SecurityBridge

Whitepaper

NIS2 Requires Complete Security Coverage. SAP Included.

What NIS2 means for governance and compliance in SAP environments

Table of Contents

Executive Summary	3
From Policy to Proof	3
Article 20: Governance and Personal Accountability	4
The SAP Blind Spot	4
So What Does NIS2 Require Organizations to Demonstrate in Practice?	5
From SAP Risk to NIS2 Evidence	5
NIS2 is a Shared Responsibility	6
How SecurityBridge Supports NIS2 Governance and Compliance for SAP	7
Underneath the Governance Layer: How the Evidence is Produced	8
Conclusion	9
About SecurityBridge	10

Executive Summary

The NIS2 Directive aims to strengthen cybersecurity resilience across essential and important entities in 18 critical sectors, including energy, transport, banking, healthcare, digital infrastructure, and manufacturing. It establishes a common set of cybersecurity requirements across the EU, backed by regulatory oversight and enforcement. For affected organizations, this raises expectations around how cybersecurity risks are governed, monitored, and reported.

For organizations whose most critical business processes run on SAP, these requirements have significant implications. SAP systems typically handle critical financial, operational, and supply-chain data, yet SAP security often remains disconnected from the wider cybersecurity program.

Article 20 brings cybersecurity directly into the governance discussion by placing accountability on members of the management body. For organizations running SAP, a gap in SAP coverage is no longer just a technical oversight. It is a documented governance failure.

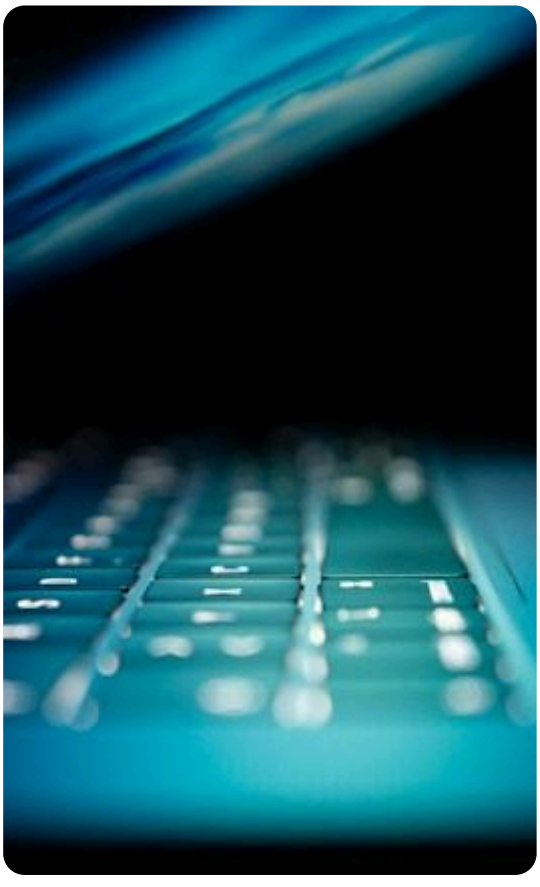
This paper is intended for the people responsible for that oversight: board members, CISOs, compliance officers, and internal audit teams. It explains why SAP security matters for NIS2 governance, what different stakeholders need to demonstrate their responsibilities, and how an SAP-native platform can support continuous, audit-ready evidence. For teams looking for greater technical detail, it also points to the underlying capabilities behind that evidence.

From Policy to Proof

Most organizations already have cybersecurity policies and established frameworks. NIS2 goes further by requiring organizations to demonstrate that the measures behind those policies are implemented, operating, and subject to appropriate oversight.

This shifts the focus from documented intent to evidence. A written policy alone does not demonstrate that control is working in practice. Organizations need to be able to show that cybersecurity measures are implemented and functioning as intended.

Article 20 makes this particularly relevant at the governance level. Cybersecurity governance is not simply a prerequisite for compliance. Management bodies are expected to approve cybersecurity risk-management measures, oversee their implementation, and be able to demonstrate that oversight.



