Omada

SOLUTION BRIEF

NIS2 and IGA

Stay compliant with Identity Governance and Administration

What is NIS2?

The NIS2 Directive is a European Union legislative framework designed to enhance the cybersecurity and resilience of critical infrastructure and services within its member states. NIS2 builds upon the original NIS Directive (Directive on Security of Network and Information Systems), which was the first EU-wide legislation on cybersecurity, by addressing some of its limitations and significantly expanding its scope and requirements.

What is IGA?

Identity Governance and Administration (IGA) is a cybersecurity domain that manages and controls digital identities and access rights across an organization. It combines identity management (IDM) and access governance to ensure that the right individuals have appropriate access to the right resources at the right times, and for the right reasons.

The intersection between NIS2 and IGA

The intersection of NIS2 and IGA lies in their mutual objective to strengthen cybersecurity and ensure the resilience of critical infrastructure and services.

Areas where NIS2 and IGA intersect:

1) Enhanced Security Requirements:

- **NIS2:** Requires organizations to implement comprehensive cybersecurity measures, including access controls, risk management, and incident response mechanisms.
- **IGA:** Provides the tools and processes to manage digital identities and access rights, ensuring that only authorized individuals have access to sensitive systems and data, which is a key component of the security measures mandated by NIS2.

2) Access Control and Identity Management:

- **NIS2:** Mandates strict access controls to prevent unauthorized access to critical systems and data.
- **IGA:** Ensures that access control policies are enforced consistently, managing who has access to what resources based on their roles and responsibilities, and regularly reviewing these access rights.

3) Risk Management and Governance:

- **NIS2:** Requires organizations to adopt a risk management framework to identify, assess, and mitigate cybersecurity risks.
- **IGA:** Supports risk management by providing visibility into access rights and potential vulnerabilities related to identity and access management, helping organizations identify and address risks associated with unauthorized access.

4) Compliance and Auditing:

- **NIS2:** Emphasizes the need for compliance with cybersecurity standards and regular audits to ensure adherence.
- **IGA:** Facilitates compliance by providing detailed audit logs and reports on access activities, helping organizations demonstrate compliance with NIS2 requirements during audits and classification.

5) Third-Party Risk Management:

- **NIS2:** Highlights the importance of securing the supply chain and ensuring that third-party providers meet cybersecurity standards.
- **IGA:** Manages third-party access by ensuring that external users and service providers are granted appropriate access rights and that these rights are regularly reviewed and monitored.

6) Employee Training and Awareness:

- **NIS2:** Requires organizations to implement training and awareness programs to enhance cybersecurity posture.
- **IGA:** Includes components that support training and awareness by educating employees on the importance of secure identity and access management practices.

7) Governance Framework:

- **NIS2:** Stipulates the need for a governance framework for cybersecurity that includes clear policies and oversight mechanisms.
- **IGA:** Contributes to the deployment of the NIS2 governance framework by defining roles and responsibilities for managing identities and access, ensuring that access policies are enforced and reviewed regularly.

NIS2 establishes a comprehensive framework to enhance the cybersecurity and resilience of critical infrastructure. IGA plays a crucial role in implementing these requirements by effectively managing digital identities and access rights. IGA is essential for embodying the NIS2 framework within organizations, achieving better control over who has access to critical systems and data, ensuring compliance with security standards, and reducing the risk of cyber incidents.

How to get there?

Omada's Global Advisory Practice consists of highly skilled and experienced professional advisors who are ready to support organizations to ensure their Identity Governance and Administration solution is fit for the NIS2 purpose. Through well-defined and proven service packages, Omada's Global Advisory Practice will help to identify, map, align, and document what is needed to comply with NIS2 within the IGA domain.