Prüfmatrix SAP S/4HANA

Die Einführung von SAP S/4HANA hat die IT-Landschaft zahlreicher Unternehmen grundlegend verändert. Die Umstellung auf diese fortschrittliche Plattform erfordert eine präzise Überprüfung und kontinuierliche Überwachung. Dabei spielen insbesondere die Datenbanken eine zentrale Rolle für die Sicherstellung der Integrität, Sicherheit und Performance von SAP S/4HANA-Systemen.

Die Fachgruppe SAP des ISACA Germany Chapter e.V. hat eine Prüfmatrix entwickelt, um die Überprüfung und Überwachung zu unterstützen. Sie enthält Risiken und Kontrollen sowie Vorgehensweisen, um die Kontrollen zu überprüfen.

Adressaten

Die Prüfmatrix richtet sich damit nicht nur an IT-Revisoren und IT-Auditoren, sondern unterstützt bei der Umsetzung von Anforderungen, die von IT-Governance und IT-Compliance entstehen. Insbesondere die SAP-Verantwortlichen sollen mit dieser Prüfmatrix in die Lage versetzt werden, das bestehende interne Kontrollsystem auszubauen und zu verbessern.

Kriterien

Bei der Auswahl der Risiken bzw. Kontrollziele wurden die allgemeinen IT-Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität, herangezogen. Darüber hinaus wurden die Ordnungsmäßigkeits- und Sicherheitsanforderungen der IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1, Stand: September 2002) zugrunde gelegt.

Aufbau internes Kontrollsystem

Ein effektives internes Kontrollsystem (IKS) ist essenziell, um die Einhaltung der Compliance- und Governance-Anforderungen im SAP S/4HANA-Umfeld zu gewährleisten. Die Prüfmatrix unterstützt Unternehmen dabei, ihre internen Kontrollprozesse systematisch zu strukturieren und Schwachstellen gezielt zu identifizieren.

Im Bereich Compliance bezieht sich die Prüfung insbesondere auf die Einhaltung regulatorischer Vorgaben, wie Datenschutz-Grundverordnung (DSGVO), GoBD, SOX oder branchenspezifische Anforderungen. Governance-Aspekte betreffen die übergeordnete Steuerung und Überwachung der IT-Systeme, um Risiken zu minimieren und Geschäftsprozesse nachhaltig abzusichern.

Zentrale Prüfbereiche in diesem Kontext umfassen:

- Berechtigungs- und Rollenmanagement zur Sicherstellung des Least-Privilege-Prinzips
- Protokollierung und Monitoring zur frühzeitigen Erkennung von Compliance-Verstößen
- Change-Management-Prozesse zur Nachvollziehbarkeit von Änderungen im SAP-System
- Datenintegrität
- Archivierung gemäß gesetzlicher Aufbewahrungspflichten

Durch die Integration dieser Kontrollmechanismen wird die Sicherheit und Ordnungsmäßigkeit des SAP S/4HANA-Systems sichergestellt.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Prüfung mit der Matrix

Diese Prüfmatrix stellt ein wertvolles Instrument für die strukturierte und systematische Prüfung wesentlicher SAP-Prüffelder dar, insbesondere im Zusammenhang mit der Datenbank und dem Betriebssystem. Er bietet eine sorgfältig zusammengestellte Sammlung von Prüfungsschritten, unterteilt in thematische Bereiche, und umfasst die Identifikation von Risiken, die Darstellung möglicher Kontrollmechanismen sowie ausführliche, schrittweise erklärte Prüfungshandlungen. Wir sind überzeugt, dass er ein essenzielles Werkzeug darstellt, um eine fundierte und wirkungsvolle Prüfung von SAP-Systemen durchzuführen und dadurch die Sicherheit dieser Systeme nachhaltig zu gewährleisten.

Die Matrix unterstützt Prüfaktivitäten, indem sie als strukturierte Grundlage für IT-Prüfungen dient. Sie ermöglicht eine nachvollziehbare Bewertung der implementierten Kontrollen und hilft dabei, die Einhaltung von Sicherheits- und Compliance-Vorgaben systematisch zu überprüfen. Dabei kann sie sowohl in internen als auch externen Prüfungen angewendet werden und bietet eine standardisierte Vorgehensweise zur Beurteilung von Schwachstellen und zur Ableitung geeigneter Maßnahmen.

Ein risikoorientierter Ansatz konzentriert sich auf die Identifikation, Bewertung und Priorisierung von Risiken, die die Integrität, Sicherheit und Ordnungsmäßigkeit eines Systems beeinträchtigen könnten. Er zielt darauf ab, die Prüfungsressourcen auf die Bereiche zu fokussieren, die die größten potenziellen Risiken bergen, um sicherzustellen, dass die relevanten und kritischen Aspekte eines Systems geprüft werden.

Durch die Anwendung dieses Ansatzes im Rahmen von Prüfungshandlungen wird es möglich, gezielt die Bereiche eines Systems zu untersuchen, die für die Geschäftskontinuität und die Einhaltung gesetzlicher Vorschriften am kritischsten sind. Das Ziel ist, Schwachstellen frühzeitig zu identifizieren und Maßnahmen zur Risikominimierung zu ergreifen. Dieser Ansatz ermöglicht eine effiziente und effektive Nutzung der Prüfungsressourcen und erhöht die Wahrscheinlichkeit, dass wesentliche Risiken erkannt und adressiert werden.

In unserer Veröffentlichung bedeutet der risikoorientierte Ansatz, dass die dargestellten Prüfungshandlungen so strukturiert sind, dass sie gezielt auf potenzielle Schwachstellen und Risiken eingehen. Dies gewährleistet, dass die Beurteilung der Ordnungsmäßigkeits- und Sicherheitsanforderungen mit einem hohen Maß an Sicherheit und Genauigkeit erfolgt.

Anwendung der Prüfmatrix

Die im weiteren Verlauf dargestellte Tabelle ist wie folgt aufgebaut:

- Kontrollnummer: Eine eindeutige Identifikationsnummer, die jeder Kontrolle zugeordnet ist. Sie dient dazu, die Kontrolle in der Dokumentation und einer möglichen Berichterstattung einfach und eindeutig zu referenzieren.
- Prüfbereich: Der spezifische Bereich oder das Modul innerhalb des SAP-Systems, auf den sich die Kontrolle bezieht.
- Risiko: Eine Beschreibung des potenziellen Risikos, das die Kontrolle adressiert. Dies beinhaltet die möglichen negativen Auswirkungen, die eintreten könnten, wenn die Kontrolle nicht wirksam ist.
- Kontrollziel: Das spezifische Ziel oder der Zweck der Kontrolle, das beschreibt, was durch die Implementierung der Kontrolle erreicht werden soll. Dies kann die Sicherstellung der Datenintegrität, die Verhinderung von unautorisierten Zugriffen oder die Einhaltung von Compliance-Anforderungen umfassen.
- Kontrollbezeichnung: Der Name oder die Kurzbeschreibung der Kontrolle. Diese Bezeichnung gibt einen schnellen Überblick über die Art der Kontrolle.
- Kontrollbeschreibung: Eine detaillierte Erklärung der Kontrolle, die erläutert, wie die Kontrolle durchgeführt wird und welche Schritte involviert sind. Sie beschreibt die Mechanismen und Prozesse, die implementiert sind, um spezifische Risiken zu managen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

- **Aufbauprüfung:** Prüfungshandlung, die darauf abzielt, die Existenz und die ordnungsgemäße Implementierung der Kontrolle zu bestätigen. Sie überprüft, ob die Kontrollmechanismen angemessen, eingerichtet und dokumentiert sind.
- **Funktionsprüfung:** Prüfungshandlung, die sich darauf konzentriert, die tatsächliche Wirksamkeit der Kontrolle in der Praxis zu bewerten. Es wird geprüft, ob die Kontrolle wie beabsichtigt funktioniert und die festgelegten Ziele erreicht.
- **Erwartetes Ergebnis:** Eine Beschreibung des erwarteten Ergebnisses, wenn die Kontrolle ordnungsgemäß funktioniert. Dies bietet eine Basislinie für die Bewertung der Wirksamkeit der Kontrolle und hilft, Abweichungen oder Schwachstellen zu identifizieren.

Wir sind zuversichtlich, dass diese Matrix Prüfern und IT-Experten dabei hilft, die Herausforderungen der IT-Revision im Kontext von SAP S/4HANA erfolgreich zu meistern. Wir danken allen Autoren und Beteiligten, die an der Erstellung dieser Veröffentlichung mitgewirkt haben.

Haftungsausschluss

Die Informationen und Inhalte in dieser Veröffentlichung wurden von der Fachgruppe SAP des ISACA Germany Chapter e.V. mit größter Sorgfalt und nach bestem Wissen und Gewissen erstellt. Diese Veröffentlichung dient als allgemeine Orientierungshilfe und soll Unternehmen sowie Fachleute dabei unterstützen, eine risikoorientierte Prüfung und Überwachung von SAP S/4HANA-Systemen durchzuführen. Er stellt jedoch keine umfassende oder abschließende Anleitung dar und ersetzt nicht die individuelle Beratung durch qualifizierte Experten.

Der ISACA Germany Chapter e.V. übernimmt keine Gewährleistung für die Aktualität, Richtigkeit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Die Nutzung der Inhalte erfolgt auf eigene Gefahr des Nutzers. Es wird keine Haftung für direkte oder indirekte Schäden, einschließlich entgangener Gewinne, Datenverluste oder sonstige Schäden übernommen, die aus der Nutzung oder Nichtnutzung der in dieser Veröffentlichung enthaltenen Informationen entstehen könnten.

