Asset Security Strategy Assessment

According to Bitkom, the German economy suffers total annual damage of EUR 289 billion caused by cybercrime. Only 10% of all companies in Germany were spared cyber attacks in 2023 and 2024. 88% report that attacks on their corporate networks have taken place.

Cybercrime has always been an issue, but with the growing trend towards remote and home office work, new attack surfaces and opportunities have opened up.

In a study published in April 2023, Gartner advises leaders in the realm of Security and Risk Management (SRM) to rethink the balance between technology investments and human-centered elements when developing and implementing cybersecurity programs. This recommendation aligns with seven key industry trends and emphasizes focusing on three key areas. Firstly, recognizing the essential role of employees in the success and sustainability of the security program. Secondly, enhancing technical security skills that provide greater transparency and responsiveness across the company's digital ecosystem. And thirdly, restructuring the modus operandi of the security function to enable agility without compromising safety.

The seven trends outlined by Gartner for SRM (Security and Risk Management) leaders

Trend 1: Human Centric Security Design

Trend 2: Improving Personnel Management for the Sustainability of Security Programs

Trend 3: Redefining the Cybersecurity Operating Model to Support Value Creation

Trend 4: Threat Potential Management

Trend 5: Immunity of Identity Infrastructure

Trend 6: Cybersecurity-Validation

Trend 7: Consolidation of Cybersecurity Platforms

Trends 1 and 2 mainly focus on people and their behavior, trends 3 and 4 take into account the requirements resulting from increasing digitalization and new working methods, and trends 5 to 7 deal with technologies, processes, and tools, with a strong focus on digital identities, governance, and access management.

New legal requirements are placing increased expectations on companies regarding cybersecurity. The European NIS-2 directive already includes significant regulations that will also be reflected in the German IT Security Act 3.0. NIS-2 expands the powers and actions of nationally competent authorities. For instance, the German Federal Office for Information Security (BSI) will now have the authority to temporarily prohibit individuals responsible for executive management or legal representation from carrying out their management duties if they fail to comply with BSI's directives.

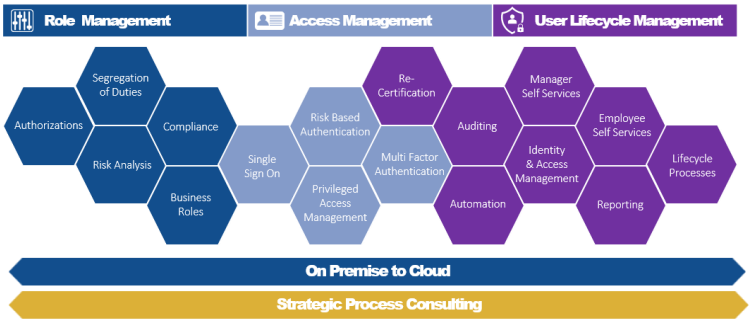
Governance and compliance are among the main pillars of the NIS-2 directive, addressing role management, access management, and user lifecycle management. Primarily, it revolves around issues of authorization and authentication, as well as appropriate permissions. In this context, access management plays a pivotal role. Without multi-factor authentication (MFA), companies are significantly more vulnerable to phishing attacks. Identity management with single sign-on (SSO) and MFA are not a luxury, but an essential prerequisite for managing and controlling identities, access, and permissions.

© 2025 by IBsolution GmbH
IBsolution GmbH | Im Zukunftspark 8 | 74076 Heilbronn | Germany
Telefon: +49 7131 2711 3000 | info@ibsolution.com | www.ibsolution.com

Identifying areas of action | Reducing vulnerabilities

It should be noted that the areas of cybersecurity are becoming increasingly extensive. The human element remains the greatest vulnerability and requires significant training to raise awareness. As one progresses through the layers, the impact becomes more technical and demanding. Once privileged users are compromised, a devastating attack is imminent. Each layer holds its importance within a comprehensive security concept. The ultimate layer is the Data Layer, which, as recommended by Gartner, must be protected by all means.

Role Management, Access Management und User Lifecycle Management erhöhen das Schutzniveau im Data Layer maßgeblich.



As part of our Asset Security Strategy Assessment, we follow a well-established approach to collaboratively develop a roadmap together with you. This roadmap outlines how security-related areas within your company need to be addressed in a future-oriented manner while considering your current situation. We examine and concentrate on specific subdomains that you can explore with us entirely or in individual components.

Asset Security Strategy Assessment @IBsolution

Base Module Asset Security Assessment **EUR 6,000**

The Base Module of the Asset Security Assessment is mandatory for our entire workshop series and provides results that are relevant for all subsequent modules. In the Base Module, you will receive an overview of all subtopics within our series. The focus here is more on a general examination of the mentioned modules and explaining their significance and mutual influence.

Module User Lifecycle Management: *Discussion of user processes based on standardized best practice processes. With a focus on on-premise SAP systems and Microsoft Active Directory.* **EUR 6,000**

Submodule Integration of Additional System Types: *Integration of additional systems into user lifecycle processes and definition of fully automated connections.* **EUR 2,000**

Submodule Cloud and Microsoft Azure Provisioning: *Expanding the scope of on-premise systems to include essential cloud systems from the SAP world or to the use of Microsoft Azure or Microsoft Entra ID.* **EUR 2,000**

Module Role Management and SAP Authorizations: *Evaluation of your SAP authorization concept in terms of currency and SAP S/4HANA readiness. Gaps are identified and solution paths are presented.* **EUR 10,000**

Module Business Role Concept: *Demonstrating the ways in which a business role concept can be implemented within your organization and how it can significantly reduce efforts in authorization maintenance.* **EUR 5,000**

Module Access Management: *We demonstrate possibilities, considering your current and future system landscape, for implementing single sign-on (SSO), multi-factor authentication (MFA), and even risk-based access (RBA) within your organization.* **EUR 2,000**

Module Cyber Security Check: *Through our 360 Degree Security Check for SAP Landscapes, we conduct a 2-day workshop to assess the current state of your IT security across all relevant security layers and identify vulnerabilities.* **EUR 10,000**

Module Tool Selection: *Based on the defined processes, business requirements, and with a focus on state-of-the-art solutions while considering the current developments in the IAM market, we conduct a tool selection process for you. The results will be comprehensibly justified.* **EUR 4,000**

Total: ~~47,000 EUR~~ 44,000 EUR

© 2025 by IBsolution GmbH
IBsolution GmbH | Im Zukunftspark 8 | 74076 Heilbronn | Germany
Telefon: +49 7131 2711 3000 | info@ibsolution.com | www.ibsolution.com