



EUROPEAN UNION AGENCY
FOR CYBERSECURITY



CROSS-SECTOR EXERCISE REQUIREMENTS

MARCH 2022

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of information and communications technology products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found on its website (<https://www.enisa.europa.eu/>).

CONTACT

To contact the authors, please email resilience@enisa.europa.eu

For media enquiries about this report, please email press@enisa.europa.eu.

AUTHORS / EDITORS

Herve Debar, Olivier Caleff, Jurica Cular, Argyro Chatzopoulou, Rossen Naydenov (ENISA), Edgars Taurins (ENISA), Andrea Dufkova (ENISA), Fabio di Franco (ENISA)

ACKNOWLEDGEMENTS

ENISA would like to thank the following ISACs for their contribution:

Financial Services ISAC (FS-ISAC), European Financial ISAC (FI ISAC), European Energy (EE) ISAC, European City ISAC (I4C+), European Rail (ER) ISAC, European Maritime (EM) ISAC

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

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

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.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2022

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0)





licence <https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated”.

Cover image and images on the cover © Shutterstock

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-570-8

doi:10.2824/941158

TP-07-22-113-EN-N



CONTENTS

1. INTRODUCTION	6
1.1. OBJECTIVE AND SCOPE	6
1.2. METHODOLOGY	6
1.3. SURVEY INFORMATION	6
2. GENERAL CONTEXT	8
2.1. WHAT IS A EUROPEAN UNION INFORMATION SHARING AND ANALYSIS CENTRE?	8
2.2. OVERVIEW OF INFORMATION SHARING AND ANALYSIS CENTRES	8
2.2.1. Overview by sector	10
2.3. STRUCTURE OF INFORMATION SHARING AND ANALYSIS CENTRES	11
2.4. EXPERIENCES OF AND PREFERENCES FOR EXERCISES	11
3. KNOWLEDGE AND SKILLS NEEDED BY INFORMATION SHARING AND ANALYSIS CENTRES	13
3.1. SKILLS ANALYSIS FROM THE SURVEY	13
3.1.1. Finance sector information sharing and analysis centres	14
3.1.2. Transport sector ISACs	15
3.2. LEGAL AND COMPLIANCE SKILLS	16
3.3. INFORMATION ANALYSIS AND TRIAGE SKILLS	16
3.4. TECHNICAL SKILLS FOR SHARING INFORMATION	18
3.5. OTHER SKILLS	19
3.6. SUMMARY	19
4. CROSS-SECTORAL EXERCISES	22
4.1. REQUIREMENTS FOR CROSS-SECTORAL EXERCISES	22
4.1.1. Stakeholders	22
4.1.2. Activities	23
4.1.3. Deliverables	23
4.2. INTERACTION CHALLENGES	29



4.3. SUMMARY	31
5. CONCLUSIONS AND THE WAY FORWARD	33
5.1. CONCLUSIONS	33
5.2. THE WAY FORWARD	34
5.2.1. Skills steps	35
5.2.2. Organisational steps	35
5.2.3. Technical steps	35
ANNEX: RESPONSES REGARDING THE RELATIVE IMPORTANCE OF SKILLS	36



EXECUTIVE SUMMARY

The European Union sees information sharing and analysis centres (ISACs) as a way of building a European cybershield. With attacks growing in both volume and sophistication, ISACs could help identify attacks and help contain them, and potentially prevent disasters such as the Petya/NotPetya ⁽¹⁾ situations. In order for this to happen these ISACs need to be able to communicate with each other and share valuable and actionable information. For this purpose this report aims to identify the skills, exercises and training needed to ensure that this information exchange is effective and efficient.

In this report we identify five EU ISACs from the following sectors:

- finance
- rail
- energy
- maritime
- government (ISAC for Cities).

They participated in a survey and interviews to identify their needs and expectations as to how cross-sectoral information exchange could take place. From our analysis we identified the following skills needed for cross-sectoral exchange through ISACs:

- technical skills – related to tools for sharing information;
- legal and compliance skills – the regulatory environment applicable to threat information exchange;
- information analysis and triage skills – knowledge on validating the received threat intelligence information;
- knowledge on recognising threats.

In addition, in developing a cross-sectoral exercise we identified:

- potential stakeholders,
- the preferred type of exercise, for example organisational,
- the preferred subject of the exercise, for example the incident response,
- potential exercise scenarios, for example the third-party / vendor attack.

In the report we also discuss the challenges that ISACs face when dealing with this type of exercise, such as the human resources and permissions from the top management needed.

⁽¹⁾ [https://en.wikipedia.org/wiki/Petya_\(malware\)](https://en.wikipedia.org/wiki/Petya_(malware))

1. INTRODUCTION

1.1. OBJECTIVE AND SCOPE

The objectives of the work presented in this report were to:

- understand if a cybersecurity skills gap exists within the various information sharing and analysis centres (ISACs), with a focus on information exchange;
- understand the nature of the skills gap (if it exists) and determine how training and/or exercises can effectively address it;
- identify the need for and characteristics of a possible cross-sectoral exercise;
- propose a set of concrete actions to effectively address the skills gap and needs of the ISACs in this area.

1.2. METHODOLOGY

In order to successfully address the objectives of this study, the project team devised a methodology comprising the following four steps.

1. **Literature review.** During this stage, relevant documentation on cybersecurity information exchange methods, activities, tools and challenges was reviewed. The aim of this step was to provide substantiated information for the implementation of the next steps.
2. **Structured survey.** A survey was created based on the results of the literature review and adapted according to the specific requirements of this study and the interested parties.
3. **'Deep dive' interviews.** The survey was followed up with several interviews in order to get a deep-dive perspective on ISACs' scope of work, organisation, key challenges, obstacles and expectations on cross-sectoral ISAC exercises. The aim of the deep-dive interviews was not to reiterate the responses to the survey, but rather to build on this information in order to obtain more suitable recommendations.
4. **Analysis of the results and extraction of conclusions.** All the information gathered from the previous steps was collated, analysed and evaluated in order to provide the recommendations in this report on skills demand, exercise structure and resources needed and communities' interaction.

The structure of the report follows the steps of the methodology described above.

The deep-dive interviews enabled additional discussions with the survey respondents, to clarify their responses and elaborate on their points of view. This way, additional information was gathered on more specific points. The points from respondents highlighted in this report are anonymised and are not presented in a specific order.

The deep-dive interviews were structured as follows: respondents were asked for some information about the context in which their ISAC operates, their responses to the questionnaire were discussed and they were asked to provide additional feedback on their points of view.

1.3. SURVEY INFORMATION

The questionnaire was sent to a predetermined list of stakeholders, all of which were directly involved in the activities of ISACs. The questionnaire was constructed and communicated using the EUSurvey tool.

The questionnaire was open between 7 June and 1 July 2021. The deep-dive interviews were conducted between 17 June and 15 July 2021.

Questionnaire responses were received from EU ISACs from various sectors (financial, energy, rail, maritime, aviation and municipal administration). More than 70 % of the participants declared their willingness to participate in the deep-dive interviews, of whom 80 % were conducted in order to better understand the context of areas covered by the survey.



2. GENERAL CONTEXT

As explained in Section 1.2 'Methodology', a survey was conducted using a structured questionnaire followed by several deep-dive interviews.

In the following sections, the questionnaire responses and feedback are analysed by section, providing a statistical representation of the responses provided along with the context retrieved during the deep-dive interviews (e.g. specificities mentioned by participants and key takeaways for constructing conclusions and recommendations).

2.1. WHAT IS A EUROPEAN UNION INFORMATION SHARING AND ANALYSIS CENTRE?

ISACs ⁽²⁾ are non-profit organisations that provide a central resource for gathering information on cyberthreats (in many cases to critical infrastructure); allow the two-way sharing of information between the private and the public sectors about root causes, incidents and threats; and allow the sharing of experience, knowledge and analysis.

Information sharing, either between national stakeholders or in cross-country cases, is an important aspect of cybersecurity. Knowledge on attackers' methods and tools, ongoing attacks, victims and protective measures, incident response, mitigation measures and preparatory controls can be shared between the relevant stakeholders.

An EU ISAC is characterised as an ISAC whose member companies are from at least two EU Member States.

Currently, there is a limited number of EU ISACs, but the plan is to develop such entities for various sectors. Some of these sectors include:

- Industry 4.0 and industry and control systems,
- energy systems and smart grids,
- transport (road, rail, air, sea and space),
- finance, e-payments and insurance,
- public services, e-government and digital citizenship,
- healthcare,
- smart cities and smart buildings (convergence of digital services for citizens) and other utilities,
- telecommunications, the media and content.

As information sharing is a core function of ISACs, it is of paramount importance that the relevant actions are identified that will enhance and support the information exchange capabilities of ISACs.

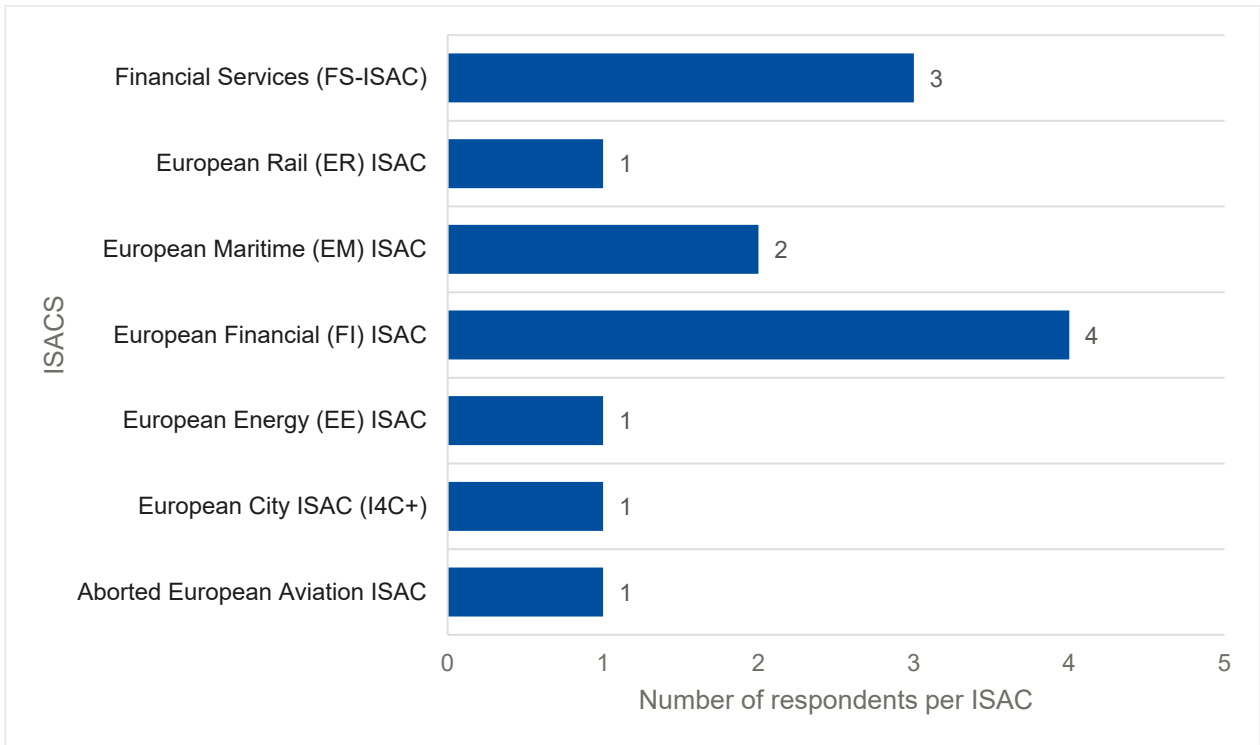
2.2. OVERVIEW OF INFORMATION SHARING AND ANALYSIS CENTRES

In this section of the questionnaire, information about the origins of the participants and the specific restrictions on information sharing was requested.

