National Cyber Security Centre
Ministry of Justice and Security

Starting an ISAC: Sectoral collaboration

Guide

Roadmap sectoral collaboration

The NCSC and its partners have created a roadmap to help you get started with a roadmap sectoral collaboration. In this roadmap, you will find three stages your organisation can undertake to create and foster a successful sectoral collaboration.

Stage 1: **Explore**

Seek like-minded people and create support:

- Start out small, together with enthusiastic (chief) information security officers.
- Set up an informal working group and get to know each other better.
- Look for common goals and other similarities during the first meeting.

Stage 2: **Build**

Build a solid foundation:

- Organise a kick-off meeting to formally start the ISAC.
- Jointly select a chair, vice-chair and secretary from those present.
- Reach agreement on how often meetings will take place and in what way you will communicate with each other.
- Set up guidelines for a membership and information sharing.

Stage 3: **Continue**

Keep working on building trust:

- Be critical of your own participation in the ISAC.
- Make room to evaluate.
- Continue to focus on the added value of information exchange.

Starting an ISAC

Would you like to increase the digital resilience of your sector? Launch an ISAC! An Information Sharing and Analysis Centre (ISAC) is an excellent way of cooperating with other organisations in your sector to increase the digital resilience of your organisation. In doing so, benefit from the years of experience of the NCSC and organisations that have established an ISAC themselves.

Starting an ISAC together with your sector competitors may come across as a major step involving a lot of time, funds and means. Fortunately, practice has proven otherwise. All that it takes to start is bringing a few fellow information specialists from your sector together and begin exchanging experiences and information. This guide is a compilation of best practices yielded by all these experiences.

Target audience

Information security officers of businesses that would like to start an ISAC.

The following ISACs contributed to this guide

Airport, Chemical/Oil, Drinking Water, Energy, Financial Institutions, Healthcare, Legal, Media, Multinationals, Managed Service Providers (MSP), Nuclear, Pensions, National Government, Port, Telecom, and Water Management.

This guide is a collaboration between

the National Cyber Security Centre (Ministry of Justice and Security) and the Digital Trust Center (Ministry of Economic Affairs and Climate Policy).

> *"By analysing incidents together and keeping each other informed about prospective or actual measures, we as MSPs can ensure that customers of various MSPs receive more or less the same advice. This approach prevents confusion among our customers, including joint customers, while also creating the calm required to address an incident properly."*
>
> **MSP-ISAC**

What is an ISAC?

An ISAC is a sectoral[1] consultative body for cybersecurity. In an ISAC, you create a trusted environment with organisations from the same sector in order to share sensitive and confidential information on incidents, threats, vulnerabilities, measures and lessons learnt in relation to cybersecurity.

There is no 'standard format' for an ISAC. Cooperation in an ISAC can be either formal or informal, structured or flexible, with physical meetings, teleconferences or consultations via a digital platform, or a mix of the three working methods. The participants can select the most suitable form themselves. This guide contains advice that you and your partners can use in making the right choices to ensure the launch of a successful collaboration. Experience has shown that cooperation works best when the participants choose the most suitable form themselves.

The need and benefit of an ISAC

Learning from one another

The aim of an ISAC is sharing knowledge and experience in order to increase the digital resilience of your organisation and the sector. By learning from incidents and the effects of mitigating measures taken by other organisations, you can anticipate matters in order to prevent or more quickly mitigate similar incidents within your own organisation.[2] While you will learn from others the one time, others may learn from you the next, as an incident for one party may lead to prevention for another.

Enhancement of cybersecurity quality

By cooperating within your sector, you will receive information more quickly and acquire or improve your situational awareness. You may be able to detect attacks that you would not have noticed otherwise. In addition, you will learn to better assess risks and the effects of mitigating measures.

Cost reduction

When operational processes are disturbed, this situation costs money. Learning from each other could decrease the chances of such incidents. By working together, you can address problems and issues together. This process costs less time and money, since you will not have to come up with a solution by yourself or reinvent the wheel.

