to a consulting company by a public organisation could also be considered a viable way, in the framework of an SLA-based agreement. This would, however presuppose the decision for operation and funding at a higher level. SMEs are quite vulnerable to quick changes in market conditions, so ideally an ISAS would not be the core business of a participating entity. Human resources and expertise can be allocated to the ISAS activity based on its proportion in the corporate business portfolio. Private companies have a good potential for information production, processing and dissemination.
- **Financial organisations**: banks and banking associations in several Member States realise the need to educate the end-users on basic IT security skills. This comes from the consideration that client-side systems are much more vulnerable to IT threats than the banks' IT infrastructure, but more and more services are available online, where money is at stake. Banks need to make sure the clients are equally well protected, therefore raising awareness on a continuous basis could lay the foundations for for an EISAS driven by the financial sector. There are a number of EU-wide initiatives of the financial sector that deal with cyber threats,

so the networking aspect is already in place, with high expertise in the sector. Although the financial sector is strictly a for-profit business, they are known for their generous donation spirit. Local banking associations could take the lead in running the ISAS with the collaboration of local banks or could allocate funding for outsourcing such an activity to e.g. SMEs or CERTs. Banks could invest in producing quality resources, and would be considered as good disseminators.

- **Professional interest groups**: a number of sectors have their own interest groups both on national and European level. High-level decisions are taken and lobby power is exercised in such interest groups, so one of these groups might present a good prospect for the EISAS management function. Education, child welfare, telecommunication, finance, etc. are all fields that would find an overarching incentive in raising awareness for the end-users. These European interest groups already employ a secretariat to look after their daily business, so the additional activity of managing an EISAS is feasible. A success factor for these professional organisations would be the involvement of their members in running the local ISAS, as a network of like-minded entities could achieve better cooperation and information exchange. In cases where large vendors, multinational service providers decide to take part in an interest group driven initiative, the terms of reference of EISAS should lay down that the network shall not be used as a marketplace of products and services, but serve as a general information sharing facility for awareness raising topics.

Type of entity	information producer	information processor	information disseminator
ISP/telco industry	5	4	5
CERTs	4	4	3
Safer internet centres	3	3	5
Child welfare organisations	1	3	4
Media/content industry	5	5	5
Public authorities	2	4	4
Academia	4	5	5
Consulting companies	2	3	3
Financial institutions	2	3	5
Professional interest groups	na	na	4

Ranking of capability, where 1 is the lowest, 5 is the strongest; na, if not relevant

3.3 Possible infrastructure for EISAS: the NISHA system

As referred to in section 2, 'Previous achievements', two complementary projects running parallel with the EISAS Roadmap have received funding from DG HOME in the framework of the CIPS

programme. [11] The FISHA [12] project started in 2009 with the objective of implementing an interpretation of the EISAS model. The focus of the project involved three main areas:

- a **technical solution** for information sharing: a P2P network and a network of local nodes,
- a **policy framework** including a dissemination concept and recommendations for a sustainable management model,
- a **communication plan** drawing up a communication matrix and a characterization of the main target groups.

The project ended in 2011 with a proof-of-concept. It proposed a cooperative technical platform to allow effective sharing and dissemination of awareness-raising information for citizens and SMEs. In the context of the EISAS pilot, FISHA provided technical means for disseminating information security information among information producers and information consumers. It enabled actors of the framework to efficiently:

- build up a common database of available awareness-raising material,
- browse within this database,
- notify each other with newly available material,
- exchange and contribute to the shared materials,
- give local information brokers access to locally adapted material.

The follow-up to the FISHA project is NISHA.[13] It builds on the achievements of the proof-of-concept with the objective of building a pilot network to demonstrate the viability of the technical and policy interpretation of the EISAS model. The project started in 2012 and will finish in early 2014. The technical solution has undergone a major review and both front-end and back-end have been upgraded.

Based on the current scheme, the portal is built on the open-source Drupal portal engine and exposes certain functionality of it. This is a commonly used module-based CMS for content publication and management. The contents on the portal are stored in a SQL database. The unity of the individual portals connected to each other is the NISHA network. The portal is coherent with the main workflow of the NISHA concept. It provides a surface for

- **information gathering**, either from the network or from outside sources through RSS feeds,
- **information selection**, including batch selection,
- **notification, translation and tagging**, including short descriptions, native language long description,
- **publication**,
- and **profiling**, making predefined profiles for dedicated users (including information brokers).

