XITING SECURITY SOLUTIONS

Your SAP Security Expert

www.xiting.com

Xiting – Your Trusted Provider for SAP Security

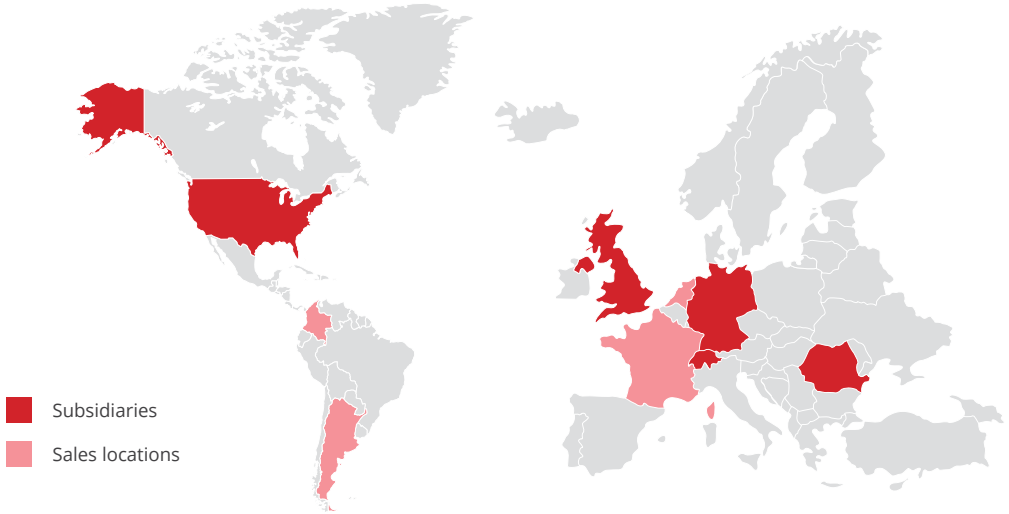
Xiting stands for comprehensive SAP security at the highest level. As an experienced SAP Gold Partner, we offer innovative solutions for SAP authorizations, identity and access management, governance, risk and compliance, cybersecurity, and security monitoring – including comprehensive cloud security.

Since its founding in Switzerland in 2008, Xiting has grown into an internationally renowned company with over 140 employees in Germany, Switzerland, Romania, the US, and the UK. Our specialized SAP security consultants support more than 700 customers worldwide – remotely or directly on site.

Get Connected – Run Secure

- Xiting is a trusted advisor and provider for comprehensive SAP security solutions and services
- Over 700 Satisfied Customers Worldwide
- Recognized Expert in Security Solutions since 2008

Locations



2008 **Founded**
in Switzerland
Zürich

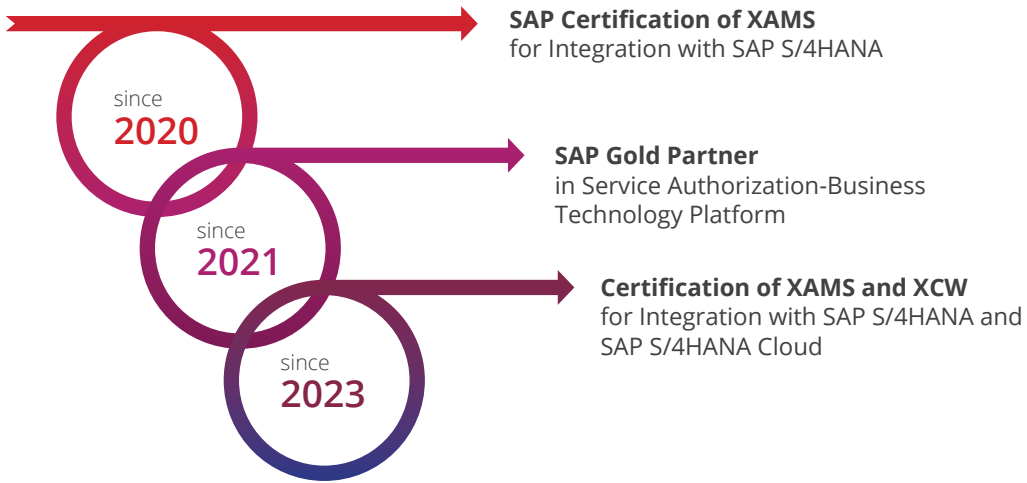
2012 **Subsidiary**
in Germany
Schluchsee

2013 **Subsidiary**
in the United Kingdom
Bristol

2016 **Subsidiary**
in USA
Apollo Beach, FL

2018 **Subsidiary**
in Romania
Cluj

Certifications



SAP Certification of XAMS
for Integration with SAP S/4HANA

SAP Gold Partner
in Service Authorization-Business Technology Platform

Certification of XAMS and XCW
for Integration with SAP S/4HANA and SAP S/4HANA Cloud

SAP Gold Partner

SAP® Certified
Integration with SAP S/4HANA®

SAP® Certified
Integration with SAP S/4HANA® Cloud

SAP Certified
Integration with RISE with SAP S/4HANA Cloud

SAP® Certified
Integration with Cloud Solutions

Xiting's Expertise:

On-Premise:

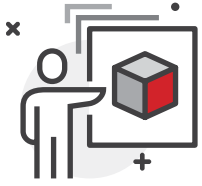
- SAP Access Control (GRC)
- SAP Security Monitoring
- SAP Authorizations Management
- SAP Identity Management (IDM)

Cloud:

- SAP Cloud Identity Access Governance (IAG)
- SAP Cloud Identity Services (IAS/IPS)
- SAP Business Technology Platform (BTP)
- SAP SuccessFactors
- SAP Concur
- SAP Ariba
- SAP S/4HANA Public Cloud
- SAP Analytics Cloud
- SAP Build

Consulting

Xiting's extensive expertise in consulting is reflected in numerous succesful national and international projects. We support companies with comprehensive SAP security consulting – from authorization and identity management to GRC and cybersecurity. Our experts analyze risks, optimize security structures, and ensure transparent, compliant, and future-proof SAP landscapes.



Trainings & Workshops

We offer a wide range of training courses and workshops – from SAP security training courses for SAP Education to practical workshops led by our security experts. We impart in-depth specialist knowledge combined with concrete project experience. Customers benefit from clear, practical advice and active involvement in implementation.

Our Training Courses:

- WNAXIT / WCHXIT – SAP Authorizations Simplified with Expert Tools
- WNAADA / WDEADA – Advanced SAP Authorizations
- WDES4M – Migrations of roles and authorizations to SAP S/4HANA
- WDESSO – SAP Single Sign-On 3.0

Our Workshops:

- BPW – Best Practices Workshop in Roles & Authorizations
- BPWS4M – Best Practices Workshop in SAP S/4HANA Migration
- BPWFIORI – Best Practices Workshop in SAP Fiori Authorizations

Managed Services

Xiting offers a wide range of SAP Support services that are custom-tailored to a company's specific requirements. They ensure efficient and smooth business processes.

Competitive Advantage:

- Convenient locations to ensure global reach
- Support for multiple languages, including English, German, Spanish, French, Italian, Romanian.
- Small teams with very low staff turnover
- Continued education
- Xiting Academy certified, fully trained in SAP Security and SAP Certified

Services we offer:

- Day-to-day SAP Security support
- Ticketing support
- Security monitoring
- Authorization redesigns, migrations, and upgrades
- Daily, weekly, monthly, and quarterly reporting (e.g., SoD, system audit, system security and health checks, ABAP guidelines, security configuration, system parameters, etc.)

Solutions and Services

Software Solutions

Do the work yourself with the help of powerful tools

(Managed) Service Consulting

Let the work be done & achieve results for specific requirements (clear consulting scope)

(Project/Sales) Consulting

Get guidance & coaching for individual requirements (any consulting scope)

Authorization Management

License Cleanup in SAP S/4HANA

Accelerated S/4HANA-Migration

Simplified SAP Fiori Administration

Test Simulation of Roles & Authorizations

Xiting **A**uthorizations **M**anagement **S**uite

Identity & Access Management

SAP User Management & Workflows

Identity Access Management SAP IDM & SailPoint

SAP BTP Security & SAP Cloud Identity Services

SSO & Secure Authentication

Xiting **C**entral **W**orkflows

Cybersecurity & Security Monitoring

AI-Driven SAP Security Operations Center (SOC)

Real-time SAP Security Monitoring & Threat Detection

Vulnerability Analysis & Compliance Monitoring

SIEM Integration

Xiting **S**ecurity **P**latrorm

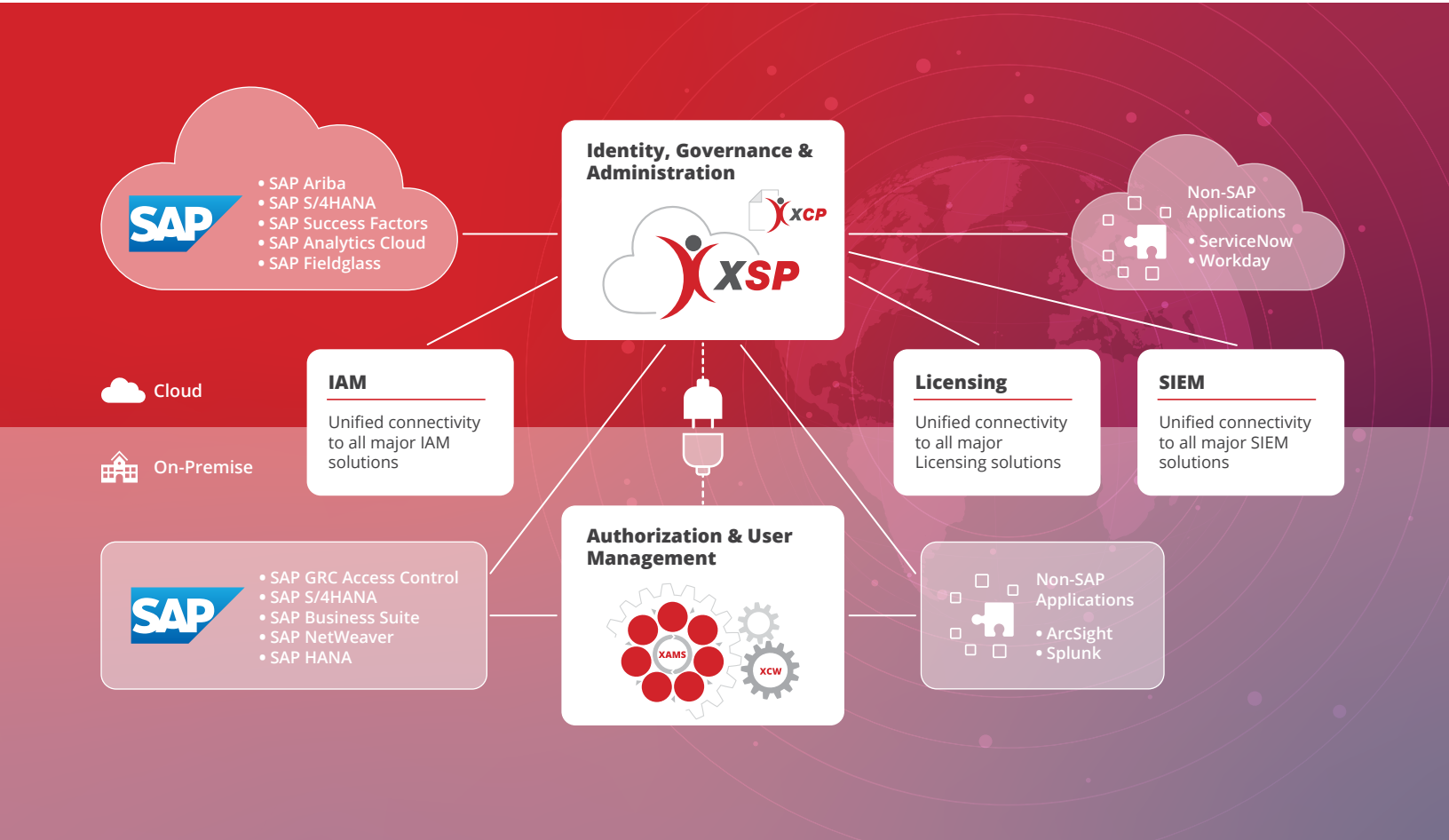
Governance, Risk & Compliance

Emergency User & Extended Access Management (EAM)

Next-Level Ruleset Management

Cross-system Risk Analysis & SoD

Identity Consolidation


• SAP Ariba
• SAP S/4HANA
• SAP Success Factors
• SAP Analytics Cloud
• SAP Fieldglass
Identity, Governance & Administration
XCP
XSP
Non-SAP Applications
• ServiceNow
• Workday
Cloud
On-Premise
IAM
Unified connectivity to all major IAM solutions
Licensing
Unified connectivity to all major Licensing solutions
SIEM
Unified connectivity to all major SIEM solutions
• SAP GRC Access Control
• SAP S/4HANA
• SAP Business Suite
• SAP NetWeaver
• SAP HANA
Authorization & User Management
XAMS
XCW
Non-SAP Applications
• ArcSight
• Splunk

Get Connected – Run Secure

From various tools to a connected security ecosystem

This approach shows how Xiting is redefining the SAP environment through holistic, security-focused identity and access governance. Xiting is transforming from a project-driven solution suite into an open, modular platform. With the Xiting Security Platform (XSP), identities, authorizations and governance processes are connected across SAP and non-SAP landscapes, while API-based connectors enable seamless and flexible integration of existing systems like IAM, licensing, SIEM, and GRC solutions.

