Fact sheet // IAM

Enforcing the NIS2 Directive with Identity and Access Management (IAM)

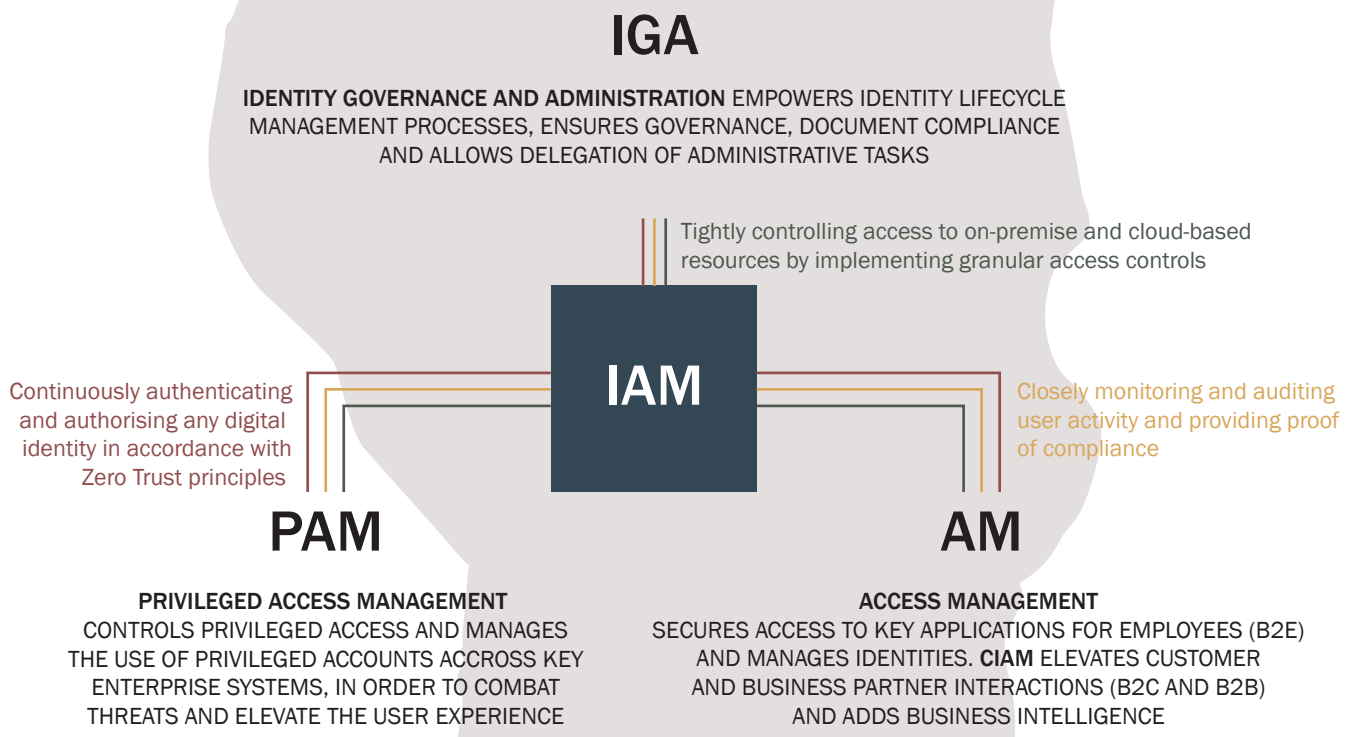
we make the fence

ICY security | Part of Columbus

Background

The NIS2 directive has been enacted by the EU to establish a high and uniform level of network and information system security across all EU member states.

IAM provides the technology that embeds the identity security processes and policies necessary to enforce the NIS2 directive.



Identity and Access Management (IAM) plays a crucial role in enforcing the requirements of the NIS2 directive:

1. **Continuously authenticating** and authorising any digital identity **in accordance with Zero Trust principles**
2. **Tightly controlling access** to on-premise and cloud-based resources **by implementing granular access controls**
3. **Closely monitoring and auditing user activity** and **providing proof of compliance**

The purpose of NIS2

The NIS2 directive was conceived to supersede the previous version, in response to several widely publicised and damaging cyberattacks, and is intended to better defend critical entities against various cyber threats.