Article 20: Governance and Personal Accountability

Article 20 requires the management body of an in-scope organization to approve the cybersecurity risk-management measures taken under Article 21, to oversee their implementation, and be accountable for failures in that oversight. Members of the management body must also receive training that enables them to assess cybersecurity risks and risk-management practices.

Two important consequences follow:

- Accountability sits with members of the management body, rather than cybersecurity being treated solely as an operational responsibility.
- Approval and oversight need to be demonstrable. Organizations need to be able to show that cybersecurity risks and the measures used to address them are being appropriately reviewed and overseen.

This is where SAP becomes particularly relevant. For many enterprises, SAP supports some of the most sensitive financial, operational, and supply-chain processes. Yet responsibility for SAP often sits with specialized technical teams outside the security organization's usual reporting structures.

If SAP risk is not included in the broader cybersecurity picture presented to management, that can leave an important gap in governance and oversight.

The SAP Blind Spot

Most organizations monitor SAP separately from the rest of their security program. NIS2 does not allow for that separation.
Security teams have visibility across endpoints, cloud, networks, and identity. But that visibility often stops when activity reaches the SAP application layer.

In SecurityBridge's own market research, security leaders describe this gap in clear terms:

> *"We go completely blind the second traffic hits the SAP landscape."*
>
> — CISO, Banking (SecurityBridge Market Survey, 2026)

> *"We have thousands of ABAP custom developments piling up and no efficient way to scan them for backdoors or insecure coding."*
>
> — CISO, Logistics (SecurityBridge Market Survey, 2026)

This gap has always represented a security risk. Under NIS2, it also becomes relevant to governance. An organization that reports comprehensively on network and endpoint security but lacks equivalent visibility into SAP may struggle to provide a complete view of cybersecurity risk.

So What Does NIS2 Require Organizations to Demonstrate in Practice?

From SAP Risk to NIS2 Evidence

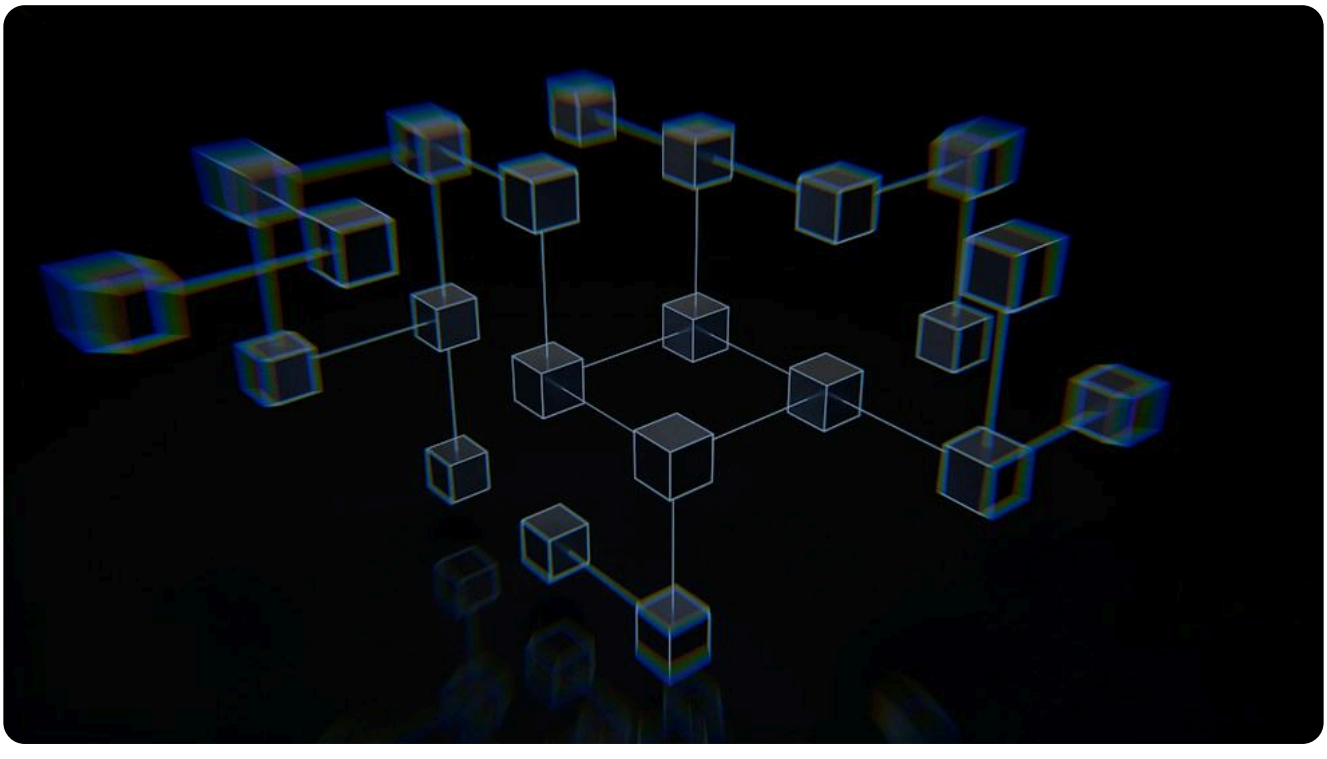
Article 21 sets out ten categories of cybersecurity risk-management measures, covering areas such as risk analysis, incident handling, access control, encryption, and supply-chain security. Article 23 introduces reporting obligations for significant incidents, beginning with an early warning within 24 hours of becoming aware of the incident.

