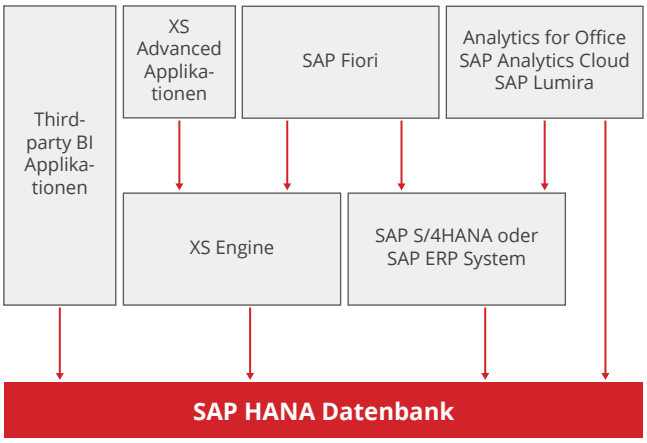
XAMS

Sicherheit schaffen in SAP HANA Datenbanken

SAP-Berechtigungskonzepte und Systemarchitekturen

Für die Risikoeinschätzung wird SAP HANA häufig als ein gewöhnliches Datenbankmanagementsystem verstanden wie jedes andere auch. Außer Acht gelassen wird dabei die enge Integration von Applikation und Datenbank, die sich auf die unternehmenseigenen Prozesse und Verantwortlichkeiten auswirken. SAP S/4HANA ist heute bei vielen Unternehmen die zentrale Applikation für eine Vielzahl an Prozessen, einschließlich des Reportings (meist über SAP Fiori Apps). Zwar ist für die Nutzung der Reporting-Funktionalitäten kein unmittelbarer Zugriff auf eine SAP HANA Datenbank nötig, doch können komplexe Modellierungen Szenarien auf den Plan rufen, die über die klassische Administration durch die SAP Basis hinausgehen und weitere Anwendergruppen in der SAP HANA Datenbank vorsehen.

Je nach Anwendungsszenario sind Direktzugriffe auf die SAP HANA Datenbank jedoch durchaus denkbar wie die Abbildung unten beispielhaft aufzeigt. Aber auch ohne Direktzugriff sind interne Kontrollen konsequent anzuwenden, um jegliches Risiko zu mitigieren, welches die Integrität und Konsistenz der Daten gefährden könnte.



Die Konsequenz ist die Notwendigkeit einer übergreifenden Risikobetrachtung einer komplexeren Systemarchitektur mit Auswirkungen auf die IT Governance. Es drängen sich mehrere Fragestellungen auf, welche durch ein Berechtigungskonzept beantwortet werden sollten:

- Welche Berechtigungen (Privilegien) benötigen die Anwendergruppen?
- Wie erstelle ich ein globales Berechtigungskonzept für meine gesamte SAP-Systemlandschaft einschließlich SAP HANA?
- Wie schütze ich die ABAP-Produktivdaten richtig?
- Wie ist eine revisionssichere Änderungsprotokollierung sichergestellt?
- Wie ermögliche ich ein angemessenes Notfallbenutzermanagement?
- Wer ist für die Verwaltung technischer Benutzer verantwortlich?

Ein integrativer Ansatz für Berechtigungen und Prozesse in SAP HANA

Für den Zugriff auf SAP HANA bildet ein Privilegien-Framework die Grundlage. Die Administrations- und Entwicklungsoberflächen unterscheiden sich mit dem Web IDE, HANA Cockpit oder HANA Studio fundamental von Bekanntem aus dem ABAP-Umfeld. Folglich lassen sich bestehende Berechtigungs- und Rollenkonzepte sowie zugehörige Prozesse zur Benutzer- und Berechtigungsverwaltung nicht analog anwenden.

Unterstützt werden kann dies aber durch die Integration der SAP HANA-Berechtigungsverwaltung im ABAP mittels der DBMS-Funktionalität oder einer dedizierten Schnittstelle zur Verwaltung der SAP HANA-Sicherheitsfunktionalitäten.

