garancy

egerer

WHITEPAPER

Turning Obligation into Advantage: NIS-2 and the Strategic Value of Identity & Access Management (IAM)

Content

Executive Summary

NIS-2 fundamentally changes how organizations must address cyber risk. Security measures are no longer just documented. They must be demonstrably effective. Nowhere is this more tangible than in Identity and Access Management (IAM). The NIS-2 Directive and its Implementation Act require unambiguous identification, strict adherence to the Need-to-Know principle, complete logging, and continuous monitoring of all digital identities. For many organizations, particularly in the midmarket, this represents a clear break from manual, organically grown processes.

As a result, Identity and Access Management is evolving from a peripheral technical topic into a strategic control instrument. Sound governance, clearly defined processes, and a robust role model form the foundation for managing risk and meeting regulatory requirements. At the same time, it becomes evident that beyond a certain level of complexity, these tasks can no longer be handled efficiently without automation.

A modern IGA solution such as Garancy ddresses precisely these requirements. It centralizes entitlement management, automates the entire identity lifecycle, supports auditable role models, and provides the historical transparency expected by supervisory authorities under NIS-2.

The core implication of NIS-2 is therefore clear: an IAM system that reliably governs access, documents every change in a verifiable manner, and makes risks visible at an early stage becomes a prerequisite for secure and resilient business operations.

> *Organizations that have already done their homework on information security and, for example, operate an ISMS based on ISO 27001, are starting from a very strong position when it comes to implementing NIS-2.*

David Capriati
Managing Consultant – Business Resilience Consulting
egerer Consulting GmbH

1. NIS-2: A Pan-European Framework for Cyber Resilience

1.1 NIS-2 Makes Cyber Risk Management Mandatory

The **"EU Directive on measures for a high common level of cybersecurity across the Union – (EU) 2022/2555,"** commonly referred to as NIS-2, is far more than a simple update of its predecessor. While the earlier directive remained largely ineffective in practice, NIS-2 introduces enforceable and far-reaching requirements. It marks a fundamental shift toward a **uniform, binding, and above all proactive approach to cybersecurity risk management across the EU.**

NIS-2 does not merely require organizations to react to security incidents. It obliges them to ensure comprehensive and robust information security. The path to that goal is clearly outlined: affected entities must significantly strengthen the resilience of both their organizational processes and their IT operations.

1.2 The Core Areas of NIS-2

Risk management sits at the heart of NIS-2. It is aligned with established standards such as ISO 31000 for general risk management and the more specific cybersecurity risk management framework of ISO/IEC 27001 that builds on it.

The objective is to identify, assess, evaluate, and treat risks using standardized methodologies. While terms such as risk score, probability of occurrence, or risk acceptance criteria may sound daunting at first, NIS-2 does not reinvent the wheel. If risk management is not already firmly established company-wide, chances are good that individual organizational units already practice standards-based risk management and that existing approaches can be leveraged. However, NIS-2 goes one step further, again aligning with relevant information security standards. The directive also covers the following areas:

1. **Governance**
   This includes the strategic anchoring and organizational setup of information security. NIS-2 places particular emphasis on executive liability and requires management to participate regularly in cybersecurity training. This ensures that the risk management strategy is supported at the highest level and backed by appropriate resources.
2. **Incident Management**
   If preventive measures fail, clear rules for handling serious security incidents are essential. NIS-2 defines what constitutes an incident and establishes mandatory reporting obligations to supervisory authorities.
3. **Business Continuity Management**
   If a cyber incident escalates into a crisis, predefined emergency plans and expanded decision-making authority help organizations return to normal operations more quickly. NIS-2 sets explicit requirements in this area as well.
4. **Technical and Organizational Cybersecurity Measures**
   This category encompasses the concrete cybersecurity requirements defined by NIS-2, ranging from employee awareness training and supply chain security to access management.

1.3 Scope: NIS-2 Sectors and the Focus on Digital Economy

One implicit goal of the NIS-2 Directive is to establish a consistently high level of cybersecurity across a broad range of industries. Accordingly, the directive applies to 18 sectors. Organizations with as few as 50 employees or EUR 10 million in annual revenue or balance sheet total may already fall within scope. While NIS-2 differentiates between essential, important, and critical (KRITIS) entities, this classification has limited impact on the actual obligations.[1]

In addition to traditional critical infrastructure sectors such as energy, transport, and healthcare, **NIS-2 significantly expands its reach into the digital economy.** NIS-2 Annexes I and II explicitly include:

- **Managed service providers** (MSPs)
- **Cloud computing service providers** (IaaS, PaaS, SaaS)
- **Data center service providers**
- **Online marketplaces, search engines**, and **social networks**

Given the systemic importance of highly interconnected digital services, the EU Commission adopted a supplementary legal act for this sector.