The NIS2 Directive strengthens security requirements, streamlines reporting obligations, and introduces more stringent supervisory measures and stricter enforcement requirements.

All 27 EU member states must incorporate the NIS2 Directive into their national laws by October 2024.

Moreover, the NIS2 Directive applies not only to the direct employees of the organization, but also to the subcontractors and the service providers supporting them. It also introduces stricter incident reporting obligations where critical entities must:

- Provide initial notification of a significant security incident within 24 hours of detection.
- Deliver an initial assessment of the incident within 72 hours of detection.
- File a detailed final report within a month of detection.

What does NIS2 cover?

NIS2 Article 21 directs member states to ensure that essential and important entities manage risk by implementing robust systems, policies and best practices covering a wide range of cyber security measures and disciplines, such as:

- Risk analysis and information system security
- Incident handling and reporting
- Crisis management
- Supply chain security
- Basic cyber hygiene* practices and cyber security training
- Human resources security and access control policies
- Zero Trust access (multifactor authentication, continuous authentication)

**In an IAM context, cyber hygiene practice could be implementing adequate password change policies and limiting/controlling the number of administrator-level access accounts.*

What sanctions can be imposed?

NIS2 imposes costly sanctions. Member states can issue fines up to EUR 10 million or 2% of annual turnover (revenue) for certain violations or breaches. In addition, critical entity management bodies (i.e., executive teams) can be held personally liable for infringements.

ESSENTIAL

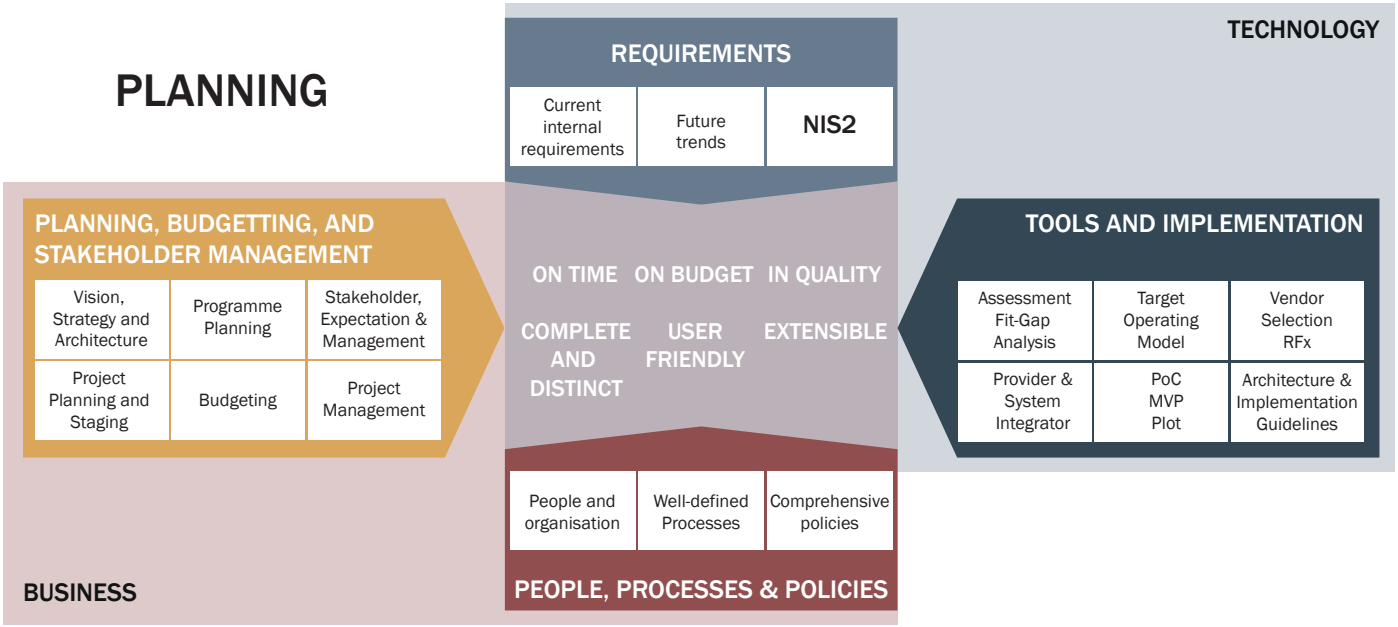
- Healthcare
- Digital infrastructure
- Transport
- Water supply
- Digital service providers
- Banking
- Financial market infrastructure
- Energy
- Waste water
- Health (pharmaceuticals, R&D, critical medical, devices)
- Space
- Public administration