Die beschriebenen Prüfungsmaßnahmen und Empfehlungen sind als allgemeine Richtlinien zu verstehen und sollten stets im Kontext der spezifischen Gegebenheiten und Anforderungen des jeweiligen Unternehmens angewendet werden. Es wird empfohlen, bei der Umsetzung der dargestellten Prüfungen und Kontrollen stets individuelle rechtliche und fachliche Beratung in Anspruch zu nehmen.

Der ISACA Germany Chapter e.V. behält sich das Recht vor, die Inhalte dieser Veröffentlichung jederzeit ohne vorherige Ankündigung zu ändern oder zu aktualisieren.

SAP S/4HANA ist eine Marke oder eingetragene Marke der SAP SE oder ihrer verbundenen Unternehmen in Deutschland und anderen Ländern.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-be-zeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
HANA-DB-LOG-01	Protokollierung	Aktivitäten auf der HANA-DATENBANK sind nicht nachvollziehbar. Bei dem Verdacht auf Missbrauch kann im Nachhinein nicht auf automatische Systemaufzeichnungen zurückgegriffen werden.	Sicherheitsrelevante Ereignisse werden protokolliert.	Einstellungen	Die SAP HANA-Datenbank-Protokollierung (auditing configuration) ist aktiviert.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob die SAP HANA-Datenbank-Protokollierung in der auditing configuration aktiviert ist. Dies kann über folgendes SQL-Statement abgerufen werden: `SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'global_auditing_state' AND VALUE !='true';` Alternativ kann eine Abfrage über das SAP HANA Cockpit erfolgen: *App "Resource Directory" -> System auswählen -> "System Overview" -> Filter by Area "Security" -> Auditing*	Die Protokollierung der SAP HANA-Datenbank wurde aktiviert. Der Wert im Feld *global_auditing_state* ist *TRUE*.

HANA-DB-LOG-02	Protokollierung	Aktivitäten auf der HANA-DATENBANK sind nicht nachvollziehbar. Bei dem Verdacht auf Missbrauch kann im Nachhinein nicht auf automatische Systemaufzeichnungen zurückgegriffen werden.	Sicherheitsrelevante Ereignisse werden protokolliert und regelmäßig überprüft.	Zugriff und Aufbewahrung	Die SAP HANA-Datenbank-Protokolleinträge werden angemessen gespeichert und aufbewahrt. Protokolleinträge werden vor dem ändernden Zugriff von Datenbankadministratoren und Betriebssystemadministratoren geschützt.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.
						Prüfung der Beschreibung der Vorgaben und der Nachweise über Art, Umfang und Speicherung der Protokolldaten.
							Prüfung, an welchem Speicherort die Protokolleinträge gesichert werden. Der Speicherort kann über folgendes SQL-Statement eingesehen werden:
							`SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'default_audit_trail_type'`
							Prüfung, an welchem Speicherort die Protokolleinträge des Audit-Levels "Emergency" gespeichert werden. Dies kann über folgendes SQL-Statement abgerufen werden:
							`SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'emergency_audit_trail_type'`
							Prüfung, an welchem Speicherort die Protokolleinträge des Audit-Levels "Alert" gespeichert werden. Dies kann über folgendes SQL-Statement abgerufen werden:
							`SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'alert_audit_trail_type'`
							Prüfung, an welchem Speicherort die Protokolleinträge des Audit-Levels "Critical" gespeichert werden. Dies kann über folgendes SQL-Statement abgerufen werden:
							`SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'critical_audit_trail_type'`
							Erfolgt die Speicherung der Audit-Protokolle in der Datenbank (*default_audit_trail_type=CSTABLE*), ist zu prüfen, wie lange die Audit-Protokolle gespeichert werden (mit Ablauf der angegebenen Zeit erfolgt eine automatisierte Löschung). Dies kann über folgendes SQL-Statement abgerufen werden:
							`SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'minimal_retention_period'`
							Alternativ kann eine Abfrage über das SAP HANA Cockpit erfolgen: *App "Resource Directory" -> System auswählen -> "System Overview" -> Filter by Area "Security" -> Auditing*
								Die Parameter zur Speicherung sind entsprechend gesetzt, so dass die verschiedenen Log-Einträge über einen angemessenen Zeitraum zur Verfügung stehen.
								Es erfolgt eine regelmäßige Auswertung.
								Es ist sichergestellt, dass Protokolleinträge vor ändernden Zugriffen geschützt sind.
								Die Speicherung der Protokolldateien erfolgt an jenen Stellen, an denen Datenbank- und Betriebsadministratoren keinen Zugriff haben (z.B. *SYSLOGPROTOCOL* als *default_audit_trail_type* oder *CSTABLE* als *default_audit_trail_type* OHNE Zuordnung des Privilegs *AUDIT_OPERATOR* an den Datenbankadministrator).