For organizations running SAP, meeting these obligations requires more than policies and periodic assessments. They need evidence that relevant controls are operating and that security-relevant activity can be identified and investigated.

This is particularly important at the SAP application layer. Generic security tooling can monitor networks and endpoints, but it does not necessarily provide the context required to understand what is happening inside SAP systems.

One boundary is important to make clear: SAP-layer monitoring can provide signals relevant to availability and change control, but backup infrastructure, system replication, failover, and full disaster recovery orchestration remain the organization's responsibility. An SAP security platform does not replace these broader resilience measures.

What organizations need from SAP security also differs depending on who is responsible for using that information.



NIS2 is a Shared Responsibility

NIS2 involves multiple stakeholders across the organization, each with different responsibilities and evidence requirements.

For the Board

The board's responsibility under Article 20 is centered on governance and oversight. The organization needs to be able to demonstrate that cybersecurity risk, including relevant SAP risk, is being reviewed and appropriately overseen.

An annual policy sign-off alone does not provide the complete picture. Management needs reliable information about the organization's current risk posture and a structured basis for responding if an incident requires regulatory disclosure.

For the CISO

The CISO is responsible for the wider cybersecurity program but often does not directly manage SAP, which typically sits with dedicated SAP Basis or security teams.

The CISO therefore needs visibility into SAP security risk that can be incorporated into the wider cybersecurity and risk-management program. This includes relevant risks across SAP environments, including components managed under RISE with SAP.

SAP security should not operate as a separate and disconnected stream of information.

For Compliance

Compliance teams need to provide evidence when auditors or national authorities request it.

For SAP, this means maintaining a reliable evidence trail that supports relevant Article 21 measures and Article 23 obligations. Rather than collecting evidence manually when an audit begins, organizations benefit from evidence that is generated and maintained continuously.

For Internal Audit

Internal audit needs to assess whether controls are operating effectively, not simply whether they have been documented.

For SAP, this requires reliable, system-generated information that allows auditors to independently assess relevant controls and security activity rather than relying solely on assurances from the teams operating the systems.

These stakeholders have different responsibilities, but they share one underlying requirement: reliable SAP security evidence that can support governance, risk management, compliance, and audit.

How SecurityBridge Supports NIS2 Governance and Compliance for SAP

SecurityBridge is the only cybersecurity platform built natively inside SAP – complete, fully integrated, and built to act, not just alert. It unifies prevention, detection, and response on one shared data layer, giving organizations real, in-system control over their most critical business systems. For NIS2, this provides management, security, compliance, and internal audit with the SAP-layer visibility, monitoring, and evidence they need to support governance and compliance requirements.

For the board, this provides documented insight into SAP risk and the evidence needed to support oversight. For the CISO, SAP risks become part of the wider cybersecurity and risk-management program rather than remaining a separate blind spot. For compliance teams, evidence is generated continuously instead of being assembled when an audit begins. For internal audit, system-generated data provides an independent basis for assessing whether relevant controls are operating as intended.

