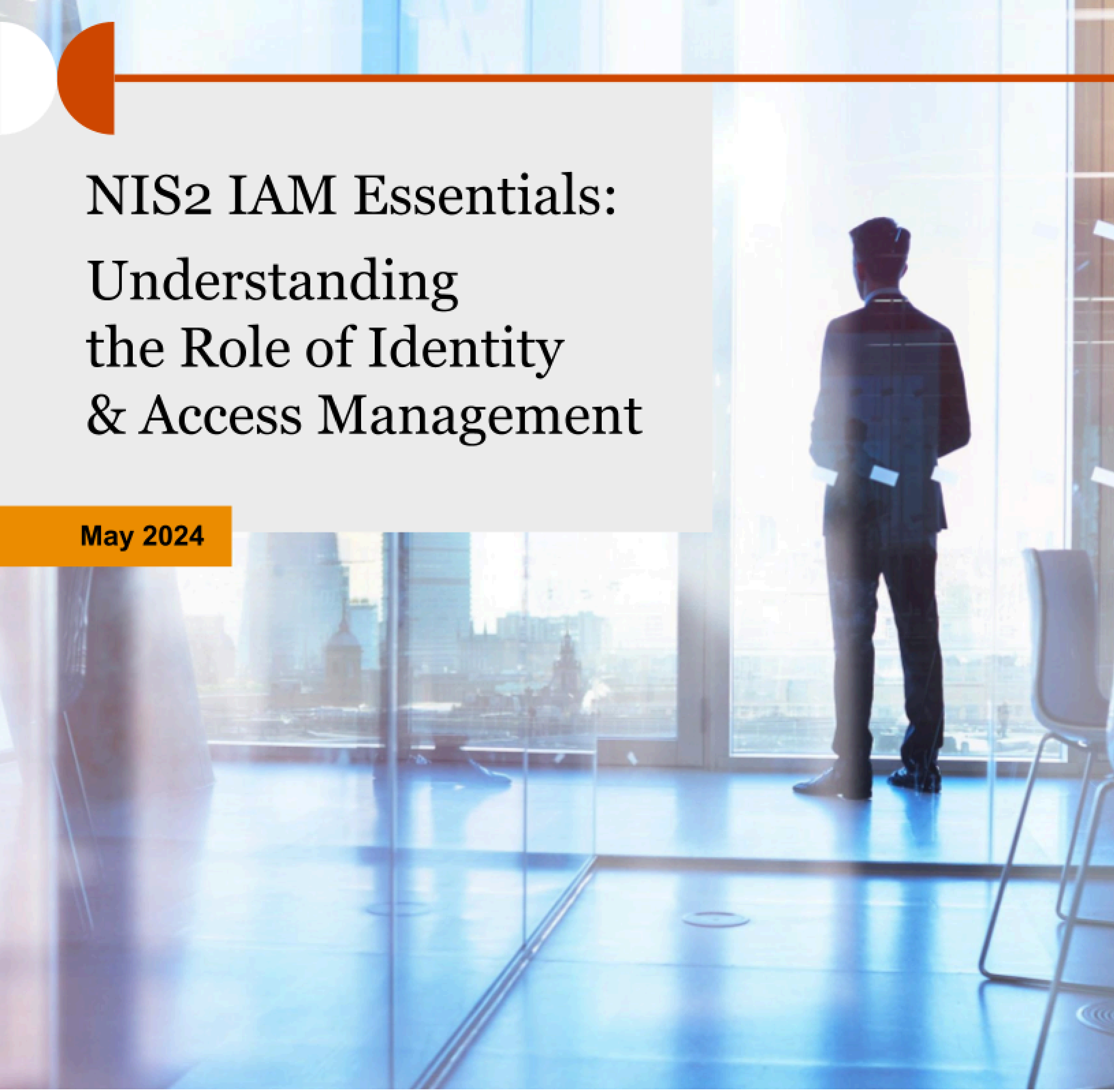
NIS2 IAM Essentials:

Understanding the Role of Identity & Access Management

May 2024



pwc

Introduction

The dawn of the Network and Information Security 2 Directive (NIS2) is coming. On the 17th of October, 2024, NIS2 will come into effect throughout all the European Union Member States, including Belgium. Meaning all organisations in scope must be compliant with the new directive which has broadened its original scope to heighten European security. Furthermore, NIS2 will be represented as best practices for European organisations, even when they are outside of the NIS2 directive scope. Whether your organisation is in scope or not, this whitepaper aims to share the essentials surrounding Identity and Access Management from the perspective of NIS2.

In this whitepaper, we will explore Seven steps that you can take right away to prepare for NIS2.

Note: If you are unsure whether your organisation falls under the scope, PwC has created a short survey that will inform you whether or not your organisation could fall under the NIS2 scope.