HANA-DB-LOG-03	Protokollierung	Es können unautorisierte Änderungen an Protokolleinträgen erfolgen.	Sicherheitsrelevante Ereignisse werden protokolliert und regelmäßig überprüft.	Vorgaben/Policy	Die SAP HANA-Datenbank-Protokolleinträge werden angemessen gespeichert.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, welche Protokollierungsvorgaben (Audit-Policies) definiert sind. Dies kann über folgendes SQL-Statement abgerufen werden:	Die Protokollierungsvorgaben (Audit-Policies) sind aktiviert.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-be-zeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
							`SELECT * FROM "SYS"."AUDIT_POLICIES" WHERE IS_AUDIT_POLICY_ACTIVE='TRUE';`	Der Wert im Feld *IS_AUDIT_POLICY_ACTIVE* ist *TRUE*.
HANA-DB-LOG-04	Protokollierung	Aktivitäten auf der HANA-Datenbank sind nicht nachvollziehbar. Bei dem Verdacht auf Missbrauch kann im Nachhinein nicht auf automatische Systemaufzeichnungen zurückgegriffen werden.	Schreibende Aktivitäten auf der HANA-Datenbank werden protokolliert, z.B. durch das Aktivieren der Audit-Trail bzw. Audit-Trace Funktionen. Folgende Operationen sollten mindestens für das jeweilige Geschäftsjahr für jeden Datenbankadministrator (inkl. der Default-User) aufbewahrt werden: 1. Data Manipulation Language Operationen (DML) (außer Select): 1.1. Insert: Fügt neue Inhalte in eine Datenbank ein. 1.2. Update: Ändert bestehende Datenbankinhalte. 1.3. Delete: Löscht einzelne bestehende Datenbankinhalte. 1.4. Truncate: Leert Datenbanktabellen 2. Data Definition Language (DDL): 2.1. Create Table: Erstellt eine neue Datenbanktabelle 2.2. Alter Table: Ändert Datenbanktabellendefinitionen 2.3. Drop Table: Löschen von Datenbanktabellen 2.4. Data Control Language (DCL): 2.5. Grant: Rechtevergabe an andere Benutzer Revoke: Entzug von Datenbankrechten	Audit Trail	Die SAP HANA-Datenbank-Audit-Trails bzw. Audit-Trace Funktionen sind aktiv.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Aufnahme und Überprüfung aller Datenbankadministratoren und -Benutzer mit weitreichenden Berechtigungen. Prüfung der Verfahrensdokumentation und der Nachweise über die implementierten technischen und organisatorischen Maßnahmen zur Protokollierung der Aktivitäten von Datenbank-Benutzern mit weitreichenden Berechtigungen (einschließlich Umfang, Speicherort, Aufbewahrungszeitraum). Überprüfung der Beschreibung, Benennung sowie der Nachweise über die Benutzer mit Schreibrechten auf die Protokolle.	Auswertung der Protokolle von privilegierten Benutzern. Die erstellen Logdateien sollten regelmäßig auf kritische Aktivitäten hin überprüft werden.	Der Audit Trail ist aktiv. Die erstellten Logdateien werden regelmäßig auf kritische Aktivitäten überprüft.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
HANA-DB-OS-01	Betriebssystem	Aktivitäten auf der HANA-Datenbank sind nicht nachvollziehbar. Dadurch Verstoß gegen die Grundsätze der Unveränderbarkeit und der Nachvollziehbarkeit möglich.	Nur Benutzer, die auf der Betriebssystemebene von SAP HANA benötigt werden, sind auf dem SAP-System vorhanden.	Systembedingt erforderliche User auf OS-Ebene	Nur autorisierte und für den SAP HANA-Betrieb notwendige User sind im SAP-System vorhanden.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Benutzerberechtigungskonzept auf Administrations-/Systemebene. Aufnahme der im Berechtigungskonzept definierten OS-Benutzer.	Prüfung, ob weitere OS-Benutzer als die folgenden im SAP-System vorhanden sind: - sapadm - -<sid>adm - Dedizierte OS-Benutzer für jede Mandantendatenbank, wenn das System für eine hohe Isolation konfiguriert ist - ggf. weitere OS-Benutzer des Hardwareherstellers. Nutzen Sie hierzu die zugehörige OS-Dokumentation des von Ihnen eingesetzten OS-Systems.	Es sind nur definierte OS-Benutzer vorhanden, die für den SAP HANA-Betrieb notwendig sind.
HANA-DB-OS-02	Betriebssystem	Es sind nicht autorisierte Benutzer vorhanden, die auf die Betriebssystemebene zugreifen können.	Nur autorisierte Datenbankbenutzer haben über die Zugriffsberechtigungen das Systemprivileg *IMPORT* und *EXPORT* für Dateien, die in den/aus dem SAP HANA-Server im-/exportiert werden.	OS File System Zugriffe	Nur definierte Benutzer oder Rollen besitzen Zugriffsberechtigung für den Import/Export von Dateien in/aus dem SAP HANA-Server.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts. Aufnahme und Prüfung des im Berechtigungskonzept definierten Umfangs von Datenbankbenutzern mit *EXPORT/IMPORT*-Berechtigungen.	Prüfung, welche Benutzer oder Rollen das *IMPORT*- oder *EXPORT*-Privileg haben, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE (OBJECT_TYPE = 'SYSTEMPRIVILEGE') AND (PRIVILEGE = 'EXPORT' OR PRIVILEGE='IMPORT');`	Nur eine eingeschränkte Benutzergruppe hat *EXPORT/IMPORT*-Berechtigungen.
HANA-DB-OS-03	Betriebssystem	Nicht autorisierte Datenbankbenutzer können auf Tabelleninhalte zugreifen und diese Daten exportieren oder Daten in Tabellen importieren. Dadurch Verstoß gegen die Grundsätze der Autorisierung, Vertraulichkeit und Unveränderbarkeit möglich.	OS-Sicherheitspatches für das Betriebssystem werden geprüft, getestet und installiert, sobald diese verfügbar sind.	OS Security Patches	OS-Sicherheitspatches für das Betriebssystem werden zeitnah geprüft, getestet und installiert.	Prüfung der Verfahrensdokumentation im Change-Management mit besonderem Fokus auf das definierte Patch-Management (einschließlich regelmäßiger Prüfung auf neue OS-Sicherheitspatches, Risikoanalyse, angemessene Testumgebung und -verfahren, Freigabeverfahren, Roll-Out-Verfahren, Monitoring).	Prüfung, ob Sicherheitspatches für das Betriebssystem zeitnah installiert werden. Hierzu ist die zugehörige Dokumentation des Betriebssystems zu prüfen. Wenn sich ein Sicherheitspatch auf den Betrieb von SAP HANA auswirkt, veröffentlicht SAP einen entsprechenden SAP-Hinweis.	OS-Sicherheitspatches für das Betriebssystem werden geprüft, getestet und installiert, sobald diese verfügbar sind.
HANA-DB-OS-04	Betriebssystem	Unzureichendes Patch-Management kann zu einer Gefährdung des unterliegenden Betriebssystems und der darauf durchgeführten Installationen führen. Dadurch Verstoß gegen den Grundsatz der Integrität möglich.	Nur autorisierte Benutzer können root-Befehle ausführen.	HANA-DB-OS-02	Nur Benutzer mit ordnungsgemäßer/weiterer Authentifizierung können root-Befehle ausführen.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzer-Berechtigungskonzepts auf Administrations-/Systemebene. Aufnahme und Prüfung der definierten Benutzer mit	Prüfung der Datei */etc/sudoers*. Die spezifische Konfiguration kann von der jeweiligen Linux-Distribution abhängen, aber die zu betrachtenden Konfigurationsoptionen sind: - Standardwerte *targettpw* Diese Einstellung erfordert die Angabe des Root-Passworts bei der Ausführung von sudo. - ALL ALL ALL=(ALL) ALL	Benutzer ohne ordnungsgemäße/weitere Authentifizierung können keine root-Befehle ausführen. Insbesondere der Standard-User *<sid>adm* ist nicht in der Lage, beliebige Befehle als root ohne ordnungsgemäße Authentifizierung auszuführen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
						Berechtigung zur Ausführung von root-Befehlen.	Dies sollte nur verwendet werden, wenn auch die Standardeinstellung *targetpw* eingestellt ist.	
HANA-DB-ENC-01	Verschlüsselung	Nicht autorisierte Benutzer können root-Befehle ausführen und dadurch das System kompromittieren. Dadurch Verstoß gegen den Grundsatz der Integrität möglich.	Der *SSFS Master Key* ist geheim zu halten. Idealerweise wird er nach der Installation geändert.	Verschlüsselung - Standardkennwörter, SFSS Master Key	Der *Secure Store in the File System (SSFS)* Master Key ist nach der Installation geändert worden. HANA bietet standardmäßig zwei Verschlüsselungen an: a) Datenverschlüsselung (Verschlüsselung des persistenten Speichers) und b) Verschlüsselung für interne Services. Für beide Verschlüsselungen werden die root keys im SSFS gespeichert. Diese sind verschlüsselt durch den Master Key des *SSFS*.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob der Master Key nach der Installation geändert wurde, über folgendes SQL-Statement: SELECT * FROM M_HOST_INFORMATION WHERE KEY = 'ssfs_masterkey_changed' <u>Alternative Prüfungshandlung:</u> Prüfung des Zeitstempels in der Datenbank über das SAP HANA-Cockpit. Unter der Gruppe "*SAP HANA Security Overview*" wird in der Kachel "Data Storage Security" die letzte Änderung der *SSFS Master Keys* angezeigt.	Das Passwort wurde nach der Installation bzw. anlassbezogen (z. B. Personalwechsel) geändert und entspricht somit nicht mehr dem Standardkennwort im Auslieferungsstand.
HANA-DB-ENC-02	Verschlüsselung	Der SSFS Master Key könnte Dritten (insbesondere durch den Installationsprozess) bekannt sein. Dadurch kann die Verschlüsselung von Daten kompromittiert werden. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit und Integrität möglich.	Der PKI Master Key ist geheim zu halten. Idealerweise wird er nach der Installation geändert.	Verschlüsselung - Standardkennwörter, PKI Master Key	Der *Public Key Infrastructure (PKI)* Master Key ist nach der Installation geändert worden.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob Public Key Infrastructure (PKI) Master Key nach der Installation geändert wurde, über folgendes SQL-Statement: `SELECT * FROM M_HOST_INFORMATION WHERE KEY = 'ssfs_masterkey_systempki_changed'` <u>Alternative Prüfungshandlung:</u> Prüfung des Zeitstempels in der Datenbank über das SAP HANA-Cockpit. Unter der Gruppe "SAP HANA Security Overview" wird in der Kachel "Data Storage Security" die letzte Änderung (Änderungsdatum) der SSFS Master Keys angezeigt.	Das Passwort wurde nach der Installation bzw. anlassbezogen (z. B. Personalwechsel) geändert und entspricht somit nicht mehr dem Standardkennwort im Auslieferungsstand.
HANA-DB-ENC-03	Verschlüsselung	Der PKI Master Key könnte Dritten (insbesondere durch den Installationsprozess) bekannt sein. Dadurch kann die Verschlüsselung von Daten kompromittiert werden. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit und Integrität möglich.	Der Root Key zur Datenverschlüsselung ist geheim zu halten. Idealerweise wird er nach der Installation geändert.	Verschlüsselung – Standardkennwörter, Root Key	Der Root Key zur Datenverschlüsselung ist nach der Installation geändert worden.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob Root Key nach der Installation geändert wurde: Die nachfolgenden Einträge können über den Public View "ENCRYPTION_ROOT_KEYS" eingesehen werden: - -ROOT_KEY_TYPE: "PERSISTENCE": Datenverschlüsselung. - -ROOT_KEY_VERSION: Version des root keys - -CREATE_TIMESTAMP: Zeitstempel der Schlüsselerzeugung	Das Passwort wurde nach der Installation bzw. anlassbezogen (z. B. Personalwechsel) geändert und entspricht somit nicht mehr dem Standardkennwort im Auslieferungsstand.
HANA-DB-ENC-04	Verschlüsselung	Der Root Key zur Datenverschlüsselung könnte Dritten (insbesondere durch den Installationsprozess) bekannt sein.	Der Root Key zur Verschlüsselung für interne Services ist geheim zu halten. Idealerweise wird	Verschlüsselung – Stan-	Der Root Key zur Verschlüsselung für interne Services ist nach der Installation geändert worden.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob Root Key nach der Installation geändert wurde: Die nachfolgenden Einträge können über den Public View "ENCRYPTION_ROOT_KEYS" eingesehen werden:	Das Passwort wurde nach der Installation bzw. anlassbezogen (z. B. Personalwechsel) geändert und entspricht somit nicht mehr