Figure 1 provides the distribution of the respondents among the various ISACs:

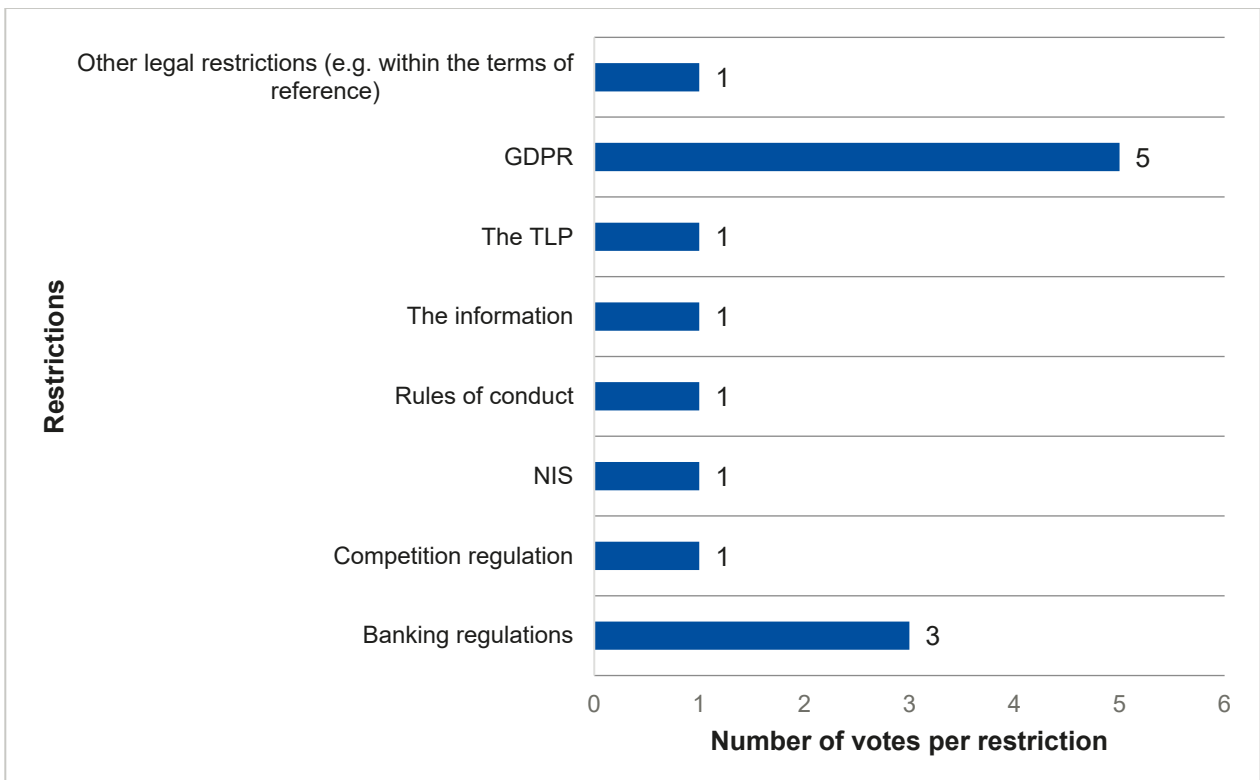
⁽²⁾ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>

Figure 1: Respondents' affiliations



Regarding the possible restrictions on information sharing, 46 % of the respondents identified restrictions imposed by the parameters in Figure 2.

Figure 2: Restrictions on information sharing



As shown in Figure 2, more than 30 % of the respondents (including from the European Rail ISAC, the European Financial ISAC and the Financial Services ISAC) identified the General Data Protection Regulation (GDPR) as imposing restrictions. This clearly indicates a need to provide guidelines with regard to compliance with the GDPR while sharing information.

It is crucial to the entire information-sharing process that obstacles are identified and removed in order to facilitate effective information exchange.

2.2.1. Overview by sector

In addition to the general impressions obtained from the interviews, two sectors stood out because their ISACs were able to provide additional information of interest.

Finance

The finance sector is clearly ahead of the other sectors when it comes to cybersecurity. It has been highly regulated for a significant amount of time, longer than the other sectors, and with a wider spectrum of regulations (Basel I, Basel II and Basel III; the Payment Card Industry Data Security Standard ⁽³⁾; and payment services directive 2) that include cybersecurity-related fraud treatment.

The finance sector has reached such a significant maturity level that it is able to provide threat landscape monitoring. The ISACs are also interested in technical exercises and training.

As such, the sector stands out as being able to inform other sectors with regard to cross-sector IT vulnerabilities, attacks and incidents, and could be in a position to take the lead and help the other sectors reinforce their skill sets.

Although it traditionally focuses on IT operation, the mechanisation of business functions (e.g. the development of automated teller machines that are vulnerable to physical attacks) ⁽⁴⁾ may create new needs for operational technology (OT). Cross-collaboration with other sectors that have a long history of deploying OT in the field (e.g. energy and transport) could help mitigate these threats.

Transport

Cybersecurity in transport is very new. Although the transport sector has not been targeted as much as other sectors by cyberattacks, there are indications that they will, like others, become a more frequent target. Good examples are attacks on ticketing systems ⁽⁵⁾ such as MyFare and digitalised train control systems ⁽⁶⁾.

The transport sector is focusing on OT and relies on other sectors for IT-related information sharing. For example, ticketing machines and information systems are like banking terminals, so there is a clear benefit of exchanging information with the finance and telecommunications sectors.

Owing to its focus on OT, the ISAC needs to also include providers of technological equipment, as they can supply a lot of information on their devices.

⁽³⁾ <https://www.pcisecuritystandards.org/>

⁽⁴⁾ <https://www.association-secure-transactions.eu/tag/atm-physical-attacks/>

⁽⁵⁾ https://www.theregister.com/2021/07/20/northern_trains_ticketing_system/

⁽⁶⁾ <https://hal.archives-ouvertes.fr/hal-01852042/document>



2.3. STRUCTURE OF INFORMATION SHARING AND ANALYSIS CENTRES

The structure of the ISACs is relatively similar. They generally consist of a partnership between private and public entities, sometimes hosted within a public entity. The partnership can be formal (with an established legal entity) or informal. Some of them were established very recently, while others have been operating (e.g. in the form of CERTs) for a long time.

ISACs cater to two populations: C-level executives and technical people. Most of the participants and recipients of information are C-level executives, and they are the focus of ISAC participation. Technical people support C-level executives as needed.

Several ISACs use the Malware Information Sharing Platform (MISP) or similar platforms, or need or would like to do so but do not yet have the capability. Others prefer more traditional means of communication, such as emails and factsheets. Situational awareness is important but unfortunately is lacking in many ISACs.

Several ISACs already practice information exchange and have networks of collaborators around Europe. Others are just starting to do so and are interested in benefiting from the experiences of previously established organisations with higher maturity levels.

In relation to the challenges of information exchange, the following points were made.

- 'There is often a large amount of information to manipulate, which requires strong capabilities. There is a trade-off between timeliness and correctness. The information exchanged should be correct, but one should not wait too long to communicate because then the recipient may not have the time to leverage the exchanged information to react to the threat.'
- 'Information-sharing processes are informal in some cases. One of the key points is trust, trusting the persons and organisations with which you exchange information.'
- 'The ISACs face difficulties when talking to victims, as they need to help victims defend themselves efficiently while at the same time extracting information from them to share with the rest of the community. Gathering information uses resources, so the trade-off between providing help and collecting data is delicate.'

2.4. EXPERIENCES OF AND PREFERENCES FOR EXERCISES

ISACs that participated in the interviews reported their experiences and their positive attitudes towards exercises.

The ISACs generally differentiated between two types of exercise:

- table top exercises focused on processes,
- red-team / blue-team exercises aimed at testing the defences of specific organisations.

When asked about the shortcomings and challenges relating to exercises, ISACs gave the following main feedback.

- ISACs may face resource issues in their daily tasks, so participation in exercises should be weighted. Resource constraints particularly affect the analysis of the information that ISACs collect.
- Time needs to be invested in the preparation and planning phase of training for the training to be effective. Therefore, human resources and especially people who have the relevant knowledge should be involved early on.

- Exercising and testing should not be implemented only once. There should be continuity in exercises and training (i.e. past exercises should be leveraged to prepare and create new exercises).



3. KNOWLEDGE AND SKILLS NEEDED BY INFORMATION SHARING AND ANALYSIS CENTRES

3.1. SKILLS ANALYSIS FROM THE SURVEY

The aim of this section was to identify the knowledge and skills that are needed by the members of each ISAC in order to effectively exchange information between them and to identify the respondents' preferred ways of implementing the necessary training.

Respondents were asked to grade a range of types of knowledge and skills (from organisational to technical) based on their importance to their ISAC. Moreover, the respondents were given the opportunity to add their own suggestions using an open-text question.

The proposed knowledge and skills were derived from the literature review and were:

- knowledge of threats (e.g. indicators of compromise (IoC), common vulnerabilities and exposures (CVE), and other relevant naming schemes);
- knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (e.g. data retention, attribution, personally identifiable information (PII) and cross-border prohibitions);
- knowledge of data sanitisation requirements and techniques;
- knowledge of the specifics of service-level agreements (SLAs), non-disclosure agreements (NDAs) and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations);
- knowledge of sharing designations (e.g. the Traffic Light Protocol (TLP));
- applied knowledge of industry standards related to the threat information exchange (e.g. Trusted Automated eXchange of Indicator Information (TAXII), Structured Threat Information eXpression (STIX), Cyber Observable eXpression (CybOX) and the Collective Intelligence Framework (CIF));
- applied knowledge of security measures that must be implemented to secure information exchange (e.g. encryption and transfer protocols);
- knowledge of validating the received threat intelligence information (making sure that it is of high quality, actionable, accurate, relevant and specific);
- knowledge of internal procedures for incident handling (if sensitive data is leaked);
- risk assessment methodologies and tools utilised to classify the information received;
- tools for sharing information (e.g. MISP).