NIS2: Increased Stringency and Scope

Broader Scope: NIS2 extends its reach to sectors such as communications, digital services, critical manufacturing, and more.

Stronger Requirements: Essential entities must implement robust systems, policies, and best practices covering various areas like risk analysis, incident handling, and business continuity.

Subcontractors Included: NIS2 requirements now extend to subcontractors and service providers supporting critical organisations.

Stricter Incident Reporting: Initial notifications within 24 hours, assessments within 72 hours, and detailed reports within a month are mandatory for critical entities.

Costly Sanctions: Fines up to EUR 10 million or 2% of annual turnover can be imposed, with management potentially held liable.

Digital Identity and NIS2

Digital Identity offers a holistic approach to safeguarding an organisation's people, applications, and machines. It acknowledges that any user, whether human or non-human, can gain privileged access under specific conditions, potentially compromising systems, traversing networks, and executing attacks.

Digital Identity addresses these risks by:

Continuous Authentication and Authorization: Adhering to Zero Trust principles, it consistently verifies and authorises both internal and external users.

Robust Access Control: It rigorously governs access to on-premises and cloud-based resources.

Comprehensive Monitoring and Auditing: It closely observes user activities, ensuring compliance and providing audit trails.

A well-rounded Digital Identity strategy is essential for safeguarding critical infrastructure against threats like malicious attacks, ransomware, software supply chain vulnerabilities, and more. Such a program aids organisations in meeting key NIS2 Article 21 requirements related to incident handling and reporting, supply chain security, encryption technologies, access control policies, and Zero Trust security.

Key components of a complete Digital Identity strategy include:

Policy-Based Management: Safeguarding administrative credentials to protect privileged accounts and meet audit and compliance standards.

Privileged Session Isolation: Preventing malware propagation and reducing risk.

Just-in-Time Access: Minimising risks associated with credential theft.

Endpoint Privilege Security: Implementing the principle of least privilege to counter ransomware and malicious attacks.

Centralised Secrets Management: Securing application pipelines and mitigating software supply chain vulnerabilities.

Identity and Access Management (IAM): Preventing unauthorised access and enforcing role-based access controls.

Multi-Factor Authentication (MFA): Bolstering security for remote workers, vendors, and contractors while supporting Zero Trust principles.

A comprehensive Digital Identity program empowers organisations to enhance security, boost visibility, and fortify their readiness for NIS2 compliance.

The role of Digital Identity in NIS2

NIS2 requirement	How Digital Identity Helps
Ransomware Protection To Defend infrastructure against ransomware attacks	**Endpoint Privilege Security:** This strategy counters ransomware by revoking standing admin privileges from endpoints and governing application behaviour through policy enforcement. **Privileged Access Management:** This approach reduces risks by isolating, monitoring, and auditing privileged sessions, effectively preventing privilege escalation.
Mandatory Incident Reporting Critical Entities should be required to submit an early notification to report an incident in 24 hours	**Audit Trails and Privileged Session Recordings:** These offer documented evidence of cybersecurity incidents. **Digital Identity Intelligence:** Automatically detects and reports abnormal behaviours indicative of a breach. **Identity and Access Management (IAM) with AI and ML:** Automatically flags suspicious user activities. **Endpoint Privilege Security:** Automatically recognizes activities characteristic of attacks originating from endpoints.
Cyber Hygiene Policies for Infra Implement robust cybersecurity hygiene practices, encompassing password management and the governance of admin accounts with restrictions.	**Privileged Access Management:** Safeguards and governs admin accounts and credentials. **Identity and Access Management:** Ensures secure management and control of user passwords and access rights. **Endpoint Security:** Eliminates local admin rights and blocks privilege escalation.

Security of Utility Sector Secure interconnected digital utilities such as transportation, water supply, energy, and smart cities from cyberattacks.	**Privileged Access Management:** Counteracts attacks by isolating sessions, overseeing credentials, and facilitating just-in-time access. **Digital Identity Intelligence:** Automatically identifies unusual behaviours indicative of an attack. **Endpoint Privilege Security:** Shields against cyberattacks by revoking permanent admin privileges from servers and workstations while governing application behaviour. **Identity and Access Management:** Safeguards and manages user passwords, reducing the risk of credential phishing and theft.
Supply Chain Security Address supply chain security vulnerabilities	**Secrets Management:** Minimises software supply chain vulnerabilities by overseeing and regulating secrets. **Secrets Management:** Safeguards passwords, keys, and certificates utilised by applications, scripts, and other non-human entities across DevOps environments and CI/CD pipelines. **Secure, Just-in-Time Remote Access:** Enforces the principle of least privilege for external vendors, streamlining forensics and audit processes through session recording.
Good Cyber Hygiene practises for users Implement strong cybersecurity hygiene practices, incorporating Zero Trust principles and robust identity and access management. Embrace advanced technologies such as artificial intelligence (AI) and machine learning (ML) to bolster security measures.	**Multi-Factor Authentication (MFA):** Validates users in alignment with Zero Trust principles. **Just-in-Time Access:** Limits access to designated time frames, reinforcing Zero Trust principles. **Adaptive MFA:** Utilises AI-driven behavioural analytics and contextual data to select appropriate authentication methods for users based on specific situations.