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
		Dadurch kann die Verschlüsselung von Daten kompromittiert werden. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit und Integrität möglich.	er nach der Installation geändert.	dardkennwörter, Root Key für interne Services			- ROOT_KEY_TYPE: "DPAPI": Verschlüsselung für interne Services. - ROOT_KEY_VERSION: Version des root keys - CREATE_TIMESTAMP: Zeitstempel der Schlüsselerzeugung	dem Standardkennwort im Auslieferungsstand.
HANA-DB-ENC-05	Verschlüsselung	Der Root Key zur Verschlüsselung für interne Services könnte Dritten (insbesondere durch den Installationsprozess) bekannt sein. Dadurch kann die Verschlüsselung von Daten kompromittiert werden. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit und Integrität möglich.	Zu Wiederherstellungszwecken erzeugte Abbilder der Datenbank werden verschlüsselt gespeichert.	Aktivierung Datenverschlüsselung Persistenter Speicher	Die Daten des persistenten Speichers werden verschlüsselt gespeichert.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob die Daten des persistenten Speichers verschlüsselt gespeichert werden. Die nachfolgenden Einträge können über den Public View "M_PERSISTENCE_ENCRYPTION_STATUS" eingesehen werden: - HOST: Host-Name - PORT: Portnummer (30003: Standard-Port für den Indexserver [Schreiben des persistenten Speichers]) - ENCRYPTION_ACTIVE: Verschlüsselung ist aktivert (TRUE/FALSE) - ENCRYPTION_ACTIVE_AFTER_NEXT_SAVEPOINT: Verschlüsselung wird für den nächsten Savepoint aktiviert (TRUE/FALSE)	Die Datenverschlüsselung der persistenten Daten (Abbilder der Datenbank auf der Festplatte des HANA-Servers) ist aktiviert. Der Wert im Feld "ENCRYPTION_ACTIVE" ist TRUE.
HANA-DB-ENC-06	Verschlüsselung	Zu Wiederherstellungszwecken erzeugte Abbilder der Datenbank werden unverschlüsselt gespeichert. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit und Integrität möglich.	Zu Wiederherstellungszwecken erzeugte Redo Logs der Datenbank werden verschlüsselt gespeichert.	Aktivierung Datenverschlüsselung der Redo Logs	Die Daten der Redo Logs werden verschlüsselt gespeichert.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob die Daten der Redo Logs verschlüsselt gespeichert werden, über folgendes SQL-Statement: Prüfung in Public View "M_ENCRYTION_OVERVIEW": `SELECT * FROM M_ENCRYPTION_OVERVIEW WHERE SCOPE = 'LOG'`	Die Datenverschlüsselung ist aktiviert. Der Wert im Feld "IS_ENCRYTION_ACTIVE"ist TRUE.
HANA-DB-ENC-07	Verschlüsselung	Zu Wiederherstellungszwecken erzeugte Redo Logs der Datenbank werden unverschlüsselt gespeichert. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit und Integrität möglich.	Die interne und externe Kommunikation ist verschlüsselt.	Verschlüsselung bei Datenübertragung	Die interne und externe Datenübertragung wird verschlüsselt. Als Cryptographic Service Provider wird der Provider "commonCryptoLib" (nicht OpenSSL) genutzt. Es werden keine selbstsignierten Zertifikate zugelassen.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob die interne und externe Datenübertragung verschlüsselt wird, über folgendes SQL-Statement: `SELECT * FROM M_INIFILE_CONTENTS WHERE FILE_NAME = 'global.ini' AND SECTION = 'communication'`	Der Wert des Parameters "sslEnforce" ist TRUE. (Anforderung sicherer SSL-Verbindungen: TRUE: es werden nur SSL-Verbindungen zugelassen; FALSE: auch unsichere Verbindungen werden akzeptiert). Der Wert des Parameters "sslCryptoProvider" ist commoncrypto (Parameter zeigt den verwendeten Cryptographic Service Provider an. Genutzt werden können OpenSSL oder die CommonCryptoLib. SAP empfiehlt den Einsatz

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
								der CommonCryptoLib (Parameterwert commoncrypto) Der Wert des Parameters "sslCreateSelfSignedCertificate" ist FALSE (Zulassen von selbst-signierten Zertifikaten. Die Nutzung ist kritisch, da hierdurch die Gefahr von Man-in-the-Middle-Angriffen erhöht wird. TRUE: selbst-signierte Zertifikaten sind zugelassen; FALSE: selbstsignierte Zertifikate sind nicht zugelassen)

HANA-DB-ENC-08	Verschlüsselung	Aufgrund unverschlüsselter interner und externer Kommunikation kann der Datenverkehr mitgelesen werden. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit, Autorisierung und Integrität möglich.	Die Kommunikation zwischen Client und der HANA-Datenbank ist verschlüsselt.	Verschlüsselung Clientverbindung zur DB	Alle aktiven (und ruhenden) Verbindungen von Clients zur HANA-Datenbank sind verschlüsselt.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob alle aktiven und ruhenden Verbindungen von Clients zur SAP HANA-Datenbank verschlüsselt sind.
							
							Die Anzahl der Verbindungen kann über folgende SQL-Statements abgerufen werden:
							
							Aufruf des Feldes "IS_ENCRYTED" (Anzahl):
							
							`SELECT CONNECTION_TYPE, IS_ENCRYPTED, COUNT(*) FROM M_CONNECTIONS GROUP BY CONNECTION_TYPE, IS_ENCRYPTED ORDER BY IS_ENCRYPTED DESC`
							
							Alternativer Aufruf des Feldes "IS_ENCRYTED":
							
							`SELECT CONNECTION_TYPE, IS_ENCRYPTED, COUNT(*) FROM "SYS"."M_CONNECTIONS" GROUP BY CONNECTION_TYPE, IS_ENCRYPTED ORDER BY IS_ENCRYPTED DESC`
								Alle Verbindungen sind verschlüsselt.
								
								Der Wert des Feldes "IS_ENCRYTED" ist TRUE.

HANA-DB-ENC-09	Verschlüsselung	Aufgrund unverschlüsselter Kommunikation zwischen Client und der HANA-Datenbank kann der Datenverkehr mitgelesen werden. Dadurch Verstoß gegen die Grundsätze der Vertraulichkeit, Autorisierung und Integrität möglich.	Nur erforderliche Remote-Verbindungen sind eingerichtet und verwendbar.	Verschlüsselung der Remote-Verbindung	Es erfolgen nur dokumentierte und autorisierte Remote-Verbindungen und ggf. über diese Verbindungen ausgeführte SQL-Statements.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob nur erforderliche Remote-Verbindungen gemäß der Dokumentation vorhanden sind, über folgendes SQL-Statement:
							
							`SELECT * FROM M_REMOTE_CONNECTIONS`
							
							Ergänzend (Tabelle "M_REMOTE_STATEMENT" zeigt die vollständigen SQL-Statements an, die über die Verbindungen ausgeführt wurde, inkl. Laufzeit und Anzahl zurückgegebener Datensätze):
							
							`SELECT * FROM M_REMOTE_STATEMENTS`
								Es sind nur Remote-Verbindungen gemäß der Dokumentation vorhanden.
								
								Es sind nur SQL-Anweisungen gemäß Dokumentation vorhanden.

HANA-DB-LS-01	Berechtigungsmanagement	Zugriff von ungesicherten und nicht bekannten oder genehmigten Remote-Systemen. Dadurch Ver-	Der Umgang mit Standardbenutzern und deren Berechtigungen ist geregelt und dokumentiert.	Berechtigungskonzept	Es gibt ein übergreifendes HANA-Datenbank Sicherheits-/Berechtigungskonzept, welches entsprechende Vorgaben z.B. zu	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob die unternehmensspezifische Anweisung den Umgang mit Standardbenutzern und deren Berechtigung regelt und dokumentiert.	Es existiert eine HANA-Datenbank Anweisung, die der allgemeinen Anweisung entspricht.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
		stoß gegen die Grundsätze der Vertraulichkeit, Autorisierung und Integrität möglich.			Systemeinstellungen von Standardbenutzern, zu unerlaubten Berechtigungskombinationen, zum Autorisierungs- und Vergabeprozess von Berechtigungen sowie zum zeitnahen Entzug von Berechtigungen, zum regelmäßigen Review von bestehenden Berechtigungen sowie zum Passwort enthält.	Prüfung des Benutzerberechtigungskonzepts.		

HANA-DB-LS-02	Berechtigungs-management	Umgang mit Standardbenutzern und deren Berechtigungen ist nicht geregelt. Dadurch Verstoß gegen Autorisierung möglich.	Die Verwendung des Benutzers SYSTEM ist streng reglementiert. Idealerweise ist der Benutzer deaktiviert.	Privilegierte Standardbenutzer SYSTEM	Der Benutzer SYSTEM wird nicht im Tagesgeschäft genutzt. Es ist zu empfehlen, den Benutzer nach der Installation und Einrichtung von personifizierten Administratorenkonten zu deaktivieren.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.
						
						Prüfung des Benutzerberechtigungskonzepts.
							Prüfung, ob der Benutzer SYSTEM deaktiviert wurde, über folgendes SQL-Statement:
							
							`SELECT USER_DEACTIVATED FROM "PUBLIC"."USERS" WHERE USER_NAME='SYSTEM';`
							
							Prüfung, wann der Benutzer SYSTEM das letzte Mal verwendet wurde (falls er nicht deaktiviert wurde), über folgendes SQL-Statement:
							
							`SELECT LAST_SUCCESSFUL_CONNECT FROM "PUBLIC"."USERS" WHERE USER_NAME='SYSTEM';`
								Es ist in einem Konzept festgelegt, wie der Benutzer SYSTEM abgesichert ist, z.B. über eine Deaktivierung.