The NISHA network is a P2P network based on CouchDB database engine. Beside the general SQL database every portal is connected to a CouchDB database. The CouchDB stores the contents created and shared (pushed to network) by the portals. Each CouchDB stores all the articles which were pushed to the network. NISHA operators can create contents on their own portals and they can also share it through the NISHA network with the other NISHA portals. Contents appear on the portal after supervisory approval.

[11] http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/index_en.htm
[12] Framework for Information Sharing and Alerting, http://fisha-project.eu/
[13] Network for Information Sharing and Alerting, http://nisha-network.eu/

Based on the initial FISHA concept, NISHA proposes a management model with four players ('the FISHA Model'):

- **Operators of the network** (the local ISAS), which are either basic nodes or supernodes by function;
- **Information Producers**, who are reputable IT product vendors or IT security specualists;
- **Local Information Brokers**, who are any entities that can help the network operators in relaying the disseminated information;
- **Information Consumers** (i.e. Citizens and SMEs), as the recipients of the information.

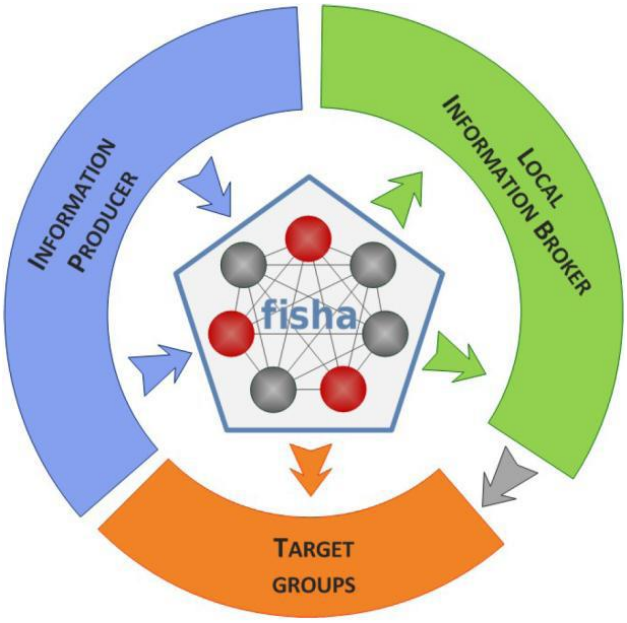


Figure 1: The functional setup of the NISHA network

Operators of the FISHA network are central in this model as they are the main players in running a national ISAS. The producers and brokers are certainly critical, but complementary to the network security organisations. According to this model, national/ governmental CERTs, as well as other organisations with a mission to raise awareness among citizens and/or SMEs in the Member States would fall within the category of network security organisations even though, to some extent, they can also be producers and brokers of IT security information.

Furthermore, the FISHA project proposed two kinds of node to be established for administering the cooperation between these players: at least two 'supernodes' and several 'basic nodes'. From a technical-administrative point of view, the organisations representing the 'supernodes' would, among other things, be responsible for managing the network of 'basic nodes'. The combined activities carried out by the 'supernodes' and the 'basic nodes' can be described as fulfilling the roles of the national ISAS. Technical criteria of 'supernodes' and 'basic nodes' are documented as part of the NISHA project, and any entity with the willingness to abide by the basic requirements of the framework can take up the role of the national ISAS.

3.4 Operating the system

The deployment plan needs to lay special emphasis on the operational aspects of the EISAS. The key to success in terms of awareness raising is the ability to reach the target groups with timely information both in quality and in quantity. The essential difference between a well-working local awareness-raising initiative and a Europe-wide cooperation is networking. While a locally funded initiative is likely to run according to predefined local requirements, the networking aspect to gather and share information may not have been considered. Regardless of a uniform technical solution, sharing materials with a cross-border community is on a voluntary basis.