While NIS-2 defines a broad framework, it often remains intentionally high-level, leaving room for interpretation. The **NIS-2 Implementation Act (EU) 2024/2690** closes this gap by specifying the directive's requirements in much greater detail. For organizations covered by Annexes I and II, this means that the general requirements of NIS-2 are superseded, where applicable, by the more specific obligations of the Implementation Act. These technical and organizational measures (TOMs) are no longer optional best practices.

Unlike a directive such as NIS-2 in general, an EU regulation such as (EU) 2024/2690 does not require national transposition. **As a result, the NIS-2 Implementation Act has been legally binding since its adoption in 2024.**

2. NIS-2 Obligations in Identity and Access Management

2.1 NIS-2 and the "State of the Art"

With the introduction of the NIS-2 Implementation Act, it becomes clear that for organizations within scope, many organizational and technical requirements move from theory into concrete practice. Numerous topics within the area of technical and organizational measures that remained abstract in the NIS-2 Directive are transformed by the Implementation Act into actionable obligations.

The directive itself nevertheless remains the starting point, as it pursues the overarching objective of "strengthening digital resilience through effective cybersecurity risk management." In practice, this objective is realized through targeted measures designed to reduce identified risks. As the digital land-

[1] For more details on the NIS 2 thresholds, the associated distinction between essential and important entities, the resulting obligations, and an interactive impact assessment, please visit: *https://egerer-consulting.de/leistungen/business-resilience/nis-2.*

scape and the associated cybersecurity risks and threats are constantly evolving, the directive contains deliberately concise wording with far-reaching implications:

„The [...] measures must – taking into account the state of the art [...] – ensure a level of security for network and information systems that is appropriate to the existing risk."

Directive (EU) 2022/2555, Art. 21 (1)

This opening phrase allows the directive to outline general areas of action while mandating that all measures comply with the state of the art. Due to paragraphs i and j of Article 21 (2), this explicitly includes **access control concepts** and solutions for **multi-factor or continuous authentication.** This represents one of the most concrete technical obligations set out in the directive as a whole.

While the requirement itself is clearly articulated, the NIS-2 Directive provides limited guidance on how it should be implemented in practice. Some additional orientation can at least be found in the introductory recitals which include the following clarification:

„Essential and important entities should apply a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management [...].

Directive (EU) 2022/2555, Recital 89

This is precisely where the NIS-2 Implementation Act comes into play. With its comprehensive set of detailed provisions, it translates abstract requirements into actionable guidance. Once again, this reflects NIS-2's alignment with established international standards: For example, ISO/IEC 27001, intentionally framed at a high level, only becomes truly tangible and implementable when combined with the specific controls defined in ISO/IEC 27002.

2.2 Identity and Access Management Under the NIS-2 Implementation Act

Building on the requirement to implement risk-mitigating measures in line with the state of the art, the legislator's expectations finally become tangible through the Implementation Act. The detailed

provisions can be found in the extensive Annex ("Technical and methodological requirements pursuant to Article 2 of this Regulation"), specifically under Section 11, **"Access control (Art. 21 (2), letters i and j of Directive (EU) 2022/2555)."**

As expected for anyone familiar with ISO/IEC 27001 and related standards, the first requirement is a formal concept designed to firmly anchor Identity and Access Management within the organization.

Section 11.2, **"Management of access rights,"** mandates strict adherence to the Need-to-Know principle. Simply following documented workflows is not enough. Organizations must also ensure that access for external parties is limited in scope and duration. Maintaining a register of granted access rights and logging all related activities is explicitly required (see (EU) 2024/2690, 11.2.2. d–f).

Overview:

Regulation (EU) 2024/2690	Focus of the Requirement
11.2.2. d (External Identities)	Controlled access for third parties (suppliers, service providers) with limited scope and duration
11.2.2. e and f (Protocol Logging)	Maintaining a register of authorizations and logging of access rights
11.5.2. a and b (Identification)	Unique identifiers for systems and users that are linked to a single person
11.5.2. c and d (Monitoring)	Monitoring of identifiers and documentation of all activities related to Identity Management

Section 11.5, **"Identification,"** introduces even more demanding requirements. Organizations certified under ISO/IEC 27001 may barely pause at the requirement for individual user IDs, having long since moved away from the convenience of shared user accounts.