Public electronic communications network security Implement end-to-end encryption along with data-centric security strategies, including cartography, segmentation, tagging, access policies, access management, and automated access controls.	**Audit Trails and Privileged Session Recordings:** Offer documented evidence of cybersecurity incidents. **Digital Identity Intelligence:** Automatically detects and reports abnormal behaviours indicative of a breach. **Identity and Access Management (IAM) with AI and ML:** Automatically flags suspicious user activities. **Endpoint Privilege Security:** Automatically recognizes activities characteristic of attacks originating from endpoints.

NIS2 versus frameworks and standards

Unlike standards like ISO/IEC 27001, CIS18, or NIST CSF, NIS2 doesn't explicitly mention IAM but emphasises Multi-Factor Authentication (MFA), continuous authentication, and logging. MFA alone isn't sufficient for compliance; organisations must demonstrate comprehensive IAM governance and adopt the Zero Trust concept.

The Importance of Logging, Auditing, and SIEM

Both the NIS2 directive and other standards emphasise the significance of having efficient logging and auditing practices. The logging system plays a crucial role in:

Incident Detection and Investigation: Analysing logs helps identify suspicious or unauthorised activities, providing vital clues for security investigations.

Compliance Audits: Logs are indispensable for demonstrating compliance with NIS2 and other standards.

Forensics and Zero Trust: Correlating logs from diverse sources (security devices, applications, IAM systems) within a Security Information and Event Management (SIEM) solution provides a centralised view. Enriching these logs with identity-related data from IAM and audit trails strengthens forensic analysis and supports Zero Trust principles by allowing you to spot access patterns and anomalies.

Data Privacy: It's essential to consider data privacy regulations like GDPR when handling security logs. SIEM solutions may offer features like data anonymization to protect sensitive information

Continuous Authentication: NIS2 allows for continuous authentication as an alternative to MFA. Continuous authentication goes beyond a single login check. It constantly assesses risk factors like:

User Behaviour: Deviations from typical patterns could flag potential compromise.

Device Health: Verifies device security posture (updates, anti-malware).

Location: Helps identify unusual access attempts

Continuous authentication strengthens the Zero Trust principle of "never trust, always verify."

Steps you can take in preparation

IAM Self-Assessment:

Start with a comprehensive self-assessment of your IAM. Include technical aspects, processes, policies, logging systems, audit trails, fallback plans, and stakeholders. Compare your findings to NIS2 requirements (specifically Articles 18-22) and develop an action plan.

Take steps to safeguard privileged access:

Adversaries can exploit privileged accounts to orchestrate attacks, take down critical infrastructure, and disrupt essential services. NIS2 advises critical entities to limit access to administrator-level accounts and to regularly rotate administrative passwords.

Strengthen your ransomware defences:

Costly and debilitating ransomware attacks are a major concern for EU regulators and one of the primary drivers of the NIS2 Directive. Introduce security solutions and best practices to proactively defend against ransomware. Use endpoint privilege security solutions to enforce the principle of least privilege, control applications, and augment next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions.

Move to a Zero Trust architecture:

Traditional perimeter-based security architectures, conceived to defend trusted enterprise network borders, aren’t suited for the world of cloud services and hybrid workforces. Adopt a Zero Trust approach, implementing several layers of defence such as least privilege access, continuous authentication, and threat analytics to validate all access attempts.

Scrutinise your software supply chain:

Supply chain attacks are a major concern for EU regulators and a prime motivator for the NIS2 Directive. Take a fresh look at your software supply chain and consider implementing a secrets management solution to mitigate risk.

Formalise your incident response plan:

NIS2 calls for faster incident reporting, with the first report due within 24 hours of an incident. Make sure your organisation is prepared. Review your event notification, information gathering, and reporting processes.

Educate your people:

Cybersecurity and cyber hygiene training are fundamental to NIS2. Step up your efforts to improve cyber awareness and foster a security-first culture.

How PwC Belgium can help

In addition to offering expertise in IAM solutions and governance, we possess extensive knowledge and experience in NIS2 regulations. Our unique blend of technical proficiency and regulatory understanding allows us to provide the best assistance to organisations striving for NIS2 compliance.

For further information, please contact one of our experts:

Sven Pauwels: sven.pauwels@pwc.com Director

Srujana Manukonda: srujana.manukonda@pwc.com Manager