XAMS provides the foundation for comprehensive SAP authorization and user management while acting as a strategic integration layer that seamlessly connects traditional SAP landscapes with the modern hybrid security platform. It ensures deep technical alignment with established SAP infrastructures, empowering organizations to maintain full control of their existing environment while securely extending and harmonizing authorization processes into a future-ready, interconnected ecosystem.

This creates a consistent, hybrid security and monitoring architecture that does not replace existing solutions, but intelligently expands, connects and runs them securely.

Our platform approach safeguards existing investments while enabling the targeted evolution of current solutions. No disruption, only a clear and future-ready perspective.

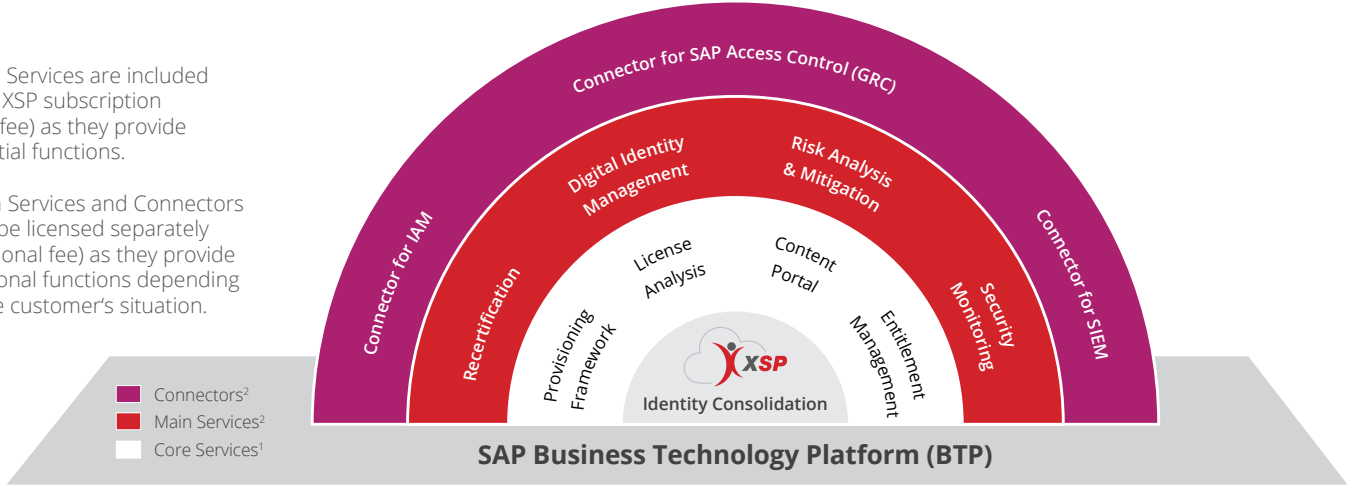
Identity, Governance & Administration (IGA) with XSP

Xiting Security Platform (XSP) offers a holistic, SAP-centric IGA approach to automating identity management and compliance:

- Central identity consolidation
- Digital identity management – Standalone, integrated IAM within XSP
- Risk analysis & mitigation
- Recertification
- Security monitoring & real-time threat detection

[1] Core Services are included in the XSP subscription (base fee) as they provide essential functions.

[2] Main Services and Connectors must be licensed separately (additional fee) as they provide additional functions depending on the customer's situation.



Our Xiting Product Family

Xiting Authorizations Management Suite (XAMS)

XAMS supports the implementation of authorization projects by automating costly and time-consuming tasks, improving compliance and significantly reducing the risk of errors.

Xiting Security Platform (XSP)

The new and innovative solution seamlessly connects on-premise and cloud systems, including SAP and non-SAP applications, to ensure comprehensive security and compliance monitoring.

Xiting Security Architect (XSA)

In combination with the **SIEM Connector** to centrally monitor and audit the entire SAP landscape and report any possible threats and findings to a SIEM solution or emails in real-time.

Xiting Content Portal (XCP)

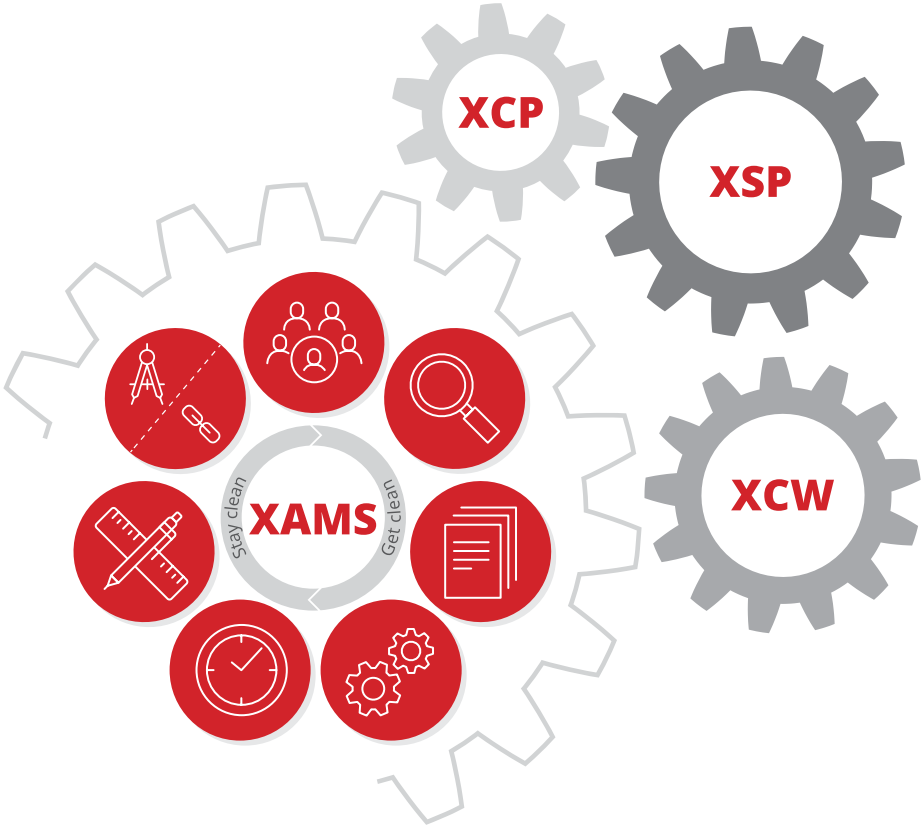
To manage and maintain ruleset content, but also offers the ability to keep rulesets up to date by subscribing to validated master content.

Xiting Central Workflows (XCW)

To centrally execute user provisioning processes to manage the users in a hybrid landscape, with integrations to SoD and critical risk analyses.

Xiting Falcora

Xiting Falcora is an AI-Driven Security Operations Center that automates alert triage and enriches SAP security signals with identity, authorization, and business context – integrated into IGA & GRC for a holistic response.


XCP
XSP
XCW
XAMS
Stay clean
Get clean

Our Solutions

Regulatory requirements and legal obligations demand that companies manage authorizations with strict controls. This often necessitates revising or developing new authorization concepts, bringing significant challenges that require deep expertise.

With the Xiting Authorizations Management Suite (XAMS), we offer our highly specialized SAP authorization expertise to our customers. XAMS simplifies authorization projects, significantly reducing critical and time-consuming phases while enhancing efficiency. Built on this foundation, our best-practice approach ensures holistic administration of SAP authorizations within ABAP environments.

Our Xiting Security Platform (XSP) extends security and compliance capabilities across hybrid landscapes including SAP cloud environments. Additionally, the Xiting Content Portal (XCP) enables organizations to efficiently manage security content, such as rulesets, security patterns, and compliance monitoring configurations, ensuring continuous security monitoring and regulatory alignment.

Xiting Security Platform (XSP)

Innovative Solution for Comprehensive SAP Security Management

Discover the comprehensive use cases of the Xiting Security Platform (XSP) – a solution designed to revolutionize SAP security management with extensive coverage, seamless integration, and advanced analytics. XSP empowers organizations to enhance security, streamline compliance, and optimize operations across hybrid and cloud environments.

XSP Core Services:

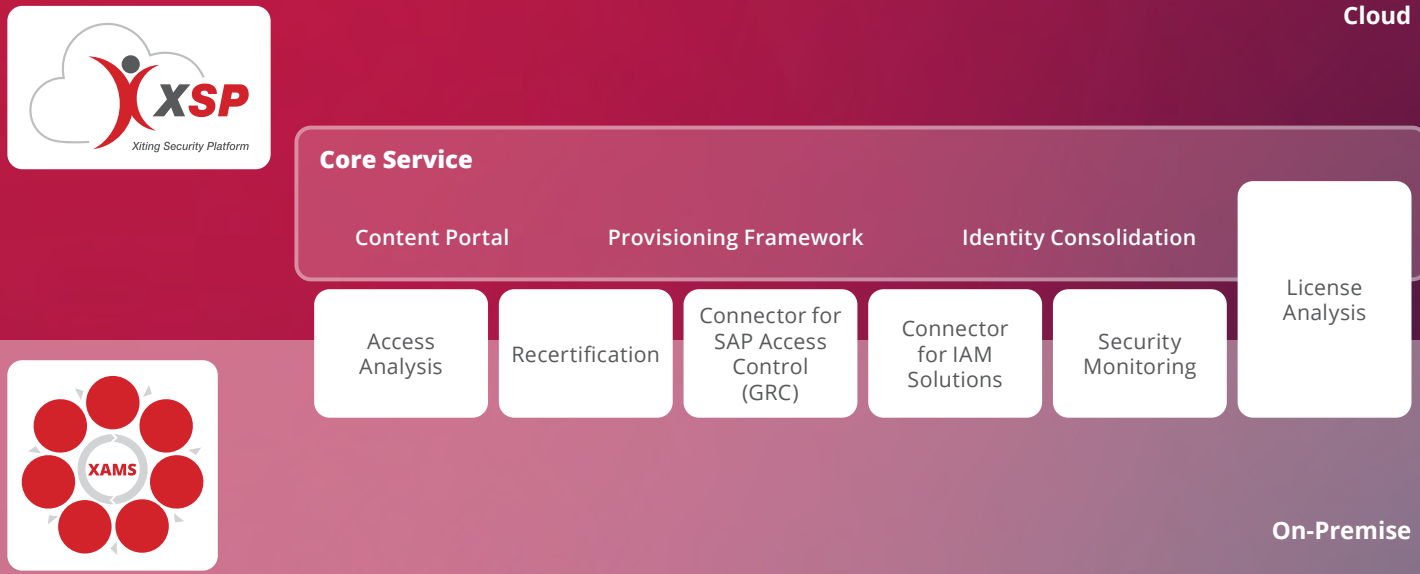
- Identity Consolidation – Centralized identity store for streamlined access management.
- Provisioning Framework – Automated and efficient user provisioning across SAP landscapes.
- License Analysis – Optimize SAP license management and ensure compliance.
- Xiting Content Portal (XCP) – Manage rulesets, security patterns, and compliance monitoring for real-time security updates and patch management.