HANA-DB-LS-03	Berechtigungs-management	Der SYSTEM-Benutzer ist aktiv und besitzt nahezu Vollzugriff auf die Datenbank. Ein Rückschluss auf den Verursacher ist grds. nicht möglich. Dadurch Verstoß gegen die Grundsätze der Autorisierung, Integrität und Unveränderbarkeit möglich.	Der Benutzer SYSTEM ist gegen Missbrauch geschützt. Der Parameter "IS_PASSWORD_ENABLED" ist auf "true" gesetzt.	Absicherung des Standard-benutzers SYSTEM	Der Parameter "IS_PASSWORD_ENABLED" ist für den Benutzer SYSTEM auf den Standardwert "true" eingestellt. Ansonsten wird der Benutzer bei Falschanmeldungen nicht gesperrt (und Brute-Force-Attacken sind möglich).	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts.	Prüfung des Parameters "IS_PASSWORD_ENABLED" über folgendes SQL-Statement: `SELECT * FROM "SYS"."USERS" WHERE "USER_NAME" = 'SYSTEM'`	Der Systemparameter "IS_PASSWORD_ENABLED" ist für den Benutzer SYSTEM auf dem Standardwert "true" eingestellt. Ergänzender Hinweis zur Prüfung der Kennwortkonfiguration: Prüfung des Parameters "IS_PASSWORD_ENABLED" in der Datei indesxserver.ini zur Kennwortkonfiguration: Pfad:/opt/hana/shared/<SID>/global/hdb/custom/config

HANA-DB-LS-04	Berechtigungs-management	Der Benutzer SYSTEM ist vor Missbrauch (insbesondere Brute-Force-Attacken) nicht ausreichend geschützt. Dadurch Verstoß gegen die Grundsätze der Autorisierung, Integrität und Unveränderbarkeit möglich.	Der Authentifizierungsmechanismus ist definiert, sicher und wird einheitlich verwendet.	Periodische Überprüfung der Zugriffsmechanismen der User	Es erfolgt eine regelmäßige Prüfung auf Benutzer, welche sich parallel mit unterschiedlichen Authentifizierungsmechanismen an der HANA-Datenbank anmelden können.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.
						
						Prüfung des Benutzerberechtigungskonzepts.
							Prüfung der Authentifizierungsmechanismen über folgende SQL-Statements:
							
							`SELECT * FROM "SYS"."USERS" WHERE "IS_PASSWORD_ENABLED" = 'FALSE'`
							
							`SELECT * FROM "SYS"."USERS" WHERE "IS_KERBEROS_ENABLED" = 'FALSE'`
							
							`SELECT * FROM "SYS"."USERS" WHERE "IS_SAML_ENABLED" = 'FALSE'`
								Es gibt nur einen Authentifizierungsmechanismus zur Anmeldung an der Datenbank.
								
								Benutzer melden sich mit SSO oder (falls SSO nicht verfügbar/möglich ist) einem festgelegten Verfahren an.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
							`SELECT * FROM "SYS"."USERS" WHERE "IS_X509_ENABLED" = 'FALSE'` Es wird jeweils eine Liste für alle (system- und personenbezogenen) Benutzeraccounts ausgegeben, sofern einer der o.g. Parameter nicht aktiviert (=false) ist. Ansonsten wird das erwartete Ergebnis erzielt.	
HANA-DB-LS-05	Berechtigungs-management	Schwachstellen in den genutzten Authentifizierungsmechanismen	Jeder digitalen Identität ist nur ein SAP HANA-Benutzer zugewiesen.	Eindeutige Benutzer-ID	Es erfolgt eine regelmäßige Prüfung auf Benutzer mit derselben External-ID (Kerberos ID).	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts.	Prüfung, ob HANA-Benutzer bestehen, denen mehr als eine Identität zugewiesen ist, über folgendes SQL-Statement: `SELECT * FROM "SYS"."USERS" WHERE EXTERNAL_IDENTITY IN (SELECT EXTERNAL_IDENTITY FROM "SYS"."USERS" WHERE EXTERNAL_IDENTITY IS NOT NULL GROUP BY EXTERNAL_IDENTITY HAVING COUNT(*)>1);` Verbale Erläuterung des Abfrageergebnisses.	Ein Benutzer kann sich nur mit einem SAP HANA-Benutzer anmelden, d.h. die Abfrage ergibt keine Treffer.
HANA-DB-LS-06	Berechtigungs-management	ermöglichen es, Zugriffskontrollen auszuhebeln. Dadurch Verstoß gegen den Grundsatz der Autorisierung möglich.	Der Aufbau des Kennworts unterliegt Vorgaben zur Mindestlänge, die eingehalten werden.	Passwortmindestlänge	Eine Passwortmindestlänge ist technisch gemäß den individuellen Anforderungen an ein sicheres Passwort umgesetzt. Vorschlagswert: 8-10 Stellen; Parameter: minimal_password_length.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts. Prüfung der Systemparameter.	Prüfung der Kennwortmindestlänge über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'minimal_password_length'`	Eine Kennwortmindestlänge von 8–10 Zeichen ist definiert. Die Festlegung erfolgt über den Systemparameter "minimal_password_length".
HANA-DB-LS-07	Berechtigungs-management	Ein Benutzer kann sich mit unterschiedlichen SAP HANA-Benutzern anmelden und die Funktionstrennungen aushebeln. Dadurch Verstoß gegen den Grundsatz der Autorisierung möglich.	Der Aufbau des Kennworts unterliegt Komplexitätsregeln, die eingehalten werden.	Passwortkomplexität	Eine Passwortkomplexität ist technisch gemäß den individuellen Anforderungen an ein sicheres Passwort umgesetzt. Vorschlagswert: Kennwort sollte mindestens einen Groß- und Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten (A1a$); Parameter: password_layout.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts. Prüfung der Systemparameter.	Prüfung der Kennwortkomplexität über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'password_layout'`	Das Kennwort unterliegt komplexen Bildungsregeln. Die Mindestanforderungen, d.h. mindestens einen Groß- und Kleinbuchstaben, eine Zahl und ein Sonderzeichen (A1a$) wurden eingehalten. Die Festlegung erfolgt über den Systemparameter "password_layout".
HANA-DB-LS-08	Berechtigungs-management	Das Kennwort ist einfach aufgebaut und kann mit wenigen Anmeldeversuchen erraten werden. Dadurch Verstoß gegen den Grundsatz der Autorisierung möglich.	Die Gültigkeit des Kennworts unterliegt Vorgaben zur Wiederverwendung, die eingehalten werden.	Passworthistorie	Eine Passworthistorie ist technisch gemäß den individuellen Anforderungen an ein sicheres Passwort umgesetzt. Vorschlagswert: 15 vergangene Kennworte bei einem Wechsel, der alle 90 Tage erzwungen wird; Parameter: last_used_passwords.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts. Prüfung der Systemparameter.	Prüfung der Kennworthistorie über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'last_used_passwords' OR LOWER(PROPERTY) = 'maximum_password_lifetime'`	Die Länge der Passworthistorie last_used_passwords ist festgelegt. Die Festlegung erfolgt über den Systemparameter "last_used_passwords".