The EISAS large-scale pilot demonstrated that cross-border information exchange among various stakeholders can work without a dedicated infrastructure, with the caveat of a simplified workflow by delivering pre-produced materials to participants. Generally, mailing lists and some web-based repository could serve the purpose of notification and information exchange at European level among the operators of the network; however, a professional solution for dissemination is still needed to minimise the need for network coordination. The NISHA system would solve this issue by merging all operational steps into one common platform.

The biggest challenge with cooperation is putting the operating costs in balance with the added value of participating in the network. Running the EISAS can't be a voluntary involvement, especially for those stakeholders, whose core activity is not related to IT security. Equipment, if needed, is a one-time investment, however maintaining the system and producing information requires active involvement that can be translated to man-hours that will incur costs. The most time-consuming activity in the EISAS information production cycle is processing the available information, meaning a lengthy translation and classification process. The success of EISAS relies on the quality of information shared among members and disseminated to target groups. These indicators need to be high enough to provide incentives for participation. Although there is a clear social benefit of a successful awareness-raising campaign, the main incentive for the participating entities is the recognition by financial support.

3.5 Proposals for funding the EISAS

As cost levels vary from country to country, definite estimates of operational expenditure of a local node cannot be given as part of the deployment plan. However, operating the technical environment and the information production workflow can be estimated in terms of workforce. Technical staff does not need one full-time equivalent for managing a local node. But information production should require at least two half-time engagement, adding up to one FTE. Additional management and communication expertise is needed to build the basic information dissemination and multiplication mechanism.

Sustainable funding models are a vital question in the existence of the EISAS network. Each phase of maturity requires a different type of funding or financial support. There are two main elements to distinguish in the NISHA concept that both require financial resources:

- the network that connects all the ISASs; that is, being a cross-border initiative
- the local ISASs, having a national responsibility.

While defining the steps of EISAS was a task carried out by ENISA, there was a clear determination from the initial phase that the concept has to run on its own. Suitable entities need to take the driving

role of managing and fundinbyig the EISAS. The complementary FISHA/NISHA projects proved that without secure funding, voluntary involvement in the programme is questionable; therefore it would be a reasonable approach to continue with deployment involving funding form the EC.

The aim of the deployment process would be to involve and extend the number of ISASs in Member States; therefore solutions need to be in place that will encourage new countries to join. There have to be financial incentives for the interested entities. The role of European financial support should remain to some extent, with the focus on supporting new ISASs and the maintenance of the network. Since the network is supposed to function on an informal basis, financial support should be provided on an individual basis. Proposals for funding should cover the extension of the network, where new ISASs should have the possibility to apply for funding for certain functional or operational tasks.

As an **incentive**, the following proposals should be considered:

- Interested entities should be able to apply for financial support to procure equipment needed to start up the ISAS. This amount should require a relatively small investment on behalf of the funding entity, and this type of support should be a one-time possibility. The funding should not be automatic when joining; there should be a funding scheme to apply for.
- New entities should be able to apply for financial support for the staff directly working at the ISAS. The conditions for this incentive have to be well defined and regulated. There have to metrics applied for this type of funding that are capable of setting some minimal standard on quality or quantity. As a rule, this type of funding should only be applied as post-financing. It is to be decided whether this type of funding should be applied for only one term or should be continuous based on the metrics.

The following considerations need to be taken into account, if the NISHA infrastructure is supported for the EISAS deployment.

- Maintenance of the network requires financial resources. The supernodes should be able to seek financial support for operating the network. It is desired that more than one supernode operate the network, and preferably the management entity providing the secretariat also runs one of the supernodes. With this condition it can be guaranteed that the network will operate, but does not regulate the number of supernodes. This proposal is based on the demand that the network operates on an EU-wide level, thus supernodes have more than national competences.
- There should be a procurement call for the maintenance of the network. Since the network is an informal network, the legal entities responsible for the supernodes should be able to form a consortium and bid for funding. This funding should be available for 1-year terms, and should cover the approximate work needed to run the network and be able to provide network support for the nodes.

At a later stage, the EISAS participants could create a **formalised network**. This will be possible when the number of ISASs reaches the critical mass, and the impact of the network can be measured on a European scale. Formalising the network can only be successful if there is sufficient interest from the majority of the participating entities. An association would be able to secure the operation of the network by entering into contract. Also, the benefit of a formalised association would be the less administrative burden from the participating nodes, as a secretariat would handle all administrative issues and could enter into contracts with third parties on behalf of the association. Thus, roles of the secretariat would be to guarantee the maintenance of the network by finding the appropriate sources

of funding. Vendors, the IT industry, European bodies and interest groups could come into consideration as contracting parties for funding the network.