XSP Additional Services:

- Security Monitoring & Real-Time Threat Detection – Proactively identify and mitigate risks.
- Cross-System Risk Analysis – Ensure compliance and mitigate access conflicts across SAP systems.
- Connectors for IAM Solutions – Integrate with leading Identity & Access Management (IAM) platforms.
- Connectors for SAP Access Control (GRC) – Maximize SAP Access Control into the cloud.
- Recertification & User Access Reviews (UAR) – Ensure continuous compliance with automated access recertifications.

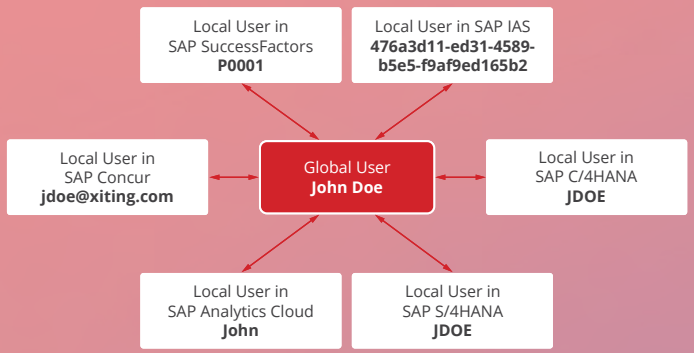
Embrace a Cloud-First Strategy

The Xiting Security Platform is built for business growth, cloud adoption, and digital transformation. With its cloud-based architecture, XSP eliminates the constraints of traditional on-premises solutions, enabling businesses to scale, adapt, and secure their SAP ecosystems more efficiently than ever before.



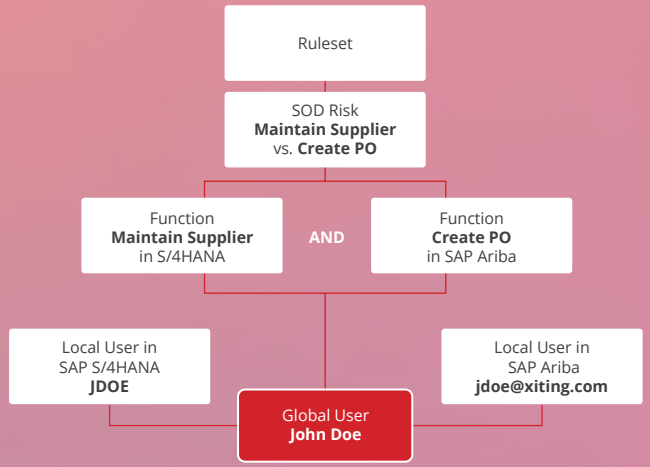
Identity Consolidation

Identity consolidation merges local users into global users, enabling comprehensive risk analysis and business role provisioning across applications, even when user IDs differ for the same person in each system.



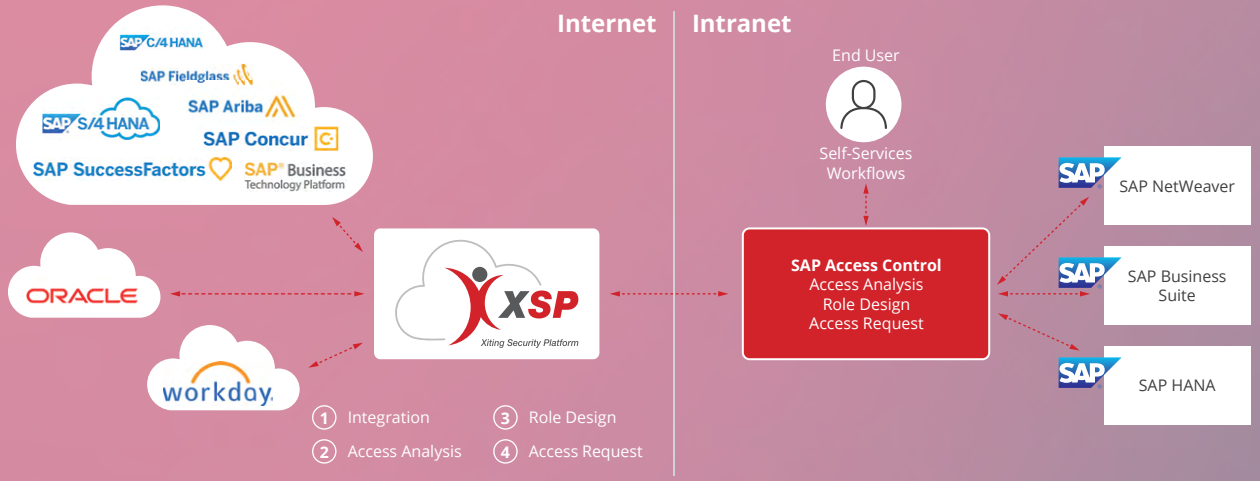
Risk Analysis & Mitigation

XSP provides a cross-system risk analysis for users and roles in on-premises, hybrid, and cloud environments. With best practice rulesets, a mitigation framework, and identity consolidation, XSP enables holistic risk assessment. This allows organizations to proactively manage risks and ensure compliance.



Seamless Cloud Provisioning

XSP extends SAP Access Control (SAP AC) beyond on-prem, enabling secure and efficient provisioning of users and roles into cloud solutions like SuccessFactors, Ariba, Fieldglass, SAC, and Cloud IAS. With risk analysis and provisioning logs retained within SAP AC, organizations maintain compliance while seamlessly managing hybrid landscapes. Elevate your access control strategy with XSP – bridging the gap between on-prem and cloud with precision and efficiency.



Optimized SAP S/4HANA License Cost Management

XSP enhances SAP's S/4HANA Trusted Authorization Review (STAR) Service by providing precise license cost identification and optimization. With Identity Consolidation, XSP enables cross-system S/4HANA license validation, ensuring businesses identify the "most expensive" license key per user across multiple systems. Eliminate unnecessary costs and maximize SAP licensing efficiency with XSP.

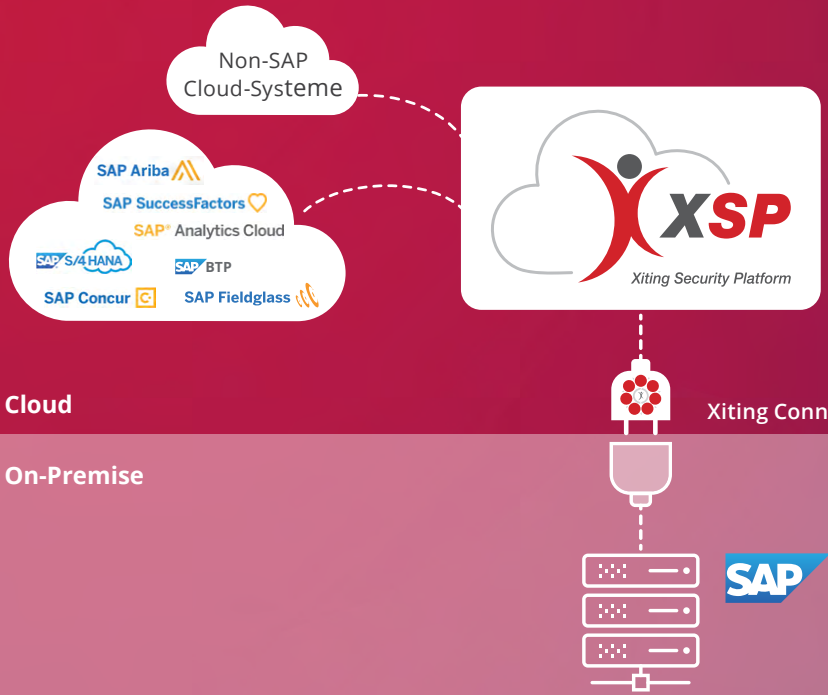
Real-Time SAP Security Monitoring

XSP empowers organizations with real-time monitoring of user activities and system logs to detect anomalies and potential threats instantly. By proactively identifying security risks, XSP fortifies SAP landscapes against internal and external security breaches. The XSP Security Dashboard provides clear risk visualization, ensuring swift action and enhanced protection. Stay ahead of threats – secure your SAP environment with XSP.

Streamlined User Access Reviews

Ensure precise access control with XSP's User Access Review, aligning user authorizations with job functions for maximum security and compliance. As a core part of XSP's Recertification Services, this structured approach minimizes risks, strengthens governance and ensures your SAP systems remain secure and audit-ready. Stay compliant, stay secure – optimize access with XSP.

Learn more about the **Xiting Security Platform** in this video:



XSP Capabilities:

- Cross-System Risk Analysis and Mitigation
- Content Hub for Ruleset Management, Security Monitoring and Patch Management
- System-wide License Analysis and Optimization for SAP S/4HANA
- Real-time Security Monitoring and Integration to SIEM
- Connectors for SAP Access Control (GRC) and IAM solutions

On-Premise SAP-Systems

- SAP S/4HANA
- SAP Business Suite (ECC, CRM, SRM, SCM, PLM)
- SAP NetWeaver
- SAP HANA

Xiting Content Portal (XCP)

A community-driven platform to maintain your GRC rulesets that redefine modern risk management.

The Xiting Content Portal (XCP) is a SaaS solution designed to empower customers with a centralized SAP risk repository and user interface. This content hub not only facilitates customers in centrally creating, building, and managing their rulesets, but it also supports them in ruleset design through a collaborative community approach.

At its core, XCP features a cloud-based web front-end that grants access to hybrid ruleset content. This content encompasses Xiting ruleset templates which represent general best practices, shared community rule content from partner companies that reflects industry best practices, and customer-specific rule content, catering to their unique best practices.

XCP not only offers best practice content, it also allows you to subscribe to standard content and keep it up to date with the update service.

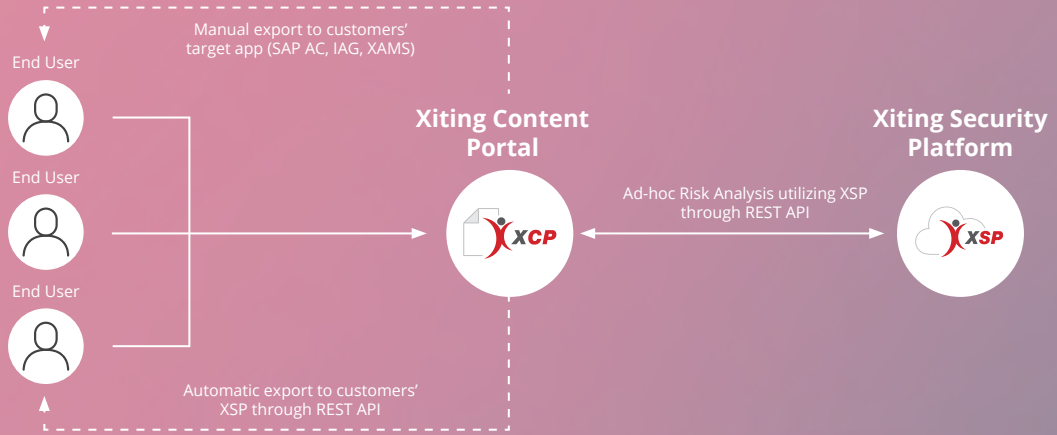
Additionally, XCP offers users the ability to:

- **Import and export rulesets:** Easily transfer rulesets to and from the platform to various applications, including Xiting Security Platform (XSP), SAP Access Control (GRC), SAP Cloud Identity Access Governance (IAG).
- **Maintain and customize rulesets through a modern UI:** Enhance usability and facilitate smooth navigation.

- **Subscribe to existing ruleset content:** Stay connected with a myriad of predefined ruleset collections.
- **Keep content up to date:** By subscribing to standard rules and effectively mapping existing content, your custom ruleset stays up to date in the long run.

Moreover, XCP is equipped with ruleset design tools that streamline the building process and insightful reports to help assess existing rulesets and roles.

