

SETTING UP AN ISAC BLUEPRINT

Empowering EU ISACs

A number of sectors could benefit from an generic blueprint with steps and tips on how to set-up a new ISAC



How to establish an ISAC step-by-step?..

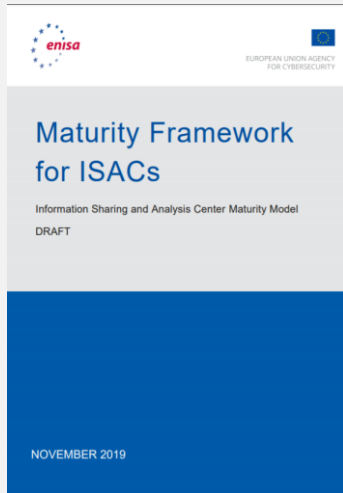
A number of models and frameworks exist!

Focus is on the first maturity stages

A 'one-size-fits-all' blueprint does not exist

Neither is the process squeaky clean sequential

There are a number of ISAC Maturity Models & Frameworks already available, which serve as input for the blueprint



ENISA ISAC Maturity Model

- Focus: all maturity stages
- 13 different ISAC functions
- 5 different maturity levels per function
 - *Initial*
 - *Developing*
 - *Maturing*
 - *Performing*
 - *Matured*



X-ISAC Guidelines to set up an ISAC

- Focus: setting up an ISAC
- 6 maturity phases
 - *Define goals*
 - *Get organized*
 - *Set up sharing rules*
 - *Choose mechanisms and tools*
 - *Ensure security and compliance*
 - *Follow up and improve*



NCSC- Starting an ISAC

- Focus: setting up an ISAC
- 3 phases
 - *Discover*
 - *Establish*
 - *Continue*



NCSC-NL – Next Gen ISACs

- Focus: all maturity stages
- 5 ISAC capabilities
 - *Strategy and Action plan*
 - *Working method*
 - *Information structure and management*
 - *Situational picture and Lessons Learned*
 - *Action*
- 3 maturity levels

Setting up an ISAC starts with building a foundation



Setting up an ISAC

Initial*

- Informal
- Ad hoc
- No analysis capability

Focus:

- ISAC foundations – getting aligned, building trust and getting started
- Moving from discussions to decisions and initial implementations

Developing

- Partial formalization
- Information-sharing
- Introduction IT-tools

Defined

- Complete structure/governance
- Basic analysis activities
- Yearplan/roadmap/KPIs

Managed

- Formal/legal entity
- Collaboration platform/tools
- Analys capacity & service offering

Optimized

- Continuous service delivery
- Influential institute
- Reiterative improvement

This is not
an exact science

* Maturity levels derived from ENISA's ISAC maturity model

Phase I - Initial

The initial fase is all about the basics: getting together, start building trust and start exploring how you envision an ISAC in your sector. At first, you will need to talk a lot to build a foundation of common understanding

Possible activities to undertake

Find a number of like-minded information security officers

Start an informal working group to discuss the possibility of a (sectoral) ISAC

Discuss differences and similarities with regards to interests of individual participating organisations

Discuss common challenges for all participating members to address in the ISAC

Discuss which potential members/stakeholders should (also) be involved as early as possible

Discuss the required job profiles of the representatives to participate

Discuss first thoughts on the overall mission and main objectives of the ISAC

Appoint a chair, (co)chair(s) and secretary

Discuss the set-up of the (first) sessions (duration, location, frequency)

Look for guidance and lessons learned from other ISACs and existing models /frameworks

Get internal support for participation in the ISAC

Schedule an official kick-off meeting

Set up agenda for meetings (and potentially take minutes)

Start 'low-key' sharing of information between members during (F2F) sessions

Legal / Formal considerations

1. Thinking

2. Deciding

3. Implementing

4. Revising

- Mission Statement
- Governance within the ISAC
- Membership criteria (thinking)

Tip #1 – take your time!

It might be tempting to move forward to fast. Keep in mind that trust is the ultimate key for success. This simply takes time to develop.



Phase II - Developing

In the 'developing' phase, the ISAC is slowly but steadily getting 'up-and-running'. Considerations turn into decisions, and the ISAC organisation, profile and activities are taking shape. During this phase, you will secure the basics of your ISAC and develop a (realistic) growth path

Possible activities to undertake

Discuss the short and longterm goals and objectives of the ISAC in detail

Discuss the type of information you would like to share within the ISAC on the short and longterm

Discuss how you want to share information on the short and longterm

Develop guidelines for initial information-sharing (e.g. the use of TLP)

Develop guidelines for membership

Discuss the short and longterm financial model

Decide on the the membership / admission criteria

Perform an in-depth stakeholder analysis

Discuss the possibility of forming an organisational legal entitiy

Inquire for IT-tools to use within the ISAC (e.g. secure mailing, videoconferencing, or filessharing)

Start with external communication/outreach (e.g. Presentation PPT, LinkedIn page, newsletter)

Establish working groups to jointly work on activities of the ISAC

Develop a roadmap/yearplan

Legal / Formal considerations

1. Discussing	2. Deciding
3. Implementing	4. Revising

- Membership criteria
- Code of Conduct/ Guidelines
- Terms of Reference
- Financial model (discussing)
- Legal entity (discussing)

Tip #2 – closely consider the (dis)advantages of formalization!

Formalization should fit the profile, context, and maturity of your ISAC initiative. Working on a comprehensive MoU can for example lure members, but it can also result in lost effort or overwhelmed potential members



The 'formal' spotlight : Members & Participants



An important theme while setting up an ISAC is your scope in terms of **members and participants** and to make '**design-choices**' about the **organizational set-up** of your ISAC. You will not only need to think about this thoroughly, but you will also need to make decisions and implement them:



- **Decide on membership criteria**
 - Type of organization
 - Role within organization
 - (thematic) expertise
 - Added value
- **Think about participation types**
 - Member(ship)s
 - Partner
 - Contributor
 - Vendors
 - Experts
- **Think about and assign ISAC roles**
 - Board
 - Chair
 - (co)chairs
 - Secretary
 - Experts



The 'formal' spotlight : Financial Model



While setting up an ISAC, it is of importance to already think about your **(long-term) financial model** and to make some decision with regards to the **financing of the ISAC on the short term**:

- **Think about types of funding**
 - In-kind contributions
 - goods, services, man(hours)
 - Membership fee(s)
 - Flat fee, levels
 - Sponsorship from vendors
 - (public) funding / support
- **Decide how to finance the ISACs initiative from the beginning**
 - Most often in-kind
 - Make an assessment of contribution required
 - Get approval (opportunity for awareness upper mgmt) and ensure availability/back-up



The 'formal' spotlight : Legal Entity



It seems early to start thinking about a **legal entity** for your ISAC organisation, but it is good to be **aware of your options** and to know how these relate to (and have an impact on) the design and operations of your ISAC

- **Think about international options**
 - In which country can we legally establish our ISAC
 - What are differences with regards to requirements, consequences and advantages
 - Some examples: AISBL, Stichting/Stiftung, etc.
- **Consideration to take into account are for example:**
 - Trust-confirming, allows for financial models, ISAC can act by itself, ensures continuity, can result in administrative burdens, filing requirements, impacts 'design-choices' organization, can be burdensome





© European Union, 2021



This document has been produced by the Empowering EU ISACs Consortium under contract SMART 2018/1022 for the European Commission, in cooperation with ENISA. The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.