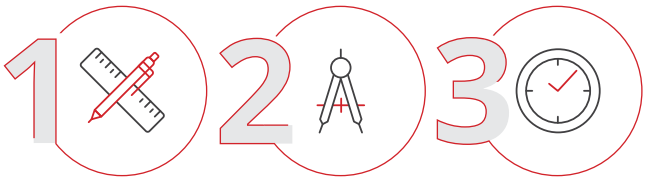
XAMS

Sicherheit schaffen in SAP HANA Datenbanken

MEHRWERT DER XAMS

Die Xiting Authorizations Management Suite (XAMS) eignet sich als bekanntes ABAP-basiertes Werkzeug bestens für die Überwachung der Sicherheitsparameter und Berechtigungen in SAP HANA. Die Funktionalitäten für SAP HANA sind in den jeweiligen XAMS Modulen nahtlos integriert. Die XAMS unterstützt Sie in den folgenden Anwendungsbereichen:

- Prüfung der SAP HANA-Sicherheitsparameter
- Prüfung der Audit Log Konfiguration
- Risikoanalyse von kritischen Berechtigungen
- Auswertung von Benutzern und Rollen
- Auswertung der Audit Logs
- Erstellung eines SAP HANA-Berechtigungskonzepts
- Security Monitoring (inkl. SIEM-Integration)
- Überwachung von technischen Benutzern
- Notfallbenutzermanagement und Auswertung



HANA Role Profiler | **HANA Security Architect** | **HANA Xiting Times**

UNSERE DIENSTLEISTUNG

Wir unterstützen Sie dabei, Ihre Organisation für Anforderungen an die Sicherheit in SAP HANA zu sensibilisieren. Darüber hinaus sind wir Ihr kompetenter und zuverlässiger Partner für die Abbildung dieser Anforderungen in einem Berechtigungskonzept – abgestimmt auf relevante Risiken und im Einklang mit Ihrem Kontrollsystem. Mit einem Regelwerk ermöglichen wir Ihnen die identifizierten Risiken im Blick zu behalten. Haben Sie bereits den ersten Schritt vollzogen und ein SAP HANA-Berechtigungskonzept implementiert, unterstützen wir Sie gerne mit einer Prüfung Ihrer Kontrollen und und geben Handlungsempfehlungen.

Best Practice Workshop

- Aufbau eines gemeinsamen Verständnisses zu SAP HANA und Klärung von Begrifflichkeiten
- Darstellung der möglichen Einsatzszenarien einer SAP HANA Datenbank
- Darstellung der SAP HANA Security-Funktionalitäten
- Erfahrungswerte von diversen SAP HANA-Berechtigungsprojekten aus der Praxis

Berechtigungskonzept

- Workshop zur Besprechung eines grundlegenden SAP HANA-Berechtigungskonzepts sowie Erarbeitung eines SAP HANA-Rollenkonzepts
- Implementation der definierten Rollen in einem SAP HANA Datenbank-System/Systemverbund
- Definition und Aktivierung der Änderungsprotokollierung (Auditierung)

SAP HANA

Security Check

- Sicherheitsüberprüfung Ihrer SAP HANA Datenbank mit Identifikation allfälliger Risiken
- Aufzeigen von Best Practices in der Berechtigungsverwaltung in SAP HANA
- Berichterstattung mit Handlungsempfehlungen

Regelwerk

- Workshop zur Definition eines SAP HANA-Regelwerks zur Risikoanalyse
- Klärung der Prozesse und Verantwortlichkeiten in der Risikoanalyse
- Implementierung des Regelwerks
- Durchführung einer Risikoanalyse
- Bewertung und Mitigation von Risiken

Weiterführende Informationen unter:
info@xiting.com
www.xiting.com

Tel: **+49 7656 9888 155**

Tel: **+41 43 422 8803**

SAP® Recognized Expertise
Governance, Risk, and Compliance

© 2021 Xiting AG. All rights reserved