Architecture



Xiting Falcora

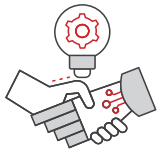
AI-Driven SAP Security Operations Center (SOC)

Enable any SOC to run SAP security efficiently – independent of the SIEM, with lower cost, higher quality, and built-in SAP expertise.

Traditional SOC models struggle with SAP. Alert volumes are high, the signal-to-noise ratio is low, and most teams lack deep SAP security and process expertise. At the same time, hybrid SAP landscapes – on-premise, SAP S/4HANA, SAP cloud and SAP BTP – make monitoring and incident response complex and expensive to operate 24/7.

Xiting's new solutions turns SAP security operations into an AI-driven SOC capability. The product ingests SAP security alerts from any SIEM, enriches them with SAP business and identity context, and uses AI to automate SOC Level 1 and 2 investigations, evidence collection and risk pre-classification.

SOC analysts stay in control while routine SAP investigations are handled consistently, transparently, and at scale.



Find our more about this **new solution**:

Key Benefits

AI-automated SAP alert triage

Automate SAP-specific L1 investigations, false-positive reduction and evidence gathering – independent of the underlying SIEM – to significantly lower cost per alert and standardize SAP SOC knowledge.

Unified monitoring across SAP cloud and on-premise

Apply a consistent telemetry and analysis model across SAP ECC, SAP S/4HANA, SAP cloud applications and SAP BTP to reduce integration complexity and give the SOC full visibility into business-critical SAP activities.

End-to-end detection, investigation and response for SAP incidents

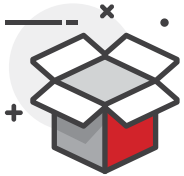
Orchestrate a unified workflow from SAP detection through investigation to response, including SOP-driven playbooks and integration into existing SOC tooling such as ticketing and collaboration platforms.

SAP-native security intelligence for higher detection quality

Leverage SAP business process, identity and authorization context to reduce false positives and detect misuse, fraud and advanced attacks that generic SIEM rules often miss.

Xiting Authorizations Management Suite (XAMS)

- Role Designer
- ABAP Alchemist
- Role Replicator
- Role Builder
- Xiting Times
- Role Profiler
- Security Architect & SIEM Connector



Xiting Authorizations Management Suite (XAMS)

The XAMS dramatically simplifies role design, maintenance, and testing, as well as vulnerability scanning of custom ABAP code, the creation and validation of SAP security concepts.

Xiting has developed XAMS with flexibility in mind. Each of the seven modules can be used individually or in combination to address specific use-cases.

Take advantage of our **XAMS Freeware**:
RFC Stocktake & User Locking Tool.

Find out more:

Modular Approach

The innovative modules of Xiting Authorizations Management Suite (XAMS) are adapted to your needs and thus enable customized solutions.

Role Designer
Quickly design SoD-free roles based on usage data using a drag & drop cockpit.

ABAP Alchemist
Improve the quality and security of existing and new ABAP code, and quickly find reusable code via the API finder.

Role Replicator
Mass role replication and batch processing tools to reduce the role maintenance effort.

Role Builder
Virtually eliminate the need to test new roles or role changes through an innovative concept called Productive Test Simulation.

Xiting Times
Eliminate the impact on end-users due to missing authorizations during Go-Live.

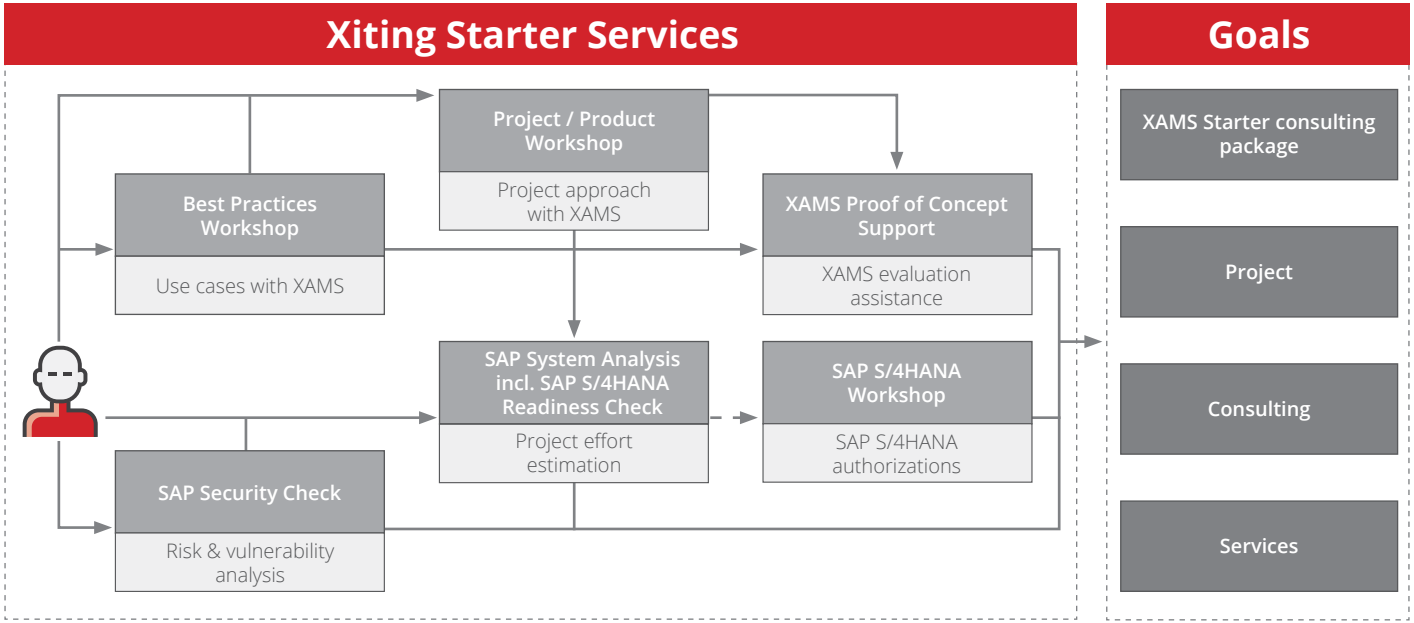
Role Profiler
Analyze and improve the quality of roles and authorizations.

Security Architect
Fully integrated SAP security concepts for ongoing audits and compliance testing.

SIEM Connector
Connect your SAP system with a SIEM solution.

Our XAMS Starter Services

Xiting offers comprehensive service packages that are fully compliant with SAP best practices, are fully customizable, and deliver unprecedented value to clients.




quality
ITing

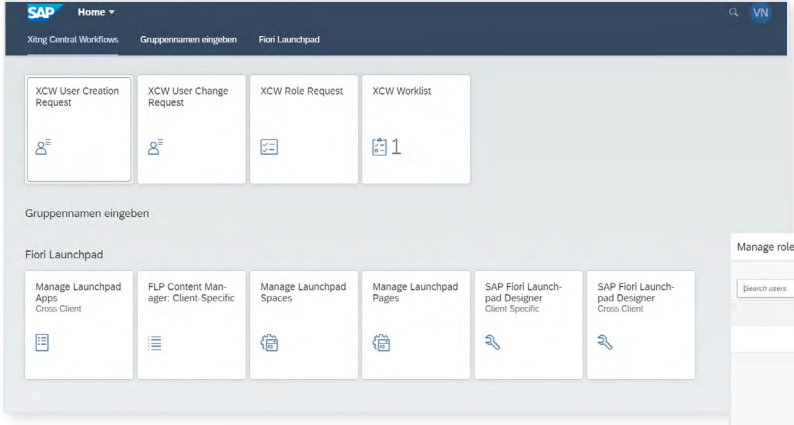
Xiting Central Workflows (XCW)

With Xiting Central Workflows (XCW) we offer standardized workflows according to SAP Best Practices, for, in our experience, the most important application scenarios in the user administration of SAP ABAP systems. This allows for automating work processes without major implementation effort and setting up self-services for password resets and user unlocks.

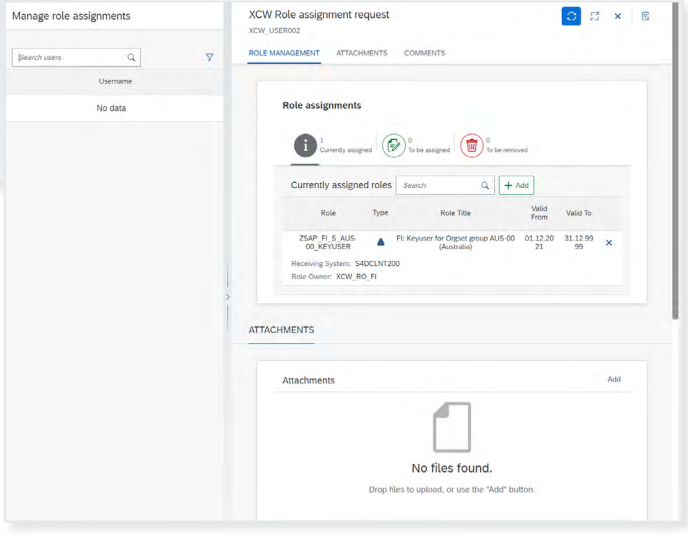
XCW ensures transparent processes and automatically documents them in compliance with auditing standards.

Challenges

- Manual role request
- No specific naming of roles
- No traceability about the reason for the application
- No explicit approval procedures
- No responsibilities for role assignments
- No regular storage of applications
- Manual intervention errors



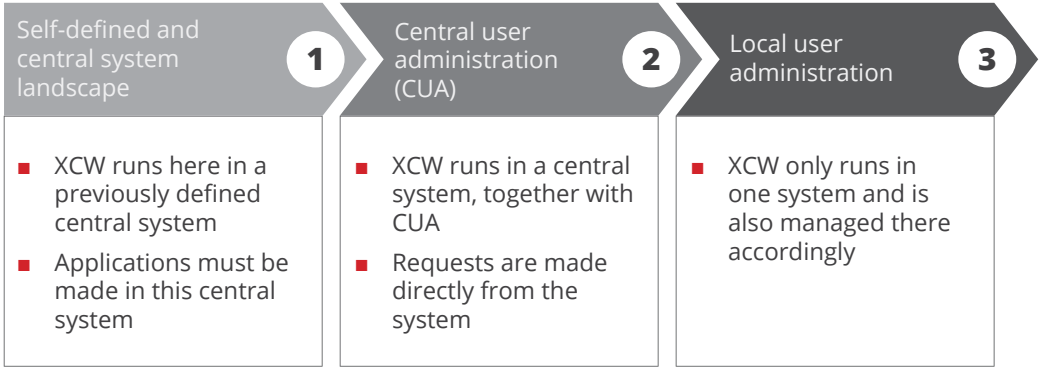
SAP Fiori Launchpad:
The start page of SAP Fiori applications and XCW



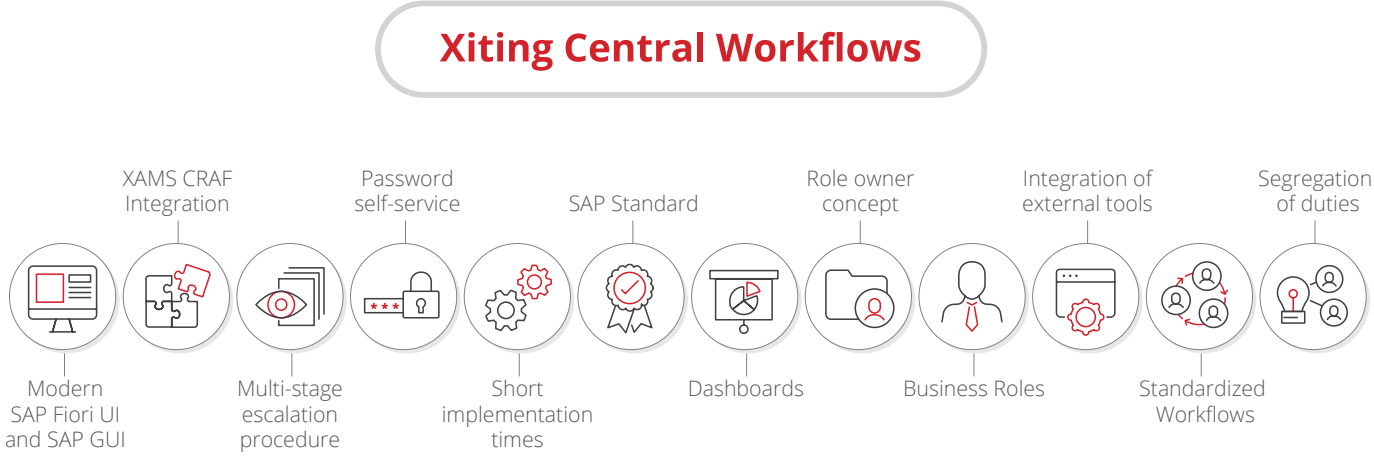
Set role request for other users

Start now with XCW – without additional infrastructure or hardware!