SecurityBridge fully covers nine of the ten risk-management measures set out in Article 21 and supports the reporting obligations under Article 23 at the SAP layer. Real-time SAP-layer detection provides structured, contextual data that can support the 24-hour early-warning requirement and feed directly into existing SOC and SIEM workflows.

Because SecurityBridge runs natively inside SAP, security controls can do more than identify risk. They can act directly
inside SAP across access, identity, configuration, and change, helping organizations move from reactive monitoring to continuous control.

SecurityBridge protects more than 8,000 SAP production systems globally across hundreds of enterprise customers.

SecurityBridge does not make an organization NIS2 compliant on its own. Compliance remains the responsibility of the organization and depends on its wider governance and cybersecurity risk-management program. SecurityBridge provides the SAP-layer visibility, controls, monitoring, and evidence needed to support that program.



Underneath the Governance Layer: How the Evidence is Produced

The evidence trail, real-time monitoring, and support for relevant NIS2 requirements described in this paper are enabled by purpose-built security capabilities operating within SAP.

A board member or compliance officer does not need to understand the mechanics of RFC monitoring or ABAP code analysis to use the resulting evidence. Technical teams and auditors, however, may need to understand where that evidence comes from.

SecurityBridge provides capabilities including:

- Threat detection and vulnerability management, supporting the identification and monitoring of SAP security risks and incidents.
- Code vulnerability analysis and patch management, helping identify security risks in custom code and known SAP vulnerabilities.
- Privileged Access Management and Identity Protection, supporting controls around privileged access, authentication, and high-risk activities.
- SIEM integration with platforms such as Splunk, Microsoft Sentinel, and IBM QRadar, allowing SAP security events to become part of the organization's existing security operations.
- Coverage for relevant RISE-managed components, helping maintain SAP security visibility as organizations move to cloud-hosted SAP environments.

A companion technical whitepaper covers this layer in greater detail, including the control-level mapping to Article 21's ten measures, how detection and evidence collection work within SAP, and the specific boundaries of coverage.

For SAP security architects, Basis teams, and technical auditors, it provides the technical detail behind the governance and compliance considerations outlined in this paper.