IMPORTANT

- Providers of public electronic communications networks or services
- Chemicals
- Food producers, processors and distributors
- Manufacturing of critical products (medical devices, computers, electronics, motor vehicles)
- Digital providers (social networking platforms, search engines, online market places)
- Postal and courier services

How Identity and Access Management can underpin and enforce your NIS2 compliance

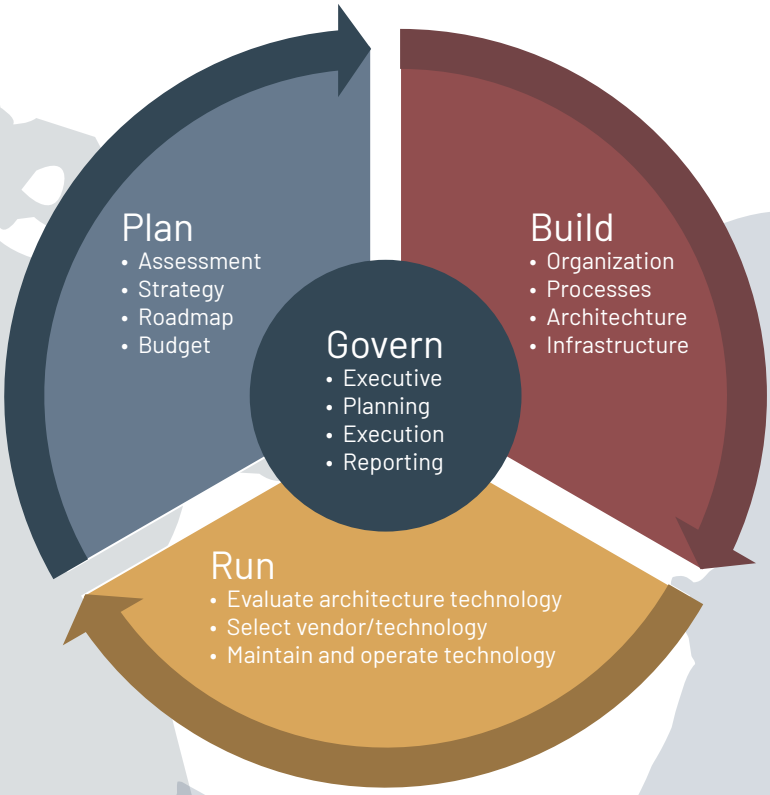
Identity and Access Management (IAM) refers to the processes, policies and technology used to manage and control access to digital resources. Thus, IAM plays a crucial role in enforcing the requirements of the NIS2 directive.



IAM processes properly supported by technology and governed by the organization can help:

- Establish and enforce roles and responsibilities by implementing granular access controls, monitoring user activity, and enforcing least privilege access policies.
- Secure authentication and authorization, ie. provide tools for managing strong authentication requirements such as multifactor authentication and password management policies, to reduce the risk of unauthorized access to network and information systems.
- Identify and respond to security incidents quickly and decisively by providing real-time monitoring and visibility into digital identity activity.
- Perform data mining for reporting purposes and employ advanced analytics (ML/AI based) to detect threats and identify potential cyber security and/or efficiency gains.

Overall, IAM serves as a critical component in enforcing the requirements of the NIS2 directive by enabling organizations to manage and control access to digital resources, identify security incidents, enforce compliance, and secure authentication.



Your IAM strategy

A comprehensive IAM strategy is fundamental for defending critical infrastructure against cyber security threats, and improve the overall organizational cyber security posture.

Developing that strategy, starts with the **Plan** phase and an assessment that will provide you with the direction and the decision making criteria for getting from here to being NIS2 compliant.