The implementation of statutory and customer-specific governance, risk, and compliance requirements can take place through individual implementation variants. Regardless of the architecture of the system landscape, user administration is mapped locally or centrally for all connected SAP ABAP systems.

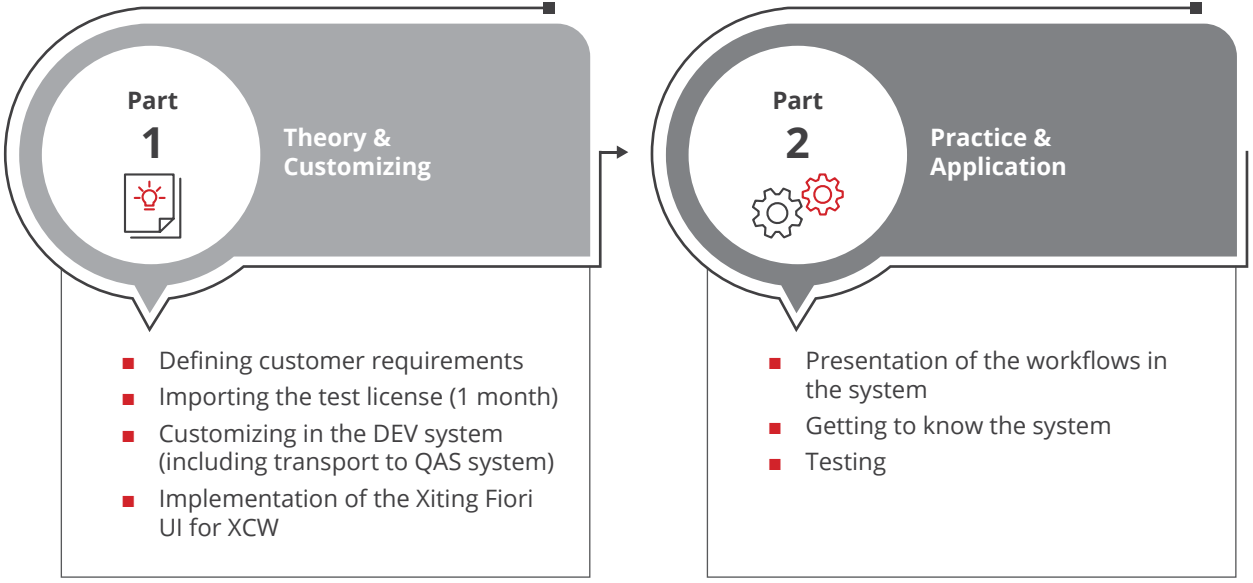


Advantages by using our solution:
Xiting Central Workflows



Your Start with the XCW Best Practice Workshop

In addition to basic knowledge of user administration in SAP ABAP systems, this workshop presents the basic configuration of XCW according to best practice. You also have the option of customizing XCW to your own requirements.



- Defining customer requirements
- Importing the test license (1 month)
- Customizing in the DEV system (including transport to QAS system)
- Implementation of the Xiting Fiori UI for XCW

- Presentation of the workflows in the system
- Getting to know the system
- Testing

* Duration depending on complexity (1 - 4 days)

XAMS and XCW Licensing Solutions:

	XAMS Essential	XAMS Essential Extended	XAMS Professional	XAMS Professional Extended
Purchase type	Perpetual Subscription Project rent	Perpetual Subscription	Perpetual Subscription Project rent	Perpetual Subscription
Maintenance and Support	✓	✓	✓	✓
Compatible	„Classic“ SAP ABAP software & SAP S/4HANA	„Classic“ SAP ABAP software & SAP S/4HANA	„Classic“ SAP ABAP software & SAP S/4HANA	„Classic“ SAP ABAP software & SAP S/4HANA
Licensing metric	SAP Named User	SAP Named User	SAP Named User / XSC System based	SAP Named User / XSC System based
Role Designer (RD)	✓	✓	✓	✓
ABAP Alchemist (AA)	✗	✗	✓	✓
Role Replicator (RR)	✓	✓	✓	✓
Role Builder (RB)	✓	✓	✓	✓
Xiting Times (XT)	✓	✓	✓	✓
Role Profiler (RP)	✓	✓	✓	✓
Security Architect (SA)	✗	✗	✓	✓
Xiting Central Workflows (XCW)	✗	✓	✗	✓
SIEM Connector (XSC) *	✗	✗	✓ *	✓ *

* SIEM Connector (XSC) can be licensed additionally. License model system based.

Practical Use Cases

Every SAP landscape has its own specific requirements in terms of security, governance, and compliance.The following use cases show how companies use Xiting to solve typical challenges in SAP and hybrid environments in a targeted manner – practically, efficiently, and with measurable added value.

Our security solutions work together in perfect harmony to provide a comprehensive, end-to-end SAP security strategy across all systems.

Expedite SAP S/4HANA Migration

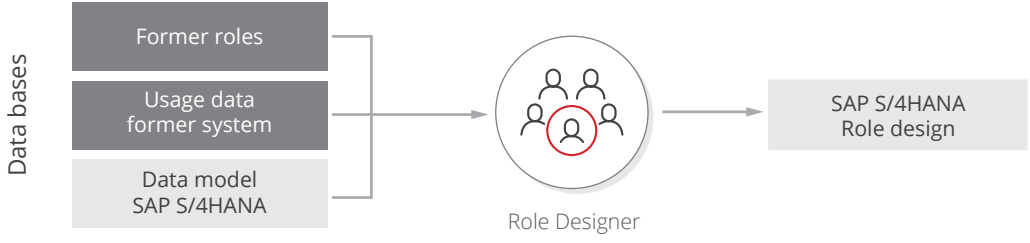
Challenge

SAP S/4HANA introduces an entirely new data model. As a result, role administrators will be required to update the existing role concept, including authorizations. Analyzing and updating old roles is a time-intensive process that consumes valuable project resources. SAP has documented many, but not all, of the required changes associated with both the new and obsolete transaction codes in an extensive document called the *Simplification List*.

Xiting Solution

Xiting has developed a solution, the Xiting Authorizations Management Suite (XAMS), which can expedite the migration of roles and authorizations to SAP S/4HANA by up to 75% compared to a manual approach.

By leveraging the latest *Simplification List*, plus any additional undocumented object changes, XAMS enables the project team to automate the migration of existing roles and authorizations to SAP S/4HANA.



XAMS Modules

Role Designer

Quickly design SoD-free roles based on usage data using a drag and drop cockpit.

Role Profiler

Analyze and improve the quality of roles and authorizations.

Services

System Analysis incl. S/4HANA Readiness Check
Xiting can provide an analysis of the current roles and transactions affected by the migration, as well as create a catalog of actions for a migration project or the role redesign.

SAP S/4HANA Migration
In the context of a SAP S/4HANA Migration, Xiting will take on the job of designing SAP roles for a successful migration to the new data model in accordance with SAP best practices.

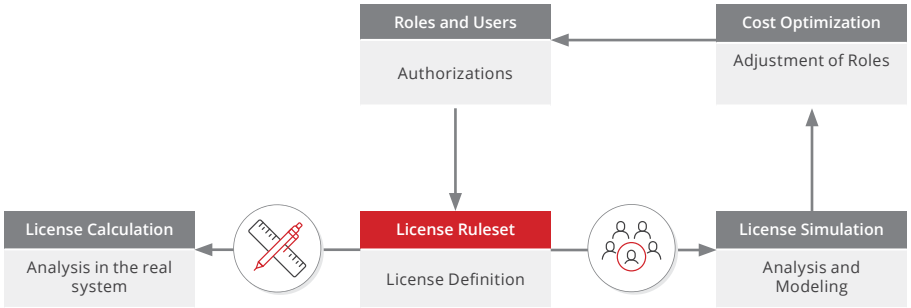
License Analysis for Cost Optimization in SAP S/4HANA

Challenge

The „minimum principle“ and „needs-based roles“ are common requirements in the SAP authorization world. With the switch from usage-based to authorization-based license measurement in S/4HANA and the introduction of new S/4HANA user licenses, implementing these principles in your authorization concept is more important than ever. This is the only way to avoid over-licensing in S/4HANA. The associated changes and the effort involved are difficult to assess for many companies.

Xiting Solution

The integration of SAP’s official license ruleset (see Note 3113382) in XAMS improves transparency and enables efficient license determination with the Role Profiler. The combination with the Role Designer also offers considerable added value. While you are modeling roles in a virtual environment, a check against the license ruleset can be carried out automatically. This allows correct license types to be identified at an early stage and taken into account during the role design. This enables immediate feedback on changes and reveals potential savings in license costs. Optimized SU24 default values further improve the informative value. The ideal time to optimize user licenses is during a redesign project or the introduction of S/4HANA. Ultimately, you can also benefit from cost optimizations during an S/4HANA migration through targeted role adjustments.



XAMS Modules

Role Profiler

Analyze and improve the quality of roles and authorizations.

Role Designer

Quickly design SoD-free roles based on usage data using a drag-and-drop cockpit.

Services

- Installation and configuration of the software solution XAMS in your SAP system landscape, including temporary usage license
- Implementation of the currently valid SAP license rules for an authorization-based analysis
- License analysis based on the existing authorization data for users and roles
- License analysis based on ST03N usage data and forecast of the expected S/4HANA licenses required
- Creation of a results document
- Presentation of results as part of a final meeting

Digital Identity Management

One identity foundation to automate access, enforce governance and stay audit-ready

Challenge

In complex SAP and cloud environments, identities are often fragmented across multiple systems, leading to limited transparency and inconsistent access models. Manual Joiner-Mover-Leaver processes cause delays, increase operational cost, and introduce errors.

Enforcing compliance and Segregation of Duties consistently remains difficult, resulting in a higher risk of unauthorized or excessive access. Frequent organizational changes further disrupt access alignment, making it hard to ensure that permissions always reflect current roles and responsibilities.

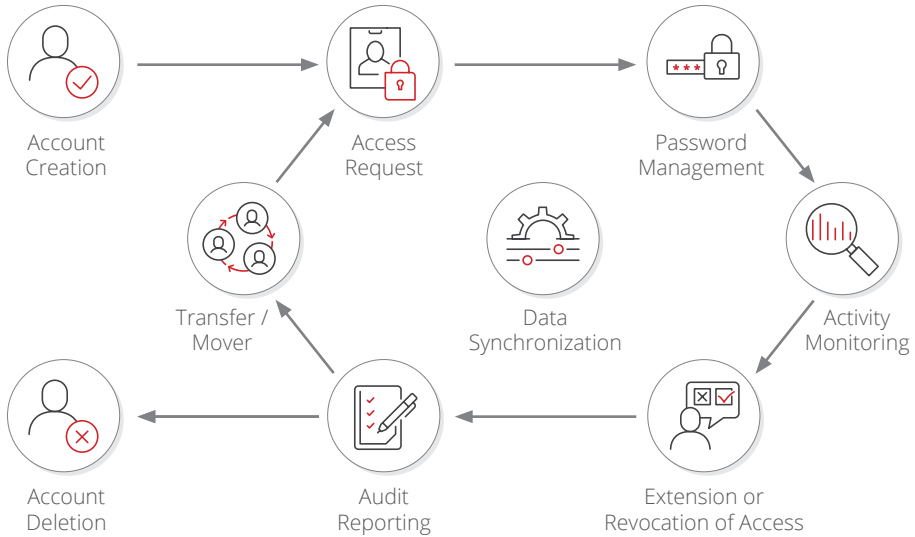
Xiting Solution

The **Xiting Security Platform (XSP)** provides a centralized identity foundation that delivers a single, authoritative view of all identities across SAP and cloud environments. Automated Joiner-Mover-Leaver provisioning ensures that access is granted, adjusted, and removed consistently based on defined rules and governance policies.