With the formalisation of the network, another way to secure financial resource to maintain the system is on the basis of membership fees for the members of the association. The benefit of this solution is that members sustain the operation of the network by paying for the services of a secretariat that administers the network. The disadvantage of such a secretariat is the operating costs of the secretariat. It is unlikely that another formal group requiring membership fees will be welcomed in Europe.

One significant drawback of the formalised model is that participants lose the concept of voluntarism and openness. The aim of EISAS is to create a community based on common interest and involvement on best effort, while a structured and formalised model leads in the direction of a closed membership group. Another important aspect of the open community is the fact that the 'information' the EISAS is dealing with is basically publicly accessible information, regardless of the various copyright policies. Limiting the flow of the already available information instead of multiplying it will not be beneficial in the course of the EISAS deployment, as the ultimate goal would be shortening the flow of usable information to the target groups.

3.6 Management aspects

A strong management approach is needed to ensure that there are continuous incentives for the participating entities in the EISAS network. Therefore, a high level of commitment is needed from any organisation that takes up the driving role of the network. Professional interest groups could take the lead in this aspect, as they possess enough lobby power and industrial support to carry out this activity. The starting point of organising a pan-European network would be a clear scope and vision of EISAS, with a terms of reference, membership criteria, and a code of conduct that will govern the operational work of the participants. The management body should cater for the possible funding options, should provide guidelines of cooperation models, and should liaise between industry partners as information producers and possible sources of funding.

The management body should also be responsible for continuous communication on behalf of the network, providing growing visibility among industry, the Commission, and the end-users. A secretariat needs to be set up to facilitate the work of the management body. In terms of technical support, either the management body should be responsible or appointed members of the network could take the lead, depending on the infrastructure used for deployment.

The introduction of a steering committee is also advisable, where strong leadership qualities merge with industry-wide recognition and reputation. Members of the steering committee should consist of representatives from industries having high outreach capacity (ISPs, content industry), academia with high innovative power, or representatives of well-established local information sharing models, and representatives of the network management organisation. The benefit of a well working steering committee would be to find links to existing schemes to raise visibility and awareness, such as the Safer Internet Day or the European Cyber Security Month, or foster the cooperation between public–private partnerships.

To this end, the management body will need to create a concept for networking and liaising between involved parties in the form of annual meetings, workshops, exchange of ideas, management of development issues. Synergies need to be exploited between existing initiatives and programmes to

help the EISAS community fit into the established IT security communities (CERTs) or the awareness-raising communities (SIC). Local best practices need to be shared among members to foster new types of cooperation in Member States.

Management also needs to be able to assess the operation of the network in terms of statistics. Metrics need to be set up to measure the impact of the system. Usable values depend on many factors, but basic considerations should include the following statistics:

- the number of Member States deploying the EISAS,
- the number of items disseminated through the EISAS as a whole, and per country,
- additional content/service offered by local ISAS,
- local visibility of the ISAS by number of website visits, downloads,
- the number and types of local cooperation mechanisms of the ISASs to multiply their information,
- ad-hoc and organised campaigns to raise awareness of the system, either by the EISAS as a whole, and per country,
- measuring the effectiveness of local campaigns by pre- and post measurement, as proposed by the EISAS basic toolset.

3.7 Legal aspects

An important factor in the EISAS concept is the availability of the information that can be used to share with the target groups. As the main concept is to make information available in native language to all European citizens and SMEs, copyright issues need to be handled in such a way that the information processing workflow does not infringe copyright policies. A lot of information is available on the Internet that the end-users should be aware of, but copyright and licensing issues sometimes inhibit sharing on a large scale.

The relevant information types the EISAS intends to use for dissemination are:

- alerts and warnings
- advisories
- best practices and awareness-raising materials, in the forms of leaflets, videos, cartoons, etc.

Information producers put a lot of effort into producing quality information that end-users can use and benefit from, but this also assumes that they want to take credit for their own materials. It is evident that the source of information is always referred to, but from a legal point of view, this is not enough. Content needs to be published in the EISAS network regularly and dissemination needs to be ensured.

