EXPERT INTERVIEW

NIS2 and the New Accountability Model for Access Governance

Guido Kraft
Field CISO at WALLIX

20+ years of experience in cybersecurity, governance, ISO 27001, TISAX, and operational security programmes across critical infrastructure and regulated environments.

Q How does NIS2 change the relationship between the CISO, leadership, and the board?

Under NIS2, cybersecurity becomes a business risk issue rather than only an IT issue. Senior management and boards are directly accountable for cybersecurity measures and resilience.

That changes the role of the CISO, who becomes the bridge between technical operations and executive decision-making. The board also needs to exercise active oversight, understand cyber risk, and ask the right questions.

Q Why is access governance becoming so central under NIS2?

Nearly everything in IT and OT comes down to access. The risk appears when users have excessive privileges or access rights that are not aligned with responsibilities.

Access governance determines who can reach what, under which conditions, and with what accountability. That is why organisations should treat it as a strategic layer that supports wider security and compliance efforts.

EXPERT INTERVIEW

wallix

Q What barriers prevent public sector organisations from implementing stronger access governance?

The biggest barriers are usually legacy systems, fragmented environments, and limited budgets.Many older applications do not support modern identity or role-based access models, which often leaves organisations relying on shared accounts or excessive privileges.Where systems cannot be redesigned, organisations can still improve control through privileged access management, stronger authentication, and auditable access paths.

Q Why are shared administrative accounts still so common?

Shared accounts persist mainly because of legacy systems and operational convenience. Many older applications still do not support modern role-based access control.Where possible, organisations should move toward named individual accounts. Where that is not possible, privileged access management can add accountability and auditability around shared access.

Q What could the next European cybersecurity regulation focus on?

The next major focus will likely be AI governance.

As AI becomes more embedded in business operations, organisations will need clearer policies around data use, accountability, risk management, and compliance.

Q How should organisations balance prevention with post-incident investigation under NIS2?

Prevention and investigation are both essential. Organisations need controls that reduce risk, but they also need visibility and traceability after an incident occurs.

Security teams must be able to understand who accessed which systems, when access occurred, and what actions were performed.

Q What does good third-party access security look like under NIS2?

Third-party access should be treated with the same rigour as internal privileged access.

Good practice means access is controlled, time-bound, monitored, and fully traceable. Organisations should avoid unmanaged external access, standing vendor privileges, and generic remote accounts.

Q Should organisations approach NIS2 as compliance or resilience?

The stronger approach is to treat NIS2 as an opportunity to improve operational resilience rather than simply satisfy compliance requirements.

If organisations improve visibility, access governance, and operational discipline, compliance becomes the outcome of stronger control.