Birthright access establishes a secure baseline for new users, while controlled access changes and workflow-driven self-service requests accelerate access delivery without compromising security. Full traceability and audit-ready governance enable continuous compliance and transparency across the entire identity lifecycle.

Managing the Identity Lifecycle

Manage human and non-human identites – including AI agents.



Main Use Cases:

- Synchronization of Credentials and Identity Data
- Joiner / Mover / Leaver
- Birthright Access
- User Self Service
- SoD Risk Analysis & Simulation
- Password Self Service
- Role-based Administration
- Auditing of Access Rights
- Audit Reporting

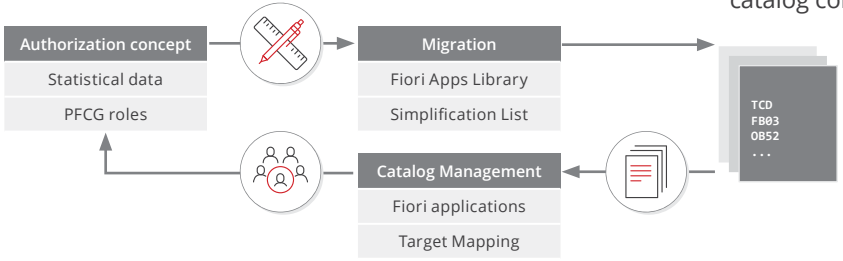
Simplify SAP Fiori Administration

Challenge

Going forward, the use of SAP Fiori applications in SAP S/4HANA is no longer optional, but mandatory. In addition, the minimum requirements for the authorization design must be determined manually with the help of the SAP Simplification List. Not only should the Fiori-related conditions in the role concepts be considered, but also the high dependence on the performance and availability of the SAP Fiori Apps Library presenting companies with new challenges. Lack of evaluation options of the decentralized Fiori Apps Library against the existing local system represents another hurdle.

Xiting Solution

With the help of XAMS, Fiori applications can be determined automatically on the basis of the existing authorization concept. For this purpose, the integrated Fiori Apps Library provides suitable Fiori applications for the objects used. Because of this, a local, high-performance comparison can be carried out. In addition, the mass maintenance of Fiori catalogs for the assignment of Fiori applications (tiles) and target mappings is possible. With the help of Excel import and export interfaces, Fiori catalogs are created quickly and complete. A clear and fast assignment of Fiori catalogs and groups is also made possible in the Role Designer. The Role Profiler then enables automatic consistency checks for Fiori catalog content in SAP roles.



XAMS Modules

Role Designer

Enables the integration of Fiori objects such as catalogs and groups into the existing authorization concept as well as the associated adjustments to the role design.

Role Replicator

Provides mass processing functions via Excel upload to simplify catalog management and object assignment in SAP Fiori administration.

Role Profiler

Produces a detailed overview of Fiori catalog mappings to roles and allows a review and synchronization of required role content (Web services) to ensure consistency.

Services

Our **SAP S/4HANA Workshop (S4W)** explains the main changes and innovations with SAP S/4HANA and the effects on a company's authorization concept. Gain an insight into the function of the authorizations of SAP Fiori applications.

Efficient Fiori App Tracking

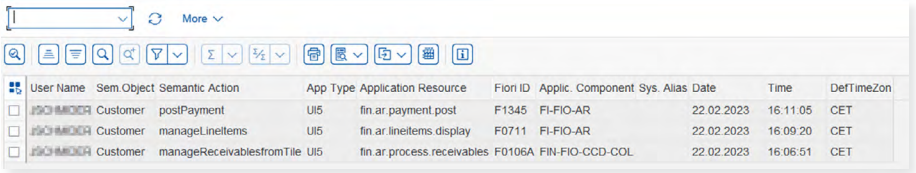
Challenge

Looking to identify the SAP Fiori apps currently in use in your system or considering introducing a new SAP Fiori app? The Fiori App Tracker, which is the latest feature of the Xiting Authorizations Management Suite, is the perfect tool for this job. It enables you to easily identify both currently used and necessary SAP Fiori apps and to streamline their integration into your role concept.

This information is not available in any trace data in SAP standard, making the Fiori App Tracker a valuable tool for simplifying Fiori administration and improving transparency in projects. It helps you to understand which Fiori apps are being used and which are not. This information is useful for optimizing Fiori roles and ensuring that users only have access to the apps they need.

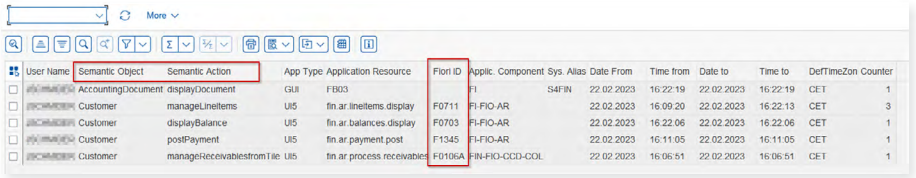
With the Fiori App Tracker, you can compare apps according to the principle of least privilege. This can help to minimize the risk of unauthorized access to sensitive data and improve the overall security of the system.

Another significant benefit is that it enables users to understand the forward navigation within Fiori Apps to related apps. This information can be useful for identifying the relationships between apps and optimizing the user experience. For example, if users frequently navigate from one app to another, combining these apps into roles and pages/spaces may be more efficient or simplify the navigation between them.



Example Usage - Detail View

The detail view offers a breakdown of individual app usage for each user, including semantic object and action, catalog, and target mapping. This view is useful for identifying optimization opportunities.



Example Usage - Summary View

The summarized view provides a high-level overview of app usage, enabling users to identify trends and patterns across multiple apps quickly, while the consolidated report aggregates usage data to gain a holistic view of app usage and identify areas of improvement.

Services

- Identify necessary SAP Fiori applications using the Fiori App Tracker
- Integrated app tracking and simulation of backend roles enable you to develop an audit-compliant authorization concept.
- Coverage analysis, compliance checks and automated role creation
- Full integration with the Xiting Authorizations Management Suite (XAMS)

Test Simulation of Roles and Authorizations

Challenge

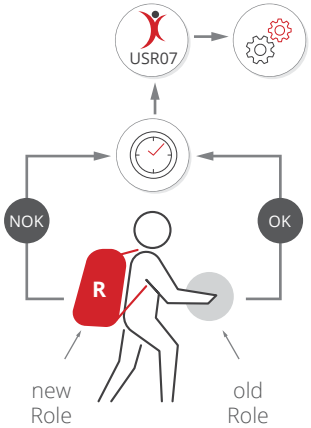
Testing of new roles or changes to existing roles is a time-consuming and expensive process because it requires the input from various stakeholders within an organization.

As part of the Xiting Authorizations Management Suite (XAMS), Xiting has developed a unique solution that virtually eliminates the need for traditional role- or user-acceptance testing (UAT).

Xiting Solution

Productive Test Simulation enables role administrators to simulate authority checks against new or changed roles without negatively impacting the productivity of end users. Efficiencies are gained by allowing the role administrators to analyze and remediate missing authorization values en masse instead of fixing individual errors as they occur. Further benefits are gained by integrated reports that allow for SU24 optimization and filtering of logged data.

During traditional UAT phases, testers must often wait for role administrators to add any missing authorizations that are encountered during testing. The XAMS can automate that process by dynamically creating and assigning delta roles with missing and allow listed authorizations anytime the tester triggers a failed authority check.



Productive Test Simulation (PTS) is made possible by the integrative operation of the XAMS modules **Xiting Times** (operation) and **Role Builder** (analysis).

XAMS Modules

Role Builder

Virtually eliminate the need to test new roles or role changes through an innovative concept called Productive Test Simulation.

Xiting Times

Eliminate the impact on end-users due to missing authorizations during Go-Live.

Services

Take advantage of Xiting's broad range of **training courses and workshops** to learn how to configure and use this technology.

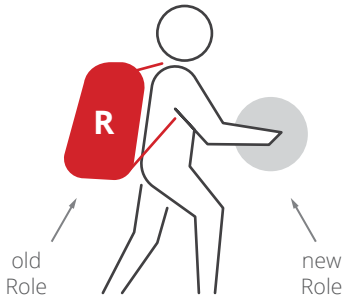
Reduce Go-Live Risk

Challenge

After a role redesign project, missing authorizations constitute a significant risk. Frustrated end-users, loss of productivity, and increased help-desk tickets are just some of the impacts of redesigns, and these challenges are the reason why many companies shy away from role remediation projects. Many companies find it easier and less expensive to just live with the inherent risks that come with over-authorized users.

Xiting Solution

Xiting has developed a solution called Protected Go-Live, which is a core part of the Xiting Times module. With Protected Go-Live, security administrators can enable end-users to temporarily get access to old roles back if an issue arises with the new roles during Go-Live. Stakeholders can build customized workflows around those temporary assignments, including various approval processes, and, of course, all actions taken are logged in an audit-compliant fashion. For end-users, the process is simple and painless as the request for old roles can be done using a simple self-service transaction directly in the system where the issues were encountered.



Working with a “backpack”
Old roles can be reactivated, thereby safeguarding operation

XAMS Module

Xiting Times

Eliminate the impact on end-users due to missing authorizations during Go-Live.

Services

Using Xiting’s **Go-Live service**, we configure the Protected Go-Live and assist in getting new roles up and running.

SAP Security Monitoring & Real-Time Threat Detection

Challenge

Central compliance monitoring doesn't have to be complicated or time-consuming when you monitor defined system settings and checks. By detecting security gaps and implementing security requirements, you can achieve a good level of security. Cybercriminals are constantly discovering new ways to penetrate systems gradually over months. Consequently, attacks are frequently detected too late, and vulnerabilities are exploited.

Systems for cyber-attack detection are therefore leading-edge technology today. These systems establish correlations between different logs collected within SAP systems and provide real-time alerts about potential threats. Depending on the specific needs, these alerts can be sent via email or directly forwarded to a connected SIEM system (SIEM = Security Information Event Management).

SAP Security Monitoring

Central Landscape Monitoring

The focus is on the central monitoring of security-relevant settings and compliance with the defined processes

Overview and Drilldown Perspective

Extensive monitoring and auditing options as well as overview and detailed perspectives

Real-Time Threat Detection

Forwarding Events to SIEM Systems

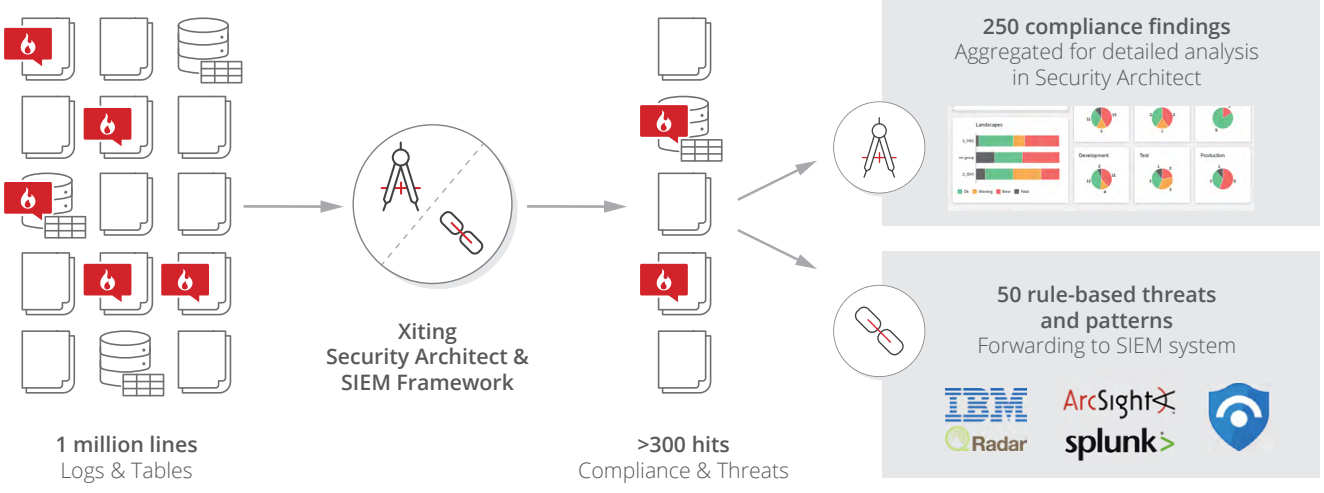
Focuses on instantaneous transfer of logs and alarms to a connected SIEM system

Threat Intelligence

Complex, rule-based detection (intrusion detection pattern) of suspicious activity in your SAP system through intelligent evaluation of log information

Xiting Solution

The Security Architect serves as a central tool for monitoring compliance in SAP systems. The SIEM Framework offers you the option of reading out various SAP logs and forwarding them to your SIEM system in a standardized format. The integrated rule engine enables the evaluation of log entries for potential threats in real time. In this way, safety-critical events can be detected and reported through complex connections.