A licensing policy is needed that would solve this issue at a pan-European level. Currently, two types of licensing schemes exist that allow setting the permission level of the original information. Since translation is a crucial step in the EISAS workflow, permission to do this needs to be granted by the information producer. The Creative Commons[14] and the Open Data Commons[15] are capable of solving this issue to some extent. The disadvantage of these licensing schemes is the amount of information available under these licences. If the EISAS network were to rely on information produced only by its

[14] http://creativecommons.org
[15] http://opendatacommons.org/

members, the amount of information would not reach the critical mass to make the EISAS network a trustworthy source. Also on this note, some of the involved entities would be regular information producers, while others in the network would be information disseminators, which would make the network unbalanced. For the sake of the EISAS, corporate licensing policies would not change. The management body would face the challenge of securing enough trusted and useful information sources to make the network work.

In terms of the infrastructure, the NISHA project proposes using the EUPL[16] licence for the software. The EUPL is the European Union Public Licence, published by the European Commission. The EC strategy is to reinforce its legal tools for facilitating sharing, reuse and interoperability. This ambition is in line with the concept of the EISAS.

3.8 Target group analysis and outreach strategy

The target groups that EISAS aims to reach, by categorisation of the initial feasibility study, are citizens (home users) and SMEs (small and medium enterprises). To understand how outreach should work, the strengths and weaknesses of the target groups must be identified, meaning that the proposed communication channels should fit with the strengths and weaknesses of the target groups.

Home users are citizens of varying age that are using ICT (information and communication technology) for personal purposes. This target group can be further divided into different categories:

- Children
- Teenagers
- Youths
- Adults
- Older users

Youths and teenagers are typically between 7 and 15 years old and have grown up in an ICT environment. Their level of knowledge is related to the state of infrastructure in their respective country. The strength of these citizens offers a high capacity for learning and open-mindedness toward new technologies. A weakness is that they may take security for granted. They feel safe because they have their parents and peers. Using innovative technologies and education-driven materials should fit the needs of this group of users. The main advantage of this group is that they are strongly related to ICT.

Adults are citizens born after the 1950s and older than 16 years of age. Their knowledge of general ICT ranges from non-existent to high-level, which makes it difficult to define the right channels of communication to reach them. A compromise could be to use common and well-established communication channels to cover a huge amount of citizens. If special communication channels are used for the subset of youths and older users, adults will likely be reached as well.

Older users are the most difficult group of users because they have not grown up with ICT. Their experience ranges between non-existent and low. They are more focused on traditional communication channels such as newspapers or news television. As they have not grown up with ICTs, they may be more doubtful of, or mistrust, technology.

The SME target group consists of employers and employees from micro, small and medium enterprises. For this analysis the most important difference between the sizes of the enterprises are the competencies in ICT and IT-Security within the enterprises. They range between non-existent and good knowledge depending on size and business line of the enterprise. For example a micro enterprise

[16] https://joinup.ec.europa.eu/software/page/eupl

typically does not have an expert for ICT or IT-Security. As the size of the enterprise increases, the probability of having an expert will also increase.

In addition to size, there are different categories of users an SME is likely to employ:

- Executive Management
- Mid-level Manager
- Employees
- System Administrator

Executive Management is the key decision maker for investment in IT security. Raising their security awareness and concerns is crucial for establishing a basic protection of ICT. If they consume information, they must be able to detect the message of IT security in an easily understood manner. This translates to why they should invest in new technologies and why they are crucial for their business.

Mid-level managers within SMEs are often not technically orientated, but experts in their own respective fields. They must be made aware of the importance of IT security in the production cycle. Their consumption of information is rather similar to that of the executive management. The difference is that the executive management makes the final decision.

The largest and most important user group is the employees. Most information security breaches are caused by human error. The awareness level of employees is similar to that of home users but the impact of breaches is much higher. Therefore, it is most important to raise their IT security awareness.

System administrators are usually responsible for configuring IT systems of SMEs, either as employees or as contractors. System administrators are therefore specialists and are technically orientated. They should also have good information security awareness, as complete systems may depend upon their capacities. Furthermore, they know how to implement IT security policies and controls.