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
HANA-DB-LS-09	Berechtigungs-management	Das Kennwort ist einfach aufgebaut und kann mit wenigen Anmeldeversu-chen erraten werden. Dadurch Verstoß gegen den Grundsatz der Autori-sierung möglich.	Die Gültigkeit des Initial-kennworts ist zeitlich be-schränkt.	Gültigkeits-dauer Initial-kennwort	Eine Gültigkeitsdauer für das initiale Passwort ist de-finiert. Vorschlagswert: Die Gültig-keitsdauer überschreitet nicht fünf Tage; Parameter: maximum_unused_ini-tial_password_lifetime.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerbe-rechtigungskonzepts. Prüfung der Systempara-meter.	Prüfung der Kennworthistorie über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POL-ICY WHERE LOWER(PROPERTY) = 'maximum_un-used_inital_password_lifetime'`	Es ist eine Gültigkeitsdauer für das initiale Kennwort de-finiert. Die Festlegung erfolgt über den Systemparameter "ma-ximum_unused_initial_pass-word_lifetime".
HANA-DB-LS-10	Berechtigungs-management	Das Kennwort ist einfach aufgebaut und kann mit wenigen Anmeldeversu-chen erraten werden. Dadurch Verstoß gegen den Grundsatz der Autori-sierung möglich.	Die Gültigkeit des Kenn-worts ist zeitlich be-schränkt. Das Kennwort ist nach Ablauf der Frist zwingend zu wechseln.	Passwort Gül-tigkeitsdauer	Eine Gültigkeitsdauer für das Passwort ist definiert. Mit Erreichung der Gültig-keitsdauer wird der User systemseitig zu einem Passwortwechsel aufgefor-dert. Vorschlagswert: Wechsel des Kennworts nach 90 Ta-gen; Parameter: maxi-mum_password_lifetime.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerbe-rechtigungskonzepts. Prüfung der Systempara-meter.	Prüfung des Intervalls zur Kennwortänderung über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POL-ICY WHERE LOWER(PROPERTY) = 'maximum_pass-word_lifetime'`	Es ist der Zeitpunkt für den Kennwortänderungszwang definiert. Der erzwungene Wechsel des Kennworts nach spätes-tens 90 Tagen. Die Festlegung erfolgt über den Systemparameter "ma-ximum_password_lifetime".
HANA-DB-LS-11	Berechtigungs-management	Das Initialkennwort be-sitzt eine lange Gültigkeit, was eine missbräuchliche Verwendung des Benut-zers begünstigt. Dadurch Verstoß gegen den Grundsatz der Autorisie-rung möglich.	Die Gültigkeit eines nicht mehr benutzten Kenn-worts ist zeitlich be-schränkt.	Gültigkeit von nicht mehr ver-wendeten Pass-wörtern	Eine Gültigkeitsdauer für nicht benutzte Passworte ist definiert. Vorschlagswert: Gültig-keitsdauer eines nicht be-nutzten Kennworts höher setzen als die Dauer für den erzwungenen Wechsel des Kennworts (max. 180 Tage); Parameter maxi-mum_unused_produc-tive_password_lifetime.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerbe-rechtigungskonzepts. Prüfung der Systempara-meter.	Prüfung der Gültigkeitsdauer für nicht verwendete Kennwör-ter über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POL-ICY WHERE LOWER(PROPERTY) = 'maximum_un-used_productive_password_lifetime'`	Die Gültigkeitsdauer eines nicht benutzten Kennworts ist geregelt. Die Festlegung erfolgt über den Systemparameter "ma-ximum_unused_produc-tive_password_lifetime".
HANA-DB-LS-12	Berechtigungs-management	Das Kennwort besitzt eine lange Gültigkeit, was eine missbräuchliche Ver-wendung des Benutzers begünstigt. Dadurch Ver-stoß gegen den Grund-satz der Autorisierung möglich.	Die Anzahl der Falschan-meldungen ist reglemen-tiert. Nach wiederholter Falscheingabe wird der Benutzer gesperrt.	Anzahl mögli-cher Falschan-meldungen	Die maximale Anzahl der Falschanmeldungen bis zur Sperre der Benutzer (maxi-mum_invalid_connect_at-tempts) ist definiert. Vorschlagswert: Maximal 3 Passwortfehlversuche bis zur Sperre des Benutzers.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerbe-rechtigungskonzepts. Prüfung der Systempara-meter.	Prüfung der Anzahl der Kennwortfehleingaben über folgen-des SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POL-ICY WHERE LOWER(PROPERTY) = 'maximum_inva-lid_connect_attempts'`	Die maximale Anzahl der Falschanmeldungen bis zur Sperre der Benutzer ist defi-niert. Die Festlegung erfolgt über den Systemparameter "ma-ximum_invalid_connect_at-tempts".
HANA-DB-LS-13	Berechtigungs-management	Das Kennwort besitzt eine lange Gültigkeit, was eine missbräuchliche Ver-wendung des Benutzers begünstigt. Dadurch Ver-	Nach der Sperrung eines Benutzers ist die Entsper-rung automatisch und standardisiert nach ei-nem definierten Zeitraum vorzunehmen.	Automatische Freischaltung der Benutzer-sperre	Die automatische Frei-schaltung der Benutzer-sperre ist definiert und führt zu einer automati-	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung des Parameters für die Dauer der Benutzersperre über folgendes SQL-Statement: `SELECT PROPERTY, VALUE FROM M_PASSWORD_POL-ICY WHERE LOWER(PROPERTY) = 'pass-word_lock_time' AND VALUE > '259200'`	Eine automatische Frei-schaltung der Benutzer-sperre ist definiert und führt zu einer automatischen Sperrung des Benutzers.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
		stoß gegen den Grundsatz der Autorisierung möglich.			schen Sperrung des Benutzers. (password_lock_time).	Prüfung des Benutzerberechtigungskonzepts. Prüfung der Systemparameter.	(Wert von 180*1440 = 259200 Minuten; Vorschlagswert der SAP ist 1440 Minuten, d.h., der Benutzer wird nach einem Tag entsperrt.)	Die Festlegung erfolgt über die Systemparameter "password_lock_time" für die automatische Sperrung des Benutzers und "maximum_unused_productive_password_lifetime"
HANA-DB-LS-14	Berechtigungs-management	Das Kennwort hat eine lange Gültigkeitsdauer, was die Gefahr einer missbräuchlichen Verwendung durch den Benutzer erhöht. Dies könnte einen Verstoß gegen den Grundsatz der Autorisierung zur Folge haben	Der Zugriff auf das System erfolgt auch unter den Administratoren nach Minimalprinzip und Einhaltung der Funktionstrennung.	Kritische Berechtigungen Catalog Read und Trace Admin	Die folgenden zwei System-Berechtigungen sind im Produktivsystem nur Administratoren oder Supportbenutzern zugewiesen: - - Catalog Read - - Trace Admin Auf der Datenbankebene sind folgende Berechtigungen (Privilege) nur den Benutzern zugewiesen, die diese im Rahmen ihrer täglichen Arbeit benötigen: - ADAPTER ADMIN - AGENT ADMIN - AUDIT ADMIN - AUDIT OPERATOR - BACKUP ADMIN - BACKUP OPERATOR - CERTIFICATE ADMIN - CREATE REMOTE SOURCE - CREDENTIAL ADMIN - ENCRYPTION ROOT KEY ADMIN - EXTENDED STORAGE ADMIN - INIFILE ADMIN - LDAP ADMIN - LICENSE ADMIN - LOG ADMIN - MONITOR ADMIN - OPTIMIZER ADMIN - RESOURCE ADMIN - SAVEPOINT ADMIN - SERVICE ADMIN - SESSION ADMIN - SSL ADMIN	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts auf Administrations-/Systemebene.	Prüfung, ob Benutzer mit privilegierten Berechtigungen bestehen, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'SSL ADMIN' AND GRANTEE NOT IN ('SYSTEM','_SYS_REPO');` Die so ermittelten Benutzer sollten gemeinsam mit dem IT-Management oder gegen ein Organigramm oder Unternehmensrichtline sowie das gültige Berechtigungskonzept validiert werden.	Administratoren haben nur Zugriff auf die Systemberechtigungen, die sie im Rahmen ihrer täglichen Arbeit benötigen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
					- TABLE ADMIN - TRUST ADMIN - VERSION ADMIN - WORKLOAD ADMIN - WORKLOAD * ADMIN			
HANA-DB-LS-15	Berechtigungs-management	Das Kennwort besitzt eine lange Gültigkeit, was eine missbräuchliche Verwendung des Benutzers begünstigt. Dadurch Verstoß gegen den Grundsatz der Autorisierung möglich.	Kritische Kombination von Rollen werden nicht zusammen vergeben.	Funktionstrennungskonflikte (SOD)	Die folgenden kritischen Berechtigungskombinationen sind im Produktivsystem nicht zusammen an einen User zugewiesen: - User Administration und Role Administration und/oder - Anlage von Szenario und Administration des Szenarios und/oder - Administration von Audit und Audit Durchführung und/oder - Anlage "Structured Privilege" und Administration "Structured Priviledge".	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts auf Administrations-/Systemebene insbesondere mit Blick auf Funktionstrennungsaspekte.	Prüfung, welche Benutzer die kritischen, weitreichenden Berechtigungen haben, über folgendes SQL-Statement. Benutzername muss hier gezielt angegeben werden. EFFECTIVE_PRIVILEGES system view, for example: `SELECT * FROM "PUBLIC"."EFFECTIVE_PRIVILEGES" WHERE USER_NAME = '<USER_NAME>';` Die User mit kritischen Kombinationen (Beispiel siehe Kontrollbeschreibung) von Berechtigungen aus dem Berechtigungskonzept sind zu überprüfen. Die Auswertung muss manuell erfolgen.	Benutzern sind keine privilegierten Berechtigungen mit kritischer Kombination zugewiesen. Benutzer, denen privilegierte Berechtigungen mit Funktionstrennungskonflikten zugeordnet sind, werden dahingehend geprüft, ob kompensierende Kontrollen vorhanden sind.
HANA-DB-LS-16	Berechtigungs-management	Es besteht das Risiko des unautorisierten Zugriffs, wie z.B. Löschen von Daten, uneingeschränkte Sicht von Daten usw. Dadurch Verstoß gegen den Grundsatz der Autorisierung möglich.	Die Berechtigung DATA_ADMIN ist nur autorisierten Benutzern zugewiesen. Idealerweise ist sie keinem User oder Rolle zugewiesen.	Privilegierte Systemberechtigung DATA ADMIN	Die Systemberechtigung DATA ADMIN ist im Produktivsystem keinem User und keiner Rolle zugewiesen und erlaubt somit keinem User, auf der HANA-Datenbank Befehle der "Data Definition Language (DDL)" auszuführen.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts auf Administrations-/Systemebene.	Prüfung, ob Benutzer existieren, welche über die Berechtigung DATA_ADMIN verfügen, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'DATA ADMIN' AND GRANTEE NOT IN ('SYSTEM','_SYS_REPO');`	Die Systemberechtigung DATA ADMIN ist keinem Benutzer und keiner Rolle zugeordnet (Ausnahme Notfallbenutzer).
HANA-DB-LS-17	Berechtigungs-management	Durch Vergabe von kritischer Kombination von Berechtigungen besteht das Risiko, dass keine Funktionstrennung gewährleistet ist und so die Berechtigungen weitreichend vergeben werden. Dadurch Verstoß gegen den Grundsatz der Autorisierung möglich.	Die Systemberechtigung DEVELOPMENT ist keinem Benutzer und keiner Rolle zugeordnet (Ausnahme Notfallbenutzer).	Entwicklungsberechtigung DEVELOPMENT in der Produktivdatenbank	Die Systemberechtigung DEVELOPMENT ist im Produktivsystem keinem User und keiner Rolle zugewiesen und erlaubt somit keinem User, Systembefehle zu verändern.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts auf Administrations-/Systemebene.	Prüfung, ob Benutzer mit der Berechtigung DEVELOPMENT bestehen, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'DEVELOPMENT' AND GRANTEE NOT IN ('SYSTEM','_SYS_REPO');` Die so ermittelten Benutzer sollten gemeinsam mit dem IT-Management oder gegen ein Organigramm oder Unternehmensrichtline sowie das gültige Berechtigungskonzept validiert werden.	Die Systemberechtigung DEVELOPMENT ist keinem Benutzer und keiner Rolle zugeordnet (Ausnahme Notfallbenutzer).

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
HANA-DB-LS-18	Berechtigungs-management	Es besteht das Risiko des unberechtigten Zugriffs auf die HANA-DATEN-BANK, um kritische Befehle wie Löschen oder Administration von Data Definition Language (DDL) Objekten auf HANA-Datenbank auszuführen. Dadurch Verstoß gegen die Grundsätze der Autorisierung, Integrität und Unveränderbarkeit möglich.	Die Systemberechtigung _SYS_BI_CP__ALL ist keinem Benutzer und keiner Rolle zugeordnet (Ausnahme Notfallbenutzer).	Privilegierte Analytics Berechtigungen _SYS_BI_CP_ALL	Die Systemberechtigung _SYS_BI_CP_ALL ist im Produktivsystem keinem User und keiner Rolle zugewiesen und erlaubt somit keinem User das Umgehen der Zugriffsmechanismen der XML-basierten Analyseprivilegien.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts auf Administrations-/Systemebene.	Prüfung, ob Benutzer mit der Berechtigung _SYS_BI_CP_ALL bestehen, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE = 'ANALYTICALPRIVILEGE' AND OBJECT_NAME = '_SYS_BI_CP_ALL' AND PRIVILEGE = 'EXECUTE' AND GRANTEE NOT IN ('SYSTEM','MODELING', 'CONTENT_ADMIN');` Die so ermittelten Benutzer sollten gemeinsam mit dem IT-Management oder gegen ein Organigramm oder Unternehmensrichtline sowie das gültige Berechtigungskonzept validiert werden.	Die Systemberechtigung _SYS_BI_CP__ALL ist keinem Benutzer und keiner Rolle zugeordnet (Ausnahme Notfallbenutzer).
HANA-DB-LS-19	Berechtigungs-management	Es besteht das Risiko des unberechtigten Zugriffs auf Systembefehle. Dadurch Verstoß gegen die Grundsätze der Autorisierung, Integrität und Unveränderbarkeit möglich.	Die Systemberechtigungen DEBUG und ATTACH DEBUGGER sind nur autorisierten Benutzern zugewiesen. Idealerweise sind sie keinem User oder Rolle zugewiesen.	Debug-Berechtigung	Die Systemberechtigungen DEBUG und ATTACH DEBUGGER sind im Produktivsystem keinem User und keiner Rolle zugewiesen und erlauben somit keinem User, auf dem Produktivsystem Objekte zu verändern.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts auf Administrations-/Systemebene.	Prüfung, ob Benutzer mit den Berechtigungen DEBUG oder ATTACH DEBUGGER bestehen, über folgendes SQL-Statement: `SELECT * FROM GRANTED_PRIVILEGES WHERE PRIVILEGE='DEBUG' OR PRIVILEGE='ATTACH DEBUGGER';` Die so ermittelten Benutzer sollten gemeinsam mit dem IT-Management oder gegen ein Organigramm oder Unternehmensrichtline sowie das gültige Berechtigungskonzept validiert werden.	Die Systemberechtigungen DEBUG und ATTACH DEBUGGER sind auf dem Produktivsystem keinem User zugeordnet (Ausnahme Notfallbenutzer).
HANA-DB-LS-20	Berechtigungs-management	Es besteht das Risiko, dass die Zugriffsmechanismen der XML-basierten Analyseberechtigungen auf aktiven Sichten umgangen werden. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Der Umgang mit Rollen und die Rollenpflege sind definiert, dokumentiert und erfolgen standardisiert.	Rollenpflege-konzept	Ein Konzept zur Pflege von Rollen ist vorhanden und wird regelmäßig geprüft.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts.	Prüfung, ob ein Konzept zur Pflege von Rollen vorhanden ist und regelmäßig geprüft und aktualisiert wird.	Es ist ein Konzept zur Rollenpflege vorhanden.
HANA-DB-LS-21	Berechtigungs-management	Es besteht das Risiko des unberechtigten Zugriffs auf alle Objekte im Produktivsystem. Dadurch Verstoß gegen die Grundsätze der Autorisierung, Integrität und Unveränderbarkeit möglich.	Namenskonventionen für Rollen wurden festgelegt, sind dokumentiert und werden angewandt.	Namenskonvention (Rollen)	Ein Konzept zur Vorgabe von Namenskonventionen ist vorhanden und wird regelmäßig geprüft.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts.	Prüfung der Einhaltung der vorgegebenen Namenskonvention für Rollen über folgendes SQL-Statement: `SELECT * FROM ROLES`	Namenskonventionen wurden definiert und durchgehend angewendet.
HANA-DB-LS-22	Berechtigungs-management	Es besteht das Risiko von intransparenten bzw. unberechtigten Zugriffen durch unzureichend gepflegte Rollen. Dadurch Verstoß gegen die	Für die Rollenpflege, die idealerweise in einem dem Produktivsystem vorgelagerten System stattfindet, existiert ein	Rollenpflege im Produktivdatenbank	Die Pflege von Rollen erfolgt im Entwicklungssystem. Die Berechtigungen zur Rollenpflege sind somit	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob Benutzer im produktiven System existieren, die Berechtigungen zur Rollenpflege besitzen, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE GRANTEE_TYPE = 'USER' AND PRIVILEGE =`	Die Berechtigungen zur Rollenpflege sind ausschließlich im Entwicklungssystem vergeben. Oder die Berechtigungen zur Rollenpflege sind im Ausnahmefall im

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
		Grundsätze der Autorisierung und Vertraulichkeit möglich.	standardisierter Change-Prozess.		grundsätzlich nur in diesen vergeben. Sofern Berechtigungen im Ausnahmefall im Produktivsystem vergeben werden, sind entsprechende Freigabeprozesse zur Änderung vorhanden und dokumentiert.	Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	`'ROLE ADMIN' AND OBJECT_TYPE = 'SYSTEMPRIVILEGE'`	Produktivsystem vergeben; dann sind kompensierende Maßnahmen (z.B. durch Festlegung von Freigabeprozessen) definiert.
HANA-DB-LS-23	Berechtigungs-management	Es besteht das Risiko eines intransparenten Berechtigungskonzept durch unzureichend geregelte Namenskonventionen.	Änderungen an Rollen werden protokolliert.	Protokollierung der Rollenänderungen	Änderungen an Rollen (für Runtime-Katalogrollen und Design-Time-Repository-Rollen (XSC)) werden protokolliert.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	Prüfung anhand der Rollen: Runtime-Katalogrollen und Design-Time-HANA-DI-Rollen (XSA) Prüfung der Parameter zur Protokollierung von Rollenänderungen über folgendes SQL-Statement: `SELECT * FROM AUDIT_POLICIES WHERE EVENT_ACTION IN ('ALTER ROLE', 'CREATE ROLE', 'DROP ROLE')`	Die Änderungen an Rollen sind protokolliert. Für alle Aktionen ist ein aktiver Datensatz vorhanden. Der Wert in den Feldern IS_AUDIT_POLICY_ACTIVE und IS_VALID ist TRUE In den Feldern USER_NAME und EXCEPT_USER_NAME sind keine Werte enthalten
HANA-DB-LS-24	Berechtigungs-management	Es besteht ein hohes Sicherheitsrisiko bei der Rollenpflege im Produktivsystem. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Für die Pflege von Repository-Rollen, die idealerweise in einem dem Produktivsystem vorgelagerten System stattfindet, existiert ein standardisierter Change-Prozess. Sofern Repository-Rollen nicht verwendet werden, ist die Pflegeberechtigung nicht vergeben.	Kritische Berechtigung - Pflege der Repository-Rollen	Die Berechtigungen zur Pflege von Repository-Rollen werden nur vergeben, wenn Repository-Rollen im Berechtigungskonzept vorgesehen sind. Die Pflege der Repository-Rollen findet ausschließlich im Entwicklungssystem statt.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	Prüfung, ob Benutzer im produktiven System existieren, die Berechtigungen zur Pflege von Repository-Rollen besitzen, über folgendes SQL-Statement ("User1" und User2" sind durch tatsächliche User zu ersetzen): `SELECT * FROM EFFECTIVE_PRIVILEGE WHERE USER_NAME IN ('USER1', 'USER2') AND GRANTEE_TYPE = 'USER' AND PRIVILEGE <> 'REPO.READ' AND OBJECT_TYPE = 'REPO'`	Im Produktivsystem ist die Berechtigung zur Pflege von Repository-Rollen keinem Benutzer zugeordnet.
HANA-DB-LS-25	Berechtigungs-management	Rollenänderungen werden nicht protokolliert. Dadurch Verstoß gegen den Grundsatz der Nachvollziehbarkeit möglich.	Die Rollenpflege erfolgt durch autorisierte Benutzer.	Pflege kritischer Rollen - Verantwortliche Benutzer	Die Pflege von Rollen erfolgt nur durch dafür verantwortliche Benutzer. Die Berechtigungen zur Pflege von Rollen sind entsprechend auf diese Benutzer eingeschränkt.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	Prüfung, ob Benutzer im produktiven System existieren, die Berechtigungen zur Rollenpflege besitzen, über folgendes SQL-Statement: Design-Time-Repository-Rollen (XSC): `SELECT * FROM _SYS_REPO.OBJECT_HISTORY WHERE OBJECT_SUFFIX = 'hdbrole'`	Rollenänderungen wurden nur durch Benutzer durchgeführt, die für die Rollenpflege verantwortlich sind.
HANA-DB-LS-26	Berechtigungs-management	Es besteht ein hohes Sicherheitsrisiko bei der Pflege von Repository-Rollen im Produktivsystem. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Die Zuweisung von Rollen erfolgt durch autorisierte Benutzer.	Pflege kritischer Rollen - Berechtigungskonzept	Die Berechtigungen zur Zuordnung von Repository-Rollen werden nur vergeben, wenn Repository-Rollen im Berechtigungskonzept vorgesehen sind.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.	Prüfung, ob Benutzer im produktiven System existieren, die Berechtigungen zur Zuordnung von Repository-Rollen besitzen, über folgendes SQL-Statement: `SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE GRANTEE_TYPE = 'USER' AND PRIVILEGE = 'EXECUTE' AND OBJECT_TYPE = 'PROCEDURE' AND`	Die Rollen wurden korrekt zugeordnet.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis
					Die Zuordnung der Repository-Rollen erfolgt ausschließlich durch die verantwortlichen Administratoren.	Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	`OBJECT_NAME = 'GRANT_ACTIVATED_ROLE' AND SCHEMA_NAME = '_SYS_REPO'`	
HANA-DB-LS-27	Berechtigungs-management	Die Rollenpflege erfolgt durch nicht autorisierte Benutzer. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Der Import von Repository-Rollen erfolgt nach einem standardisierten Change-Prozess. Der Import von Repository-Rollen wird protokolliert.	Pflege kritischer Rollen - Protokollierung	Der Import und die Aktivierung von Repository-Rollen werden protokolliert und regelmäßig geprüft, um sicherzustellen, dass keine Programme und andere Repository- Elemente in das System, ohne Verwendung des Transportprozesses, eingebracht werden.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	Prüfung, ob der Import und die Aktivierung von Repository-Rollen protokolliert werden, über folgendes SQL-Statement: `SELECT * FROM AUDIT_POLICIES WHERE EVENT_ACTION IN ('ACTIVATE REPOSITORY CONTENT', 'IMPORT REPOSITORY CONTENT')`	Der Import und die Aktivierung von Repository-Rollen werden protokolliert. Es besteht für alle Aktionen ein aktiver Datensatz. Der Wert in den Feldern IS_AUDIT_POLICY_ACTIVE und IS_VALID ist TRUE. In den Feldern USER_NAME und EXCEPT_USER_NAME sind keine Werte enthalten.
HANA-DB-LS-28	Berechtigungs-management	Die Zuweisung von Rollen erfolgt durch nicht autorisierte Benutzer. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Änderungen am System erfolgen durch autorisierte Benutzer.	Zugriff auf Entwicklungsumgebung	Die Entwicklungsumgebung *Web IDE* wird ausschließlich von Entwicklern genutzt, die dafür vom Unternehmen bestimmt wurden.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	Prüfung, welche Benutzer Zugriff auf die Entwicklungsumgebung haben, über folgendes SQL-Statement: `SELECT * FROM USER_PARAMETERS WHERE VALUE = 'WEBIDE_DEVELOPER'`	Es werden die berechtigten Entwickler als Benutzer angezeigt.