In order to make the connection of a complex and distributed SAP landscape as simple as possible, the SIEM framework can be operated in a central environment. An SAP ABAP central system is defined, which connects all other SAP systems in the landscape via RFC, controls the log and event collection and communicates with the SIEM system.

In combination with a SIEM system, the Security Architect and the SIEM Framework make even large SAP landscapes evaluable and transparent in real time. They are therefore a crucial component for the integration and development of a holistic security monitoring.

XAMS Modules

Security Architect

Enables central security monitoring beyond its auditing capabilities.

SIEM Connector

Xiting‘s solutions for holistic security monitoring enable companies to better protect SAP systems against internal and external threats and reduce vulnerabilities.

Services

- Integration of SAP landscapes into SIEM systems
- Avoidance of exponentially high costs in SIEM operation
- 250+ Compliance & Threat checks
- 50+ complex intrusion detection patterns for real-time log analysis

Simplify Role Design

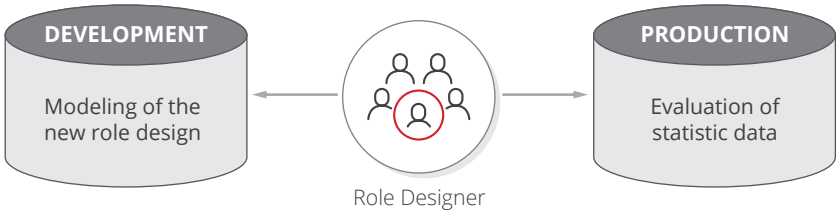
Challenge

Role redesign projects are time-consuming and expensive, which is why many organizations delay them or avoid them all together. One of the problems of role remediation projects is that they involve a variety of different stakeholders beyond the technical teams, including regular end-users, whose productivity may suffer because of their involvement in such projects.

Xiting Solution

Xiting has developed the Xiting Authorizations Management Suite (XAMS), which automates and simplifies many of the tasks involved in a role redesign project, including:

- Analyzing and identifying issues in the current role concept
- Optimizing SU24 to improve the quality of the roles
- Maintaining organizational fields and batch-processing of roles
- Preventing and mitigating SoD conflicts
- Simulating the impact of role changes
- Automating role testing with zero end-user involvement
- Reducing the risk during Go-Live
- Automated scanning of custom ABAP code for missing authority checks
- Optimizing SAP licensing by tuning the roles of over-authorized users
- Simplifying SAP security audits



XAMS Module

Role Designer

Quickly design SoD-free roles based on usage data using a drag and drop cockpit.

Services

Using XAMS, Xiting can redesign ABAP roles without disrupting the work of the business users. Xiting's automation technologies drastically reduce the duration or role remediation projects and deliver sustainable role concepts based on SAP best practices.

The **System Analysis Service** offers an analysis of identified SAP environments to provide recommendations and time/cost estimates in preparation for a role redesign project.

Ensuring Role Quality

Challenge

Regardless of whether using single, derived, composite or even value (enabler) roles, maintaining an authorization concept is challenging and often requires a lot of resources. That is why roles tend to deteriorate in quality over time, especially as business processes change, for example, due to mergers and acquisitions.

Xiting Solution

The Role Profiler module is a solution consisting of over 95 analysis reports that can help identify, fix, and prevent quality problems in roles and authorizations. The Role Profiler can help perform:

- **Reporting & Analysis**
  Quickly identify common issues, such as open or manual authorizations.
- **SU24 Hardening**
  Assist in updating and maintaining the SAP proposal database (SU24).
- **Role Versioning**
  Detect changes to roles and automatically create a new version that administrators can easily revert to if the need arises.
- **Coverage Analysis**
  Analyze role and transaction usage and coverage.
- **Violation of Segregation of Duties**
  Detect roles with critical authorizations or combinations (SoD). XAMS can even be integrated with SAP GRC.
- **Display Role Enforcement**
  Identify display roles that contain authorizations that lead to more than display (e.g., change, delete, insert, etc.).
- **Critical Access Watchdogs**
  Identify roles with access to master data or HR data.
- **SAP S/4HANA Compatibility**
  Analyze role compatibility against SAP S/4HANA Simplification List and much more.

XAMS Module

Role Profiler

Analyze and improve the quality of roles and authorizations.

Services

Xiting's consultants carry out a security check in SAP systems, identifying potential vulnerabilities in an SAP security concept based on best practice recommendations for security settings. In addition to checking the quality and security of authorizations, Xiting also checks other key subjects regarding system settings, documents, and users.

Emergency Access Management (EAM) / Privileged Access Management (PAM)

Challenge

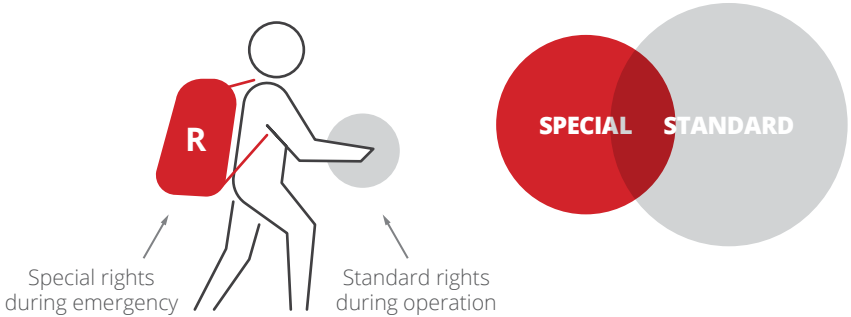
High privileged accounts pose a significant security and compliance risk to your organization. It is important to effectively manage privileged access to ensure compliance. This includes approval processes for the use of privileged access, as well as review processes after a session has concluded.

Xiting Solution

Our solutions utilize the standard SAP reference user for privileged access. A reference user extends a users' authorizations so that privileged access can be assigned indirectly by leveraging the reference user. Our tools then trace and monitor any activity that the end user performs during the privileged sessions and provide 20+ log files to be analyzed during the review process.

In comparison to other solutions that offer EAM/PAM functionality, the end user remains in his or her own user context. That means that all log files, table entries, change documents, etc., are written in the user's context. While reviewing change logs, e.g., during an audit, the user's name will be displayed instead of a generic technical user, as most other solutions use.

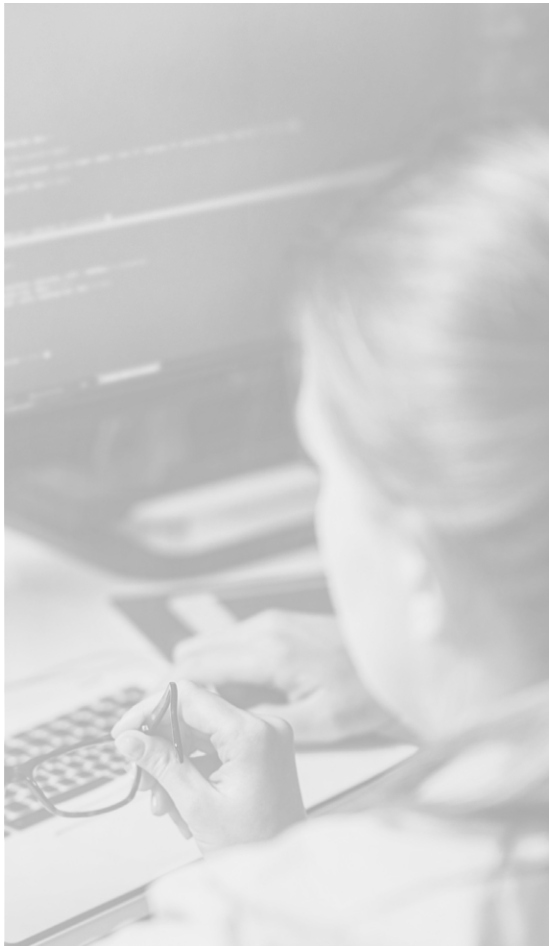
PAM access can be requested either via workflow for ad-hoc use, or pre-approved for emergency scenarios. Ad-hoc use can be requested via workflow and also allows delayed start of session which means that the privileged access can be approved ahead of time (e.g., during a maintenance window).



XAMS Module

Xiting Times

Enables the privileged access management scenario with the same capabilities as have been seen in the services Protected Go-Live and Productive Test Simulation.



Creation of Security Strategy Document

Challenge

SAP Security is a very broad and complex topic. New features are regularly made available by SAP, and defining the best practices of which features to use, or settings to enforce, requires considerable experience.

That applies particularly to large system landscapes where global policies and minimum-security standards are not only difficult to define, but are even harder to monitor and enforce.

Xiting Solution

With the Security Architect, an administrator can generate, publish, and monitor SAP Security Concept best practices at the push of a button. When combined with Solution Manager, the administrator can manage the global SAP Security Concepts and compare them against connected systems.

Security Architect can create an entire security concept (in the form of a document) by using best practices templates, which are included, and can be adapted to the needs of an organization.

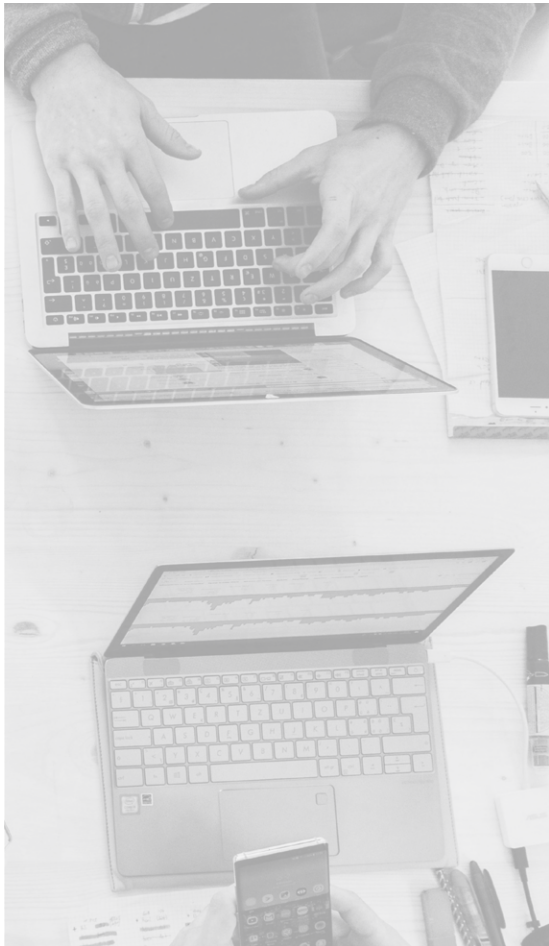
Check Mode helps compare a system's actual state with the target state. This process can be carried out locally for one system as well as from a central system (e.g., Solution Manager) for several systems.

Thus, it is possible to test and monitor a system security configuration at any time and to save test results. Compliance with the requirements can then be compared over time and tracked accordingly.