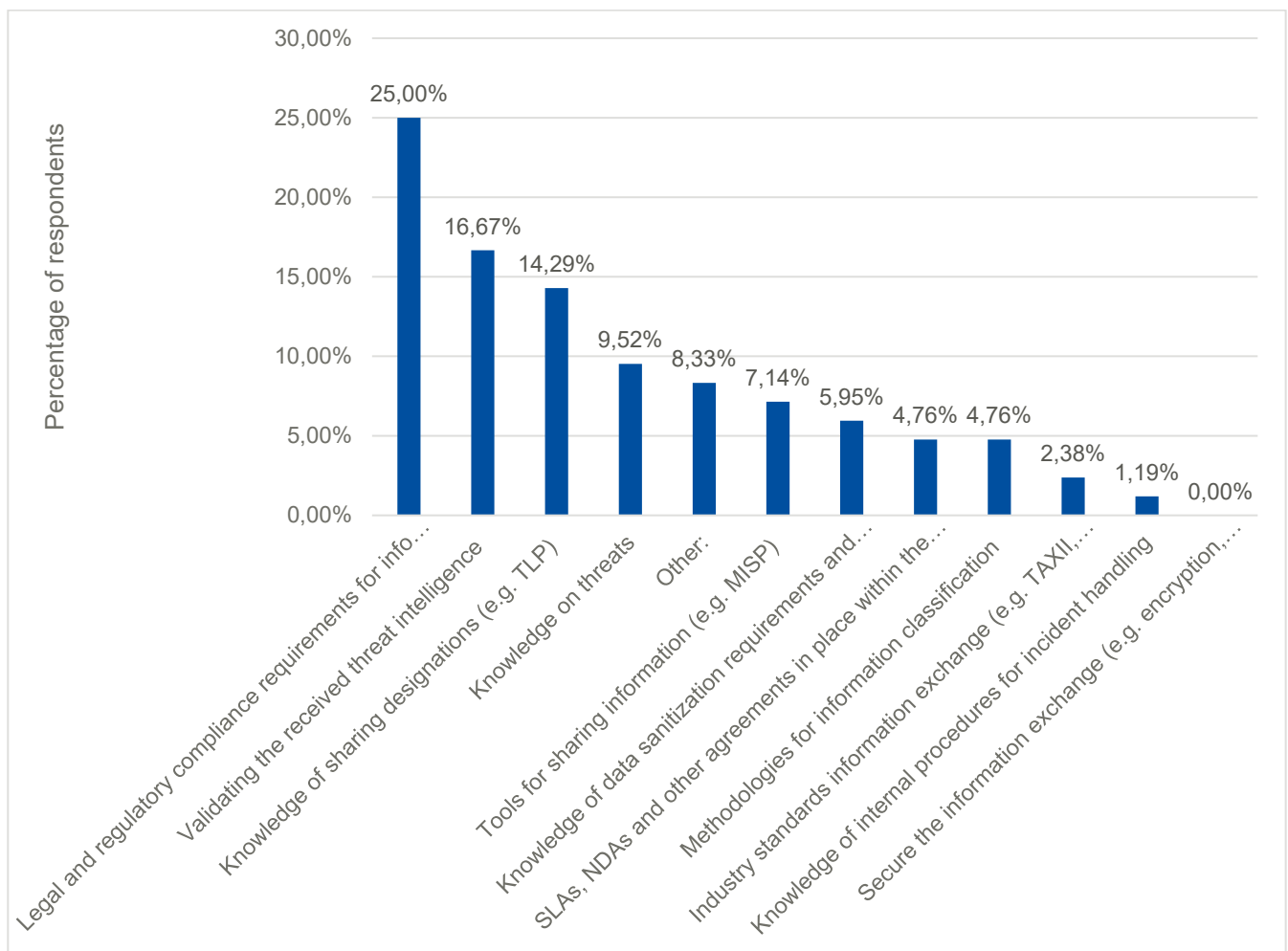
Different sectors have different preferences for knowledge and skills, as shown in Figures 3 and 4. The information obtained for the finance and transport sectors was more representative than that obtained for other sectors, as we received more responses for these sectors. There was not enough information to analyse the skills of EU ISACs from other sectors, although this information is captured in the overall analysis of skills, as described in Section 3.6 'Summary'.

3.1.1. Finance sector information sharing and analysis centres

The finance sector ISACs include the European Financial ISAC and the European branch of the US Financial Services ISAC.

Based on the responses obtained, the finance ISACs value most the knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (Figure 3). This could be because the finance industry is one of the most regulated industries and compliance affects information sharing. Knowledge of validating the received threat intelligence information was the second most valuable skill mentioned. This could be because there is an enormous amount of threat intelligence information and being able to manage that is a valuable skill. The second least valuable skill was that associated with knowledge of internal procedures for incident handling, which could be because the industry is well aware of what needs to be done in the event of an incident. This could also be because the industry has been dealing with cybersecurity incidents for some time. Applied knowledge of security measures that must be implemented to secure information exchange, for example using encryption and secure transfer protocols, was the least valuable skill reported. This could be because for some time the finance industry has been well aware of how to secure communications coming from payment transactions.

Figure 3: Knowledge and skills in the finance sector

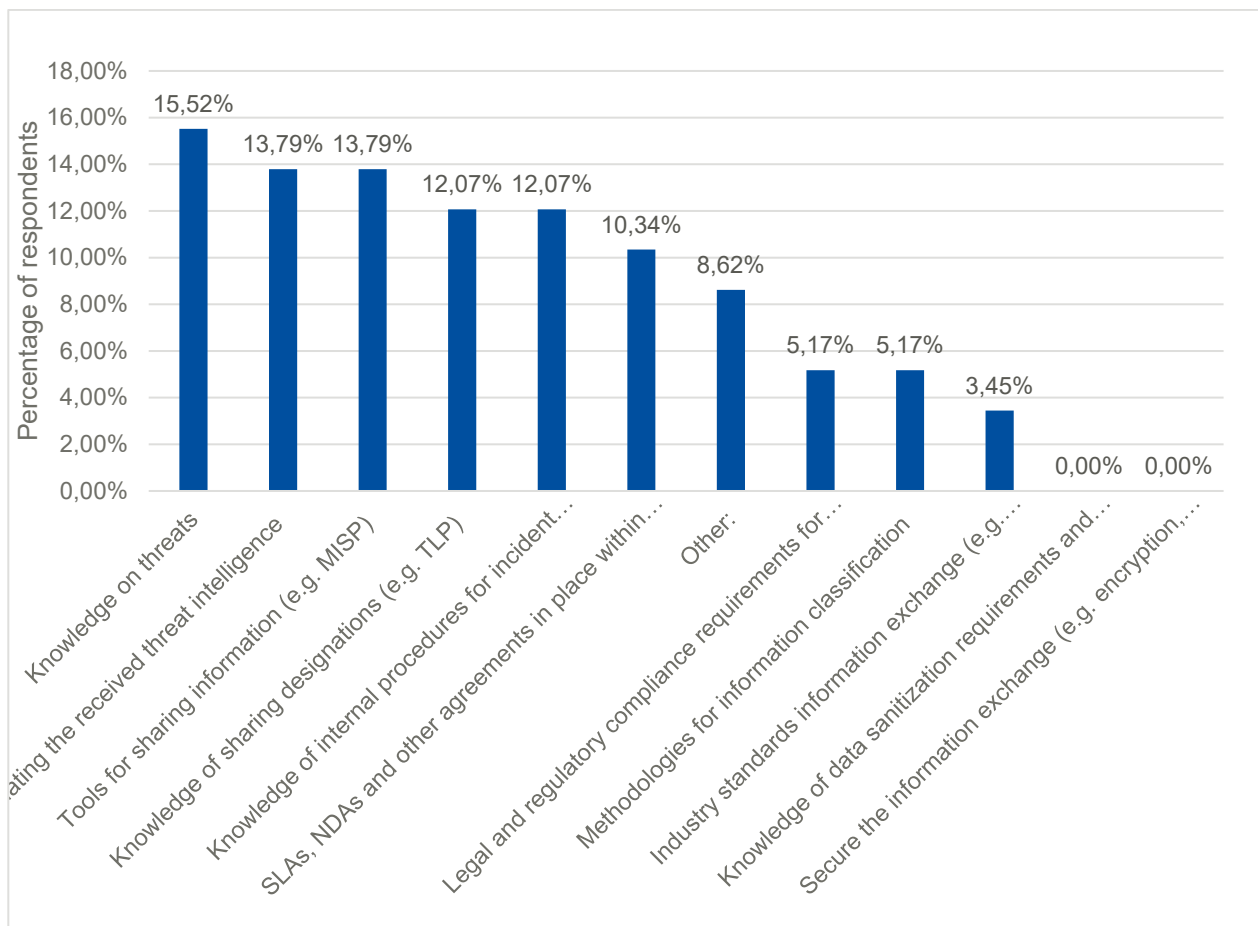


3.1.2. Transport sector ISACs

The transport sector ISACs include the maritime, rail and aviation ISACs.

The transport sector has a different view on skills from the financial sector. The most valuable skills are associated with the knowledge of threats (Figure 4). This could be associated with the fact that threats are still difficult to identify, because they can affect not only IT, but also OT. Therefore, identifying threats affecting transport systems is considered one of the most valuable skills to the industry. The second most valuable skill is the same as in the finance sector – validating the received threat intelligence. It seems that the wealth of threat intelligence information available to the sectors is not easily manageable. Therefore, ISACs should focus on developing this skill in the future. Skills associated with a knowledge of data sanitisation and secure information exchange are least valuable. It seems that ISACs in the transport sector have covered the basics of secure communication exchange, and that these skills are not required at this point in time.

Figure 4: Knowledge and skills in the transport sector



3.2. LEGAL AND COMPLIANCE SKILLS

Respondents reported that the most important knowledge required is that of the regulatory environment applicable to threat information exchange. This, combined with the responses related to risk assessments and SLAs/NDAs, indicates that the highest-ranking skill set for EU ISAC operators is related to the legal and compliance framework. (Survey results: 'applicable legal and regulatory compliance requirement' – 33 points, rank 1; 'risk assessment' – 12 points, rank 6; and 'SLA/NDA' – 10 points, rank 7.)

Why is this skill set important?

As mentioned in Section 2.2, one of the major obstacles to information sharing identified by the survey participants is legal and regulatory obligations. Therefore, having concrete knowledge of the relevant requirements, how these may affect information sharing and how information sharing could be implemented in compliance with them is of paramount importance.