HANA-DB-LS-29	Berechtigungs-management	Durch den Import von Repository-Rollen können weitreichende Berechtigungen entstehen. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Für die Anlage von HDI-Containern, die idealerweise in einem dem Produktivsystem vorgelagerten System stattfindet, existiert ein standardisierter Change-Prozess.	Anlage neuer HDI-Container	Die Rechte zur Anlage neuer HDI-Container werden nur im Entwicklungssystem vergeben, da mit diesen neuen Schemata erstellt werden können.
					
					Sofern in Ausnahmefällen Berechtigungen im Produktivsystem bestehen, sind entsprechende kompensierende Maßnahmen zu ergreifen.
						Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.
						
						Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.
							Einzelprüfung der Rechte zu Anlage neuer HDI-Container je Schema über folgendes SQL-Statement:
							
							`SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE GRANTEE_TYPE = 'USER' AND PRIVILEGE = 'EXECUTE' AND OBJECT_TYPE = 'PROCEDURE' AND OBJECT_NAME = 'GRANT_CONTAINER_SCHEMA_ROLES' AND SCHEMA_NAME = '_SYS_DI'`
							
							Liste aller Benutzer und Rollen, denen die Berechtigung direkt zugeordnet ist, über folgendes SQL-Statement:
							
							`SELECT*FROM GRANTED_PRIVILEGES WHERE OBJECT_NAME = 'GRANT_CONTAINER_SCHEMA_ROLES'`
								Die Benutzer mit den entsprechenden Berechtigungen werden aufgelistet.
								
								Sofern in Ausnahmefällen Berechtigungen im Produktivsystem bestehen, können kompensierende Maßnahmen nachgewiesen werden.

HANA-DB-LS-30	Berechtigungs-management	Änderungen am System erfolgen durch nicht autorisierte Benutzer. Dadurch Verstoß gegen den Grundsatz der Integrität möglich.	Die Rolle *SAP_INTERNAL_HANA_SUPPORT* wird ausschließlich zu Supportzwecken zeitlich und auf einen User begrenzt verwendet.	Kritische Berechtigung SAP HANA Support Rolle	Die Rolle *SAP_INTERNAL_HANA_SUPPORT* wird aufgrund Ihrer Kritikalität nicht mehreren Benutzern zugeordnet.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene. Prüfung des Benutzerberechtigungskonzepts insbesondere des Vergabeverfahrens.	Prüfung in der Systemdatenbank (1) über folgendes SQL-Statement: `SELECT*FROM GRANTED_ROLES WHERE ROLE_NAME = 'SAP_INTENAL_HANA_SUPPORT'` Prüfung in der Systemdatenbank (2) über folgendes SQL-Statement:	(1) Systemdatenbank: Es wird die Zuordnung der Rolle *SAP_INTERNAL_HANA_SUPPORT* zu ausgewählten Benutzern und den entsprechenden Zeitraum angezeigt. (2) Systemdatenbank: Es erfolgt eine Auflistung

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Kontroll-nummer	Prüfbereich	Risiko	Kontrollziel	Kontroll-bezeichnung	Kontrollbeschreibung	Aufbauprüfung	Funktionsprüfung	Erwartetes Ergebnis

							`SELECT*FROM M_INIFILE_CONTENTS WHERE SECTION = 'authorization' AND FILE_NAME = 'nameserver.ini' AND KEY = 'internal_support_user_limit'`
							
							Prüfung in der Tenant-Datenbank (3) über folgendes SQL-Statement:
							
							`SELECT * FROM M_INIFILE_CONTENTS WHERE SECTION = 'authorization' AND FILE_NAME = 'indexserver.ini' AND KEY = 'internal_support_user_limit'`
								der vorgegebenen Einschränkungen für die Rolle *SAP_INTERNAL_HANA_SUPPORT*.
								(3) Tenant-Datenbank: Es erfolgt eine Auflistung der vorgegebenen Einschränkungen für die Rolle *SAP_INTERNAL_HANA_SUPPORT*.

HANA-DB-LS-31	Berechtigungs-management	Über die Anlage neuer HDI-Container besteht die Möglichkeit, Berechtigungsstrukturen zu ändern. Dadurch Verstoß gegen die Grundsätze der Autorisierung und Vertraulichkeit möglich.	Die Rollen *CONTENT_ADMIN* und *MODELING* sind nicht in den Produktivsystemen vergeben.	Kritische Standardrollen
				
				CONTENT_ADMIN und *MODELING*
					Die Rollen *CONTENT_ADMIN* und *MODELING* werden aufgrund des Berechtigungsumfangs nicht in den Produktivsystemen vergeben.	Prüfung der Richtlinien zur Informationssicherheit und zum Schutz des Zugriffs auf privilegierter Ebene.
						
						Prüfung des Benutzerberechtigungskonzepts.
							Prüfung, ob Benutzer existieren, die über die Rolle *CONTENT_ADMIN* bzw. *MODELING* verfügen, über folgendes SQL-Statement:
							
							<u>Rolle CONTENT_ADMIN:</u>
							
							`SELECT * FROM GRANTED_ROLES WHERE ROLE_NAME ='CONTENT_ADMIN'`
							
							<u>Rolle MODELING:</u>
							
							`SELECT * FROM GRANTED_ROLES WHERE ROLE_NAME ='MODELING'`
								Die Rollen *CONTENT_ADMIN* und *MODELING* sind in den Produktivsystemen keinen Benutzern zugeordnet.

Tabelle 1: Prüfmatrix

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Autorenteam

- Martin Becker
- Ümran Narci
- Ahmet Altinata
- Ulrike Gaupp
- Karl-Ludwig Hahne
- Steffen Wodsack
- Markus Keil
- Adnan Bouziani
- Martin Lamm
- Natalja Geick
- Philipp Spangenberg
- Besir Kartal
- Markus Willmann
- Andreas Schneider

Vorstand

- Dr. Tim Sattler (Präsident)
- Thomas O. Englerth (Vizepräsident – Zertifizierungen)
- Dirk Meissner (Vizepräsident – Finanzen und Verwaltung)
- Markus Gaulke (Vizepräsident – Weiterbildung)
- Prof. Dr. Matthias Goeken (Vizepräsident – Veröffentlichungen)
- Julia Hermann (Vizepräsidentin – Kommunikation und Marketing)
- Matthias Kraft (Vizepräsident – Fachgruppen)

Möchten Sie zu diesem Positionspapier mit uns Kontakt aufnehmen. Dann schreiben Sie uns bitte an: FG-SAP@isaca.de

Interessieren Sie sich für weitere Veröffentlichungen des ISACA Germany Chapter? Dann besuchen Sie uns jetzt auf: https://www.isaca.de/de/veroeffentlichungen-des-isaca-germany-chapters