The table below shows several channel of communication which could potentially cover the needs of the defined target/ user groups. For successful outreach purposes, information disseminators with the ability to reach the target groups through these communication channels are advised to be involved in local cooperation mechanisms.

	Target groups	Advantage	Disadvantage
Comics, cartoons	Youths, Employees	Real-world context	Difficult for detailed messages
Distant Training	Youths, Adult, Employees, IT and Business Management	Detailed message content, geographically independent	Expensive, Needs trainer
Email	All	Cheap channel to target all	Messages may be undermined, addresses must be known
Newspaper	All (excluding Youths)	Cost-effective medium to reach mass audience	Clutter factor, Short life of papers
SMS / Twitter	All (maybe excluding older users)	Can be delivered direct	Effective for alerts, not for raising awareness
TV (alternative YouTube)	All	High-impact, as close as face-to-face communication	Costs
Radio	All	High frequency at a reasonable cost, Specific audience per music	Commercialisation, Radio spot lacks the permanence of a printed message, A single station can seldom offer broad market reach
Website or Newsfeeds	All (excluding older users)	Can be updated, Content for multiple audiences, Easy links to other information	May be undermined because of abundance of websites, requires development
Competitions, Quizzes or Games	All	Reach wide audience and engaging them to thinking about it	Difficult for detailed messages

4 A SWOT analysis of EISAS

A basic approach to evaluating the conditions of deployment of the EISAS in a structured way is through a SWOT analysis. These factors sum up the main characteristics of deployment.

STRENGTHS	WEAKNESSES
- The same type of IT security AR information would reach the end-users across Europe - Metrics would allow regional assessment of IT security awareness - Coordinated campaigns can take place in Europe (complementing Safer Internet Day, European Cyber Security Month, etc.) - Use of multiplying channels reaches a vast number of end-users - Information sharing is in native language	- Time consuming to build up and promote a national ISAS - Resource-consuming: time, money, skill, cooperation - Hard to compete with well-established international AR sites, initiatives - No interest in voluntary AR engagement, if requirements are fixed but incentives are not
OPPORTUNITIES	**THREATS**
- An alliance of like-minded organisations can drive the EISAS initiative; the common denominator will be raising the IT security awareness level of end-users - A uniform technical infrastructure is available for the deployment phase - An ISAS can complement an existing national AR initiative - A well-functioning EISAS is a good basis for agreements with information producers, information brokers - A cross-border cooperation framework will enhance collaboration among stakeholders from information production to information dissemination to end-users	- Lack of funding inhibits the start-up of such a network (lack of local funding to maintain national ISAS, lack of funding for maintaining the European network) - Few number of interested entities from Member States volunteer to run a local ISAS - No entity taking responsibility for facilitating the network operation - EISAS is only successful in long term, if involved entities have a common understanding of the aims and a common background of expertise (IT security AR)

5 Action plan for deployment

The action plan assumes the motivation of an entity to take the lead in organising the EISAS network in several Member States and undertake the management role of running the network.