The obligation for continuous monitoring, clearly outlined in c and d, is anything but a one-time task. It effectively requires **comprehensive monitoring and documentation of all (digital) identities across the organization** (see (EU) 2024/2690, 11.5.2. a–d).

2.3 Synthesis: A Strict Burden of Proof

Organizations that are subject to the NIS-2 Implementation Act must be able to answer the following questions with precision:

- → **Who** had access to **which** systems and data, and **when?**
- → **Who** had their access rights revoked and **when?**
- → **How** was the entire lifecycle documented?

These IAM obligations defined in Regulation (EU) 2024/2690 go far beyond policies and conceptual frameworks. Without supporting state-of-the-art tools, continuous monitoring and logging – repeated throughout NIS-2 – are difficult to achieve in practice.

3. Strategic Steps to Achieve NIS-2 Compliance: The Consulting Perspective

Implementing NIS-2 obligations is not the responsibility of IT. Rather, it should be clear from the above that achieving NIS-2 compliance is a strategic implementation project. The overall goal is to identify and close the gaps between legal requirements and the organization-wide status quo.

3.1 Assessment

The first step toward NIS-2 compliance in IAM should always be a realistic assessment:

1. **The governance framework**
   Is there a policy that defines IAM fundamentals in line with NIS-2, including responsibilities, accountabilities, and principles such as Least Privilege?
2. **The processes**
   What do current IAM workflows look like? Who can initiate user provisioning/deprovisioning or entitlement assignments, who executes, who controls?
3. **Technical/administrative implementation**
   How are identities actually created, access rights set, and how are documentation and a consolidated "single view" ensured?

3.2 Governance and Processes: The Foundation for a Healthy "Identity Landscape"

Technical solutions without clear governance quickly fall short, especially under NIS-2. Ultimately, it's all about managing cybersecurity risk. The requirement for state-of-the-art measures is not an end in itself. It is intended to reduce risks to information security.

The first step should therefore be to establish a robust set of rules, for example in the form of:

- → **Role concepts:** Developing roles that follow the Least Privilege principle. The goal is to grant users only the permissions they need for their current tasks, no more and no longer.
- → **Identity lifecycle:** Implementing clear, automated workflows. Especially when employees leave, immediate and complete revocation of all access rights must be ensured to eliminate the risk of orphaned or unauthorized accounts.
- → **Access recertification:** Regularly verifying whether assigned rights are still required. This is key to reducing excessive permissions that accumulate over time. The well-known "permission creep" must be avoided.

3.3 The Challenges of Growing Organizations: Scaling and Audit Readiness

Many upper midmarket companies on the path to becoming an enterprise face a dilemma: Their complexity is already too high for continued manual control, but their resources for large, monolithic enterprise security suites are limited.

The commonly observed starting situation in IAM: Basic cybersecurity structures such as policies and (C)ISO roles exist, but large parts of the IT landscape (and therefore IAM) are fragmented.

Over time, different organizational units have developed their own ways of "handling things," and access approvals are processed via email, Excel spreadsheets, and/or decentralized tools.

Bottom line: Manual procedures are still widely used. And these procedures are poorly aligned with the requirements emerging from NIS-2:

Problem	NIS-2 Risk
Lack of scalability	Large headcounts and frequent role changes create an unmanageable entitlement landscape and outdated permissions.
Susceptibility to errors	Manual joiner, mover, and leaver processes are error-prone; accounts of former employees remain active.
Lack of transparency	Missing centralized documentation makes proof (e.g., under 11.2.2. e) impossible.
Increased attack surface	Undetected over-privileging (access creep) provides ideal entry points for lateral movement attacks.

4. Interim Conclusion: IAM and NIS-2 Without Automation Will Be Difficult

By now it should be clear: without technical solutions that automate processes and provide tamper-proof, audit-ready logging, it becomes nearly impossible beyond a certain organizational size to fully meet the requirements of the NIS-2 Implementation Act. For the IAM domain in particular, technical solutions are almost mandatory to:

- → **provide complete documentation** across the entire identity and access lifecycle,
- → **reduce the attack surface** through strict access principles (Least Privilege), and
- → **ensure auditability** for supervisory authorities.