In more detail, this skill set includes the following.

- EU ISAC operators must understand and be able to apply the EU legal framework related to the directive on security of network and information systems, which mandates that information about cyberthreats and cyberincidents be made available to certain parties.
- Operators must understand and be able to apply the EU legal framework related to the GDPR, which mandates that personal information should be protected. Incident-related information often includes personal data. Processes should be put in place to allow the sharing of information that is valuable to all involved parties, without compromising the protection of the personal data of the data subject. These processes should be constructed in such a way that the main goals of information exchange are achieved along with GDPR compliance (e.g. the sender of the information retains the ability to correctly classify the information shared and the receiver of the information can manage the received information according to its classification and treat it accordingly).
- Operators must understand and be able to apply risk assessment methodologies. Compliance with legal and regulatory requirements is connected with risk assessment. Risk assessment is applicable to the early stages of information sharing (during the information classification process) and in the last stages during information handling and sharing by the recipient. Especially for the latter, owing to the differences in environments in which the ISACs operate, cross-sector information exchange also requires that the information is independently assessed by the receiving party to add further protection and classification if needed.
- Operators must have the knowledge, understanding and ability to understand and comply with SLAs and NDAs in place between ISACs to support information exchange. This skill includes having knowledge of the other parties' structures and of the procedures that will be deployed in relation to information exchange.

In the context of cross-ISAC skills, a mutual understanding of the regulations applicable to each of the domains in which the ISACs are operating may be beneficial to ISAC employees.

3.3. INFORMATION ANALYSIS AND TRIAGE SKILLS

The second most important skill highlighted by the survey was knowledge in validating the received threat intelligence information. This, combined with the responses related to threat information and naming schemes and sharing designations, indicates that the second-highest-ranking skill set for EU ISAC operators is related to information analysis and triage. As ISACs are by nature information exchange points, it is crucial that ISAC members have strong informational skills. (Survey results: 'information validation' – 31 points, rank 2; 'knowledge of threats' – 25 points, rank 3; and 'knowledge of the TLP' – 19 points, rank 5.)

Why is this skill set important?

For information exchange to be effective and the desired goals to be achieved, it is important that the personnel involved have the ability to identify and understand the content and value of the information received and apply the appropriate processes.

During interviews, many interviewees mentioned that they were interacting with C-level executives. This skill set should therefore include a significant component related to the ability to communicate with C-level executives, ensuring that they understand the issues and are properly informed to make decisions in their own organisations.

This skill set includes **information quality assessment**, which is the core work of ISACs and therefore a core skill for ISAC employees. During the information quality assessment, the receiving party should assess various aspects of the information received, especially the trustworthiness of the source, its accuracy, its actionability and its relevance, and implement timely, suitable and specific actions.

- **Trustworthiness of the source.** One of the key elements of the quality assessment is the determination of the trustworthiness of the source of the information. If the source is not reputable or trusted, the information received should be viewed as such and if desired special validation processes should be implemented before any further decisions are implemented.
- **Accuracy of the information.** Information exchanged must be accurate to be actionable. ISAC employees must have the ability to evaluate the accuracy of the information received. In this context, the relevant personnel will need to evaluate the mechanisms through which the information has been collected, stored and transmitted, and contextual information about the source. This is closely related to the TLP and the various tools used.
- **Actionability of the information.** Information exchanged must be actionable, both for the ISAC and its constituency. The ISAC personnel involved in information sharing should have the knowledge and skills to decide if the information received should be shared, how it should be shared, and whether it should be associated with recommendations (and, if so, which ones). The above are closely related to the existence of knowledge of the threats, their naming conventions and their relative criticality.
- **Relevance of the information.** Information exchanged must be of interest to the organisations or industry sector receiving it. In the context of cross-ISAC information exchange, the ISAC personnel involved in information sharing must be able to understand the needs of their peers in other sectors and decide if the information collected is relevant to them. This usually requires predetermined and jointly negotiated criteria for information of interest, and ISAC employees should be trained on the use of these criteria.
- **Specific actions.** The information must be sufficiently precise to enable the receiving ISAC to act on it. As with relevance, this requires predetermined and jointly negotiated criteria for information of interest, and the ISAC personnel involved in information sharing should be trained on the use of these criteria.
- **Timely actions.** Timeliness is of the utmost importance for information sharing. Information shared too late has limited value for the ISAC's constituency. Information shared too early may be incomplete or inaccurate. The ISAC personnel involved in information sharing must decide if the quantity and stability of the information collected is sufficient to make sharing relevant to the other ISACs.

In general, the ISAC personnel involved in information sharing must be able to decide when to invest in harvesting and analysing information about a specific incident before sharing, and when to stop gathering information and investing in communication and analysis. This is a

difficult trade-off and experience helps in the honing of this skill. The related knowledge and skills are prime candidates for interactive learning and hands-on exercises.

3.4. TECHNICAL SKILLS FOR SHARING INFORMATION

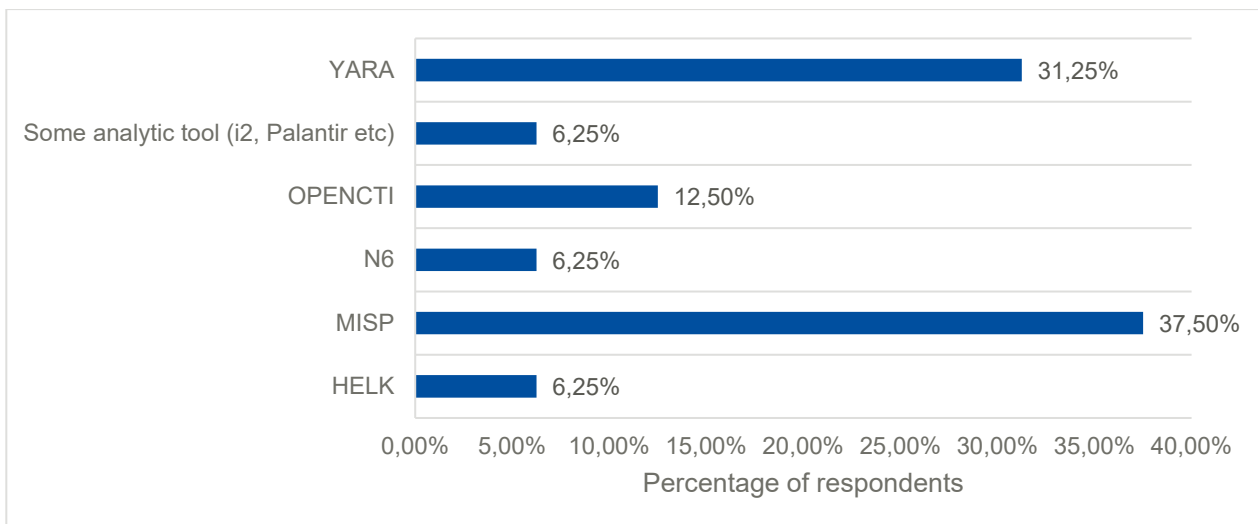
The fourth most important set of skills highlighted by the survey were those related to tools for sharing information. This, combined with the responses regarding the information representation standards and languages and the data sanitisation techniques, indicates that an important skill set for EU ISAC operators is related to tools that facilitate the accurate and efficient exchange of information. As cybersecurity is a highly technological domain, technical skills were expected to be important for the proper exchange and handling of information. (Survey results: ‘knowledge of tools for information sharing’ – 23 points, rank 4; ‘knowledge of information representation standards and languages’ – 6 points, rank 8; ‘data sanitisation requirements and techniques’ – 5 points, rank 9; and ‘specific cybersecurity standards’ – 5 points, rank 9.)

Why is this skill set important?

As mentioned in Section 3.3, information involved in exchanges between ISACs should possess specific high-quality characteristics, and the exchange of information should be implemented in accordance with specific time limitations, in order for the information to be effective for and valuable to all involved parties. This combination of requirements has led to the increased utilisation (or desirability) of specific tools (e.g. MISP). Knowledge of the correct, effective and efficient use of these tools and the implementation of the actions required to process information (incoming or outgoing) is needed by the ISAC personnel involved in information sharing.

As there are a number of tools available, and because effective training can be implemented only if focused on a specific tool, the survey included a question regarding participants’ preferences for tools (Figure 5).

Figure 5: Preferences for tools



The relatively high preference for MISP may be attributed to the fact that, during the interviews, several parties mentioned their desire to use MISP (either by choice or owing to pressure from their constituency), or that they have deployed a MISP instance that is not yet in full production. In addition, several ISACs are closely cooperating with CERTs, and MISP is clearly the tool of choice for many of the CERTs in Europe.

In more detail, this skill set includes the following.

- **MISP.** MISP is a complex tool. The ISAC personnel involved in information sharing must be able to filter information relevant to cross-sector analysis. This involves personnel having access to and using the right tools and filters (already in place) or developing and deploying their own filters. The ISAC personnel involved in information sharing should have a deep understanding of the capabilities and constraints of the MISP and use it as effectively as possible.
- **Standard databases such as CVE, Common Platform Enumeration (CPE) and MITRE ATT&CK.** The ISAC personnel involved in information sharing must leverage the existing information in these databases, as they provide a common platform for expressing events of interest. Using these standard databases supports the goals of information accuracy, relevance and actionability.
 - CVE is a dictionary of vulnerabilities, best accessed through the National Vulnerability Database of the National Institute of Standards and Technology. CVE provides a common source of information that enables precise identification of vulnerabilities, ensuring appropriate risk analysis, the identification of vulnerable systems, impact and potential remediations. Properly tagging with the appropriate CVE (and CPE) is done by the sender of the information and is key to the proper handling by the recipient.
 - CPE is a dictionary of vulnerable software and hardware products. It provides the product identification for CVE in the National Institute of Standards and Technology's national vulnerability database. It is a key element of CVE, along with the common vulnerability scoring system.
 - MITRE ATT&CK provides a base to enable knowledge about attacker tactics and techniques to be standardised. It provides a common high-level description of attacker activities, facilitating information sharing. It proposes mitigation methods to limit attacker activities when such activities are discovered in an organisation.
- **Standard IoC description languages such as YARA.** These enable the accurate configuration of detection sensors with regard to the threat.
 - YARA is a tool and language used by malware researchers to search for specific patterns in files to detect the presence of malware. The YARA language has been widely adopted to describe indicators of compromise. Using YARA supports the goals of information accuracy, relevance and actionability.

In the context of cross-ISAC skills, a mutual understanding of the applicable standards in each of the domains in which the ISACs are operating may be beneficial to the ISAC personnel involved in information sharing.

In general, the ISAC personnel involved in information sharing must be able to effectively and efficiently use the agreed tools for information sharing. The related knowledge and skills are prime candidates to be addressed through interactive learning and hands-on exercises.

