Case Study

A German IT Service Provider Enhances Compliance with Syteca Session Monitoring to Secure Privileged Access

The challenge

Three control-relevant domains were at the center of our client's focus:

- **Access Management (AM)** – particularly in AD and Azure AD
- **Change Management (CM)** – for example, within SAP system landscapes
- **Network & Infrastructure (NI)** – including core components used in service delivery

To ensure secure handling of privileged access – such as to the SAP database – a tool for comprehensive, audit-proof traceability had previously been missing. In a highly regulated environment, this represented a significant gap in terms of ISO-compliant security controls.

> "With Syteca, we have full transparency over the activities of our administrators and external service providers. Especially in the SAP environment, this has been a real asset – not least with regard to audit requirements. The solution runs reliably, integrates well into our daily operations, and proved its value quickly. Techway supported us from the very beginning with hands-on expertise and practical guidance."
>
> **Marc Golenko, SAP Operations Team Lead**

The customer

Organization type: IT service provider

Location: Germany

Market: Germany

Must comply with: ISO/IEC 27001:2022

Pending issues: Complete documentation of activities performed with elevated privileges, Fast detection and containment of potentially harmful actions, Support for forensic investigations and audit documentation, Early detection of suspicious or unauthorized access

Within the scope of ISO/IEC 27001:2022, the following key requirements were identified:

Customer's objectives	Results achieved	Benefits	ISO/IEC 27001:2022 Control
Traceability of privileged activities	Session recording including screen, keyboard, applications, and metadata	Complete documentation of activities performed with elevated privileges	▪ Privileged Access Rights ▪ Assessment of Events
Response to security-related incidents	Real-time analysis and automated actions (e.g. session blocking, process termination)	Fast detection and containment of potentially harmful actions	▪ Response to Incidents ▪ Monitoring Activities
Evidence preservation for audits and forensics	Export of session data in protected, audit-compliant formats	Support for forensic investigations and audit documentation	▪ Collection of Evidence
Support for role-based access control	Context-aware access model, secondary authentication, and role-based visibility	Prevention of role conflicts and misuse of shared accounts	▪ Segregation of Duties ▪ Information Access Restriction
Live monitoring and alerting	Monitoring of privileged sessions, configurable alerts and escalation handling	Early detection of suspicious or unauthorized access	▪ Monitoring Activities

To meet these objectives, the company implemented the Syteca platform – a comprehensive solution for privileged session monitoring and privileged access management (PAM). Syteca is specifically designed to support organizations in achieving ISO/IEC 27001:2022 compliance.

The decision to implement Syteca followed a targeted evaluation of various approaches to monitoring privileged access. Compared to traditional **logging solutions** and **SIEM-based methods**, our solution stood out by offering a unique combination of **session recording**, granular access control, and intelligent real-time monitoring. The platform successfully combines **technical, organizational, and audit-relevant requirements** in a single solution – without adding unnecessary complexity to the system environment or introducing new operational risks.

Another key factor was the solution's **practical usability in day-to-day operations**: Syteca **integrated smoothly into existing processes**, offered a **short learning curve** for administrators, and today enables **comprehensive and compliant monitoring of both internal teams and external service providers.** Especially in the context of **financially relevant systems such as SAP**, this made it possible to establish a risk-based control environment that meets both internal standards and the expectations of external auditors.

The Result

The following table highlights key functional areas of the **Syteca platform** as implemented at Raiffeisen-IT GmbH. Together, we ensure that **security-relevant activities are documented in an audit-proof manner, suspicious actions are detected at an early stage**, and **privileged access rights are controlled and transparently managed** – forming an essential part of the company's **internal control system (ICS) and ISO 27001-compliant governance framework**.

Session recording with real-time playback

Activities of privileged users (e.g. SAP admins) are fully recorded and stored in a searchable format.

Audit-compliant export formats for evidence

Session data can be exported in protected formats suitable for audit and forensic purposes.

Metadata analysis and event logging

Each interaction is enriched with contextual metadata (e.g. applications launched, keystrokes entered, USB devices connected).

Live monitoring & alerting

Critical actions (e.g. write access to databases) trigger predefined alerts.

With Syteca, Raiffeisen-IT GmbH was able not only to close a critical gap in the implementation of its internal control system (ICS), but also to significantly enhance its ISO/IEC 27001:2022 compliance. The solution provides a robust foundation for transparency, accountability, and auditability in the management of privileged access – while offering the flexibility needed to continuously evolve the control framework in line with regulatory requirements.