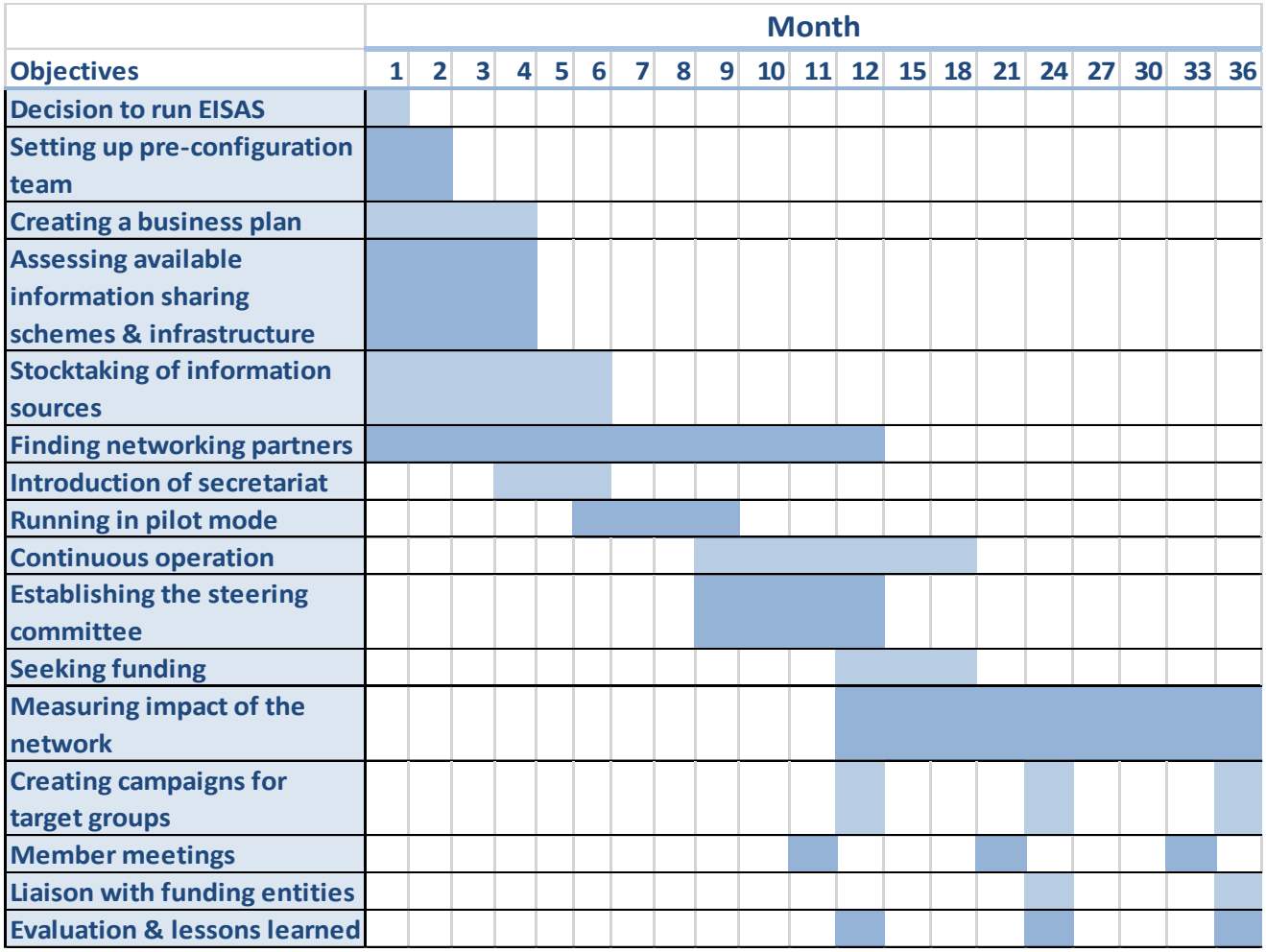
The action plan lists a set of objectives with the accompanying tasks needed for implementation. Each objective defines a desirable timeframe and the criteria for the successful implementation. Threats that may inhibit the step in deployment are also taken into consideration.

	TASKS	TIMEFRAME	SUCCESS CRITERIA	THREATS
Decision to run EISAS	Documented decision on reasons and aims	Month 1	Long-term determination is needed	Change in management's approach
Setting up pre-configuration team	Staff & equipment	Month 1-2	Dedicated team	Unbalanced expertise in technical, financial, legal field
Creating a business plan	Setting the vision, listing the necessary equipment, costs & sources of revenue	Month 1-4	Clear and detailed plan, balanced focus on all aspects of operation	Underestimation of costs
Assessing available information sharing schemes & infrastructure	Review EISAS, NISHA materials, other available concepts, focus on infrastructure and information types, specify target groups	Month 1-4	The infrastructure should be chosen for at least 3 years, participants should receive an easily deployable product	Lack of support in technical deployment, complicated workflow
Stocktaking of information sources	Finding possible supply from all EISAS information types	Month 1-6 Continuous	Copyright issues are solved, incentives are offered for the information producers	Lack of interest in sharing copyrighted materials
Finding networking partners	Communication on intention to future/possible participants; description of benefits and requirements	Month 1-12 Continuous	At least 3 partner need to join, letters of intent are needed from more	Lack of interest from addressed partners; indecision to join slows the action plan