Establishing a governance framework and effective processes still comes first. Once that is in place, a suitable IAM solution can be selected and implemented. It then ensures efficient, secure, and audit-proof fulfillment of regulatory obligations.

In the following section, we show how a modern IAM platform can overcome the challenges described above. You'll learn how the right technology helps you meet NIS-2 requirements and sustainably strengthens your organization's cyber resilience.

5. Garancy: The Technical Implementation

The following section illustrates how the regulatory and organizational requirements outlined above can be put into practice using Garancy.

The examples demonstrate how an IGA solution not only ensures compliance, but also helps address many of the structural challenges described in Chapters 2 and 3, such as fragmented processes, limited transparency, and increasing pressure to provide audit-ready proof of entitlements.

5.1 The Role of IGA in Modern Identity Management

Modern Identity Management, also referred to as IAM, consists of three complementary segments with clearly separated functional areas: IGA, AM, and PAM.

Access Management (AM) is primarily responsible for authentication methods (Single Sign-On, MFA) and enforcing access decisions. For this purpose, Identity Providers (IdPs) are provided, which applications connect to via standard protocols. **Privileged Access Management** (PAM) addresses the specific risks of privileged administrative accounts. **Identity Governance & Administration** (IGA) focuses on controlling which identity receives which permissions and for what reason.

Garancy is fully positioned in the IGA segment. It manages identities, roles, and entitlements across all connected target systems and ensures that only verified, traceable, and approved access is created.

These functions form a central foundation for ensuring the unambiguous identification required by regulations, restricting access to what is necessary, and guaranteeing full traceability of the entire entitlement lifecycle.

Garancy therefore takes on the task of implementing the organizational and technical concepts that are indispensable for modern, risk-oriented identity management: transparency, entitlement control, automation, and auditability. The governance and process requirements outlined above are thus not merely described on paper but technically enforced and transferred into daily operations.

5.2 Centralized Management and Control of Entitlements

The ability to centrally manage identities and entitlements across systems is a key prerequisite for reliable and legally compliant entitlement management. Garancy acts as the central authority and consolidates all relevant information in one place. Communication with target systems is handled via suitable connectors, enabling both read and write data flows.

As early as the onboarding of a target system, an **initial load** imports all existing users (accounts) and their entitlements in full, giving Garancy an **accurate representation of the current state.** This dataset can be regularly reconciled with the live data of connected systems using Live Balancing (Reconciliation) to ensure consistency. Garancy can detect discrepancies between desired and actual states and correct them automatically based on rules.

Provisioning ensures that all changes approved by Garancy are implemented directly and consistently in target systems. This prevents outdated or manually created entitlements from persisting without control or documentation. The result is a centrally orchestrated entitlement landscape that is clearly structured, traceable, and continuously up to date. This creates exactly the transparency and traceability required by NIS-2 and the Implementation Act in the form of an up-to-date register of all access and access rights (see 11.2.2. e and f).

5.3 Role Models as the Foundation for Need-to-Know

An **effective role model** is the decisive lever for enforcing the **Need-to-Know principle** over the long term. Garancy consistently implements this principle through business roles that translate business activities into clearly defined entitlement packages.

Roles abstract the often highly technical permissions of target systems and make them understandable and governable for business departments. As a result, entitlement assignment is no longer driven by individual decisions based on technical details, but by a business-understandable logic. Each role represents a clearly defined task profile. A person receives only the role required for their current responsibilities.

The role model itself is developed in a structured way. To ensure baseline access, fundamental permissions are bundled into base roles, for example by department or job function. Additional specialized or exceptional tasks are mapped through separate roles. Using role mining to analyze real entitlement data helps identify patterns from which additional roles or optimizations of the existing model can be derived.

The result is a consistent, maintainable role model that not only enforces the need-to-know principle effectively, but also strengthens business ownership and reduces technical complexity to a controllable level.

5.4 Automated Identity and Entitlement Processes

Secure Identity Management requires an **automated end-to-end lifecycle** that covers all phases from onboarding through transfers to offboarding, while also accounting for temporary absences such as parental leave, sabbaticals, or annual vacation. Garancy provides **fully automated processes** for this. Typically, an HR system supplies the required data on internal employees on a daily basis.