3.5. OTHER SKILLS



The survey also shows that certain skills are less important for ISACs. The skills not ranked are more 'generic' skills that are further away from the core competences of ISACs (e.g. general intelligence information analytical skills (not tools but frameworks, etc.), communication and group facilitation skills, and applied knowledge of different security measures to be implemented to secure information exchange (e.g. encryption and transfer protocols)).

3.6. SUMMARY

The different ISACs have different knowledge and skills needs.

Table 1 provides a summary of the knowledge and skills needed as reported by the EU ISACs.

Table 1: Ranking of knowledge/skills by importance

Order of importance	Knowledge/skills
<div style="text-align: center;">   </div>	<p>Knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (e.g. data retention, attribution, PII and cross-border prohibitions)</p>
	<p>Knowledge of validating the received threat intelligence information (making sure that it is of high quality, actionable, accurate, relevant and specific)</p>
	<p>Knowledge of threats (e.g. IoC, CVE and other relevant schemes)</p>
	<p>Tools for sharing information (e.g. MISP)</p>
	<p>Knowledge of sharing designations (e.g. TLP)</p>
	<p>Risk assessment methodologies and tools to be utilised for classification of the information received.</p>
	<p>Knowledge of internal procedures for incident handling (if sensitive data is leaked)</p>
	<p>Knowledge of the specifics of SLAs, NDAs and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations)</p>
	<p>Applied knowledge of industry standards related to the threat information exchange (e.g. TAXII, STIX, CybOX and CIF)</p>
	<p>Knowledge of data sanitisation requirements and techniques</p>
	<p>Knowledge of newly created railway-specific cybersecurity standards (e.g. IEC62443 deviated standard and TSI.57001)</p>
	<p>General intelligence information analytical skills (not tools but frameworks, etc.)</p>
	<p>Communication and group facilitation skills</p>
	<p>Knowledge of how to establish trust between the ISACs and their members</p>
	<p>Least important</p>

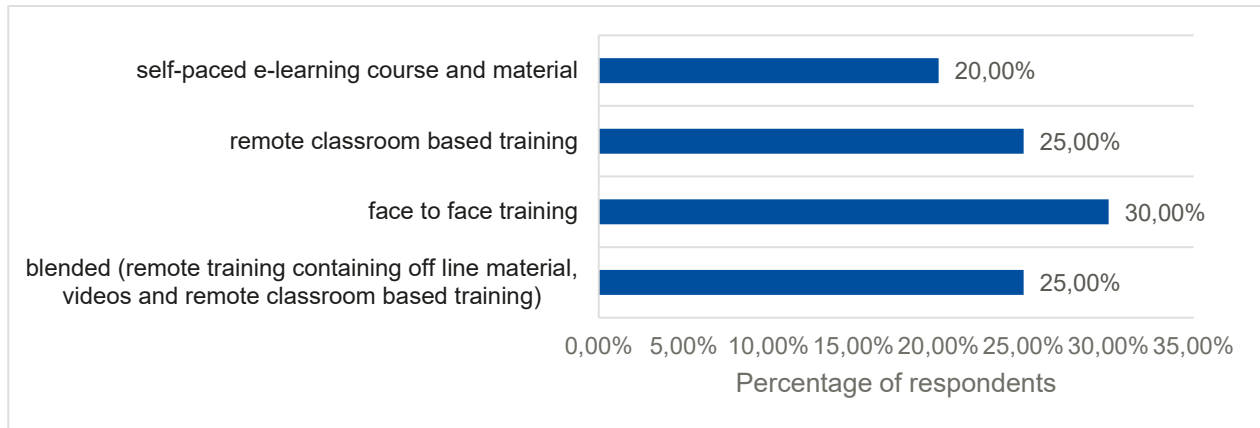
In conclusion, the following knowledge and skills were identified as most important for the ISACs in order to facilitate effective information exchange:

- knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (e.g. data retention, attribution, PII and cross-border prohibitions);
- knowledge of validating the received threat intelligence information (making sure that it is of high quality, actionable, accurate, relevant and specific);
- knowledge of threats (e.g. IoC, CVE and other relevant naming schemes);
- tools for sharing information (e.g. MISP).

Regarding the last point (tools for sharing information), the responses to the question on the tool that ISACs would like to be trained on were split mostly between MISP (46 %) and YARA (38 %). They should be considered in different scenarios, however, as MISP is generally focused on threat and intelligence sharing, while YARA is more focused on malware analysis.

Finally, based on the responses to the question on preferences for training methods, the survey shows that all the delivery methods were deemed acceptable, with a slight preference for face-to-face training (Figure 6). This preference should be considered during the design of the relevant training courses.

Figure 6: Preferences for training methods



In summary, the skills required for cross-sector information exchange cover the following.

- **Legal and regulatory framework.** Beyond regulations that are applicable to all sectors, understanding of sector-specific regulations and context may be required to facilitate the exchange of information on cross-sector cyber incidents, indicators of compromise and early warnings of ongoing malicious activity, among other things.
- **Information analysis and triage skills.** In the context of cross-sector information exchange, ISAC operators should be able to rely on pre-negotiated criteria to decide when a piece of information is relevant to another sector. This should be complemented by the practical evaluation of the value of the information. Another key aspect of information analysis is being able to synthesise the information for C-level decision-makers.
- **Technical skills.** The required technical skills are quite standard in the ISAC community and are in general similar to those required by CERT personnel.

4. CROSS-SECTORAL EXERCISES

4.1. REQUIREMENTS FOR CROSS-SECTORAL EXERCISES

In this section we assess the needs and requirements for conducting cross-sectoral ISAC exercises. The aim is to check what types of exercise, methods of exercise, delivery, organisation, and resources – those already available and those that need to be created/developed – would be the most suitable and useful for ISACs, bearing in mind their stages of development and maturity levels.

For a better understanding and to enhance the survey analysis we introduced several definitions related to the cyber exercises’ domain in general.

4.1.1. Stakeholders

Table 2 shows the types of potential stakeholders involved in exercises and descriptions of their roles and responsibilities. Depending on the type and scope of an exercise, all roles listed below may or may not be necessary.

Table 2: Exercise Stakeholders Type

Type	Description
Sponsors	Sponsors take responsibility for the exercise programme and grant a clear mandate and full authority to the exercise leadership and design teams; approve overall programme goals and objectives; advocate within the organisation to other executives/managers and stakeholders
Leadership	The leadership is responsible for overseeing all aspects of the table top cyber exercise, using a strategic approach; for assigning resources as needed and enforcing stakeholders’ commitments; and for tracking the progress of the action/improvement plan and its enforcement
Planners	The group administratively responsible for planning and executing the exercise in a realistic manner; for organising the additional resources required; and for representing all key constituencies, including observers
Facilitators	Facilitators lead participants through the exercise by setting the context and facilitating discussion to ensure that they remain aligned with the scope of the exercise within its given time frame
Observers	A limited group that passively witnesses/observes the proceedings and course of events, taking notes of participants’ actions, decisions and effectiveness. Its aim is to provide feedback; to assess the preparations of the organisations or individuals within them; and to learn lessons for

	future exercises through after-action reports, which include recommendations on how to amend plans to address these gaps
Participants / role players	Participants / role players participate or simulate one specific role or multiple specific roles during exercises and initiate actions to handle, respond to or mitigate the injects
Very important persons	These are visiting individuals from top management layers of participating organisations, or third-party organisations with an interest in running exercises

4.1.2. Activities

- An exercise is a simulated operation involving planning, preparation and execution that is carried out for the purpose of training and evaluation.
- Table top exercises are discussion-based sessions where team members meet in an informal classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation.
- A hotwash is a debrief conducted immediately after an exercise or test with staff and participants.
- A cold debrief is a post-exercise activity where individuals or teams are provided with feedback sometime after the exercise, including improvements that can be made to processes and outcomes, and potentially an action plan. Such feedback usually involves the use of objective performance data.

4.1.3. Deliverables

- An exercise scenario describes the strategic and operating environment in sufficient scope and detail to allow the accomplishment of the exercise and training objectives.
- An after-action review is an analytical review of training events that enables the training audience, through a facilitated professional discussion, to examine actions and results during a training event.
- A corrective action report addresses areas of assessment, gaps and corrective actions to remedy the gaps.

There are several types of cybersecurity exercises, usually depending on the participants' roles within their organisations and sponsors' expectations:

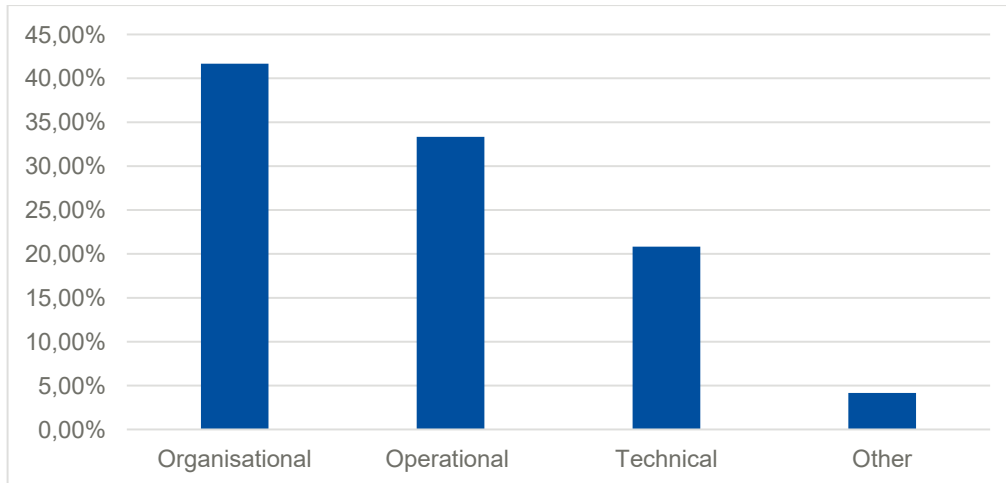
- governance-oriented or organisational exercises, with senior-level involvement, usually constructed as table top exercises with the goal of confirming the existence of specific processes and activities and organisations' level of preparedness;
- operationally oriented exercises, designed to test organisations' ability to roll out predefined sets of rules, processes, procedures and tools;
- technically oriented exercises, designed to test and improve highly technical skills possessed by the ISACs' technical staff;
- mixed types of exercises that are conducted concurrently or one after the other in a logical sequence, such as the Cyber Europe sets of exercises ⁽⁷⁾.

As shown in Figure 7, more than two thirds (above 70 %) of the respondents stressed their need to participate in high-level organisational (40 %) and operational (35 %) exercises. Some 20 % of respondents signalled their need to organise technical exercises. As concluded from the interviews, most of the ISACs surveyed are at an early stage of development and are

⁽⁷⁾ Cyber Europe has a 2-year cycle and at the time of writing the next exercise is to be held in June 2022.

focused on establishing a clear structure and mandate and trust-building mechanisms, so it is understandable that they have a need for high-level exercises at this stage of development. In the natural evolution of any group/entity such as an ISAC, there is a need to conduct both governance-oriented or organisational exercises, and technical exercises for day-to-day activities, but structuring is required to reach a high maturity level.

Figure 7: Preferences for types of exercise

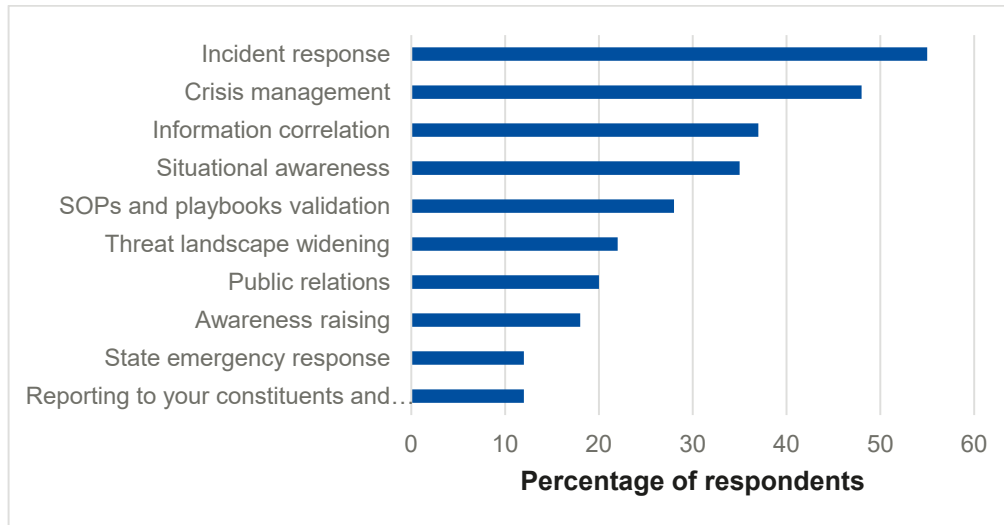


Some respondents stressed the need to conduct all levels of exercises at some point and the need for all exercises to be practical in order to simulate real-world situations and test the communication mechanisms between ISACs and sectors. Exercises are seen as a way to validate the models deployed and identify gaps and blind spots in the global processes of incident handling in ISACs' communities.

Moreover, cybersecurity is a multidisciplinary domain covering a wide range of topics, aspects and areas. As it is impossible to cover them all in a single exercise, one of the aims of this report was to identify the areas or domains of cybersecurity perceived by participants as the most important to cover in the exercises.

Participants were asked to rate their preferred exercise subjects from 1 to 5, with 1 being the most preferred and 5 being the least preferred. Results were then analysed according to the number of votes for each subject and the ratings provided by the participants, and presented as votes for each subject. As shown in Figure 8, the two subjects with the most votes were 'incident response' and 'crisis management', followed by 'information correlation' and 'situational awareness'. The least important subjects of cross-sectoral exercises, according to the survey, were 'reporting to your constituency and getting feedback' and 'state emergency response'. The responses provided and this analysis clearly align with the general mandate of the ISACs as organisations in which exchanging information during incident management or crisis management processes is the most important task.

Figure 8: Preferences for domains to be covered in the exercises

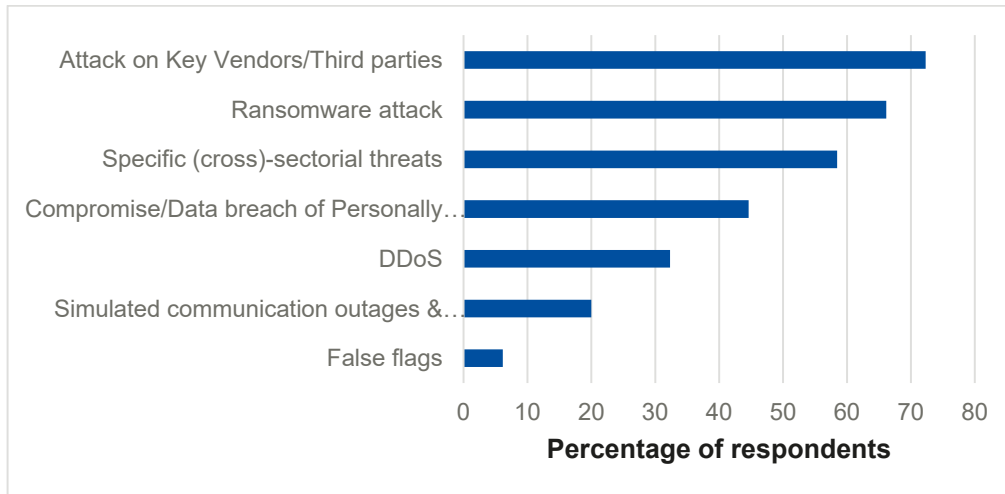


NB: SOP, standard operating procedure.

Each exercise is built on an imaginary scenario that can create a stage for testing reactions, operational procedures and cross-sectoral communities. Unfortunately, the real-world cyber landscape offers a wide range of scenarios, as the number of attacks and new attack vectors are constantly rising. Even though real-life cases may well be different from previously run exercises, the latter will benefit ISACs by training stakeholders and giving them confidence in the processes and procedures that have been designed, proof-tested, and eventually improved and updated.

Participants were asked to rate their preferred exercise scenarios from 1 to 5, with 1 being the most preferred and 5 being the least preferred. Results were then analysed according to the number of votes for each subject and ratings provided by the participants, and presented as votes for each subject. As shown in Figure 9, the most preferred exercise scenario was the ‘attack on key vendors / third parties’, followed by the ‘ransomware attack’ scenario. The least preferred scenario was ‘false flags’, which is best applied in a mature context. Bearing in mind that recent global cybersecurity incidents and crises involved vendor / third-party attacks followed by ransomware deployment (and later extortion), it is clear why the participants chose this type of attack scenario as the most suitable for a cross-sectoral exercise, as these are currently considered the most significant global cyberthreats, as mentioned in the various ENISA threat landscape publications.

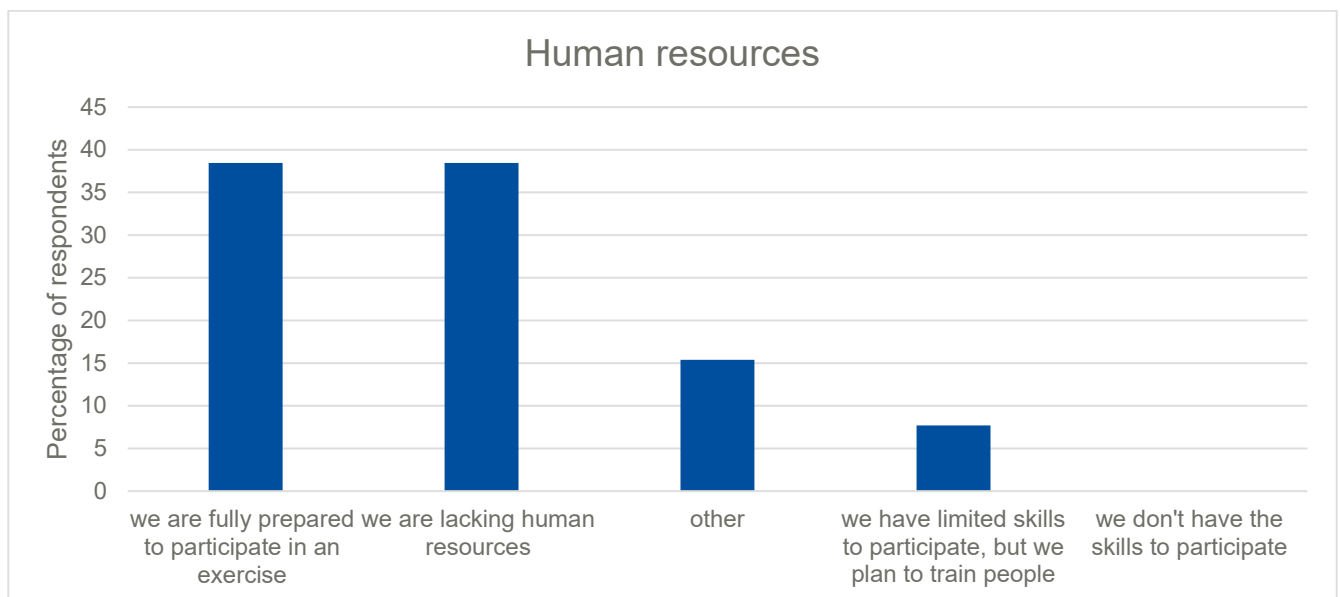
Figure 9: Preferences for exercise scenarios



Along with the expectations on cross-sectoral exercises, types and possible scenarios, through the survey and this report we also aimed to assess the level of preparedness of ISACs to participate in the exercises. The success and purpose of every exercise fully correlates with the participants' level of preparedness and established capabilities. Among the resources necessary for participating in the exercises, human resources are the most important.

The analysis we conducted based on the survey results shows that this may be the major obstacle to and challenge in organising large-scale cross-sectoral ISAC exercises (Figure 10). Almost 40 % of the respondents signalled that their ISAC is 'currently lacking in human resources, or expecting workloads that do not permit other activities'. The other 40 % are both fully equipped and fully skilled regarding human resources to participate in the exercise or have plans to improve skills in the near future.

Figure 10: Human resources



The respondents also stressed that they would be willing to reallocate their resources as necessary to participate in the exercises if participating would be of value to their members and sector.

Preparing, planning and participating in the exercises usually requires taking over some of the exercise roles. The usual roles and the roles used for the purposes of the survey are shown in Table 3.

Table 3: Exercise team roles

Team	Description
Leadership team	Responsible for overseeing all aspects of the table top cyber exercises, using a strategic approach
Planning team	Advises and validates the development of the exercise scenarios / injects and objectives
Facilitation team	Leads participants through the exercises by setting the stage and facilitating discussion
Observer team	Witnesses the proceedings and events and assesses the preparations of organisations or individuals within them and gives recommendations on how their plans can be amended to address gaps

Like the finding that a high percentage of ISACs lack the human resources needed to participate in cross-sectoral exercises, the analysis of the survey showed that small percentages of the ISACs surveyed are willing to take leadership (23 %) or planning (23 %) team roles. In line with this finding, the highest percentage of ISACs (38 %) were willing to take the least demanding observation team role. This suggests that lack of human resources and appropriate skills may be a significant obstacle to and challenge in organising cross-sectoral exercises. **However, for an exercise to be fully useful, ISACs should not just observe – ISAC core team members should do what they would actually do if there was a real incident/crisis.**

When it comes to taking roles in cross-sectoral exercises, almost 90 % of the respondents described ENISA taking over the leadership, planner or facilitator role. **Like the abovementioned conclusion, for an exercise to fulfil its purpose, ISAC core team members should be at least planners, with some involvement in facilitation activities too.**

Besides the human resources necessary for successful cross-sectoral exercises, there are other types of resources and activities that can be regarded as prerequisites for establishing a good basis and exercise environment. For the purpose of this report, we surveyed participants on the importance of the following resources and activities:

- a dedicated communication platform,
- alternative/backup communication platforms,
- holding initial, midterm and final planning meetings,
- guidelines and instructions,
- 'getting to know the participants' sessions.

A large majority of respondents (60 %) reported that holding initial, midterm and final planning meetings was the most important activity, followed by the existence of a dedicated communication platform and guidelines and instructions. Besides the listed resources and activities, participants stressed the need to conduct the exercise using an existing communication platform and a dedicated table top exercise environment. The aim is to proof-test existing means of communication under stress.

Along with existing human and other resources within ISACs, specific skills and capabilities can be gained through specialised pre-exercise training:

- dedicated conferences on ISAC exercises,
- specialised training on table top exercises,
- exercise platform training,
- senior-level pre-exercise meetings,
- selected exercise scenario training.

A significant percentage of the respondents (46 %) reported that dedicated conferences on ISAC exercises were the most useful form of pre-exercise training, followed by senior-level pre-exercise meetings (23 %).

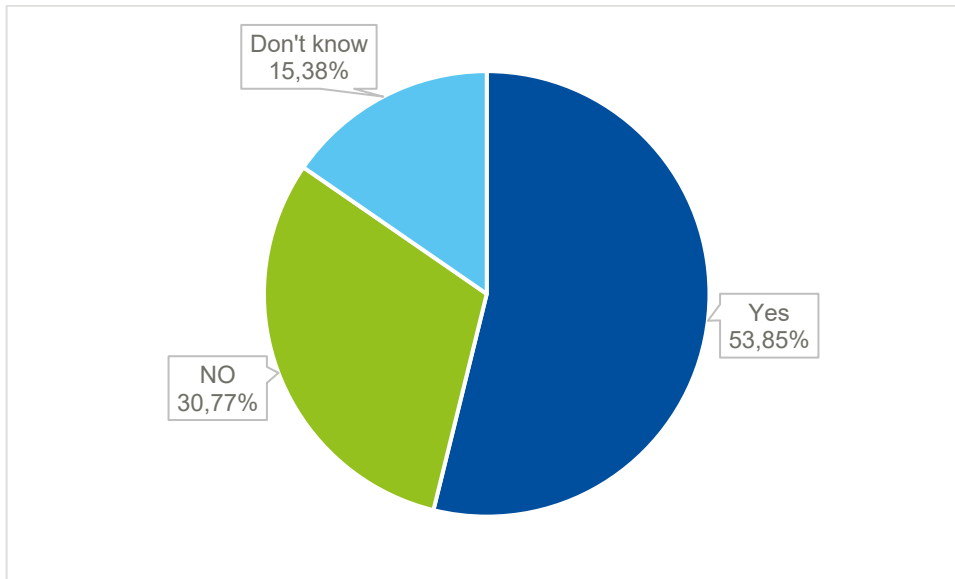
The last aspect in this section of the survey was an assessment of participants' preferences for the following debriefing and after-exercise reporting mechanisms:

- hot debrief
- cold debrief
- after-action review
- recommendations
- action plan.

Respondents mostly reported that hot debriefs (38 %) were the most useful post-exercise activity, followed by recommendations (30 %) and after-action reviews (23 %).

As for whether anonymised executive reports and reports on lessons learned should be shared with the wider public (e.g. Member State authorities, Computer Security Incident Response Teams Network and cooperation groups, extending to the global ISAC community – based in the United States – and to non-EU neighbouring countries, such as the United Kingdom and European Free Trade Association countries) or exclusively within the participants' networks, 53 % (7 out of 13) of respondents accepted the possibility of sharing them with the wider public (Figure 11).

Figure 11: Sharing reports with the wider public



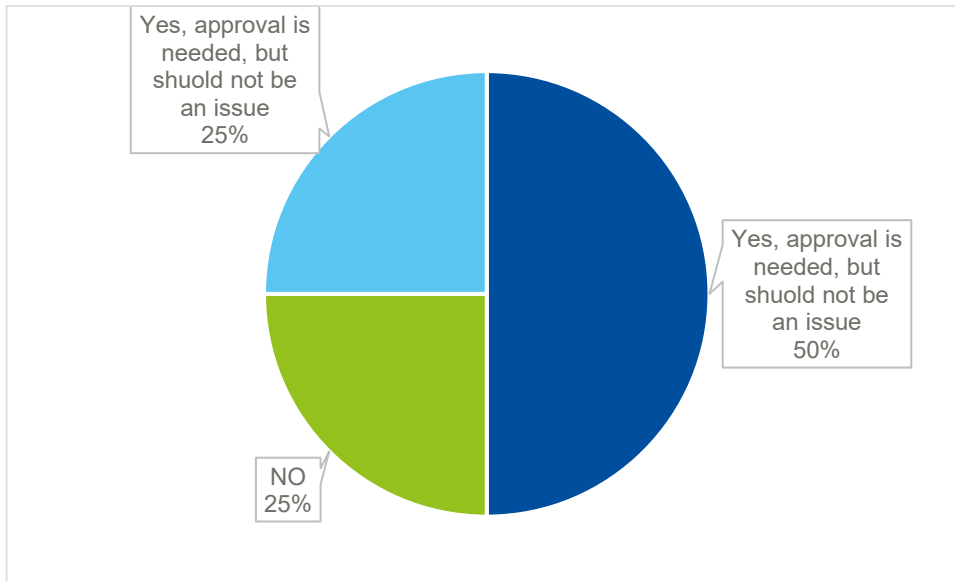
However, sharing such reports depends on the contents and level of confidentiality required to safeguard the contents, which may contain sensitive information on ISACs' organisation, structure and procedures. A possible solution is to prepare a sanitised report for sharing with the wider public and for public relations purposes.

4.2. INTERACTION CHALLENGES

In this section we assess the current state of play regarding interactions between the communities and different stakeholders, and possible obstacles or aggravating issues related to participating in cross-sectoral exercises.

Participating in any kind of exercise is resource consuming and is not a priority for many organisations. In addition, some organisations may have different kinds of legal, regulatory or statutory limitations in terms of engaging in this kind of activity. From the information collected through the survey, 50 % of the respondents need approval for participation but getting approval should not be an issue, 25 % need approval and are not sure about the final decision, and 25 % need no approval to participate in a cross-sectoral exercise (Figure 12).

Figure 12: Approval for participating



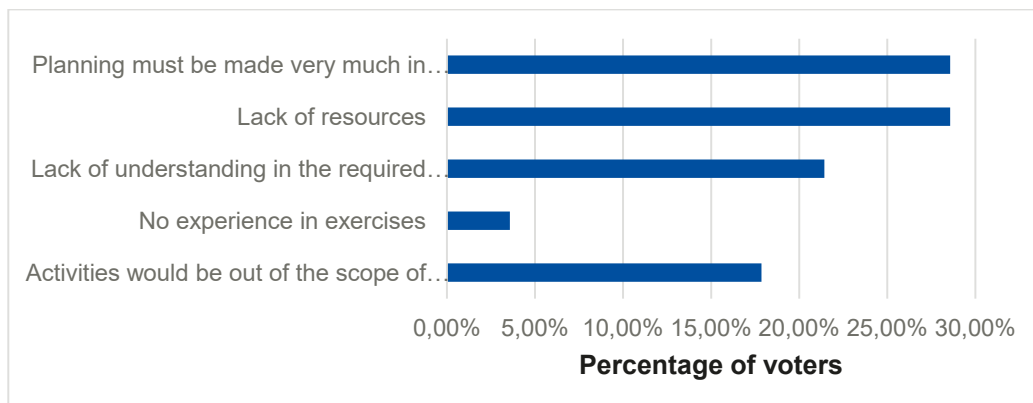
As for the final outcomes of participating in cross-sectoral exercises, through the survey we aimed to assess the usefulness of the following specific goals:

- internal awareness raising,
- establishing cross-sectoral connections,
- improving standard operating procedures (SOPs) and strategies,
- identifying weaknesses in internal Restriction of Privileges (RoPs),
- identifying potential gaps in cross-sectoral communication,
- developing the internal skill set.

Some 30 % of respondents saw the goal of identifying potential gaps in cross-sectoral communication as the most important to be reached, and the goal of establishing cross-sectoral connections had the same percentage of responses. The goal recognised as least important was identifying weaknesses in internal RoPs.

Organising and participating in cross-sectoral exercises can be negatively affected by a number of aggravating issues. As shown in Figure 13, participants recognised a lack of resources and the fact that planning must be done very much in advance as the most significant among them.

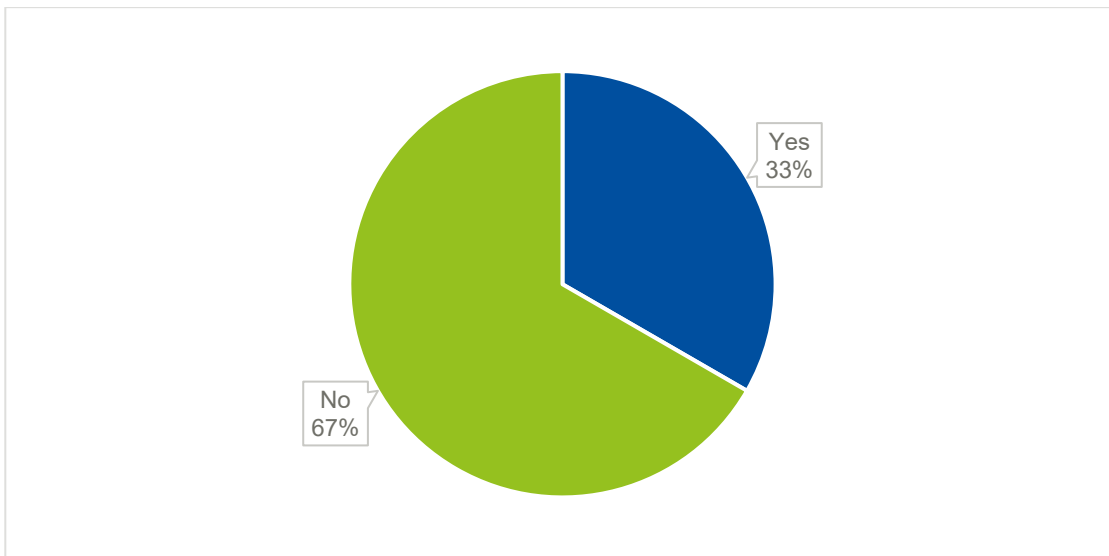
Figure 13: Aggravating issues anticipated



However, as shown in Figure 14, when surveyed directly on previous experience of running and/or participating in any kind of exercises within ISACs (e.g. table top exercises, communication checks, technical hands-on exercises, internal ISAC exercises, seminars and workshops), 67 % of respondents declared that they had no experience. All of the participants with previous experience confirmed that this activity was highly useful for their ISAC and that important lessons could be learned on the following issues:

- coordination weaknesses,
- how to communicate with the media,
- willingness to share actionable information,
- who should be contacted and involved,
- missing incident response strategies,
- missing ‘automation’ in continuous monitoring,
- missing clarification of roles (Public Private Partnerships PPP, national computer security incident response team, national banks, regulators, etc.),
- need for communication processes to be improved.

Figure 14: Previous experience of running and/or participating in any kind of exercise within your ISAC



The last question in this section of the survey asked which stakeholders, besides ISACs, may be useful as participants in cross-sectoral exercises. Almost 50 % of participants reported that sectoral authorities are the most important stakeholders to have as participants in cross-sectoral exercises, followed by national/governmental computer security incident response teams (15 %) and ENISA (15 %). National security agencies are recognised as the least important stakeholders in this regard.

4.3. SUMMARY

The survey provides some clear ideas on what ISACs expect to gain from cross-sectoral exercises, their levels of preparedness and the possible obstacles to successful exercise implementation.

ISACs prefer organisational exercises, with the aim of checking and improving their capabilities in the incident response and crisis management domains. ISACs also prefer exercises related to the current ‘attack trends’ globally, such as attacks on key vendors and ransomware attacks.

Regarding the human resources that are available and levels of equipment and skill sets, around half of the ISACs surveyed are well equipped and the other half are lacking in human resources and are not in a position to carry out new activities such as participating in exercises.

The ISACs surveyed recognise the importance for success of the timely preparation of exercises, with an initial step being the presentation of the context of the exercise, and planning in advance using a formal preparation process.

Most of the ISACs surveyed are willing to share the final results of the exercises with the wider public. Sectoral authorities are seen as the most important stakeholders to include in exercises.

5. CONCLUSIONS AND THE WAY FORWARD

Using the data collected and the interviews conducted the following conclusions can be drawn. The conclusions were confirmed through a validation process.

5.1. CONCLUSIONS

From the questionnaire analysis and interviews, we identified the following common areas of interest.

- ISACs see training and exercises as excellent opportunities to improve skills.
- The interdependencies between sectors was clearly identified as a key challenge to address.
- Owing to the heterogeneous maturity levels, there is a clear need to address and involve C-level executives in information exchange exercises and training. Strategic aspects of information exchange should be addressed.
- The ISACs see little difficulty in participating in exercises and training organised by others, on the condition that they have sufficient resources to participate.
- An indirect benefit of organised training and exercises, and learning new skills, is building trust in the community.
- The ISACs clearly identified that knowledge of applicable legislation is key to dealing with information exchange.
- Owing to the different levels of maturity, there needs to be a minimum level of technical and organisational competence to be able to exchange information.

Based on the analysis in this report, the ISACs need to have a minimum level of technical and organisational skills to participate in cross-sectoral exercises. As identified in this report, at a minimum, expertise is required in:

- the regulatory environment applicable to threat information exchange;
- validating the received threat intelligence information;
- threat information and naming schemes and sharing designations;
- the use of tools for information sharing.

The skills can be connected with the selected cross-sectoral exercises in the following ways.

Table 4: Connection of skills so to cross-sectoral exercise domains

Exercise domains	Skills required
Organisational	<ul style="list-style-type: none"> • Knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (e.g. data retention, attribution, PII and cross-border prohibitions) • Knowledge of internal procedures for incident handling (if sensitive data is leaked)

	<ul style="list-style-type: none"> • Knowledge of the specifics of SLAs, NDAs and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations) • Knowledge of data sanitisation requirements and techniques • Communication and group facilitation skills • Applied knowledge of different security measures to be implemented to secure information exchange (e.g. encryption and transfer protocols)
<p>Incident response</p>	<ul style="list-style-type: none"> • Knowledge of validating the received threat intelligence information (making sure that it is of high quality, actionable, accurate, relevant and specific). • Knowledge of threats (e.g. IoC, CVE and other relevant schemes) • Tools for sharing information (e.g. MISP) • Knowledge of sharing designations (e.g. TLP) • Risk assessment methodologies and tools to be utilised to classify the received information. • Knowledge of internal procedures for incident handling (if sensitive data is leaked) • Knowledge of the specifics of SLAs, NDAs and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations) • Applied knowledge of industry standards related to threat information exchange (e.g. TAXII, STIX, CybOX and CIF) • Knowledge of data sanitisation requirements and techniques • Communication and group facilitation skills • Applied knowledge of different security measures to be implemented to secure the information exchange (e.g. encryption and transfer protocols)
<p>Crisis management</p>	<ul style="list-style-type: none"> • Knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (e.g. data retention, attribution, PII and cross-border prohibitions) • Knowledge of internal procedures for incident handling (if sensitive data is leaked) • Knowledge of the specifics of SLAs, NDAs and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations) • General intelligence information analytical skills (not tools but frameworks, etc.) • Communication and group facilitation skills

5.2. THE WAY FORWARD

Based on the results and the feedback from the ISACs, the cross-sectoral exercise could be an organisational exercise with a scenario on an incident response attack on a key third party / vendor.

For the exercise to be successful, the ISACs need to consider the following skills and organisational and technical steps.

5.2.1. Skills steps

Having the right skills in the information sharing and analysis community is a firm requirement. Indeed, being able to recognise a threat, analyse it and propose measures is something that is essential for the cybersecurity community. It is one thing to be able to share information properly with the community within the ISAC, and another to be able to share information outside this community. In many cases, the people in the ISAC community have a certain knowledge of information threat analysis or information sharing, but they may not always be experienced in sharing information outside the ISAC, which usually requires skills in understanding the needs of the other sector the ISAC is sharing the information with.

The EU ISACs should focus their efforts on:

- **improving their knowledge of applicable legislation related to information exchange;**
- **improving their knowledge of technical skills in information analysis and exchange.**

5.2.2. Organisational steps

ISACs need to have clearly defined roles to be able to exchange information. Currently, such roles are not clearly defined. In addition, ISACs should introduce SOPs for sharing information outside their communities. Therefore, ISACs need to identify and assign specific roles to enable information exchange to the outside community and follow predefined and tested procedures.

The EU ISACs should focus their efforts on:

- **developing proper roles and responsibilities for sharing information outside the ISAC community;**
- **developing SOPs for cross-sectoral information sharing;**
- **exchanging good practices in cross-sectoral information exchange.**

In the interviews and in ENISA's experience, trust is of the utmost importance in information sharing, especially when sharing with the outside community. The organisation of cross-sectoral exercises and/or training is a natural way of building trust among the communities. In addition, to build further trust, staff exchange or cross-participation in ISAC events is beneficial.

5.2.3. Technical steps

There is a need to test the effectiveness of the steps implemented in response to the recommendations above (this may also include continuous improvement). This could be done by introducing cross-sectoral exercises on technical and organisational aspects of information exchange.

Automation is a key component of effectively and efficiently ingesting technical information such as IoCs. Accordingly, having a common platform or a platform that supports commonly supported formats is beneficial, especially for sharing operational information, which has a short lifespan.

The EU ISACs should focus their efforts on:

- **SOP testing and live information exchange testing;**
- **cross-sectoral training using specific technical tools.**

ANNEX: RESPONSES REGARDING THE RELATIVE IMPORTANCE OF SKILLS

Tables A1–A3 depict the responses of the participants on the subject of required skills. Table A1 provides the raw information from the survey and Table A2 contains the aggregated information (Table A2 also provides the responses to the open-text questions; the results are aggregated per area of knowledge/skill). For example, for the knowledge on threats (e.g. IoC, CVE and other relevant naming schemes), three respondents chose it as the most important, one as the second most important, one as the third most important, and so on.

Table A1: Responses regarding the importance of knowledge/skills importance

Knowledge/skills	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
Knowledge of applicable legal and regulatory compliance requirements affecting threat information exchange (e.g. data retention, attribution, PII and cross-border prohibitions)		2nd	3rd		3rd		1st	2nd	4th	3rd	1st		2nd
Knowledge of validating the received threat intelligence information (making sure that it is of high quality, actionable, accurate, relevant and specific).	3rd	1st		2nd	5th			1st	3rd	5th	3rd	1st	5th
Knowledge on threats (e.g. IoC, CVE and other relevant naming schemes)	2nd	3rd	1st			1st		5th		1st	4th		
Tools for sharing information (e.g. MISP)	4th			4th		2nd			1st	2nd	5th	3rd	4th
Knowledge of sharing designations (e.g. TLP)	1st		5th			4th		3rd			2nd	2nd	
Risk assessment methodologies and tools to be utilised to classify the received information		4th	2nd	3rd					2nd				
Knowledge of internal procedures for incident handling (if sensitive data is leaked)		5th			2nd	3rd						5th	
Knowledge of the specifics of SLAs, NDAs and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations)	5th				1st		2nd						
Applied knowledge of industry standards related to threat information exchange (e.g. TAXII, STIX, CybOX and CIF)			4th		4th					4th			

Knowledge/skills	Importance
Knowledge of validating the received threat intelligence information (making sure that it is of high quality, actionable, accurate, relevant and specific).	31
Knowledge of threats (e.g. IoC, CVE and other relevant naming schemes)	25
Tools for sharing information (e.g. MISP)	23
Knowledge of sharing designations (e.g. TLP)	19
Risk assessment methodologies and tools to be utilised to classify the received information	12
Knowledge of internal procedures for incident handling (if sensitive data is leaked)	11
Knowledge of the specifics of SLAs, NDAs and other agreements in place within the ISAC (describing the responsibilities of its members and participating organisations)	10
Applied knowledge of industry standards related to threat information exchange (e.g. TAXII, STIX, CybOX and CIF)	6
Knowledge of data sanitisation requirements and techniques	5
Knowledge of newly created railway-specific cybersecurity standards (e.g. IEC62443 deviated standard and TSI.57001)	5
General intelligence information analytical skills (not tools but frameworks, etc.)	5
Communication and group facilitation skills	2
Knowledge of how to establish trust between the ISACs and their members	1
Applied knowledge of different security measures to be implemented to secure information exchange (e.g. encryption and transfer protocols)	0



About ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of information and communications technology products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found on its website (<https://www.enisa.europa.eu/>).

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira

700 13 Vassilika Vouton, Heraklion, Greece

[enisa.europa.eu](https://www.enisa.europa.eu)



ISBN 978-92-9204-570-8
doi:10.2824/941158