Once you know the direction you need to take, you can **Build** the tactical and operational foundation – the processes, policies and controls - for the IAM infrastructure necessary to implement your NIS2 (and Zero Trust) requirements.

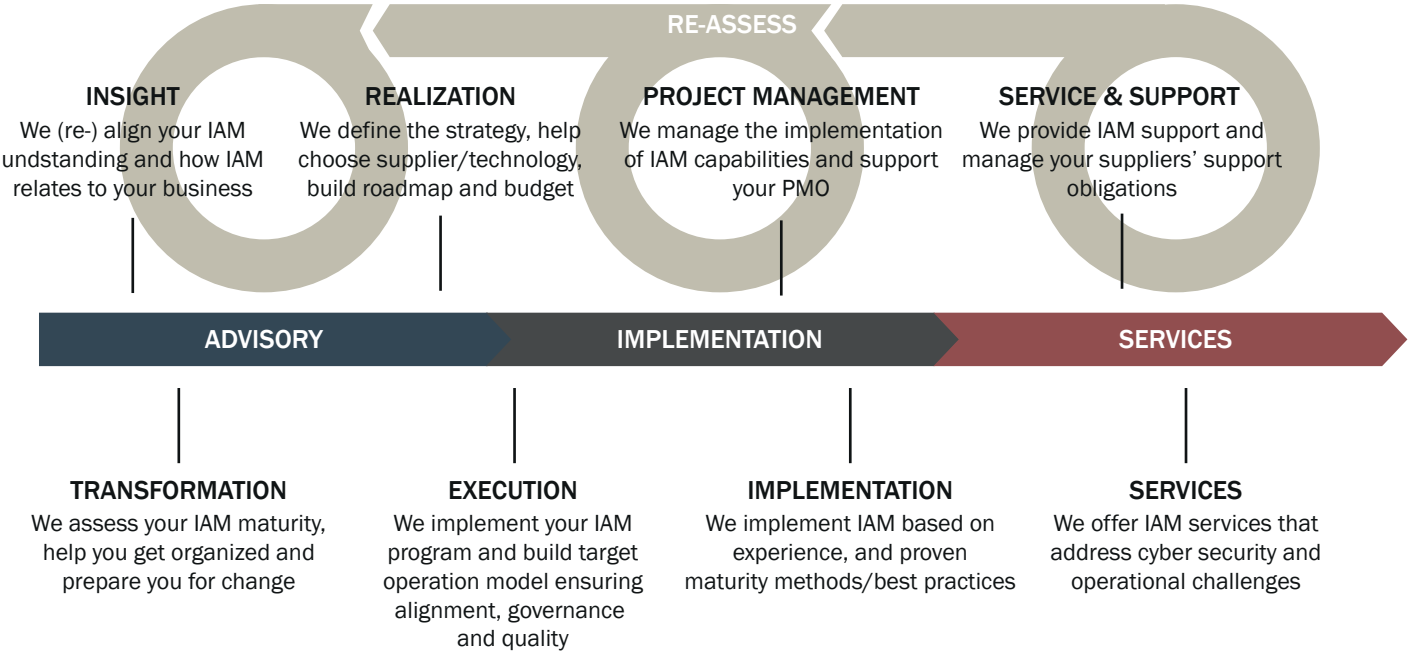
In the **Run** phase you may want to reach out to the market and select vendors/technology, implement technology, operate and maintain it.

An IAM program can help organisations address key NIS2 Article 21 requirements. Gartner research states that organizations without formal IAM program will experience 50% more project failures, cost 40% more and realize fewer business objectives.

How we assist you

ICY Security is a specialist in Identity and Access Management. With years of experience as consultants, vendors and customers we can help:

- Assess your present IAM situation, guide you towards your desired situation, plan, prepare and engage your organization through business-oriented Advisory.
- Extend, implement (or re-implement) your IAM requirements as well as manage your project streams, together with your and any other external (vendor) team in Implementation.
- Support your IAM operational requirements in Services.



Contact us for more information about NIS2 and how Identity & Access Management can underpin and enforce your way to NIS2 compliance.

Contact

+45 3150 3087
info@icysecurity.dk

ICY security
Part of Columbus