	TASKS	TIMEFRAME	SUCCESS CRITERIA	THREATS
Introduction of secretariat	Build continuous liaison with all relevant stakeholders	Month 4-6	Dedicated team, ability to help members of the network	Slow response
Running in pilot mode	Deploy chosen infrastructure with at least 3 participants; test functionalities; identify and fix main bugs, keep a repository of minor bugs	Month 6-9	Ability to fix bugs and apply further developments	Delay in full functionality
Continuous operation	Allow new participants to join the network using a stable version of the software	Month 9 onward	Support from secretariat, new applying members	Low number of dissseminated items, inability to reach target groups
Establishing the steering committee	Invite potential members to the steering committee	Month 9-12	View of the steering committee members is accepted by the network members	Inactivity of steering committee members
Seeking funding	Develop a clear model and scope for funding; supply underlying numbers to support funding inquiry	Month 12 onward	Identifying alternative channels for funding	Lack of sufficient funding sources, miscalculated financial plan
Measuring impact of the network	Producing statistics on operation	Quarterly from start of operation	Unbiased information	Delay in information submission
Creating campaigns for target groups	Finding local partners for promoting EISAS to the target groups	Annually (in conjunction with existing campaigns)	Well established local dissemination and cooperation mechanisms are in place	Low impact of campaigns
Member meetings	Sharing experience, best practices, involving new members	Annually	Representation from all participants	Negative opinions can undermine dedication of the network

	TASKS	TIMEFRAME	SUCCESS CRITERIA	THREATS
Liaison with funding entities	Demonstrating	Annually (on demand)	Demonstrating growing impact of network	Weak performance compared to business plan
Evaluation & lessons learned	Analysing operation, revision of expectations	Annually	Identifying gaps and discrepancies of the network	Loss of interest in case of negative outcomes

The action plan is proposed for a timeframe of three years, where the first year of deployment is broken down into more details, while the second and third years assume continuous operation with reoccurring tasks. In terms of time investment, a Gantt-diagram illustrates the deployment schedule in a more straightforward way.



6 Conclusion

EISAS is a concept that aims to fill the gap in IT security awareness information sharing to European citizens and SMEs. The EISAS Roadmap has the deliberate aim of designing a system that is capable of standing on its own, with the ultimate objective of enhancing the resilience of the European cyber domain.

In the course of the EISAS programme, a feasibility study has been delivered, a basic toolset was designed for the exchange and dissemination of information, and a large-scale European pilot was conducted to validate the findings of the toolset in a cross-border environment. As a last step of the EISAS Roadmap, this deployment feasibility study, outlines the direction for the deployment of the concept.

Such a deployment requires dedication and effort. The success factor of the deployment lies in the **motivation** of the main actor willing to take the driving role in managing the whole network. The action plan for deployment is addressed to this special entity, detailing all the achievable milestones to ensure sustainable operation. Incentives need to be kept in the forefront, so participation in the network will grow to a scaleable level with measurable impact.

A good balance of the main aspects of deployment need to be considered:

- A good target group and communication channel analysis to ensure that the appropriate types of information reach the end-users, which also assumes cooperation mechanisms at local level to raise the visibility of EISAS to an appropriate level,
- A reliable infrastructure that helps the information production workflow to help the operators of the network, and also provide a user-friendly interface to attract users,
- Alternatives of funding the network that allow a sustainable, long-term operational model,
- Clear legal conditions that support the flow of the information types, solving the issues of copyright and content licensing,
- Operation and management issues that keep the voluntary feature of the concept, while providing a framework of governance and supervision.

References

Related ENISA papers

[1] ENISA (2007), EISAS – European Information Sharing and Alerting System

[2] ENISA (2011), EISAS – European Information Sharing and Alerting System for Citizens and SMEs: Implementation through cooperation

[3] ENISA (2011), EISAS – Basic toolset 1.0, Feasibility Study of Home Users' IT Security

[4] ENISA (2012), EISAS – Enhanced Roadmap 2012

[5] ENISA (2012), EISAS Large-Scale Pilot, Collaborative Awareness Raising for EU Citizens & SMEs

Legislation

[6] European Commission Communication on Critical Information Infrastructure Protection – COM (2009)1493

[7] European Commission Communication: A strategy for a Secure Information Society – COM (2006)0251

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu