The landscape of European ISACs in 2023

NASK

The landscape of European ISACs in 2023

NASK

AUTHORS

Paulina Popow
Emilia Zalewska-Czajczyńska

SCIENTIFIC REVIEW

Marek Pawlik, Ph.D., D.Sc. Eng., Professor of Railway Research Institute (IK)

ISBN: 978-83-65448-95-8
DOI: 10.60097/NASK/978-83-65448-95-8

National Research Institute NASK
12 Kolska Street
01–045 Warsaw

Dear Sir/Madam,

We are thrilled to present the much-anticipated report, “The Landscape of European ISACs in 2023”, prepared by experts from the Cybersecurity Strategy and Development Department at the NASK National Research Institute. Our aim is to provide you with comprehensive overview on the functioning of the largest European Information Sharing and Analysis Centres (ISACs), as well as to discuss their significance within the cybersecurity ecosystem.

Information Sharing and Analysis Centres were established in response to meet the need for cooperation and rapid information exchange between private and public sector organisations. They have been one of the cornerstones of the European Union’s strategy to protect against cyberattacks for many years. ISACs enable not only the exchange of information on cyberthreats between private and public sector entities and the joint development and implementation of best practices in the field of cybersecurity.

This report presents the concept of ISACs and analyses their operations in Europe. It highlights diversity of sectors that utilise ISAC services, including, among others, energy, financial and transport sector. It also asserts the importance of international cooperation in effectively countering global cybersecurity threats.

In 2023, European ISACs have played a pivotal role in coordinating cybersecurity activities, leading to enhanced protection of critical infrastructure and heightened awareness of threats among all stakeholders.

We encourage you once again to explore the contents of the report, which we hope will contribute to the further consolidation of the European cybersecurity ecosystem. I would like to express my gratitude and appreciation to the reviewer of the report, Marek Pawlik, Ph.D., D.Sc. Eng., Professor of Railway Research Institute (IK), as well as the authors of the report – Emilla Zalewska-Czajczyńska and Paulina Popow.

Paweł Zegarow

Head of Cybersecurity Strategy Development Department
NASK National Research Institute

Table of Contents

Introduction

Information Sharing and Analysis Centres (ISACs) are vital in building collective resilience to cyber threats. This type of organisation has grown significantly in recent years, both at national and international levels. This publication, entitled “The landscape of European ISACs in 2023”, provides a comprehensive analysis of the role and functions of ISACs operating in Europe, and identifies the opportunities and challenges they face.

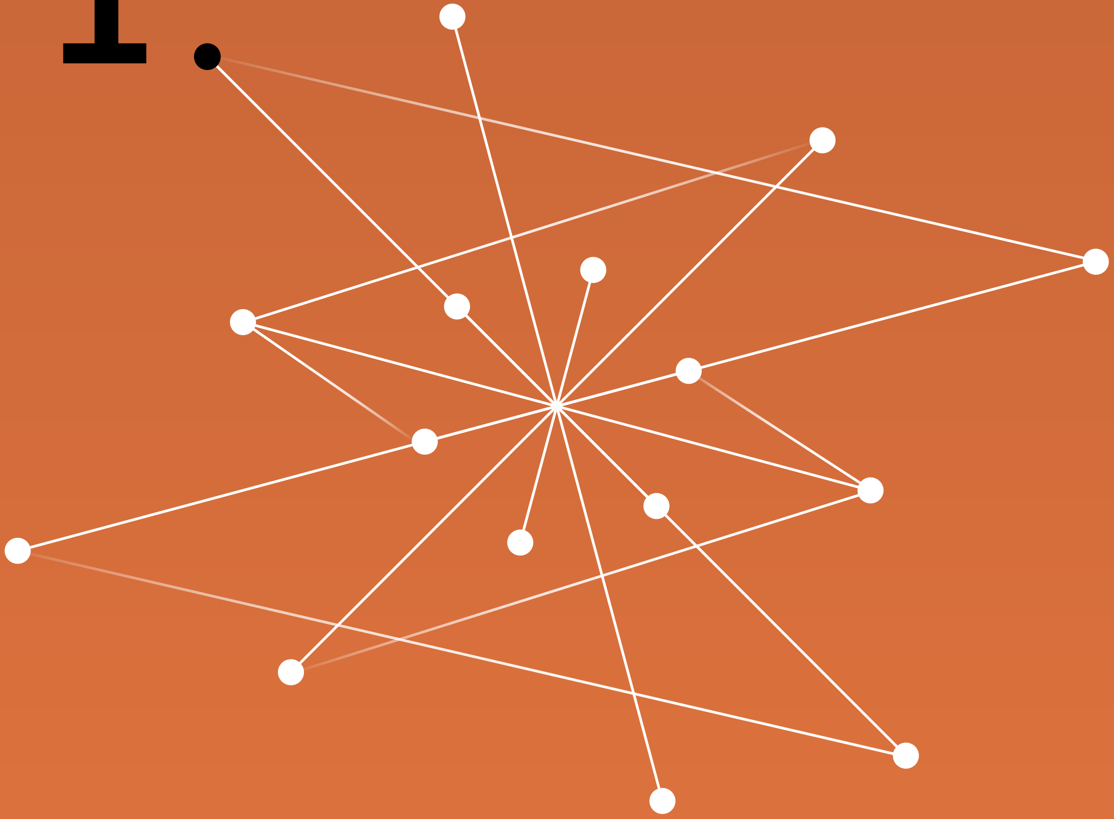
The publication is divided into three parts. It begins with a theoretical introduction, including the history of the emergence of ISACs, their definition and a discussion of the similarities and differences between such organisations in the United States and Europe. This part also includes basic information on cooperation for cybersecurity and information sharing models.

The second component of the publication is a report on a study of 10 European ISACs conducted by the authors in 2023. It contains an account of the methodology employed in the survey, findings, and a synthesis of the main conclusions. It concludes with a series of recommendations derived from the analysis of the survey results.

The publication includes also a set of infographics providing detailed information on selected European ISACs that participated in a study.

The main objective of this publication and the study it describes is to present and analyse the landscape of European ISACs in a comprehensive manner. Such organisations constitute an integral component of cybersecurity systems at various levels – it is therefore worth to enhance awareness and knowledge about them. The examples of activities of the ISACs presented in the publication can also serve as a model and inspiration for other organisations active in the field of cybersecurity

1.



About ISACs – theoretical introduction

The modern era is characterized by the dynamic development of technology, which is also associated with a steady increase in the number and sophistication of threats occurring in cyberspace. In the face of growing challenges, it is imperative that public and private sector entities enhance their security measures on an ongoing basis. One initiative to facilitate this process is the establishment of Information Sharing and Analysis Centres (ISACs). These organisations are primarily tasked with creating a platform that enables sharing of information, experiences and best practices in the field of cybersecurity. This allows ISAC members to collectively create an environment that is more resilient to cyber threats

1.1 History of the creation of ISACs

The inaugural ISACs were established in the United States in the 1990s. Two pivotal events – the first terrorist attack on the World Trade Centre in 1993 and the Oklahoma City attack in 1995 – significantly influenced the inception of these entities.[1] The need to increase the security of the state's key resources was then recognised. In order to address this issue, the Presidential Commission for the Protection of Critical Infrastructure was established in 1996.[2] As part of its activities, a report was created that proposed recommendations for enhancing the security to improve security in this area. One of the ideas was to establish organisations that would facilitate information sharing and strengthen cooperation between public and private entities.[3] On May 22, 1998, Bill Clinton, then president of the United States, signed a directive on the protection of critical infrastructure, thereby establishing the foundation for the implementation of the concept of creating such centres.[4] The first organisation of this kind, the Financial Services ISAC (FS ISAC), was established in the financial sector less than a year after the presidential directive was signed.

[1] European Union Agency for Cybersecurity (ENISA), *Information Sharing and Analysis Center, Cooperative models*, 2018, Information Sharing and Analysis Center (ISACs) – Cooperative models – ENISA (europa.eu), [accessed 15.04.2024].

[2] J. Sadowski, *Ochrona Infrastruktury Krytycznej. Uregulowania prawne*, „Zeszyty Naukowe. Organizacja i Zrządzanie", 2018, no. 6, p. 1237.

[3] European Union Agency for Cybersecurity (ENISA), op. cit.

[4] *Presidential Decision Directive/NSC-63 – Critical Infrastructure Protection of 22 May 1998*, Critical Infrastructure Protection (PDD 63) (fas.org), [accessed 15.04.2024].

Currently, there are 26 ISACs in the United States, whose activities since 2003 have been coordinated by the National Council of ISACs (NCI). The centres regularly submit reports of their activities to the Council and, with its support, organise regular meetings and exercises. The NCI plays an active role in supporting the establishment of new ISACs, especially in those sectors and subsectors of critical infrastructure where there is a lack of clearly established methods for exchanging cybersecurity information. Additionally, NCI maintains an ongoing registry of ISACs operating in the United States, which is available on the Council's website.[5]

1.2 Definitions of ISACs

Definition of ISACs in the United States

According to the definition proposed by NCI, ISACs are non-profit organisations created and led by their members. They are based on public-private partnerships and focus on the needs of the sector they represent. The objective of ISACs is to provide support to their members through the implementation of initiatives designed to enhance security and resilience against cyber threats. A specific emphasis is on helping owners and operators of critical infrastructure to ensure the security of the facilities they oversee and the personnel they employ. In addition, ISACs, based on the information they collect and analyse, alert their members to potential threats and provide resources to protect themselves and to strengthen overall resilience against cyber threats.[6]

Definition of ISACs in Europe

ENISA – the European Union Agency for Cybersecurity – defines an ISAC as a non-profit organisation focused on collecting, analysing, exchanging information on cyber threats and on cross-sector cooperation. ISACs aim to strengthen cybersecurity by integrating the private and public sectors and sharing knowledge between them. These organisations are instrumental in bolstering the resilience of a given sector of the economy

[5] National Council of ISACs (NCI), National Council of ISACs | About NCI (nationalisacs.org), [accessed 15.04.2024].

[6] National Council of ISACs | About NCI (nationalisacs.org), ibidem.

against cyber threats. The activities of ISACs also contribute to the implementation of national cybersecurity strategies, in alignment with EU regulations, and promote the exchange of information and best practices in the field of cybersecurity.[7]

1.3 ISACs in the United States and Europe – similarities and differences

Objectives of activity

In both the United States and Europe, Information Sharing and Analysis Centres pursue a common objective with regard to their activities: to support building of resilience in the area of cybersecurity in various sectors of the economy. On both continents, these organisations serve as platforms for the exchange of knowledge, best practices and warnings about cyber threats.

Functioning of a public register

One of the major differences between European and American ISACs is the functioning of a publicly available registry of such organisations. As previously stated, in the United States such a registry is maintained and made publicly available on the NCI website. It includes a list of ISACs with a brief description of their activities and a links to their respective websites. In contrast, there is no such register in Europe, with the consequence that information about European ISACs is scattered and less accessible.

Legal regulation

In both the United States and Europe, there is no single, specific legal act that regulates the activities of ISACs. However, on both continents, there are regulations that contribute to supporting the operation of such entities.

[7] European Union Agency for Cybersecurity (ENISA), op. cit.

In the United States, the initial legislative measure was the aforementioned presidential directive from 1998, which promoted the establishment of ISACs to protect critical infrastructure from cyber threats. In turn, CISA – the Cybersecurity Information Sharing Act, was enacted in 2015, which, among other things, set out guidelines for non-governmental entities to share cyber threat data with government institutions. Although this act does not directly mandate the creation of ISACs, it provides substantial support for the information sharing process within such organisations. CISA also guarantees liability protection for companies that share information in accordance with its guidelines.

In Europe, the NIS Directive was adopted in 2016. It concerns measures for a high common level of security of network and information systems across the Union, which is the first EU legislation to comprehensively regulate cybersecurity.[8] While the directive did not contain provisions that explicitly addressed to ISACs, it helped to raise awareness of their importance for the exchange of information between various entities in the context of cybersecurity.

An amendment to the EU's cybersecurity legislation, the NIS 2 Directive, was adopted in 2022.[9] Similar to its predecessor, NIS 2 Directive does not contain direct provisions related to ISACs. However, Article 29 is of particular significance for such organisations, as it concerns mechanisms for cybersecurity information sharing. Member States have been obliged to allow NIS 2 covered entities and others as appropriate, to engage in the voluntary exchange of cybersecurity information, including cyber threats, vulnerabilities, techniques and procedures. The provision also requires Member States and ENISA to support the creation of appropriate mechanisms for such information sharing to be conducted in a secure manner.

Furthermore, recital (9) of the NIS 2 Directive makes reference to analysis and information sharing centres in the context of their utilisation of the TLP (Traffic Light Protocol) confidentiality code. However, there is no clarification whether this provision refers specifically to ISACs or any kind of organisations carrying out information sharing and analysis activities.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 measures for a high common level of security of network and information systems across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148.

1.4 Cooperation of European ISACs for cybersecurity

International cooperation is one of the key elements in building European cyber resilience. Cyber threats do not stop at national borders, making it necessary to establish strong international alliances in the field of cybersecurity. Individual ISACs are responsible for the collection of information on incidents in the sectors they represent, including finance, energy, healthcare or transport. However, to increase the efficiency of their operations, they also cooperate with each other and with a diverse array of entities, such as EU institutions and industry associations.

Cooperation with European institutions

European institutions play a significant role in the promotion of information sharing and the enhancement of cybersecurity. In the context of the activities of ISACs, ENISA is a particularly noteworthy organisation. It plays and important role in supporting the establishment and operation of ISACs. One of its most significant contributions is the “ISAC in a Box” initiative. This comprehensive toolkit provides support at all stages of ISAC development, from creation to mature operation. It covers four phases of ISAC evolution, offering guidance on key aspects such as governance, risk management, and incident response.

The “ISAC in a Box” tool provides practical information and guidance on a range of topics, such as formulation of goals and budgets, the development of policies, and the attraction of members. These issues are particularly important for organisations that are in the developmental phase. At the next stage, the toolkit proposes methodologies for the effective governance of the established organisation, the cultivation of trust between members, and the optimisation of the information exchange process. ISACs that in have already developed these elements can proceed to verify the measures taken, assess the dynamics of the organisation’s development and identify factors that need to be changed. For organisations that completed this phase of development, “ISAC in a Box” provides guidance on how to achieve organisational maturity, which means ensuring the continuous development and upgrading the level of sophistication of the activities undertaken.

Furthermore, ENISA is engaged in research activities related to the functioning of ISACs. The agency has produced a report that identifies the types of skills and organisational and technical activities that are necessary to ensure effective information exchange among ISACs.[10]

It is worth noting that ENISA's activities are primarily focused on ISACs at the European level. However, national ISACs can also benefit from the documents and information available on the agency's website, which cover topics related to creating and developing such entities.

Another European institution that plays an important role in supporting the activities of ISACs is the European Commission. One of its initiatives is *Empowering EU-ISACs*,[11] which aims to mobilise public and private entities to create new sectoral ISACs in the European Union, by providing them with organisational, technical, legal, and training support. In addition, the European Commission fosters the development and enhancement of the maturity level of existing organisations and cooperation between them.

Additionally, some activities of ISACs are also supported by EUROPOL (European Union Agency for Law Enforcement Cooperation). In 2013, the agency established the European Cyber Crime Centre – EC3, whose principal objective is to provide assistance to Member States' law enforcement agencies in combating criminal activities perpetrated in cyberspace and to enhance the protection of citizens, businesses, and state institutions in European countries.[12] One important aspect of the EC3's activities in the context of ISACs is its cooperation with the FS-ISAC in countering financially motivated cybercrimes against banks and other financial institutions.[13]

As evidenced by the aforementioned examples, the landscape of cooperation between EU institutions and ISACs is highly diverse. It encompasses a range of forms of support, including organisational, legal, technical, and financial, and advisory assistance, as well as efforts to enhance awareness and knowledge. Cooperation with EU institutions helps ISACs adapt to current legal regulations, expand their activities, reach new members and improve ability to address global cyber threats.

[10] European Union Agency for Cybersecurity (ENISA), *Cross-Sectors Exercise Requirements*, 2018, Cross-Sector Exercise Requirements – ENISA (europa.eu), [accessed 15.04.2024].

[11] Empowering EU-ISACs, Home | Empowering EU-ISACs, [accessed 15.04.2024].

[12] European Cyber Crime Centre, European Cybercrime Centre – EC3 | Europol (europa.eu) [accessed 15.04.2024].

[13] EUROPOL, *FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime*, 19.09.2019, FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime | Europol (europa.eu), [accessed 15.04.2024].

Cooperation with other ISACs

European ISACs also engage in collaborative efforts with one another, as well as with analogous organisations based in other global regions. One example of intercontinental cooperation between ISACs is the partnership among organisations operating in the energy sector. In addition, joint events are organised as part of this partnership, allowing new contacts to be made between regions and building mutual trust between organisations.[14]

Cooperation with other types of entities

A significant area of cooperation between ISACs and other entities is the relationships established with industry organisations operating at European and national level. Such collaboration enables ISACs to extend their activities within a given sector. As an example, Auto-ISAC has formed a partnership with the European Automobile Manufacturers' Association – ACEA and the European Association of Automotive Suppliers – CLEPA. With the support of these industry organisations, Auto-ISAC, which was originally founded and operated in the United States, has expanded its activities into the European market and reached out to prospective new members. In turn, ACEA and CLEPA gained the opportunity to establish connections with entities from the United States.[15]

Another group of entities with which ISACs collaborate are national and European Computer Emergency Response Teams (CERTs). They play a particularly important role in ensuring an adequate response to cyber threats and their activities include, among other things, monitoring systems, analysing incidents, identifying threats, applying appropriate countermeasures and restoring proper functioning of systems. Through efficient cooperation and information sharing between CERTs and ISACs, members of ISACs are better equipped to respond to incidents in a timely and effective manner. An example of such cooperation is the exchange of information in the area of aviation cybersecurity between EUROCONTROL (EATM-CERT) and the Aviation ISAC. This partnership also includes joint

[14] EE-ISAC, *Japanese & European energy communities sign partnership agreement on cyber security*, 17.05.2017, Japanese & European energy communities sign partnership agreement on cyber security – EE-ISAC – European Energy – Information Sharing & Analysis Centre, [accessed 15.04.2024].

[15] European Automobile Manufacturers' Association (ACEA), *European manufacturers and suppliers join with Auto-ISAC* , 12.10.2022, European manufacturers and suppliers join with Auto-ISAC – ACEA – European Automobile Manufacturers' Association, [accessed 15.04.2024].

threat analysis and the development of best practices and procedures that contribute to building cyber resilience in the global air transport network.[16]

1.5 Information sharing in the context of cybersecurity

Information sharing in the context of cybersecurity can occur in two forms: ad hoc or as part of an ongoing, long-term relationship. These two models can be further distinguished as mandatory or voluntary. The choice of the appropriate model for a given situation depends on factors such as the level of trust between parties, the purpose of the information exchange, and the legal regulations in this regard.[17]

The mandatory information sharing model is predicated on the assumption that this is required by law or by prior agreements (e.g. contractual) between the parties. The covered entities must therefore provide certain information, as they may be subjected to predetermined sanctions in the event of non-compliance. This model is typically observed in the relationship between entities subject to specific legislation and relevant state authorities. In the context of cybersecurity, an example of a regulation requiring mandatory information sharing is the NIS 2 Directive, which requires certain entities to report specific types of incidents.

In the case of the voluntary information sharing model, the decision to share information is made at the initiative of the parties involved. The extent and form of the data to be shared is also determined by them. In contrast to the mandatory model of information exchange, the parties are not subject to sanctions if they decide not to share certain information. This model usually applies when the cooperating parties decide to share information between themselves to pursue common objectives.

[16] EUROCONTROL, *EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity*, 2.10.2019, EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity | EUROCONTROL, [accessed 15.04.2024].

[17] C. Goodwin, J.P. Nicholas, *A framework for cybersecurity information sharing and risk reduction*, Journal of Cybersecurity Research, 2020, 15(3), p. 13.

In the context of ISACs, the voluntary information exchange model is more commonly used.

The entities involved in an organisation, share knowledge related to cybersecurity, based on mutual trust. The data shared within ISACs relate in particular to issues such as:

- INCIDENTS – both successful and attempted attacks;
- THREATS – potentially dangerous activities that may pose a risk of an incident, e.g. distribution of malicious files or software, theft of email, or IP addresses;
- VULNERABILITIES – e.g. in software;
- REMEDIAL MEASURES – methods of repairing security vulnerabilities and protecting against threats, and actions after an incident has occurred;
- OPERATIONAL KNOWLEDGE – enabling appropriate responses to incidents;
- BEST PRACTICES – including security controls and the development of threat response processes;
- STRATEGIC ANALYSES – carried out on the basis of information gathered.[18]

It is important to note that members may decide in advance that certain types of information must be shared on a mandatory basis. However, implementing a fully mandatory information-sharing model have the unintended consequence of discouraging potential members from joining the organisation.

[18] Ibidem.

Challenges and constraints in the information sharing process

The exchange of information between members is a fundamental function of ISACs. It is worth emphasising that this process must be conducted in strict accordance with the applicable legal regulations. Among the pieces of legislation that have a real impact on the exchange of information within ISACs is the General Data Protection Regulation (GDPR).[19] It has been in force since 2018 and aims to protect the privacy and personal data of European Union citizens. The Regulation obliges members of ISACs to pay particular attention to the information exchange so it complies with the principles of lawfulness, fairness, transparency, data minimisation and security of processing, as set out in Article 5. Furthermore, restrictions on the exchange of information may also be included in internal rules and policies that impose obligations on entities to keep certain information confidential.

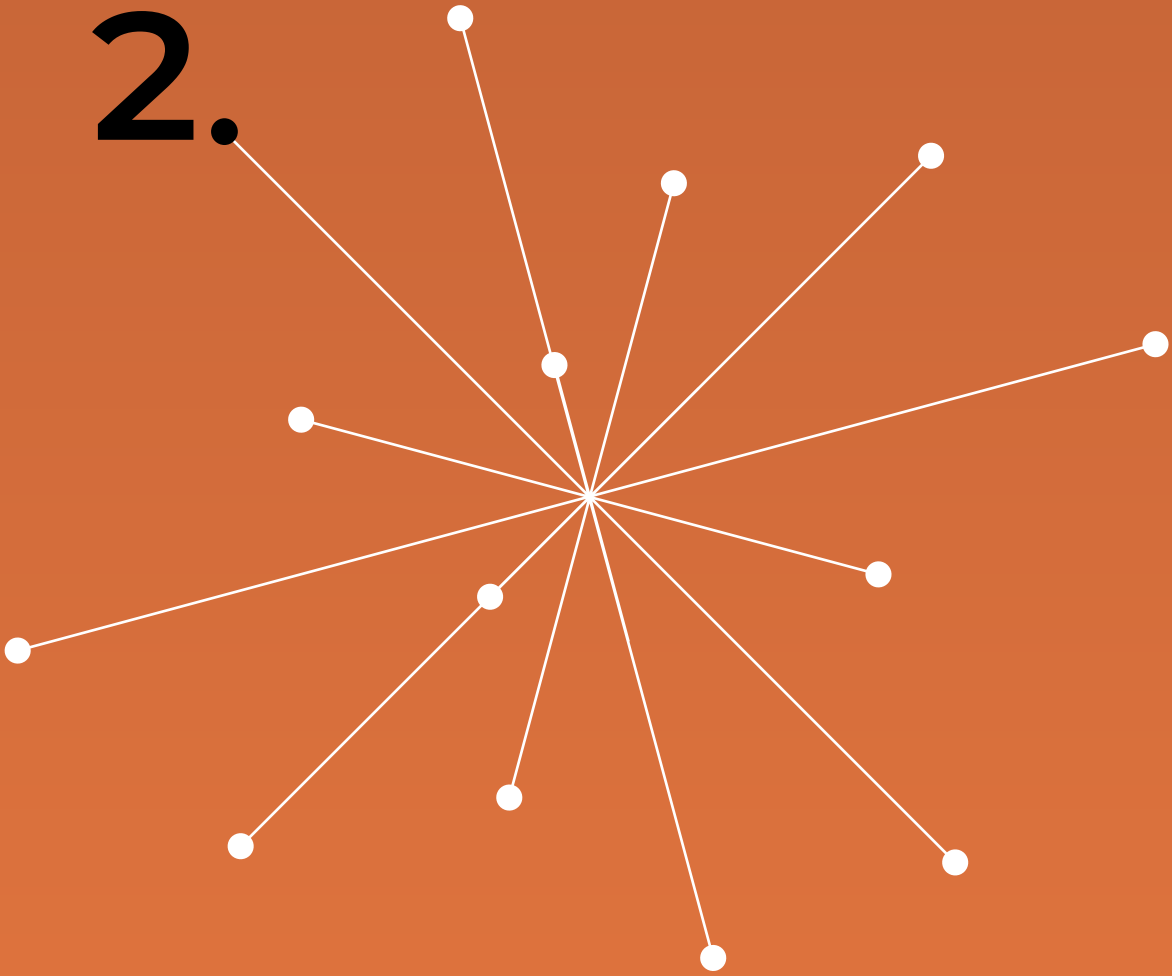
A further challenge is the disparity in the level of sophistication of the IT systems of the European ISAC members. This can make it difficult to tailor a method of information sharing that is adapted to the technical capabilities of each ISAC member. An additional issue is the need to ensure the security of the transmitted data, which in turn may entail considerable costs that not every entity is able to bear.

A key challenge for an ISAC is to foster a sense of security and trust among the members. Organisations are constituted by entities that are, in most cases, competitors in the market. Consequently, they may be reluctant to divulge information that could potentially be exploited by competitors for unscrupulous purposes.

The geographical origin of ISAC members can also be a challenge. This gives rise to variation in approaches to security management and in national legal systems. Moreover, communication between members can be hampered by differences in language and terminology. A considerable number of specialised cybersecurity terms are only used in English and have no equivalent in other languages. This can result in differences in the definition and comprehension of a word across different countries.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ EU.L.2016.119.1, 04.05.2016.

2.



Study on the landscape of European ISACs in 2023

2.1 Purpose of the study

In February 2018 ENISA has published a research report on “Information Sharing and Analysis Centres (ISACs) – Cooperative Models”. Its purpose was to analyse European ISACs, identify the challenges they face and highlight best practices.[20] Then, in August 2022, the European Commission, as part of its Empowering EU ISACs initiative, published “Overview and Report on EU ISAC Initiatives”, in which it presented selected information on European ISACs.[21]

The above-mentioned work of ENISA and the Commission was the starting point for this study aimed at examining how the landscape of European ISACs looked like in 2023. The intention was to collect detailed data that would enable the formulation of conclusions about these organisations, their structure, modus operandi, activities and the challenges they face. An important objective of this research project was also to gather information on best practices among ISACs and to develop a list of recommendations based on these findings. In addition, as part of the publication of the study’s result, it was intended to create a platform for interested participating organisations to present their individual profiles.

2.2 Methodology

The survey was conducted between June and September 2023. It comprised three phases.

Initially, in June, information on ISAC-type organisations operating in the European region was searched in publicly available sources. Furthermore, the authors contacted ENISA representatives to obtain more detailed information.

As a result of these activities, 15 organisations were identified that met the following criteria:

a. they self-identified as ISACs;

[20] European Union Agency for Cybersecurity (ENISA), op. cit.

[21] Empowering EU ISACs, *Empowering EU ISACs. Overview and Report on EU ISAC Initiatives*, 2022.

b. they were already fully established, i.e. they had members and were undertaking activities;

c. they were internationally active and had members from more than one country;

d. they met the conditions set out in ENISA's proposed definition of ISAC, namely that their activities were not for profit and focused on the collection, analysis and sharing of cyber threat information.

In the case of three organisations, no contact details could be found. An invitation to participate in the study was therefore sent to 12 ISACs. 10 agreed to participate.

In the second stage of the study, a research questionnaire was sent to these 10 organisations. It took the form of an online survey, was available in English, and consisted of 19 main questions and seven supplementary questions.

The questionnaire began with seven questions on basic information about the ISAC: full name, date of foundation, headquarters, number of members, sector of activity, website and function within the ISAC of the person completing the questionnaire. All these questions were open-ended.

The questionnaire then contained 12 more detailed questions. These were divided into two sections: "Organisation and membership of ISAC" and "Activities". The first one consisted of five questions on the organisational form of ISAC, the type of members, the elements of the structure, the sources of funding and the criteria for accepting new members. The second section contained seven main questions on the objectives of ISAC, activities undertaken, methods of communication and information sharing, means of promotion, challenges, ongoing initiatives and cooperation.

The questions on communication and promotion methods allowed participants to select any number of answers from the provided options. In the remaining cases, respondents were permitted to select a maximum of three options that were most relevant to their organisation. The aim of this limitation was to encourage participants to select only those answers that represented a truly relevant part of the ISAC's activities. Instructions on how to answer each question were provided within the question itself.

In addition, three questions – on the types of activities, methods of communication, and cooperation – required respondents to answer supplementary questions. In the case of the first two areas, these questions related to the frequency of activities or the use of communication methods. In the case of cooperation, a supplementary question sought to identify the specific organisations with which a given ISAC cooperated.

In the second part of the questionnaire, five main questions and all supplementary questions were closed. However, the main questions also included an “other” option, which allowed participants to type in their own answer. Two questions concerning the ISAC’s initiatives and the organisations it cooperates with were open-ended.

The full text of the survey in English is attached to this publication as Annex 1 and the Polish translation is attached as Annex 2.

The research questionnaire was completed by all 10 ISACs that received it. Subsequently, respondents were asked whether they would be interested in publishing detailed data about their organisation. Six organisations expressed interest and are presented in the section entitled “Characteristics of Selected European ISACs”.

2.3 Results

General characteristics of the ISACs surveyed

Seven ISACs that participated in the study operate exclusively within the European region. One ISAC has two distinct divisions, one European and one global. Two organisations are global ISACs that conduct part of their activities in Europe, but do not have a separate division for this area.

The oldest of the ISACs surveyed was established in 1991. The others were established in 2008 or later, two of them in 2021.

Sectors of activity

The ISACs surveyed indicated that they operate in nine sectors. These are: telecommunications, maritime, rail and air transport (including civil aviation), health, public administration at city and regional level, automotive (OEMs and suppliers), energy, and finance.

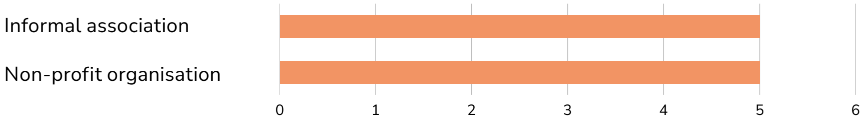
TABLE 1 Sectors of activity of ISACs surveyed

Sectors of activity of ISACs surveyed
1. Telecommunications
2. Maritime transport
3. Rail transport
4. Air transport (including civil aviation)
5. Health
6. Public administration at city and regional level
7. Automotive (OEMs and suppliers)
8. Energy
9. Finance

Organisational form

Five ISACs described themselves as non-profit organisations. The remaining five responded that they operate as informal associations.

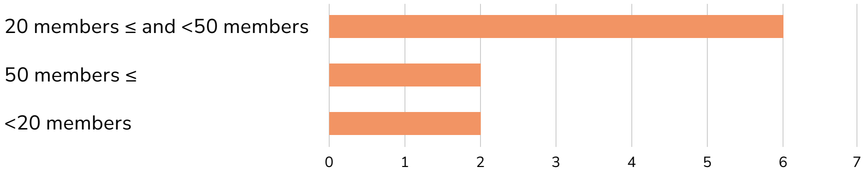
FIGURE 1. Organisational form of ISACs surveyed



Organisation members

The ISACs surveyed exhibited considerable variation in the number of members, with the smallest organisation comprising just nine members and the largest having 809 members. Two organisations have less than 20 members (9 and 15 respectively), six organisations have between 20 and 50 members (30, 35, 37, 42, 42 and 47 respectively), and two organisations have more than 50 members (116 and 809 respectively).

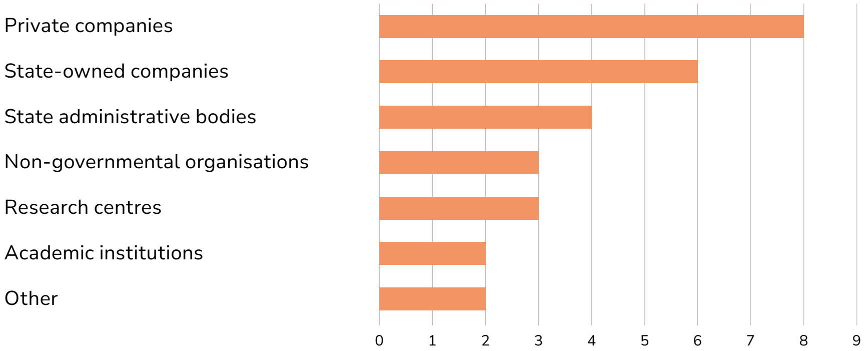
FIGURE 2. **Number of members of the ISACs surveyed**



In response to the question regarding the types of entities that comprise the membership of ISACs, respondents were permitted to select more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

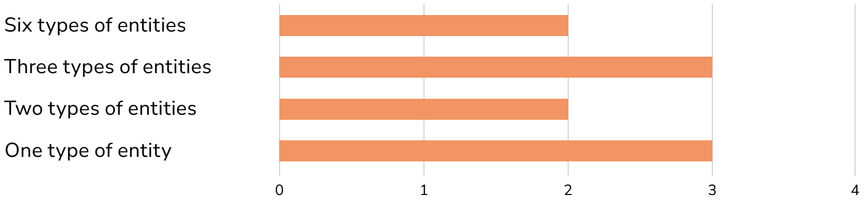
Eight ISACs indicated that their membership consisted of private companies, while six reported that their members were state-owned companies. Four organisations responded that their members were state administrative bodies. NGOs and research centres each received three indications in the survey and academic institutions received two indications. Two ISACs chose the "other" option and identified the CERT community with its representative bodies and law enforcement agencies as their members.

FIGURE 3. **Types of members of ISACs surveyed**



Three ISACs comprise a single entity type. Two ISACs have two types of entities in their membership, three ISACs have three types of entities and two ISACs have six types of entities.

FIGURE 4. **Number of types of entities in ISACs surveyed**

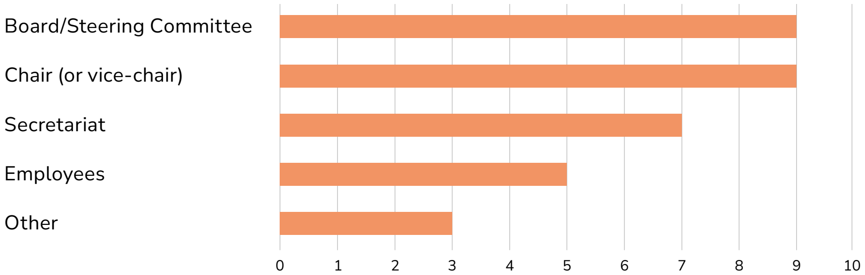


Organisational structure

Regarding the organisational structure of ISACs, respondents were permitted to select more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

Nine ISACs responded that they have a designated chair and, eventually, a vice-chair. Nine organisations indicated that they have a board/steering committee. Seven ISACs answered that they have a secretariat. Five organisations reported that they employ staff. Three ISACs also selected the answer "other", indicating that they have organisational structures such as a Core Team, Task Force, Council and working groups. There was also one response that ISAC has volunteers.

FIGURE 5. **Organisational structure of the ISACs surveyed**

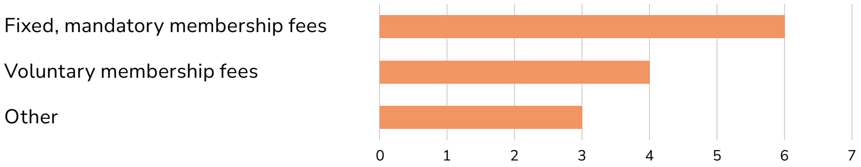


Sources of funding

When asked about sources of funding, ISACs could choose more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

Six ISACs indicated fixed, mandatory membership fees as their source of funding. Four organisations replied that their source of funding were voluntary membership fees. Three organisations selected the “other” option and reported sponsorship support and in-kind support, including volunteer work, as their sources of funding.

FIGURE 6. **Sources of funding of the ISACs surveyed**

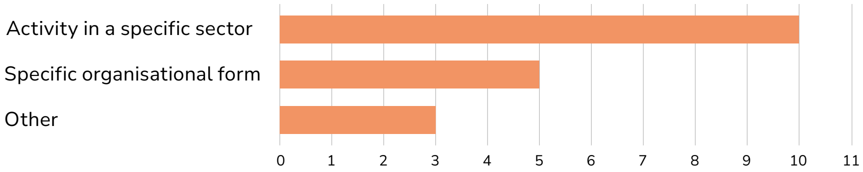


Acceptance criterion for new members

When asked about acceptance criterion for new members, ISACs could choose more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

All ten ISACs surveyed indicated that the criterion for admission to their organisation is that the interested entity is active in a particular sector. Five ISACs also replied that such a criterion is that the entity has a specific organisational form. In addition, three ISACs chose the answer “other” and indicated as criteria: having a registered office/activity in the EU, obtaining the support of at least one actual member, undertaking a certain type of activities and committing to a membership charter. Notably, none of the ISACs selected the answer proposed in the survey, which was that the criterion for admission is the size of the entity.

FIGURE 7. **Criteria for the admission of new members to the surveyed ISACs**

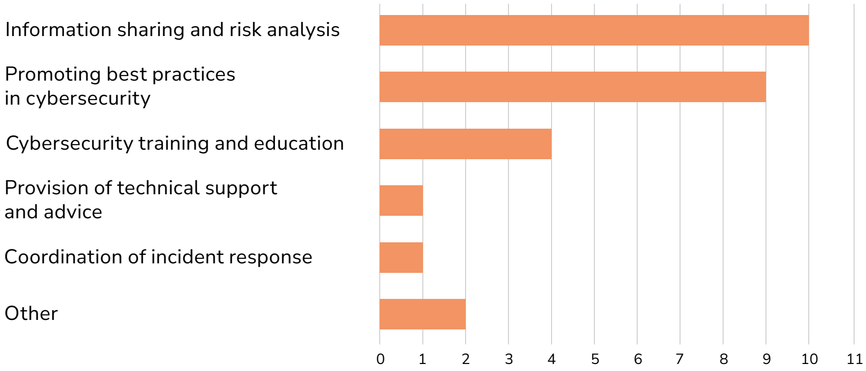


Main objectives and activities

Regarding the main objectives and activities of ISACs, respondents were permitted to select more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

All ten ISACs surveyed indicated that the dissemination of information and the analysis of risks represent a primary objective. In addition, nine organisations stated that one of their objectives was to promote cybersecurity best practices. Four organisations responded that one of their main objectives is to conduct cybersecurity training and education. There was one response each for objectives such as coordinating incident response and providing technical support and advice. Two ISACs selected the "other" option and indicated that they aim to build trusting relationships, provide a platform for discussion between members and organise events.

FIGURE 8. **Main objectives pursued by the ISACs surveyed**



A total of nine ISACs indicated that one of their primary activities was to engage in working group activities. Six organisations indicated that such work was conducted on a monthly basis or more frequently, three – on a quarterly basis and one – every six months.

Six ISACs stated that one of their main activities was the production of reports and analyses. Four of these reported doing this monthly or more often, one – quarterly and one – annually.

The survey yielded three responses each for four types of activities: organising conferences; conducting joint exercises and simulations; representing the sector's interests to public authorities; and organising integration meetings. All ISACs that selected the answer regarding organising conferences reported doing so on a quarterly basis. For the activity of conducting joint exercises and simulations, two organisations indicated that they undertook it every six months and one reported that they did so quarterly. Integration meetings were organised by two ISACs every six months and by one – once a month or more often. For the activity of representing the sector's interests before public authorities, the question of frequency was not asked because of the continuous nature of this type of activity.

One ISAC additionally, under the "other" option, indicated that one of its main activities was the review of legislation and standards.

FIGURE 9. **Main activities of the ISACs surveyed – by type**

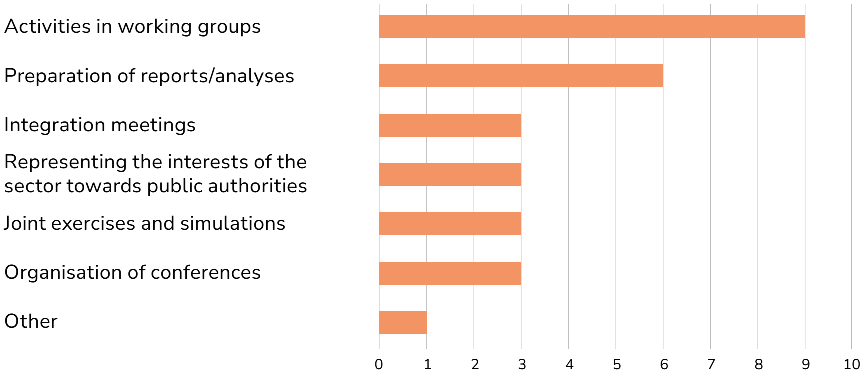
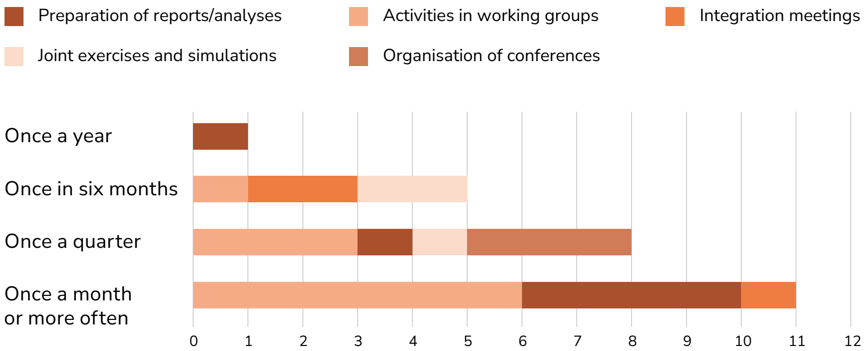


FIGURE 10. **Main activities of the ISACs surveyed – by frequency**



Methods of communication and information sharing

When asked about the methods of communication and information sharing, ISACs could choose more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

Nine ISACs responded that they utilise a mailing list for the purposes of communication and information sharing. Seven organisations indicated that they used an online platform or portal for members for this purpose. Furthermore, seven respondents reported that they communicated and exchanged information through regular meetings, with five stating that they met once a month or more often for this purpose and two indicating that they met once a quarter. Six ISACs responded that their form of communication and information sharing was ad-hoc meetings.

In addition, three responses were provided under the "other" option where organisations identified specific tools and channels they use to communicate and share information.

FIGURE 11. **Methods of communication and Information sharing of the ISACs surveyed**

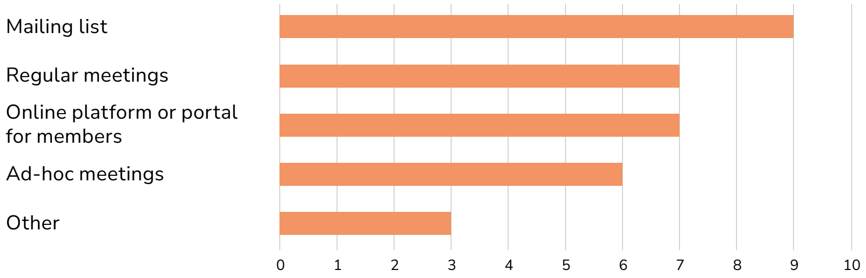
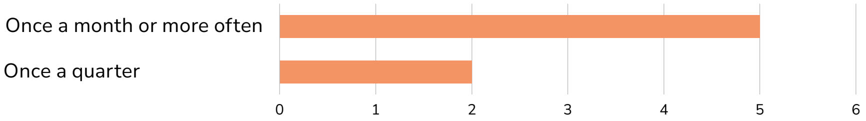
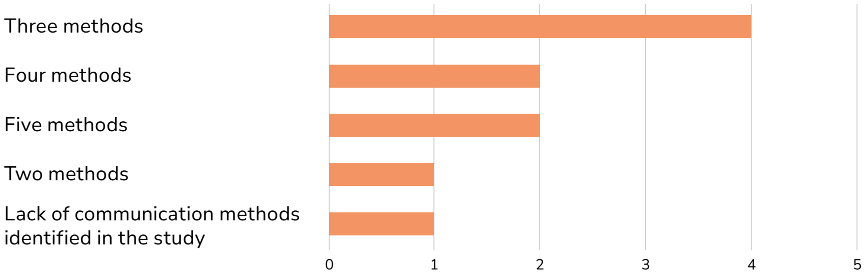


FIGURE 12. **Regular meetings – frequency**



Four ISACs reported that they used three methods of communication and information exchange. Two organisations surveyed responded that they use five and four such methods respectively. One ISAC declared utilising two methods and one stated it did not use any methods of communication and information exchange.

FIGURE 13. **Number of communication and information exchange methods used in the surveyed ISACs**



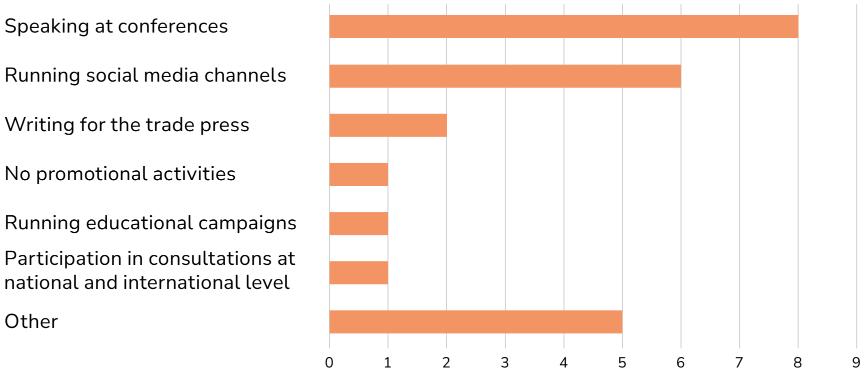
Methods of international promotion of the activities

Regarding the methods of international promotion of the activities, respondents were permitted to select more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

Eight ISACs indicated that they promoted their activities internationally by having their representatives speak at conferences. Six organisations indicated that they used social media channels for promotional purposes. Two ISACs responded that they promoted their activities internationally by writing to the trade press. One response each was given for participating in consultations at national and international level and conducting educational campaigns.

Five organisations also selected the answer “other”. They indicated that they used methods of international promotion such as sending e-mails to those who might be interested in membership, sending information by “word of mouth”, applying for EU-funded projects, being active in sectoral organisations/associations and posting information about the ISAC on members websites. One ISAC stated that it did not carry out any promotional activities.

FIGURE 14. **Methods of international promotion of the activities of the ISACs surveyed**

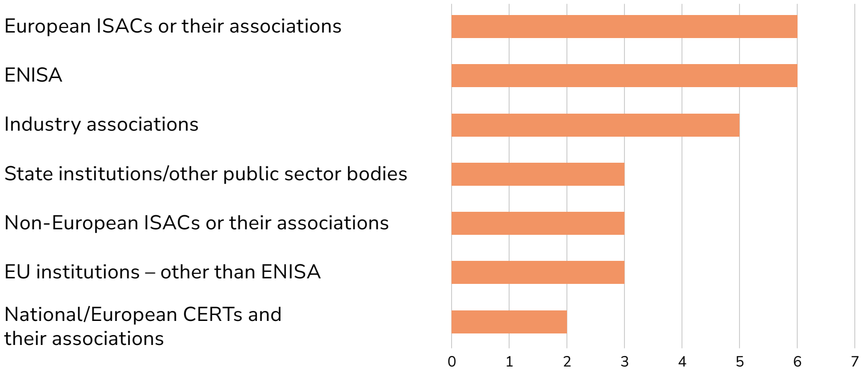


Cooperation with other entities

Regarding the cooperation with other entities, respondents were permitted to select more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

All ten ISACs surveyed responded that they cooperated with other entities. Six of them stated that they cooperated with ENISA and three that they cooperated with another European institution. Six ISACs replied that they cooperated with European ISACs or their associations, and three that they cooperated with non-European ISACs or their associations. Five organisations reported that they cooperated with industry associations. Three ISACs stated that they worked with state institutions or other public sector bodies. Two organisations indicated that they cooperated with national or European CERTs and their associations.

FIGURE 15. **Cooperation of the ISACs surveyed with other entities**



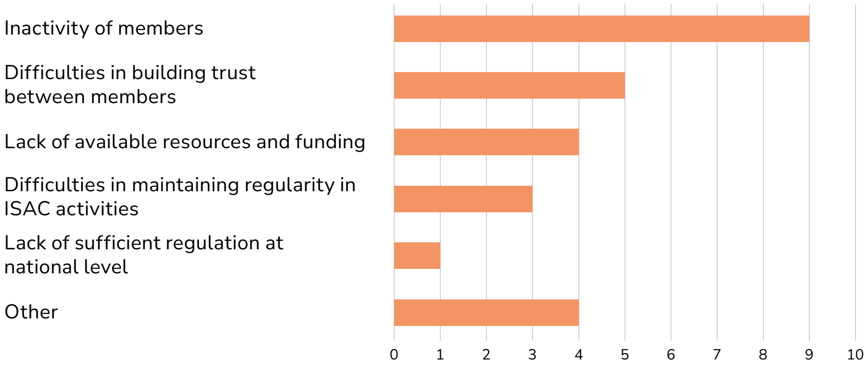
Challenges to ISACs' operations

When asked about the challenges, ISACs could choose more than one answer. Therefore, the total number of responses obtained exceeds the number of ISACs that participated in the study.

Nine ISACs indicated that one of the main challenges they faced was a lack of activity among their members. Five organisations stated that they faced difficulties in building trust between members. Four ISACs mentioned a lack of available resources and funding as a challenge. Three reported difficulties in keeping the organisation active on a regular basis. One also indicated that a lack of sufficient regulation at national level was a problem. None of the organisations surveyed chose the answer proposed in the survey that the existence of competition between members was a challenge.

In addition, four ISACs chose the "other" option. They cited the lack of widespread awareness of the role of ISACs, their lack of recognition in the EU and the lack of sufficient regulation at European level as difficulties in carrying out their activities.

FIGURE 16. **Challenges to the activities of the surveyed ISACs**



2.4 Conclusions

Due to the particular characteristics of the subject matter under investigation, the respondents were selected on the basis of specific criteria. As a result, the study encompasses a limited number of organisations. Nevertheless, the data collected permits the formulation of preliminary conclusions regarding the characteristics and activities of the ISACs surveyed.

The majority of the 10 organisations that took part in the survey were established in the last 10 years, with four having been established in 2019 or later. These figures indicate that the development of ISACs in Europe is relatively recent particularly in comparison to the United States. At the same time, those organisations that reported a higher number of members in the survey are predominantly active in both Europe and the United States.

Sectors of activity

When asked about their areas of activity, all ISACs surveyed indicated that they were active in only one sector. This means that that none of the respondents perceived their activities to be cross-sectoral in nature. Furthermore, for all ISACs, working in a specific sector was a criterion for admission to their organisation. It can thus be concluded that affiliation with a particular sector constitutes a pivotal aspect of the surveyed organisations' characteristics.

The below table compares the areas in which the surveyed ISACs declared to belong to the sectors regulated by the NIS and NIS2 Directives[22]. It should be emphasised that this is a simplistic exercise, as it is based on the self-identification of ISACs as belonging to a particular sector or sub-sector. A more precise identification of their sectoral affiliation would require a more comprehensive analysis of the composition of the organisations' membership, which is well beyond the scope of this study. Accordingly, the following summary is only indicative and intended to provide an overview of the commonalities between the stated areas of activity of the ISACs surveyed and the sectors falling within the scope of the NIS and NIS 2 regulations.

[22] Annex I of the NIS Directive and Annex I and Annex II of the NIS Directive 2, respectively.

TABLE 2. **Overview of sectors covered by the NIS and NIS 2 Directives and areas of activity indicated by ISACs**

NIS – sectors and subsectors	**NIS 2 – sectors and subsectors**	**Areas of ISACs' activity – by responses**
Energy: • electricity • oil • gas	Energy: • electricity • district heating and cooling • oil • gas • hydrogen	Energy
Transport: • air transport • rail transport • water transport • road transport	Transport: • air transport • rail transport • water transport • road transport	Transport: • air transport • rail transport • maritime transport
Banking	Banking	Finance
Financial market infrastructures	Financial market infrastructures	Finance
Health sector	Health	Health
Drinking water supply and distribution	Drinking water	
Digital infrastructure	Digital infrastructure	
	Waste water	
	ICT service management (business-to-business)	
	Public administration entities – central governments and regional level	Public administration – cities and regions
	Space	
	Postal and courier services	
	Waste management	
	Manufacture, production and distribution of chemicals	
	Production, processing and distribution of food	

	Manufacturing: • of medical devices and in vitro diagnostic medical devices • of computer, electronic and optical products • of electrical equipment • of machinery and equipment n.e.c. • of motor vehicles, trailers and semi-trailers • of other transport equipment	Automotive sector (original equipment manufacturers (OEMs) and suppliers)
Digital service providers	Digital service providers	
	Research	
		Telecommunications

A correlation between the areas of activity of the surveyed ISACs and the sectors and sub-sectors defined in the NIS and NIS 2 Directives reveals that some ISACs are active in the entirety of the sectors delineated in the Directives, while others are active in specific sub-sectors or parts of sectors or sub-sectors.

The sectors reported by ISACs as their areas of activity overlap, at least in part, with the five sectors covered by the NIS Directive and the seven sectors covered by NIS 2. In the case of two sectors – transport and manufacturing – the scope of activity of the ISACs surveyed does not overlap with the sector as a whole, but with particular sub-sectors. One ISAC reported activity in the telecommunications sector, which is not distinguished as a separate sector in either the NIS or NIS 2 Directives. However, some of the organisations operating in this sector may fall within the scope of other sectors covered by the Directives.

Given that the above summary is based on general information provided by the respondents themselves, it cannot be excluded that in reality these organisations and their members do not fit exclusively into the sectors and sub-sectors to which they have been assigned in the Table 2. Nevertheless, an analysis of this overview demonstrates that while European ISACs are active, at least partially, in most of the sectors and sub-sectors listed in the NIS Directive, this is not the case in its amended version. Indeed, NIS 2 encompasses numerous new areas where, according to the research findings, such organisations have yet to emerge.

It should be noted that the two new sectors introduced by the NIS 2 Directive, namely public administrations (at the central and regional levels) and manufacturing, are exceptions to the aforementioned rules. Two ISACs have a partial overlap in their respective scopes, encompassing both of those sectors. In the case of one of the organisations, the subscope is even wider than that specified in the Directive. Indeed, it also covers public administration at the city level, i.e. the local level, which, according to NIS 2, is only regulated on an optional basis if a Member State decides to do so.

In 2023, the creation of a European ISAC has been announced, which will operate in a sector added by the NIS 2 Directive – space[23]. It seems plausible to suggest that the expanded sectoral scope of NIS 2 when compared to the previous version of the Directive will encourage entities from the newly regulated sectors to establish more ISACs. The functioning of communities such as ISACs to share best practices and strengthen overall sectoral resilience may in fact make it easier for these entities to comply with the obligations imposed by the extended legislation.

Structure of ISACs

The structure of ISACs surveyed is predominantly comprised of private companies, with academic institutions representing the least common constituent. An analysis of the number of types of entities belonging to the organisations shows that they are characterised by a diverse membership structure. Half of the respondents consist of two or three types of entities. The other half chose two extreme answers – three ISACs indicated that they had only one category of organisation in their membership and two indicated that they had six different categories of organisation in their membership. The variation in the number of member types may be explained by the specifics of the sectors or subsectors in which the organisations operate – some may be dominated by a particular type of entity, such as state-owned enterprises.

With regard to the internal structure of the ISACs surveyed, the responses indicate that each ISAC has at least one individual or group of individuals designated to assume a leadership role – be it a Chair and possibly a Vice-Chair or a Management Board. The vast majority of organisations have both functions. Most ISACs also have a secretariat, and half of them

[23] More details: https://www.euspa.europa.eu/opportunities/isac, [accessed 13.05.2024].

reported that they employed staff. Only one organisation indicated that it had just one position in its structure – the Chair/Vice Chair.

From the above information it can be concluded that all the ISACs surveyed have an established internal structure, and for most of them it is extensive.

Financing of ISACs

An analysis of the responses from ISACs regarding sources of funding yields intriguing insights. Almost all organisations indicated that these sources were membership fees – either mandatory, voluntary or both. Only one organisation stated that it had no financial resources and relied solely on voluntary contributions in kind from its members.

This means that all organisations surveyed rely primarily on the financial and non-financial support they receive from their members to operate. Acquiring additional external financial support was only mentioned by one ISAC, which indicated that its activities were supported by sponsors. None of the organisations chose the response proposed in the survey that they receive state funding.

It is noteworthy that when queried about the obstacles encountered by ISACs in the execution of their duties, a significant proportion of respondents identified the lack of accessible resources and funding as a primary challenge. This may indicate that in some cases support from members alone is proving insufficient. The lack of sufficient opportunities to obtain external funding or other forms of support may be a factor inhibiting the development of ISACs. Inadequate resources may prevent organisations from undertaking certain types of activities (e.g., conducting realistic simulations) or building a structure (e.g., hiring staff).

Objectives and activities of ISACs

The activity objective common to all ISACs surveyed is information sharing and risk analysis. This is not a surprising result, given that this type of activity is implied by the very name of these organisations. Nine ISACs also stated that one of their main objectives was to promote cybersecurity best practices. It can be assumed that these activities are interrelated, as the development and promotion of best practices in a given area is made possible by lessons learned from risk and information analysis. This is also consistent with the next most commonly reported objective of ISACs, which is cybersecurity education and training.

On the other hand, coordinating incident response and providing technical support and advice were the least frequently selected answers by the organisations surveyed, with only one indication each. This may mean that members are largely pursuing these objectives outside ISACs, for example, through Computer Security Incident Response Teams (CSIRTs).

In terms of activities undertaken, almost all ISACs stated that they operated within the framework of working groups. According to the survey results, this activity is most often carried out at least once a month, while no organisation reported doing this less frequently than once every six months. In addition, those ISACs that declared that they carried out working group activities less frequently than once a month – i.e. at least once a quarter or once every six months – indicated that they performed other activities even less frequently. This suggests that working in groups is the most basic and regular form of activity for the ISACs surveyed.

Among the other answers proposed for the question on activity, “Preparation of reports and analyses” was the second most frequently selected. All other responses received the same, smaller number of indications. This leads to the conclusion that the activities carried out by ISACs are quite diverse, with a predominance of participation in working groups and production of reports and analyses.

The responses of the ISACs surveyed regarding the frequency of their activities indicate that they carry out their activities on a fairly regular basis. The most frequently selected option was “once a month”, followed by “once a quarter”. The answer “once a year” was chosen by only one organisation for one activity, and the answer “less than once a year” was not selected.

Methods of communication and information sharing in ISACs

The results of the survey indicate that the overwhelming majority of ISACs employ a minimum of three or more methods for the dissemination of information and the facilitation of communication among members. The most prevalent method is the mailing list, which was used by almost all organisations surveyed. The second most frequently indicated communication channel is the online platform or portal for members.

In addition, almost all ISACs reported that they communicated and shared information through meetings – either regular or ad hoc. This means that nine out of ten ISACs surveyed share information both through communication tools (mailing lists and potentially a platform/portal for members) and in real-time meetings.

Furthermore, of those ISACs that reported regular meetings, the majority stated that they met at least once a month. The others indicated that they met at least quarterly. This shows that this form of communication and information exchange is used by ISACs on a regular basis.

Promotion of ISACs' activity

Almost all the ISACs surveyed utilise a combination of methods and channels to disseminate information about their activities on an international scale. These methods are twofold. On the one hand, organisations promote themselves through publicly available channels – through appearances by representatives of the organisation at conferences and through social media profiles. On the other hand, some choose to promote their activities by contacting potential interested parties on an individual basis or through "word of mouth". In the case of one ISAC, this is the only form of promotion used.

In addition, some ISACs indicated that they also raised their visibility by actively participating in EU projects and activities within their respective sectors. When juxtaposed with the other findings, a further distinction can be made between the two types of promotion employed by ISACs – promotion through individual activities (e.g. social media profiles, contacting potential members) and promotion through involvement and cooperation with other actors (e.g. speaking at conferences, participating in EU projects).

Cooperation of ISACs' with other entities

All ISACs indicated that they cooperated with other entities – most often with more than one. This suggests that co-operation, not only internally but also externally, is an important part of the functioning of this type of organisation.

The results demonstrate a strikingly diverse range of such collaborative endeavours. The entities involved range from industry associations to governmental institutions or other government-related entities, and national CERTs. The largest proportion of ISACs' responses referred to cooperation at European Union level, in particular to ENISA, which was mentioned by more than half of the respondents. Other EU institutions, and European CERTs and their associations were also mentioned by some ISACs.

Furthermore, the survey results suggest that the ISACs surveyed engage in cooperative activities with other organisations, both within Europe and from other regions, including the United States and Japan. Within the European continent, the European Council of ISACs was the most frequently cited cooperation platform by respondents.

Challenges to ISACs' operations

Among the operational challenges identified by ISACs in the survey, those related to their members clearly come to the fore. Almost all organisations reported a lack of member engagement and half reported difficulties in building trust between members. Both issues have the potential to impede the effective functioning of an organisation, which is fundamentally based on these two pillars – an active community and a sense of mutual trust. The lack of member involvement may also be linked to another challenge identified by some respondents, the difficulty of maintaining regularity in the organisation's activities.

At the same time, however, none of the respondents chose the answer proposed in the survey, namely that competition between their members was a challenge. This is an intriguing observation, given that the responses to other questions suggest that the ISACs surveyed include organisations operating in the same sector, often including private companies, which are likely to compete on a daily basis. This suggests that the collective objectives pursued within ISACs may supersede the individual interests of members in relation to activities outside these organisations.

As previously stated, numerous actors indicated that a lack of financial resources constituted a significant obstacle. This problem may be one of the reasons for other difficulties identified in the responses to this question, such as a lack of member engagement. Indeed, if they perform tasks for the organisation free of charge, this may discourage them from investing more time or effort. In addition, a lack of funding can also have a negative impact on the scope of ISACs' operations, as without sufficient resources they are unable to carry out more complex activities that require the purchase of equipment or the hiring of staff.

Another challenge pertains to the lack of awareness about ISACs and their role. As one respondent observed, this hinders the ability of such organisations to attract new members and funding.

The lack of visibility of ISACs may also be related to another issue raised by the organisations surveyed, which is the absence of sufficient regulation of the activities of ISACs at the EU level. At present, no EU legislation explicitly addresses the activities of such organisations (NIS 2 Directive only indirectly covers this issue through provisions on voluntary information exchange). The lack of EU regulations of the activities of ISACs may contribute to the fact that governments and other types of actors overlook their role in building cyber resilience and focus on the strengthening of other types of organisations identified in cybersecurity legislation.

In addition, as one respondent observed, the absence of legal framework for information sharing within ISACs presents a significant challenge for their members, who may be reluctant to engage in such activities without the assurance of immunity from liability. This suggests that those participating in such an ISAC may perceive a prevailing state of legal uncertainty, which may ultimately dissuade them from fully engaging in information sharing.

2.5 Recommendations

1. Establishment of European ISACs in new sectors and sub-sectors

The creation of new European ISACs can be an essential element in strengthening cybersecurity in specific sectors of the economy. Particular attention should be paid to the sectors and sub-sectors covered by the NIS 2 Directive. The revised regulations now encompass a considerably broader scope of entities than was the case with the previous iteration of the Directive, and some of them will have to comply with EU cybersecurity requirements for the first time. Therefore, this can be a major challenge for them, and they will need the support that participation in ISACs can provide. ISACs allow member organisations not only to strengthen their resilience by sharing threat information, but also to exchange experiences and best practices, and learn from each other.

2. Building platforms for cooperation between ISACs from different sectors

Many incidents affect multiple sectors simultaneously. Developing platforms for collaboration between ISACs can enable faster identification and appropriate response to cyber threats that occur in more than one sector of the economy. In addition, representatives from different sectors have varying experiences and knowledge that can be shared between ISACs to help develop the most effective ways of dealing with incidents of diverse nature.

3. Development of tools for information exchange between ISACs

The establishment of appropriate communication and knowledge flow tools could facilitate cooperation between ISACs. These would allow organisations to share and update information on incidents and to create a common database of incidents and threats accessible to all ISACs involved. Such communication tools could also be used to organise various types of meetings between ISACs, including those to share knowledge and best practices on various aspects of ISAC operations.

4. Strengthening cooperation between ISACs of different levels of maturity

In order to establish new ISACs in sectors where such organisations have not yet been developed, it is important to provide them with support from already developed ISACs. These organisations can share their experiences and practices from the process of their own formation and improvement, so that new ISACs can, for example, avoid making certain mistakes. Such cooperation could also benefit mature ISACs, which would have the opportunity to gain a fresh perspective from newly established organisations.

5. Strengthening cooperation between European and national ISACs

Developing channels for regular communication between national and European ISACs could prove mutually beneficial. By cooperating with European organisations, national ISACs could access information from their members in other countries. European ISACs, on the other hand, would be able to increase their knowledge of the specificities of different aspects of cybersecurity on a country-by-country basis. In this way, both types of ISACs would be able to expand their pool of information, which could have a positive impact on their practices in building resilience to different types of threats.

6. Inviting diverse entities to become ISAC members

Greater diversity in the membership of an ISAC can have a beneficial impact on developing the knowledge base and broadening the range of activities that can be undertaken. For example, it is worth considering bringing academic institutions and research centres into the organisation, which can assist in many ways, such as:

- conducting advanced cybersecurity research, including threat analysis and development of protection methods;
- conducting cybersecurity courses and training for other ISAC members;
- involving experts and researchers from various fields;
- informing the public about the ISAC’s activities.

Each new type of entity in an ISAC brings a different type of knowledge, experience and resources. For example, it may provide the organisation with infrastructure and tools that it would not have access to without such a member. In addition, the involvement of representatives from a variety of actors within a particular sector can have a positive impact on the wider dissemination of awareness about the functioning and role of the ISAC.

7. Building financial support systems for ISACs

Funding is one of the most essential aspects for the smooth operation of ISACs. It enables organisations to acquire and maintain adequate resources, such as tools and infrastructure, and to provide training and workshops to their members. A lack of sufficient funding limits the ability of ISACs to expand. It is therefore recommended that financial support programmes be developed from which such organisations could benefit. ISACs themselves can also increase the promotion of their activities and share their outcomes and achievements in order to reach the widest possible range of potential actors who can support them financially.

8. Establishment of a publicly accessible register of ISACs

At present, information pertaining to each European ISAC can be located in disparate locations and frequently necessitates an exhaustive search. For this reason, it is worth considering the creation of a publicly accessible register of European ISACs that would collate fundamental data about them, including the sectors they represent, a concise description of their activities, contact details, and website addresses. Such a register would make it easier to find information about or contact individual ISACs. It would also be helpful to organisations considering membership of such organisations. A register would also provide greater visibility for ISACs.

9. Promoting the activities of ISACs within sectors and subsectors

ISACs may undertake dedicated activities to promote their work within the sector or sub-sector in which they operate. Examples include the organisation of training courses, workshops and webinars. This would help to raise the ISACs' visibility within the sector or sub-sector and attract new potential members. Regular publication of the results of the ISACs' work in the form of reports, analyses or recommendations could also be an effective means of reaching a wider range of stakeholders in a given sector. They could also be presented at conferences and other sectoral events.

10. Raising public awareness of ISACs

Raising public awareness of ISACs requires action in several areas simultaneously. It is crucial for ISACs to possess a well-designed website that provides essential information about the organisation, including a detailed description of its activities, the criteria for membership, and contact details. Another important aspect of raising awareness of ISACs is the utilisation of social media platforms, where these entities can disseminate updates about their activities, events, and publications on an ongoing basis. These channels also may serve to build a community around ISACs, thereby encouraging active participation in the organisations.

3.

Characteristics of selected European ISACs

The graphics below present data on six European ISACs. These are entities that, after participating in the study, gave additional consent for their detailed characteristics to be published in this report.

Auto-ISAC Europe*

Full name

Auto Information Sharing and Analysis Centre Europe

Founding date

2021

Headquarters

Stuttgart, Germany

Members

42

Sector of activity

automotive sector (OEMs and suppliers)

Organisational form

non-profit organisation

Types of member entities

private companies

Membership criteria

- activity in a specific sector
- a specific form of organisation

Main activities

- joint exercises and simulations – once a quarter
- preparation of reports/analyses – once a month or more often
- working group activities – once a month or more often

Communication methods

- regular meetings – once a month or more often
- ad hoc meetings
- an online platform/portal for members
- a mailing list
- workshops
- annual summit

Other activities

- establishment of an automotive cybersecurity education programme – the Automotive Cybersecurity Training (ACT)
- participation in the development of best practices, described in the National Highway Traffic Safety Administration (NHTSA) report "Cybersecurity Best Practices for the Safety of Modern Vehicles, September 2022"

Website

https://automotiveisac.com/europe

https://www.linkedin.com/company/auto-isac/

@AutoISAC

* Part of the global Auto-ISAC, founded in 2015 and headquartered in Washington, USA.

Aviation ISAC

Full name

Auto Information Sharing and Analysis Centre Europe

Founding date

2014

Headquarters

Annapolis, USA*

Members

122**

Sector of activity

aviation

Organisational form

non-profit organisation

Types of member entities

- private companies
- state-owned companies

Membership criteria

- activity in a specific sector

Main activities

- preparation of reports/analyses – once a month or more often
- working group activities – once a month or more often
- organising conferences – once a quarter

Communication methods

- regular meetings – once a month or more often
- an online platform/portal for members
- a mailing list

Other activities

- organisation of meetings at the regional and global level
- organisation of Tabletop Exercises (TTX)
- organisation of Capture the Flag (CTF) competitions
- preparation of reports and analyses on a daily, weekly and monthly basis

Website

https://www.a-isac.com/

* Headquarters of global ISAC.

** The number of global ISAC members.

ECCSA

Full name

European Centre for Cybersecurity in Aviation

Founding date

2017

Headquarters

–

Members

42

Sector of activity

civil aviation

Organisational form

informal gathering

Types of member entities

- private companies
- state administrative bodies
- non-governmental organisations

Membership criteria

- activity in a specific sector
- a specific form of organisation
- adherence to the ECCSA Membership Charter

Main activities

- preparation of reports/analyses – once a month or more often
- working group activities – once in six months
- integration meetings – once in six months

Communication methods

ad hoc meetings

an online platform/portal for members

Other activities

- support to vulnerability disclosure
- issuing of ECCSA alerts
- issuing of ECSSA monthly threat report
- issuing of ECCSA technical threat notes

Website

https://www.easa.europa.eu/en/eccsa

EE-ISAC

Full name

European Energy Information Sharing and Analysis Cente

Founding date

2015

Headquarters

Brussels, Belgium

Members

35

Sector of activity

energy

Organisational form

non-profit organisation

Types of member entities

- private companies
- state-owned companies
- non-governmental organisations
- academic institutions
- research centres

Membership criteria

- activity in a specific sector
- a specific form of organisation

Main activities

- preparation of reports/analyses – once a quarter
- working group activities – once a month or more often
- representing the interests of the sector towards public authorities

Communication methods

- an online platform/portal for members
- a mailing list

Other activities

- development of EE-ISAC MISP, a version of the platform dedicated to EE-ISAC members
- organisation of an annual Conference on Power Grids Cybersecurity for the energy sector in cooperation with ENISA, EU DSO, E.DSO and ENCS
- conclusion of the Trilateral Memorandum of Understanding with the US E-ISAC and JE-ISAC to promote international cooperation and information sharing through public-private partnerships

Website

https://www.ee-isac.eu/

FI-ISAC

Full name

European Financial Institutes – Information Sharing and Analysis Center

Founding date

2008

Headquarters

–

Members

30

Sector of activity

financial sector

Organisational form

informal gathering

Types of member entities

- private companies
- CERT Community and representative bodies
- law enforcement

Membership criteria

- activity in a specific sector

Main activities

- integration meetings – once in six months
- representing the interests of the sector towards public authorities

Metody komunikacji

–

Other activities

–

Website

https://fi-isac.eu

ETIS

Full name

ETIS – European Telco Information Sharing and Analysis Center

Founding date

1991

Headquarters

Brussels, Belgium

Members

47

Sector of activity

telecom industry

Organisational form

non-profit organisation

Types of member entities

- private companies
- state-owned companies
- research centres

Membership criteria

- activity in a specific sector
- a specific form of organisation

Main activities

- joint exercises and simulations – once in six months
- working group activities – once a month or more often
- organising conferences – once a quarter

Communication methods

- regular meetings – once a month or more often
- ad hoc meetings
- an online platform/portal for members
- a mailing list

Other activities

- participation in the development of the "Telco IT Benchmarking (TeBIT)" report and the telecom security landscape
- connecting telecom operators' security experts with organisations that develop annual benchmarks for telecom security
- organisation of the annual Telco Security Landscape in cooperation with TNO

Website

www.etis.org

kalendarz wydarzeń ETIS: https://www.etis.org/events

EU City ISAC

Full name

EU City Information Sharing and Analysis Center

Founding date

2021

Headquarters

Bremen, Germany

Members

37

Sector of activity

public administrations of cities and regions

Organisational form

informal gathering

Types of member entities

state administrative bodies

Membership criteria

- activity in a specific sector
- a specific form of organisation

Main activities

- joint exercises and simulations – once in six months
- working group activities – once a month or more often
- integration meetings – once a month or more often

Communication methods

- regular meetings – once a month or more often
- ad hoc meetings
- a mailing list

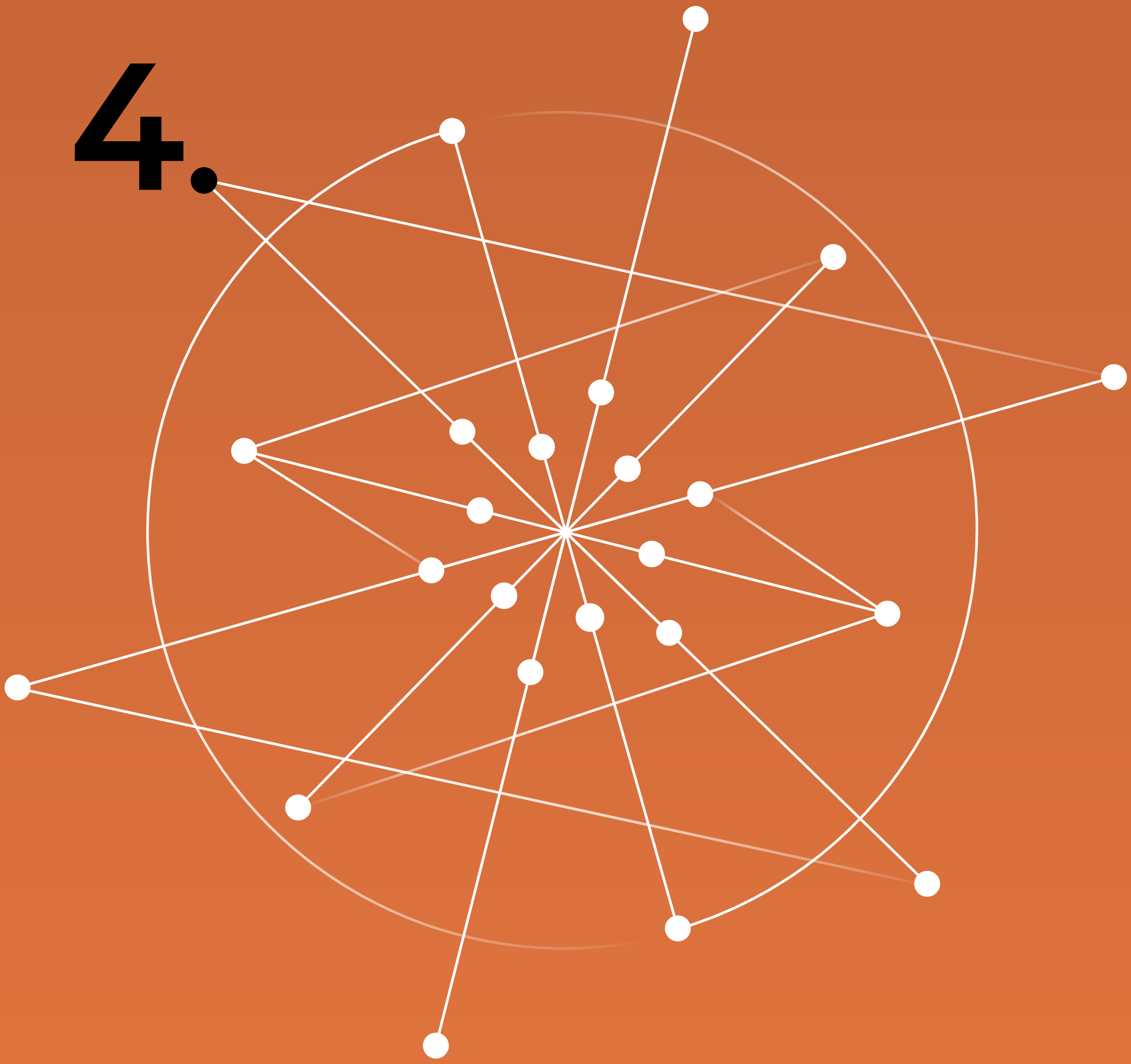
Other activities

- conducting exercises in the form of joint-defence simulations, similar to the ”Locked Shields”, organised by NATO

Website

https://isac4cities.eu/

4.



Summary

This report attempts to provide “a bird’s eye view” of European ISACs. This perspective has made it possible to outline the landscape of these organisations and collect basic data on their characteristics. What emerged was a picture of diverse actors, each with their own unique characteristics, but also with some commonalities.

The chosen research method obviously has some limitations. The collection of information through the questionnaire did not allow for additional questioning of respondents about interesting issues raised in their answers. The predominant type of closed questions in the survey may also have limited the amount of information provided by organisations. However, the authors were primarily interested in collecting structured data on the organisations surveyed, which would allow them to be analysed quantitatively. Therefore, the questionnaire method was chosen as best meeting this objective.

The picture of European ISACs presented in the report therefore does not provide a detailed insight into their structure and internal functioning but rather maps certain areas. The authors hope that this study will serve as a good starting point for further in-depth analyses of selected aspects of the operation of organisations of this type. Undoubtedly, further research efforts could yield many interesting findings, potentially valuable for both the ISACs themselves and entities interested in supporting them.

The topic of opportunities and risks for the development of ISACs will certainly not lose its relevance in the nearest future. Indeed, the landscape of challenges in cybersecurity is constantly changing. On the one hand, new types of cyber threats are emerging as a result of factors such as technological developments or changes in the geopolitical situation. On the other hand, legal changes that impose new obligations on further groups of actors are also a challenge. These developments are also accompanied by new societal expectations in terms of safety, which organisations must take into account. As a result, platforms such as ISACs are becoming increasingly important as a means of providing mutual support in the face of these challenges.

Providing such initiatives with the right conditions for development should be considered as a crucial element of a strategy for cybersecurity at national and EU level. To achieve this, it is essential to build awareness of the importance of ISACs in strengthening the overall resilience to threats.

Bibliography

1. *Presidential Decision Directive/NSC-63 – Critical Infrastructure Protection of 22 May 1998*, Critical Infrastructure Protection (PDD 63) (fas.org), [accessed 15.04.2024].

2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 measures for a high common level of security of network and information systems across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148.

4. EE-ISAC, *Japanese & European energy communities sign partnership agreement on cyber security*, 17.05.2017, Japanese & European energy communities sign partnership agreement on cyber security – EE-ISAC – European Energy – Information Sharing & Analysis Centre, [accessed 15.04.2024].

5. *Empowering EU-ISACs*, Home | Empowering EU-ISACs [acessed: 15.04.2024].

6. European Union Agency for Cybersecurity (ENISA), „ISAC in a Box”, ISAC in a Box – ENISA (europa.eu), [accessed: 15.04.2024].

7. European Union Agency for Cybersecurity (ENISA), Cross-Sectors Exercise Requirements, 2018, Cross-Sector Exercise Requirements – ENISA (europa.eu), [accessed: 15.04.2024].

8. European Cyber Crime Centre, European Cybercrime Centre – EC3 | Europol (europa.eu), [accessed: 15.04.2024].

9. EUROPOL, FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime, 19.09.2019 r FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime | Europol (europa.eu), [accessed: 15.04.2024].

10. European Automobile Manufacturers' Association (ACEA), European manufacturers and suppliers join with Auto-ISAC, 12.10.2022 r., European manufacturers and suppliers join with Auto-ISAC – ACEA – European Automobile Manufacturers' Association, [accessed: 15.04.2024].

11. EUROCONTROL, *EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity*, 2.10.2019 r., EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity | EUROCONTROL, [accessed: 15.04.2024].

12. European Union Agency for Cybersecurity (ENISA), *Information Sharing and Analysis Center, Cooperative models*, 2018, Information Sharing and Analysis Center (ISACs) – Cooperative models – ENISA (europa.eu) [accessed: 15.04.2024].

13. National Council of ISACs (NCI), National Council of ISACs | About NCI (nationalisacs.org) [accessed: 15.04.2024].

14. Goodwin, C., Nicholas, J. P., A *framework for cybersecurity information sharing and risk reduction*, Journal of Cybersecurity Research, 2020, 15(3), s.13.

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ EU.L.2016.119.1, 04.05.2016.

16. Sadowski J., Ochrona Infrastruktury Krytycznej. Uregulowania prawne, „Zeszyty Naukowe. Organizacja i Zarządzanie" 2018, no 6.

Appendix 1

Survey in English

(version completed by survey participants)

On behalf of the Polish National Research Institute NASK, we thank you for your interest in participating in our survey. The collected data will serve to conduct research on the landscape of ISACs functioning in Europe. The results will be published in the form of a report in English and Polish. An additional aim of the report will be to promote the activities of the ISACs participating in the survey. Hence, we encourage you to answer all questions, including the open ones so that the work of your ISAC could be comprehensively presented in the publication. Thank you for your time!
Cybersecurity Strategy and Development Department at NASK.

INFORMATIONAL DATA ON ISAC

1. Full name of the ISAC: ....
2. Founding date of the ISAC: ....
3. Headquarters of the ISAC (if applicable): ....
4. Current number of the ISAC members: ....
5. Sector(s) to which the ISAC members belong: ....
6. The ISAC's website/social media: ....
7. Role in the ISAC of a person filling in the survey: ....

I. ORGANISATION AND MEMBERSHIP OF ISAC

1. What is the organisational form of your ISAC (for ex. a non-profit organisation, an agency, an informal gathering)?

   ....

2. What types of entities are members of your ISAC? (please indicate all matching answers)

- **a.** state administrative bodies
- **b.** state-owned companies
- **c.** private companies
- **d.** academic institutions
- **e.** research centres
- **f.** non-governmental organisations
- **g.** other (please specify): ....

3. What elements of the organisational structure does the ISAC have? (please indicate all matching answers)

- **a.** chair (alternatively vice-chair)
- **b.** management board/steering committee
- **c.** secretariat
- **d.** employees
- **e.** other (please specify): ....

4. How the ISAC's activities are funded? (please indicate all matching answers)

- **a.** fixed, mandatory membership fee
- **b.** voluntary membership contributions
- **c.** state funding
- **d.** other (please specify): ....

5. What criteria must be met to become a member of your ISAC? (please indicate all matching answers)

- **a.** activity in a specific sector
- **b.** the form of organisation specified by the ISAC
- **c.** the size of the organisation specified by the ISAC
- **d.** other (please specify): ....

II. ACTIVITY

6. What are the objectives pursued by your ISAC?
(please choose up to 3 answers that suits best to the ISAC's focus areas)

a. information exchange and risk analysis

b. incident response coordination

c. provision of technical support and advice

d. training and education on cybersecurity

e. promotion of best practices in the area of cybersecurity

f. other (please specify): ....

7. What activities are undertaken within the ISAC?
(please choose up to 3 answers that suits best to the ISAC's focus areas)

a. organising conferences (if selected, then question 7a)

b. joint exercises and simulations (if selected, then question 7b)

c. preparing reports/analyses (if selected, then question 7c)

d. representing the interests of the sector towards public authorities

e. integration meetings (if selected, then question 7e)

f. activities in working groups (if selected, then question 7f)

g. other (please specify): ....

7a. How often does the ISAC organise conferences?

a. once a month or more often

b. once a quarter

c. once in six months

d. once a year

e. less than once a year

7b. How often does the ISAC organise joint exercises and simulations?

a. once a month or more often

b. once a quarter

c. once in six months

d. once a year

e. less than once a year

7c. How often does the ISAC prepare reports/analyses?

a. once a month or more often
b. once a quarter
c. once in six months
d. once a year
e. less than once a year

7d. How often does the ISAC organise integration meetings?

a. once a month or more often
b. once a quarter
c. once in six months
d. once a year
e. less than once a year

7e. How often does the ISAC conduct activities in working groups?

a. once a month or more often
b. once a quarter
c. once in six months
d. once a year
e. less than once a year

8. What are the methods of communication and information exchange within your ISAC? (please indicate all matching answers)

a. regular meetings (if selected, then question 8a)
b. ad-hoc meetings
c. an online platform or portal for members
d. mailing list
e. other (please specify): ....

8a. How often does the ISAC organise regular meetings?

a. once a month or more often
b. once a quarter
c. once in six months
d. once a year
e. less than once a year

9. How does your ISAC promote its activities internationally?
(please choose up to 3 answers that suits best to the ISAC's focus areas)

a. social media channels

b. speaking at conferences

c. participation in consultations on national and international level

d. running educational campaigns

e. writing for the trade press

f. other (please specify): ....

10. What challenges do you see for the ISAC's activities (please choose up to 3 answers that you find most relevant to your ISAC's experience)

a. inactivity of members

b. difficulties in building trust between members

c. difficulties in maintaining regularity in ISAC activities

d. competition between members

e. lack of available resources and funding

f. lack of sufficient regulation at national level

g. other (please specify): ....

11. Does the ISAC have any initiatives that you would particularly like to share? Please provide their names and brief descriptions (3–4 sentences).

....

....

12. Does the ISAC cooperate with other organisations, including European or national ISACs?

a. Yes (if selected, then question 12a)

b. No

12a. Please list the organisations the ISAC cooperates with and give a brief description of the cooperation.

....

....

Thank you for filling in the survey!

Appendix 2

Survey in Polish

(translation of the original English version)

W imieniu Państwowego Instytutu Badawczego NASK dziękujemy za zainteresowanie udziałem w naszym badaniu. Zebrane dane posłużą do przeprowadzenia badań na temat krajobrazu ISAC-ów działających w Europie. Wyniki zostaną opublikowane w formie raportu w języku polskim i angielskim. Dodatkowym celem raportu będzie promocja działalności ISAC-ów biorących udział w badaniu. Zachęcamy zatem do udzielenia odpowiedzi na wszystkie pytania, również te otwarte, aby działalność Państwa ISAC-a mogła zostać kompleksowo zaprezentowana w publikacji. Dziękujemy za poświęcony czas! Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni NASK.

PODSTAWOWE INFORMACJE O ISAC-U

1. Pełna nazwa ISAC-a: ....

2. Data założenia ISAC-a: ....

3. Siedziba (jeśli dotyczy):...

4. Aktualna liczba członków ISAC-a: ....

5. Sektor/sektory, do których należą członkowie ISAC-a: ....

6. Strona internetowa/kanały w mediach społecznościowych: ....

7. Funkcja w ISAC-u pełniona przez osobę wypełniającą ankietę: ....

I. ORGANIZACJA I CZŁONKOSTWO W ISAC-u

1. Jaka formę organizacyjna ma ISAC? (np. organizacja non-profit, agencja, nieformalne zgromadzenie)?

....

2. Jakie rodzaje podmiotów są członkami ISAC-a?
(proszę zaznaczyć wszystkie pasujące odpowiedzi)

a. organy administracji państwowej
b. przedsiębiorstwa z udziałem państwa
c. przedsiębiorstwa prywatne
d. instytucje akademickie
e. ośrodki badawcze
f. organizacje pozarządowe
g. inne (proszę podać): ....

3. Jakie elementy struktury organizacyjnej posiada ISAC?
(proszę zaznaczyć wszystkie pasujące odpowiedzi)

a. przewodniczący (ewentualnie wiceprzewodniczący)
b. zarząd/komitet sterujący
c. sekretariat
d. pracownicy
e. inne (proszę podać): ....

4. W jaki sposób finansowana jest działalność ISAC-a?
(proszę zaznaczyć wszystkie pasujące odpowiedzi)

a. stała, obowiązkowa opłata członkowska
b. dobrowolne wpłaty członków ISAC
c. finansowanie przez państwo
d. inne (proszę podać): ....

5. Jakie warunki należy spełnić, aby zostać członkiem ISAC-a?

a. działalność w określonym sektorze
b. forma organizacji określona przez ISAC-a
c. wielkość organizacji określona przez ISAC-a
d. inne (należy określić): ....

II. DZIAŁALNOŚĆ ISAC

6. Jakie cele są realizowane przez ISAC-a?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

a. wymiana informacji i analiza zagrożeń

b. koordynacja działań w przypadku incydentów

c. zapewnienie wsparcia technicznego i doradztwa

d. szkolenia i edukacja w zakresie cyberbezpieczeństwa

e. promowanie najlepszych praktyk w dziedzinie cyberbezpieczeństwa

f. inne (proszę podać): ....

7. Jakie działania prowadzone są w ramach ISAC-a?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

a. organizacja konferencji (jeśli wybrano, to pytanie 7a)

b. wspólne ćwiczenia i symulacje (jeśli wybrano, to pytanie 7b)

c. przygotowywanie raportów/analiz (jeśli wybrano, to pytanie 7c)

d. reprezentowanie interesów sektora przed organami państwowymi

e. spotkania integracyjne (jeśli wybrano, to pytanie 7e)

f. praca w grupach roboczych (jeśli wybrano, to pytanie 7f)

g. inne (należy określić): ....

7a. Jak często ISAC organizuje konferencje?

a. raz w miesiącu lub częściej

b. raz na kwartał

c. raz na sześć miesięcy

d. raz w roku

e. rzadziej niż raz w roku

7b. Jak często ISAC organizuje wspólne ćwiczenia i symulacje?

a. raz w miesiącu lub częściej

b. raz na kwartał

c. raz na sześć miesięcy

d. raz w roku

e. rzadziej niż raz w roku

7c. Jak często ISAC przygotowuje raporty/analizy?

a. raz w miesiącu lub częściej

b. raz na kwartał

c. raz na sześć miesięcy

d. raz w roku

e. rzadziej niż raz w roku

7e. Jak często ISAC organizuje spotkania integracyjne?

a. raz w miesiącu lub częściej

b. raz na kwartał

c. raz na sześć miesięcy

d. raz w roku

e. rzadziej niż raz w roku

7f. Jak często ISAC prowadzi prace w grupach roboczych?

a. raz w miesiącu lub częściej

b. raz na kwartał

c. raz na sześć miesięcy

d. raz w roku

e. rzadziej niż raz w roku

8. Jakie są metody komunikacji i wymiany informacji w ramach ISAC-a? (proszę zaznaczyć wszystkie pasujące odpowiedzi)

a. regularne spotkania (jeśli wybrano, to pytanie 8a)

b. spotkania ad-hoc

c. platforma internetowa lub portal dla członków

d. lista mailingowa

e. nne (należy określić):..

8a. Jak często ISAC organizuje regularne spotkania?

a. raz w miesiącu lub częściej

b. raz na kwartał

c. raz na sześć miesięcy

d. raz w roku

e. rzadziej niż raz w roku

9. W jaki sposób ISAC promuje swoją działalność?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

a. kanały w mediach społecznościowych

b. wystąpienia przedstawicieli na konferencjach

c. udział w konsultacjach na poziomie krajowym i unijnym

d. prowadzenie kampanii edukacyjnych

e. przygotowywanie artykułów do prasy branżowej

f. inne (proszę podać): ....

10. Jakie wyzwania dostrzegają Państwo dla działalności ISAC-a?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

a. brak aktywności członków

b. trudności w budowaniu zaufania między członkami

c. trudność w utrzymaniu regularności w działaniu ISAC

d. konkurencja między członkami

e. brak dostępnych zasobów i finansowania

f. brak dostatecznych uregulowań prawnych na poziomie krajowym

g. inne (proszę podać): ....

11. Czy ISAC prowadzi jakieś inicjatywy, którymi w szczególności chcieliby się Państwo pochwalić? Prosilibyśmy o podanie ich nazw i krótkich opisów (3–4 zdania).

....

....

12. Czy ISAC współpracuje z innymi organizacjami, w tym z europejskimi lub krajowymi ISAC?

a. Tak (jeśli wybrano, to pytanie 12a)

b. Nie

12a. Prosimy o wymienienie organizacji, z którymi współpracuje ISAC i podanie krótkiego opisu te współpracy.

....

....

Acknowledgements

Many thanks to all the ISACs that agreed to participate in the survey. It is thanks to their commitment that this publication could be produced. Special thanks also go to our reviewer, Marek Pawlik, Ph.D., D.Sc. Eng., Professor of Railway Research Institute (IK) for his valuable comments and guidance. We were also greatly supported by the help of Dr hab. Prof. Aleksandra Gasztold and Katarzyna Nakonieczna from the NASK Publishing Department.

About NASK

NASK is a National Research Institute whose mission is to develop and implement solutions for the development of ICT networks in Poland and to improve their efficiency and security. It carries out research and development projects and projects aimed at improving the security of Polish civilian cyberspace. An important area of the Institute's activity is also user education and the promotion of the idea of an information society, primarily to protect children and young people from the dangers of new technologies.

About the Strategy and Cybersecurity Development Department

The Cybersecurity Strategy and Development Department monitors developments in national and international regulations on cyber security and new technologies. It conducts activities aimed at identifying trends that have a direct impact on the cybersecurity ecosystem and identifies strategic directions for the development of this field. The mission of the Cybersecurity Strategy and Development Department is also to provide advice at the strategic level and to support the entities of the national cybersecurity system in building capacity and capability in the area of cybersecurity. The Cybersecurity Strategy and Development Department develops the cyberpolicy.nask.pl information service, which is a compendium of knowledge and good practices on strategic, regulatory and organisational aspects of cybersecurity.

NASK