New employees are detected automatically and immediately equipped with the necessary roles and accounts so they can work from day one. If organizational conditions change, for example due to a department transfer or a new function, Garancy adjusts assigned roles and entitlements immediately and withdraws any access that is no longer required.

When an employee leaves, all accounts across all connected systems are reliably disabled or deleted. This prevents orphaned access, which represents a relevant security risk in many IT landscapes. The previously described issue of manual, error-prone onboarding and offboarding is therefore sustainably mitigated.

External personnel are subject to especially strict controls, as their access often may only be granted for a limited time. Garancy supports **time-bound roles and automatically expiring entitlements,** allowing access duration and scope to be governed precisely. Information on external personnel can be provided via additional source systems or, alternatively, entered manually via a workflow.

In Garancy, **persons, identities, and accounts are clearly separated** from one another. This ensures that every entitlement is unambiguously assigned to a natural person. This is a mandatory prerequisite for transparency and traceability as well as for Segregation of Duties (SoD) requirements. At the same time, this unambiguous mapping meets the Implementation Act's expectations regarding the identification and monitoring of identifiers (11.5.2. a–d) described in Chapter 2.2.

5.5 Continuous Review and Validation of Access Rights

Continuous control of access rights and permissions is indispensable to ensure that a person's actual rights always match their current responsibilities within the organization. Garancy supports this process through **configurable recertification campaigns.** These can be performed at the individual level as well as at the role level.

When reviewing individuals, the organization assesses whether assigned roles are still required. This allows **outdated or unnecessary access to be removed reliably.** In parallel, roles themselves are reviewed regularly. This includes analyzing whether the permissions contained in a role still match the needs of the corresponding task or whether cleanup is required.

This continuous review prevents excessive or inappropriate entitlements from accumulating over time. The goal is primarily to reduce the attack surface, but also to mitigate insider threats and privacy violations. At the same time, it creates **transparency for business departments and security stakeholders** and forms an important building block for low-risk, controlled operations of the overall entitlement landscape. IGA thus supports exactly the continuous, risk-reducing measures required in Section 2 and essential for a robust security level.

5.6 Full Transparency Through Historical Audit Trails

A key characteristic of an effective IGA system is the ability to precisely capture, log, and historically analyze all security-relevant events. Garancy ensures that **all changes to persons, roles, accounts, and permissions are fully documented.** This enables fact-based answers to the essential questions: "Who accessed what and when? Who granted or revoked access rights and permissions? How was it documented?"

The collected log data is fed into the Access Intelligence Manager (AIM), which stores and correlates the data in a structured data warehouse. This creates a **complete history of the entitlement landscape.** Organizations can trace at any time which entitlements existed at a given point, who performed the change, and how roles and identities evolved over time.

This transparency not only enables reliable fulfillment of legal proof obligations. It also provides significant operational value in security management, for example, when investigating incidents, conducting internal audits, or preparing for external audits.

6. Efficient Implementation and Support in the Midmarket

Many mid-sized companies are confronted with increasing regulatory and technical complexity but do not have the resources for large-scale IAM programs. Garancy is therefore designed to become **operational in a short time** while providing a robust foundation for future expansion stages.

Predefined governance models, proven integration patterns for common target systems, and clearly structured role models significantly shorten time to value. Complementary services such as role design consulting, support in defining responsibilities, or assistance with technical onboarding for complex systems further ease adoption.

The "start fast, expand later" approach enables companies to establish a functioning, audit-ready entitlement management capability within a short timeframe that meets regulatory requirements while creating a sustainable foundation for future development.

7. Conclusion

A **modern IGA solution like Garancy** is far more than a technical tool. It translates regulatory requirements from NIS-2 into operational practice and creates the **foundation for resilient, scalable, and auditable Identity & Access Management.** Garancy combines centralized control, transparent role models, automated processes, and continuous oversight into a consistent overall picture that supports both security and efficiency.

This makes one thing clear: the NIS-2 requirements described above can only be met sustainably when governance and technology work together. Garancy provides the right technical foundation for this and makes NIS-2 not only achievable, but manageable.

Contact us to learn more about our software. Garancy can be customized and is available both on-premise and in the cloud.

https://garancy.com/

NIS-2 compliance starts with the right strategy. Combining regulatory expertise with technical implementation know-how, **egerer Consulting** supports organizations in translating NIS-2 requirements into pragmatic, effective measures.

https://egerer-consulting.de/leistungen/business-resilience/nis-2