XAMS Module

Security Architect

Delivers ready-to-use security concepts for SAP that are based on best practices, SAP security guidelines, and Xiting's decades of experience in the field of SAP security. It significantly reduces the effort involved in SAP security audits, instantly checks the compliance of the SAP landscape, and monitors progress and compares results for individual compliance reports.



Optimize RFC Interfaces

Challenge

RFC interfaces play a crucial role in many SAP implementations by enabling data exchange between SAP systems as well as between SAP and non-SAP systems. Unfortunately, many RFC interfaces are “over-authorized” and have more powerful roles than necessary. This opens up critical vulnerabilities in SAP landscapes.

Xiting Solution

The Xiting Authorizations Management Suite (XAMS) solution can safely reauthorize RFC interfaces and associated technical users without negatively impacting the operation of the interface.

XAMS achieves this by analyzing the interface’s activity in the productive landscape and automatically creating actionable reports that role administrators can use to quickly create matching roles in a development environment. This concept has helped countless customers, such as AUDI and DAIMLER, to optimize RFC interfaces without interrupting operation.

SAP endorses Xiting’s solution as the best-practice approach for an RFC Redesign in OSS Note 1682316.

XAMS Modules

Role Builder

Virtually eliminate the need to test new roles or role changes through an innovative concept called Productive Test Simulation (PTS).

Role Profiler

Analyze and improve the quality of roles and authorizations.

Services

Xiting's **service for analysis and authorization optimization of technical users for RFC and background processing** enables compliant maintenance of a system landscape.

Xiting optimizes system users' authorization and eliminates any excessive authorizations without negatively impacting ongoing business processes.

Handling of Organizational Structures in the Role Concept

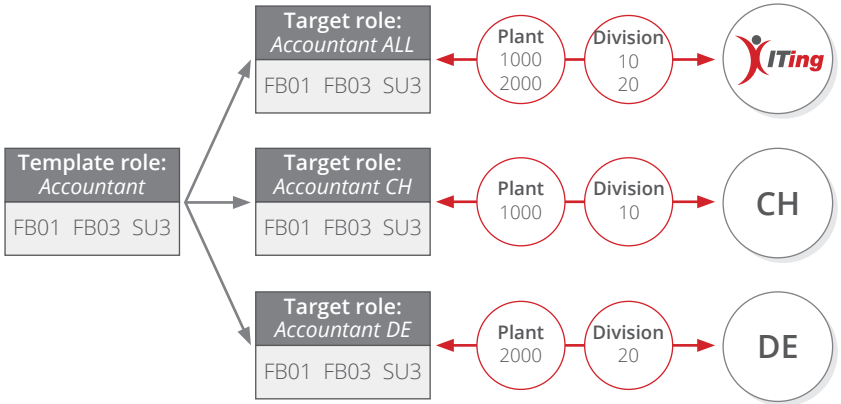
Challenge

Sustainable and transparent authorization management of complex corporate structures in accordance with GDPR cannot be mapped efficiently in the SAP standard system. This makes the development and operation of organizational structures in the role concept not only time-consuming, but also error-prone. New requirements, in terms of organizational set-up and the subsequent changes to organizational structures, tie up important resources.

Xiting Solution

The Role Replicator uses organization sets to define the specific organization values that need to be applied to roles. By utilizing the tools in the Role Replicator, the task of implementing and maintaining organization sets is quick and hassle-free.

- Automatically transfer existing customizing structures from the SAP system
- Mass-replicate roles and characteristics of organizational levels in a single step
- Apply batch changes to organizational levels
- ICS reporting for comparing defined organization sets (target) with SAP roles (actual)



XAMS Module

Role Replicator

Mass role replication and batch processing tools to reduce the role maintenance effort.

Services

As part of Xiting's ERP authorization projects, we transfer the restrictions from a company structure into a role concept, thereby, not only ensuring dedicated access, but also delivering a maintainable role concept.

Mass Processing of Users, Roles & Authorizations

Challenge

In complex, multi-layer, and multi-system landscapes, creating new users or roles represents a major challenge for security and basis administrators. It is extremely easy to lose track of naming conventions, security design concepts, internal rules, and external regulations.

Xiting Solution

The Role Replicator enables quick and mass administration of roles and users. The integrated upload and download functions using Excel offer additional ease of use when processing large volumes of data. The most popular functions in the Role Replicator tool include:

- Mass creation of users and mass processing of user master data, including role assignments
- Mass assignment of single roles to composite roles as well as mass deletion of roles
- Mass maintenance of role descriptions as well as mass maintenance for other languages
- Mass maintenance of SAP Fiori components like catalogs, groups, pages, spaces, and sections
- Versioning of roles enables changes to be tracked, role backups to be taken prior to upgrades, older versions of roles to be compared to newer versions, and restoration of older versions to be made, if required

XAMS Module

Role Replicator

Mass role replication and batch processing tools to reduce the role maintenance effort.

Services

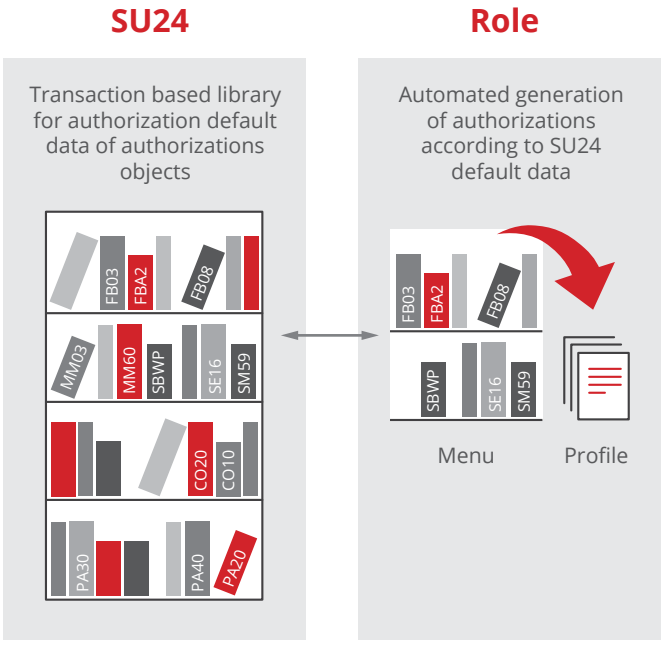
Take advantage of Xiting's broad range of **training courses and workshops** to learn how to configure and use this technology. Xiting will be happy to assist in using this technology in consulting projects.

SU24 Optimization

Challenge

Enhancing the quality and security of SAP roles? Dealing with a large maintenance workload and unpredictable risks due to manually added or modified authorizations? Aware of the difficulties associated with a role upgrade and looking to prepare for it in the best way possible?

Transaction SU24 forms the basis for the secure and efficient creation of roles; it is therefore one of the most important transactions in SAP Security. Maintaining the values in SU24 can often be overlooked, causing role creation and maintenance to be error prone.



Xiting Solution

The XAMS software includes tools with multiple integration points to help SAP customers automate the maintenance of SU24 values. By optimizing SU24 values, the task of role creation and maintenance is significantly reduced.

XAMS Modules

Role Profiler

Analyze and improve the quality of roles and authorizations.

ABAP Alchemist

Improve the quality and security of existing and new ABAP code, and quickly find reusable code via the API finder.

Role Builder

Virtually eliminate the need to test new roles or role changes through an innovative concept called Productive Test Simulation.

Services

SU24 Optimization Service
In accordance with SAP best practices, Xiting's consultants maintain and optimize SU24 efficiently.

Streamline Security Audits

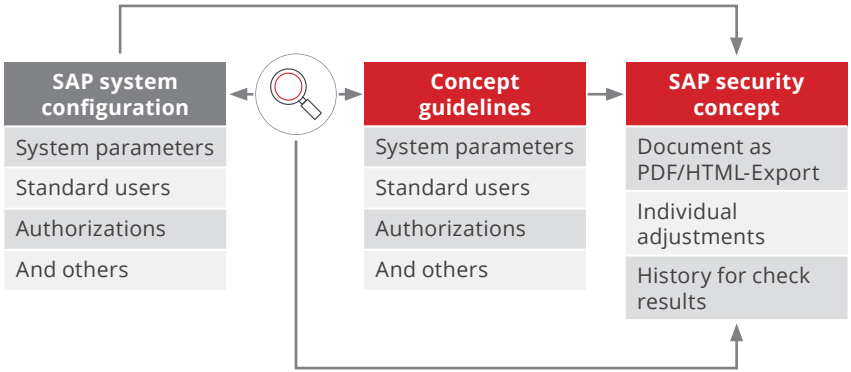
Challenge

SAP security audits are an excellent tool to identify issues and vulnerabilities that malicious users or disgruntled employees could exploit to negatively impact the brand or bottom line of an organization. At the same time, nobody wants to get hit with audit findings that should have been mitigated in advance.

Xiting Solution

The Security Architect module is a solution that allows security administrators and other system stakeholders to continuously monitor SAP systems for issues that could get flagged during an audit.

Based on Xiting's decades of experience in SAP security and Xiting's close collaboration with major auditing firms, Security Architect delivers ready-to-use, yet easily customizable, security concepts that describe how SAP systems and its various components and applications should be set up and configured. Built-in checks then compare the information in the concept with actual system parameters and report on any discrepancies.



XAMS Module

Security Architect

Fully integrated SAP security concepts for ongoing audits and compliance testing.

Services

Use the **SAP security monitoring & ICS service** to have security specifications analyzed and optimized. Designing and configuring an ICS will ensure ideal preparation for audits.

Reduce SoD Conflicts

Challenge

Segregation of Duties (SoD) conflicts can have major financial implications for organizations, such as in cases of fraud. A SoD conflict arises when a single user is authorized for a combination of specific critical business processes. For example, a SoD conflict exists if the same user can create new vendors and release payments to vendors. Such a conflict enables the potential for fraud and other compliance issues, which is why many large organizations leverage Governance, Risk, and Compliance (GRC) solutions to identify and mitigate SoD conflicts.

Xiting Solution

While Xiting is not a competitor in the GRC market, the company has developed integrations with Access Control, SAP's GRC solution, enabling role administrators to identify and mitigate SoD conflicts already present during the role design phase. The advantage of being able to identify potential conflicts before committing to role changes is that it takes less effort to mitigate these risks before they materialize in the production landscape.

In addition, Xiting delivers rule sets containing critical authorizations suitable for small- and medium-sized customers for which deploying a full-fledged GRC solution would be excessive. Xiting's SoD analytics engine is available in Role Profiler and Role Designer, part of the Xiting Authorizations Management Suite (XAMS).

XAMS Modules

Role Profiler

Analyze and improve the quality of roles and authorizations.

Role Designer

Quickly design SoD-free roles based on usage data using a drag and drop cockpit.

Services

Xiting's security consultants implement and configure the **XAMS** solution, enabling an organization to provide extended rights for emergency actions in an efficient and verifiable manner.

Contact

North America

Alessandro Banzer
CEO USA

Email: abanzer@xiting.com
Tel: +1 813 598 7494

Derek Prieto
Vice President Sales

Email: dprieto@xiting.com
Tel: +1 786 271 4242

Latin America

Andrea Londoño
Business Development Representative

Email: alondono@xiting.com
Tel: +57 31 1326 7358

Xiting AG

Chüchelacherstrasse 5
8165 Schöfflisdorf
Switzerland

Tel: +41 43 422 88 03
Fax: +41 43 422 87 93

Xiting GmbH

Obere Ringstraße 17
79859 Schluchsee
Germany

Tel: +49 7656 8999 002
Fax: +49 7656 8999 009

Xiting LLC

235 Apollo Beach Blvd
Suite 314, Apollo Beach, FL
33572 United States

Tel: +1 813 598 7494
Fax: +1 813 433 5670

Email: info@xiting.com

Web: www.xiting.com

Xiting UK Ltd.

56 Broad Street
Chipping Sodbury
Bristol BS37 6AG
United Kingdom

Tel: +44 1454 838 785

Xiting ROM SRL

Strada Constantin Brâncuși 21
400458 Cluj-Napoca
Romania

Tel: +40 364 630 823

www.xiting.com