European Commission

ISAC INFORMATION SHARING PLATFORM

Architecture overview

Capgemini invent

INTRASOFT INTERNATIONAL

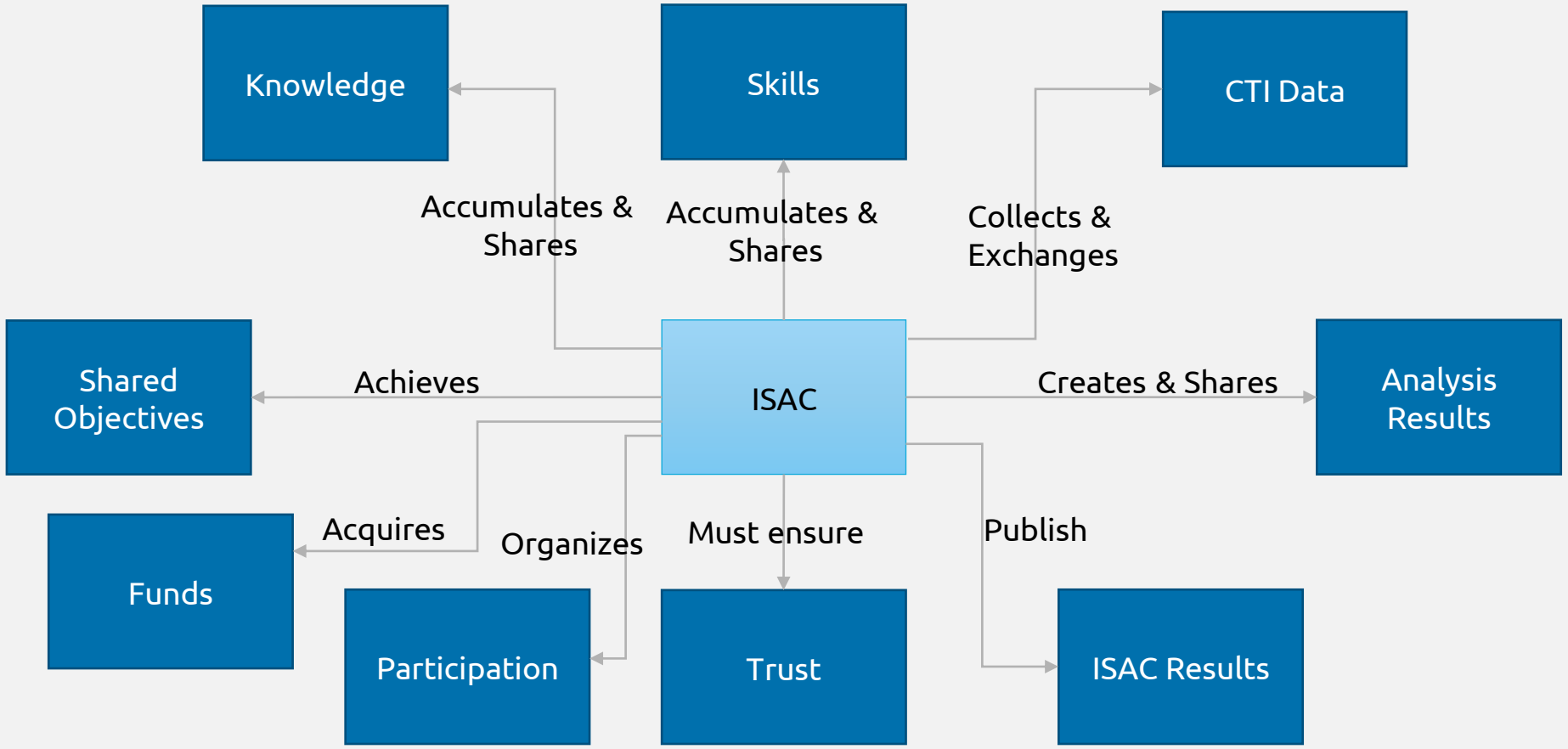
DFN CERT

Spark Legal network

TNO innovation for life

Business Object Context Model of an ISAC

This Context Model lists the 'topics and things' (the Business Objects) an ISAC is concerned with. It also states what an ISAC 'does' with those topics and things.



The history of the Technical Platform Requirements

Requirements collection process

We started with descriptions on EU ISAC generic objectives and current ways of working.

From there, we derived an initial set of functional requirements, expressed in terms of Technical Platform Functionalities.

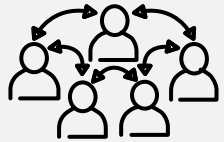
Those Technical Platform Functionalities were validated and refined with stakeholders:

- With ENISA in dedicated online meetings
- With representatives of existing EU ISACs in dedicated online meetings
- With representatives of emerging EU ISACs and other interested parties during online events (e.g. Inter-ISAC Meeting, Thematic Workshops)

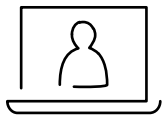
All input was used to refine the various Technical Platform Functionalities, leading to a comprehensive and prioritized list.

Basic IT Platform Functional Architecture

The overview of identified *potential* functionalities of the Technical Platform

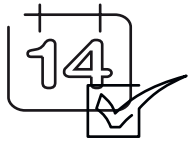


Knowledge Exchange



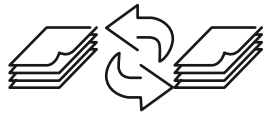
Secure Web Conferencing

Discussion Forum



Shared Planner

Webinars



Document Sharing

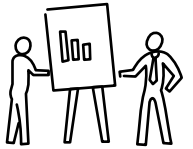
Mailing List

E-Learning

Online Chat

External Presentation

Public Website

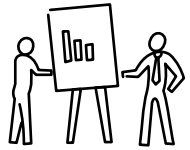


Reporting

Analysis & Collaboration

Analysis Tools

Data Exchange



Reporting

Underlying Services

IAM

Logging & Monitoring

Encryption

Hardening

Anti-Malware

Security Validation

Platform Security Attributes

- Defense in Depth fully implemented across infrastructure, applications and data (including network protection, multi-factor authentication, separation of roles, data encryption in transit and at rest). Security control maintenance (e.g. certificate management) done by centralized IT management authority.
- User activity auditing in place and monitored by the centralized IT management authority.
- Platform administration (‘system admin tasks’) done by the centralized IT management authority.
- User administration and user access management will be managed by ISACs (admin role per ISAC).
- A security test is part of platform delivery.

Deployment and Infrastructure Attributes

- Centrally hosted deployments, SaaS style.

- Multi-tenant deployment, meaning ISACs share a physical instance of the applications and tools, which are logically separated:
  - Separate user management
    - User ids cannot be part of other ISACs user groups (no identity mixing)
  - Separate data management
    - ISACs cannot access each other’s data

Continued Involvement of the Target Community

- The ISACs Basic IT Platform is incrementally validated by representatives of the target community.
- The Empowering ISACs projects engages the target community through periodic Sounding Board meetings. Both the end-user and prospective operations stakeholders are members of the sounding board.
- The Sounding Board provides input on the direction of the evolution of the ISACs Basic IT Platform.

Sounding board objectives

Objectives and expected workload

ISACs (EE-ISAC, ER-ISAC, EM-ISAC)	▪ Validate usability of the services (from an end-user perspective) ▪ Align on detailed requirements for the IT tooling
ENISA IT	▪ Validate usability from a maintenance perspective
EC ENISA	▪ Involvement as key stakeholders of the project