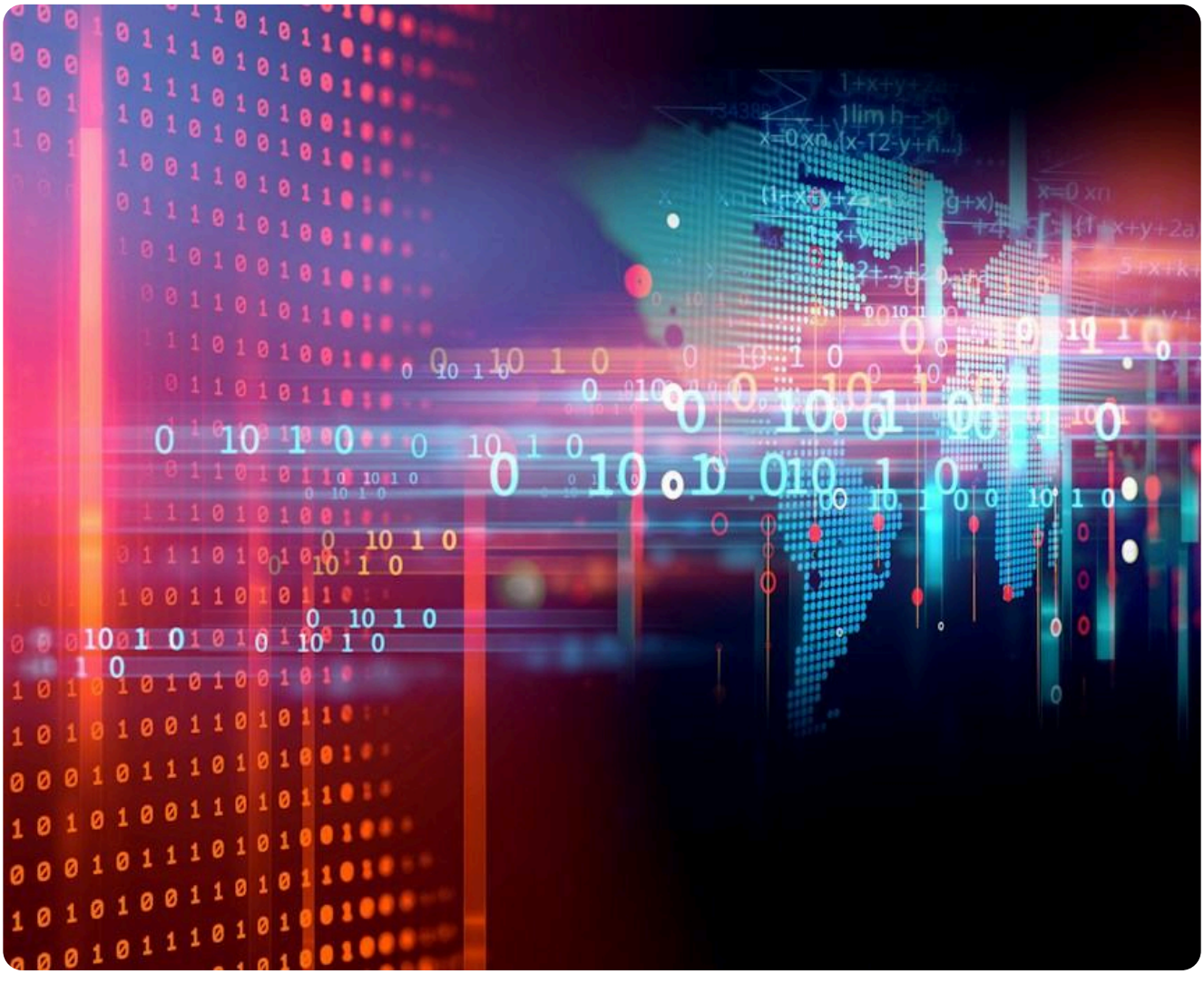
Conclusion

NIS2 does not require organizations to reinvent cybersecurity governance. It raises the expectation that organizations can demonstrate how cybersecurity risks are managed and how relevant measures operate in practice across the systems their businesses depend on.

For many enterprises, SAP is one of those systems.

Closing the SAP governance gap therefore requires more than an SAP security policy or periodic assessment. Boards, CISOs, compliance teams, and internal audit need reliable visibility into SAP risk and access to evidence that supports their respective responsibilities.

By bringing SAP security monitoring, risk visibility, and evidence into a shared platform, organizations can better integrate SAP into their wider NIS2 governance and cybersecurity risk-management program.



About SecurityBridge

SecurityBridge is the leading provider of a comprehensive, SAP-native cybersecurity platform. Trusted by organizations worldwide to safeguard their most critical business systems. Our platform seamlessly integrates real-time threat monitoring, vulnerability management, and compliance capabilities directly into the SAP environment, empowering organizations to protect their data's integrity, confidentiality, and availability with minimal manual effort. With a proven track record, including a stellar customer success rating and over 5,000 SAP systems secured globally. SecurityBridge stands out for its ability to accurately provide a 360° view of the SAP security posture, ease of use, rapid implementation, and transparent licensing. We are committed to innovation, transparency, and customer-centricity, ensuring businesses can confidently navigate the evolving landscape of SAP security threats.

Locations

Germany (Headquarters)

Münchener Str. 49, 85051 Ingolstadt

+49 (841) 93914840

United States

228 Park Ave S, New York, New York

+1 416 821 0850

Netherlands

Kraijenhoffstraat 137A, 1018RG Amsterdam

+31 647 100 101

Singapore

4 Battery Road, Bank Of China Building, #25-01, Singapore (049908)

+65 9126 6097

Take the Next Step Towards NIS2 Compliance

Discover how SecurityBridge helps you strengthen SAP security, manage risks, and demonstrate compliance with NIS2 requirements:

Explore NIS2 for SAP

Request a demo

Certifications:







For more information please

Contact Us