Strengthen image

An ISAC will show present and potential customers that you take service continuity and the protection of sensitive data very seriously. In addition, participating in such collaboration could help to prevent possible reputational damage.

Leading by doing

Cooperating on cybersecurity could form part of the corporate social responsibility (CSR) policy within your organisation.

How do you establish an ISAC?

Trust, shared interests and equality are necessary preconditions for success. If you start building trust and defining shared interests from the very first, while acting on the basis of equality within your ISAC, you will have chosen the route towards the best results.

Trust

Trust is the key to cooperation. You must be able to assume that the information which you share will not appear in tomorrow's newspapers. Furthermore, you need to trust that information will not be forwarded and that the other will stick to the agreements made. Without trust, an ISAC is doomed to failure.

What means are at your disposal to build trust? Examples include membership guidelines or agreements about how and with whom information may be shared. For the latter purpose, the Traffic Light Protocol (TLP)[3] is recommended. Another way to build trust more quickly is working with regular representatives; in other words, meeting with the same people as much as possible.

Consider going out together for a drink or a bite to eat after a meeting. Getting to know each other in an informal setting will be beneficial. Just remember to invest in your relationship, always be reliable, keep your promises and set a good example.

> *"Although it takes time to build trust, do not let this fact stop you from getting started. The result is well worth it!"*
>
> ***Nucleair-ISAC***

[1] Although the most common type of ISAC is sectoral, the ISAC model also allows you to cooperate in your supply chain or region. Consult www.ncsc.nl/english/cooperation for more specific advice on establishing a supply chain or regional cooperation.

[2] See also https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

[3] https://www.first.org/tlp

Shared interest

What interest do you or your organisation have in contributing to an ISAC and what about the other participants? Discuss this fact together and be frank about your motivations. You will soon discover what the shared interest is. If you work towards a mutual goal, it will present added value to the ISAC. Bear in mind that different interests may continue to exist, as long as they have been discussed and do not conflict with each other. Conflicting interests lead to working at cross-purposes, which would soon bring the ISAC to an end.

Equality

In the best collaborations, the participants are on an equal footing, meaning that there are no hierarchical relations. If organisations are accountable to one another outside the ISAC, they will probably not be prepared to share a lot of information within the ISAC.
It is difficult to share sensitive matters if it could later be used against you.

The next three stages describe specific steps for establishing an ISAC. You decide yourself in which order these steps are completed, since each cooperation is unique and requires a customised approach.

Stage 1: Explore

Find like-minded parties and create support

In your sector, find like-minded parties who are willing to collaborate and who are actively working to increase digital resilience in their organisation and sector. Start out small, together with information security officers who are keen on dealing with cybersecurity issues at a tactical level on a daily basis. Participants from three to five organisations will already give you a proper start. They will be able to translate the information being shared in an ISAC to the activities of specialists in their own organisation.

Starting out small will help in getting off to a quick start, building trust and determining how the partnership should look. Experience has shown that 20 to 25 organisations is the limit. The larger the group, the more difficult it is to schedule meetings. Participants will be less willing to share information and trust one another, whereas retaining trust becomes difficult in the longer term.

"As part of the approach to dealing with digital threats and vulnerabilities, two security officers took the initiative of establishing a Legal-ISAC. We approached colleagues at other firms, who immediately responded with great enthusiasm. When we planned an initial meeting, we came up with specific objectives aided by the NCSC. We then got off to our official start; information on this launch was recently published,[4] which led to further requests for participation. It has been quite a success!"

Legal-ISAC

Momentum to launch an ISAC can come from an incident within your own organisation or a major incident making the news. A point of departure could also be regular meetings with colleagues from your sector. You often encounter the same individuals in various situations, as a result of which you could decide together that starting an ISAC might be a good idea.

When you have found a few colleagues from other organisations within your sector who share an interest in and realise the importance of starting a partnership, it is a good time to gather them in an informal working group.

Become better acquainted, be frank and ask a lot of questions during the first session. Take the time to answer the questions below and only continue once you have reached consensus on the answers. This process will be the cornerstone of a successful collaboration. It may be necessary to convene a number of meetings to answer all the questions.

The following questions could prove useful in this regard:

Who are we and what do we have in common?
Consider such things as processes, systems, dependencies, mutual challenges and incidents.

What is the shared objective?
Examples of a shared objective are exchanging information on threats and incidents, standardising processes within the sector, or discussing new developments and trends.

Do we need any other organisations to achieve this objective?
Use each other's knowledge and network. A limited stakeholder analysis could prove useful. While the aim could of course be to have an ISAC with many members, it is important to ensure a solid foundation.

What kind of information would we like to share?
Consider in this respect various levels of information (operational, tactical, strategic), types of information (cybersecurity, privacy, cybercrime, fraud, and so on) and important themes (cloud security, cyber threat intelligence, risk management, asset management, Internet of Things, network segmentation, honeypots, and so on). Use these aspects to determine which officials in an organisation should join the ISAC.

Are we the right individuals to participate in the ISAC?
Together, determine who the invitees will be to the initial ISAC meeting. As a result, the individuals who took the initiative and who are now meeting might not be the people who should be in the ISAC. So ask yourself whether you are the right person to participate and ask the others at the table to consider this question as well.

Tip: Do not start out with a large group. For one, it will be easier to build trust; for another, the criteria for participation still need to be established. It is easier to grow a group than to shrink it.

Recommendations

- Be transparent about your own organisational objectives and interests.
- In this regard, be frank about what you can and cannot offer, as well as what the obstacles are.
- Avail yourself of existing structures or networks staffed by enthusiastic and skilled individuals.
- Use the answers to the above questions as input on the membership guidelines (see also Stage 2).

[4] https://www.loyensloeff.com/en-us/news-events/news/dutch-law-firms-together-against-cybercrime, https://www.nautadutilh.com/en/information-centre/news/dutch-law-firms-together-against-cybercrime

Stage 2: Build

Ensure a solid foundation

Organise a kick-off to mark the formal beginning of the ISAC. Do so after having conducted the initial exploratory discussions with enthusiastic colleagues. It is important to have an answer to the questions discussed earlier. What brings you together? What is your shared objective?

A kick-off is an event to mark the beginning of your collaboration. Before getting into particulars, it is important to invest time and effort in getting to know each other, making agreements and confirming them.

Becoming acquainted

While you will often already know one or more of the other participants, this fact does not necessarily mean that you know them well or already trust them sufficiently. Allocate time during the kick-off to invest in these aspects. There are various ways to do so. You can organise a speed dating session, in which everyone can ask each other work-related and personal questions. Another pleasant option is sharing a lunch or dinner, or getting together for drinks.

Roles

Once you have gotten to know each other well, jointly select a chair, vice-chair and secretary from those present. These three roles must be filled to ensure that the discussion is structured, to safeguard the process and to enable effective discussions. It goes without saying that the participants themselves are responsible for the collaboration succeeding. Which subjects are discussed, which information is shared and which results follow depends on everyone's active cooperation.

“The most important job of the chair or vice-chair is to understand what the primary information security risks and incidents are for the ISAC members, as well as to ensure that these points are addressed. Whenever we are together, it is wonderful to see how much knowledge there is within the ISAC, and how willing everyone is to share their knowledge and experience with the others – including when things have gone wrong.”

Multinationals-ISAC

The chair does not only preside over the meeting, but is also the driving force behind the ISAC. The chair challenges the members to share information and encourages them to play an active role in the collaboration. Moreover, the chair engages in discussion during meetings as well. Any external communication on the ISAC's activities is provided in the first instance by the chair, who acts on behalf of the ISAC members.

“The chair facilitates the ISAC meetings and encourages networking in which cyber incidents are shared as widely as possible with one another. Improving and sharing knowledge continues to serve as our motto to make the Netherlands more resilient together.”

National Government-ISAC

The vice-chair substitutes for the chair and is involved in drawing up the agenda for the ISAC meetings. Together with the chair, the vice-chair is the first point of contact for requests from other organisations wishing to join the ISAC.

“Acting as chair or vice-chair of an ISAC gives you a lot of energy to reach the next level in cybersecurity and resilience not just for your own organisation, but also for the entire sector.”

Pensions-ISAC

The secretary plays an important role alongside the chair before, during and after meetings. The secretary ensures that the processes (agreements, procedures) are followed according to what has been agreed. In addition, the secretary ensures that all participants are acquainted with and have signed the membership guidelines. The secretary organises the meetings, sends the invitations, drafts the agenda and is responsible for the meeting minutes, as well as for keeping membership records. Of course, the secretary can also contribute to the general discussion.

“As secretary, you are the linchpin of the ISAC. Together with the chair and vice-chair, you provide direction to the ISAC and ensure that it functions as well as possible. It is very rewarding!”

NCSC

Frequency

It is a good idea to reach agreement on how often meetings will take place: quarterly, monthly or by some other arrangement. Existing ISACs generally meet between four and eight times each year. In addition, it is important to agree where the meetings will take place and how long they will last. Once the frequency has been decided, dates can be scheduled for the entire year. Such an annual schedule will help to ensure continuity in the discussion of subjects and attendance by the members.

Communication

Drawing up a mailing list will prove beneficial. A mailing list is a private list (which service is offered by various web hosting companies) to which you add the members' email addresses (only personal email addresses, not work mailboxes). Remember to take security measures that ensure integrity and confidentiality.[5]

This list is private in the sense that only members can email to it. The private nature ensures that members can easily get in touch outside the meetings to exchange information or ask questions. This approach will help to further engender mutual trust. Agree who will keep the membership records and manage the email list. In most cases, the secretary will assume this responsibility. Eventually, it may prove useful to establish a secure place which members can access in order to share documents, such as a team site. This process will aid information exchange.

Membership guidelines

Membership guidelines require a lot of time and consideration because they form the foundation of the ISAC.[6] Note that this document most definitely is not a legal text from which rights can be derived, but first and foremost an informal agreement. In the guidelines, fundamental choices are made on admission criteria for new organisations (scope of the collaboration) and criteria for the individual representatives (level, role, and so on). The guidelines also include process agreements on admitting new organisations and their representatives, as well as on amending the guidelines. This document should also contain agreements on the absence of an organisation. Attendance and the willingness of the participants to share are of course the key to success, as collaboration is pointless without these elements. Finally, the document also contains agreements on how to deal with the information that you share.

For information sharing, the NCSC recommends the use of the Traffic Light Protocol (TLP)[7] from FIRST. Within the cyber domain, this information exchange protocol is renowned and widely known. It is crucial that all members understand this protocol and act accordingly in order to ensure trust.

[5] https://www.ncsc.nl/english/current-topics/factsheets/factsheet-secure-the-connections-of-mail-servers.html; https://www.ncsc.nl/english/current-topics/factsheets/factsheet-use-two-factor-authentication.html

[6] See the template for ISAC membership guidelines at www.ncsc.nl/english/cooperation.

[7] www.first.org/tlp of the Forum of Incident Response and Security Teams (FIRST).

Stage 3: Continue

Keep working on building trust

Keep paying attention to retaining and increasing trust within your collaboration. Also ensure that you constantly work to maintain internal support within your own organisation, including after the kick-off. To this end, continue to communicate openly both internally and externally about what you can or cannot deliver. Prepare for meetings by bringing along information on incidents and try to use any knowledge that you have acquired within your own organisation. This will show the added value of the ISAC and information sharing to your colleagues and supervisors.

Tip: A mutual website or news item can increase visibility and support.

The first 'real' meetings after the kick-off could feel a bit unfamiliar. This feeling will undoubtedly pass. The following could increase the value of the meetings:

Agenda[8]

The chair, vice-chair and secretary together draw up the agenda for the next meeting, and send it to the participants not later than two or three weeks in advance to allow them to prepare. It is a good idea to have certain subjects always on the agenda, while leaving room for current topics and any questions that participants may have. If feasible in terms of time, it is also recommended to include a break, which provides an opportunity for informal interaction and consequently contributes to mutual trust.

Annual plan

During the first meeting of the year, it will be beneficial to brainstorm about the annual plan. An annual plan includes topics, themes and developments that you would like to discuss with one another. Assign each topic to an 'owner', who then ensures that they are periodically covered. This process could involve a guest speaker being invited to talk on the subject or the owner giving a presentation. Another approach is to schedule certain subjects in advance to be discussed during various meetings throughout the year. This planning can be done in a number of ways. You could provide different meetings with different themes, or you could simply list subjects and schedule them for various meetings. Of course, flexibility is always called for in order to deal with any current issues.

Annual report

Some ISACs choose to compile a brief annual report at the end of the year, describing what the ISAC dealt with and how it contributed to the digital resilience of the sector or the organisations in it. Such an annual report could help participants to explain the need and benefit of the ISAC within their own organisation, as well as to 'justify' their time commitment.

Practical matters

Do not forget to deal adequately with the practical matters that crop up when you organise a meeting, such as booking a meeting venue, registering participants, arranging presentation facilities and possibly making catering arrangements (lunch or concluding drinks). You could either choose always to use the same central location or to take turns hosting. The latter option has the benefit of dividing the costs among multiple organisations. It also gives the host organisation the opportunity to present a current topic within their organisation.

Tip: If whoever is speaking agrees, the ISAC could decide that you may bring along a colleague to the presentation. Once the presentation is finished, such colleagues can leave and allow the ISAC to maintain its private nature.

Active participation

Successful collaboration depends on active participation and well-prepared participants. For instance, particularly in larger organisations, it is important that you actively collect information on identified threats, incidents, experiences, lessons learnt and any other activities which could be of value to the other ISAC participants.

'Red Round'

An incident for one party could result in prevention for the next. Sensitive information about cybersecurity incidents can be shared under TLP:RED in a 'Red Round'. This process entails that everything shared during this round is kept private – so no minutes or notes are to be taken. If you do feel that it is necessary to use the information from the Red Round (e.g. for organisations not in the ISAC), you must always consult the source of the information as to whether and how this information may be used.

[8] See the agenda template at www.ncsc.nl/english/cooperation.

New members

Once the ISAC is up and running, you will find that there are more organisations wishing to share in its success. In other words, you will receive membership requests, which will have to be reviewed together. This procedure requires unanimous support within the ISAC for admitting an organisation and its chosen representative. Unanimity is required to ensure that trust within the ISAC is maintained. Otherwise, the willingness to share information will diminish, which in turn reduces the value of the ISAC. The admission process differs among ISACs and is set out in the membership guidelines.

> *"As a result of really getting to know your colleagues after a number of meetings, you also are able to connect informally whenever things crop up within the sector. This situation truly improves knowledge sharing."*
>
> **Energy-ISAC**

Familiar faces

Familiar faces at the meeting table are vital for trust, it is necessary to work with one or at most two permanent representatives from each organisation. Should the ISAC decide to allow a back-up representative in addition to the permanent representative, it is a good idea to reach an agreement on how often such back-up representatives should attend at a minimum in order to retain trust within the group.

Replacing the chair, vice-chair and secretary

Reach an agreement on how often the chair, vice-chair and secretary will be replaced. Should this change occur regularly or is there a maximum term to act in this capacity? What is the procedure for being installed, retiring and transferring duties? Establish all these aspects in the membership guidelines.

> *"Within the Port ISAC, we as port-related businesses and organisations realise how dependent we are on each other as well as on systems, and how much we can still learn. We do not just consider Rotterdam as the largest European port in this respect, but we also seek the connection with Europe's second port, Antwerp. For this reason, we paid a first visit to Antwerp three years ago for an inside view. Although we did expect that we shared quite a few challenges and ambitions, we were surprised to learn how much we could learn from each other and reinforce one another. As a result, we meet every year now."*
>
> **Port-ISAC**

Inside view

In the wake of the meetings, members can be provided with an inside view of each other's organisations. This process will aid in getting to know one another informally, which contributes to mutual trust. It will also help to create an understanding of the various backgrounds. By learning about which processes are relevant to an organisation, you can begin to understand why certain topics are important to participants.

Challenges

Establishing and maintaining an ISAC requires you to meet challenges. Possible challenges are summed up below.

Trust

Although it has been mentioned repeatedly, it can never do any harm to repeat it once again: exchanging potentially sensitive information always requires trust. Trust grows slowly and requires constant maintenance. Abusing trust will jeopardise the information exchange and thus the continued existence of the ISAC.

> *"Never hesitate to explain that something is bothering you and accept everyone's level of maturity in addressing cybersecurity."*
>
> **NCSC**

Commitment

An ISAC is a voluntary collaboration which has been established on the basis of intrinsic motivation. However, 'voluntary' does not mean that there are no obligations. The ISAC's success hinges on all participants' continually investing in it.

Added value and group size

At times, everyone wonders why certain organisations are in an ISAC. As this situation has often evolved over the years, it can prove very difficult to request that a party which has little added value leave the group. It is nonetheless necessary to remain vigilant on providing added value as an ISAC participant. Evaluate your own participation critically, but also engage in discussion with one another. Closely monitoring what each participant contributes to and takes away from the ISAC is important. This process can also be used to determine which organisation(s) the group is still lacking.

Tip: Plan an evaluation every two years to take a critical look at the ISAC.

Competition

Working together in an ISAC could mean that you will share sensitive information with your competitors. If your revenue model is not cybersecurity, stating unequivocally to each other (and perhaps to the outside world as well) that you are not competing on cybersecurity may be a good idea.

In the event that this aspect is part of your revenue model and you are competing in this sense, there are still ways to encourage information sharing. For instance, this process could entail only having representatives in the ISAC who are directly responsible for cybersecurity and not allowing ones who play a commercial role in their organisation.

> *"Competition entails that you clearly state the differences in your communication. We do not do so, as we feel that we should be fighting cybercrime together with other banks and institutions. Ultimately, it is all about the trust that our customers have in the security of the entire banking system."*
>
> **FI-ISAC**

Complacency

Complacency is always a danger. The fact that you know each other so well should give cause to remain aware of the fact that it is important to be critical of one another and not to shy away from discussing any frustration. For this reason, it is always a good idea to set objectives, adopt new ones and adapt them continually; for example, by drawing up an annual plan. Take the time to schedule an evaluation by reviewing whether the answers to earlier questions on the justification for the collaboration still apply. Remember always to focus on the added value of the information which is shared.

Cross-sectoral or cross-border information sharing

In addition to the cooperation within ISACs, major added value can come from information exchange and collaboration between ISACs at the national, European or global level. This fact is particularly true for sectors which are similar in maturity, share mutual dependencies and/or use the same processes and systems. There are also an increasing number of European ISACs in which one of the members can participate in order to gather information for the own ISAC.

Further reading

ISAC best practices

- Information Sharing and Analysis Center – Cooperative models (2018). https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Publications of other ISACs

- European Energy ISAC [EE-ISAC]. www.ee-isac.eu
- Financial Services ISAC [FS-ISAC]. www.fsisac.com
- National Council of ISACs [NCI]. www.nationalisacs.org

Information sharing

- Introduction to information sharing (2016). https://www.isao.org/products/isao-300-1-introduction-to-information-sharing
- Sharing cybersecurity information: Good practices stemming from the Dutch public-private approach (2015). https://www.gccs2015.com/sites/default/files/documents/Sharing%20Cyber%20Security%20Information%20GCCS%202015.pdf
- Guide to cyber threat information sharing (2016). https://www.nist.gov/publications/guide-cyber-threat-information-sharing
- Building a national cyber information-sharing ecosystem (2017). https://www.mitre.org/publications/technical-papers/building-a-national-cyber-information-sharing-ecosystem

Publication
National Cyber
Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl/english/cooperation
samenwerken@ncsc.nl
@ncsc_nl

October 2018