Governance in SAP Delivery

Challenges des IT Service Verantwortlichen

Ömer Canitez und Jörg Altmeier

CC Energie und wikima4 AG

DSAG

DSAG-Jahreskongress 2023

19. - 21. September 2023
Messe und Congress Centrum Bremen

ABSTRACT

IT-Verantwortliche stehen immer häufiger der Herausforderung gegenüber, die Governance der in ihrem Unternehmen eingesetzten SAP-Systemen zu gewährleisten.

Neue Regulatorien, verstärktes externes Auditing und Businessanforderungen stehen einer immer enger werdenden Ressourcensituation gegenüber.

Das Referat wird aufzeigen, wie sich IT-Verantwortliche mit geeigneten Mitteln und Vorgehensweisen in diesem Spannungsfeld erfolgreich und nachhaltig bewegen.

CC ENERGIE

BKW groupe E

Dienstleister im Energiesektor

- **Gegründet 2006**
  von BKW Energie AG (Sitz in Bern) und
  Groupe E (Sitz in Granges-Paccot, Freiburg)
- **500’000 Kunden**
- **680’000 Zählpunkte**
- **SAP IS-U, SAP CRM, SAP PI/PO**

energie
united competences

Customer Service Center

- **433’000** Kontakte **/** Jahr

Billing

- **2.6 Mio** Rechnungen / Jahr

IT & Projects

- 128'000 Online-Kunden
- 500 SAP Benutzer

wikima4

Software-, Implementierungs- und Service Provider

wikima4
Control meets efficiency.

Product Suite

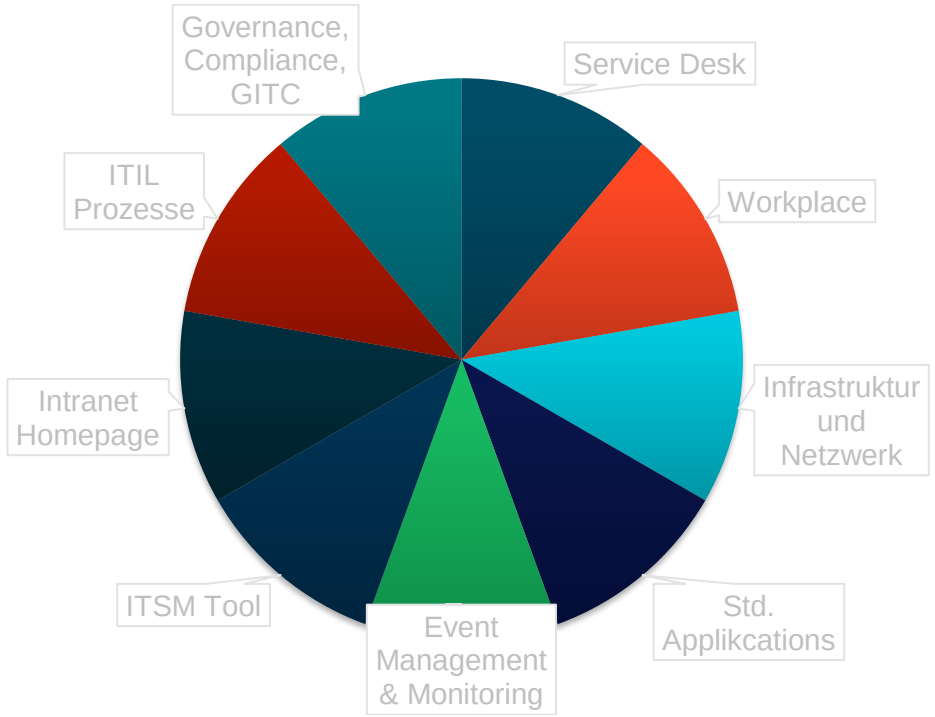
- Compliance SOD
- Internal external security
- Analytics
- Licence optimisation
- Identity management
- Role designer & tuner
- Auditor
- Agile access management
- GDPR

Service Suite

- Internal control systems
- Process documentation
- Identity access management
- Licence optimisation
- Audit
- SAP authorization management

Ömer Canitez und Jörg Altmeier

Internationaler IT-Manager
Aufgewachsen in Norddeutschland
Lange Jahre selbständig/Firmengründer
Verschiedene Managementpositionen in
Hamburg, Genf, Paris, München, Murten
> 25 Jahre Managementerfahrung



- Seit über 25 Jahren beratend im Umfeld Projects, Processes, Quality, Information, Security und Knowledge tätig. Schwerpunkte: Verbindung von Enterprise Resource Planning Systemen mit Qualitätsmanagement- und Sicherheits-Konzepten.
- Managing Partner der wikima4 AG in Zug/ CH. Special Expertise in Governance, Risk & Compliance und Identity Management, SAP Services Partner, SAP Software Partner
- Studien in Betriebswirtschaft (Diplom) und Total Quality Management (Master) in Saarbrücken und Kaiserslautern.
- Leiter der Interessensgemeinschaft SAP (IGSAP) der ISACA, Switzerland Chapter; Certified Information Security Auditor (CISA), zertifizierter TQM Leader der Eopean Organisation for Quality (EOQ) und zertifizierter Business Excellence Coach der Schweizerischen Arbeitsgemeinschaft für Qualitätsförderung (SAQ).
- Lehrbeauftragter an diversen Hochschulen.
- Autor diverser Fachpublikationen.(u.a. der Studie zur SAP Security)

Job description of a Delivery Responsible

- **The Delivery Responsible is responsible for overseeing the successful and timely delivery of products, services, or projects within an organization. This role involves coordinating and managing all aspects of the delivery process to ensure that customer requirements and organizational goals are met.**

- **Key Responsibilities**
  Project Planning, Resource Management, Team Leadership, Risk Management, Quality Assurance, Communication, Problem Solving, Documentation, Customer Satisfaction, Continuous Improvement.

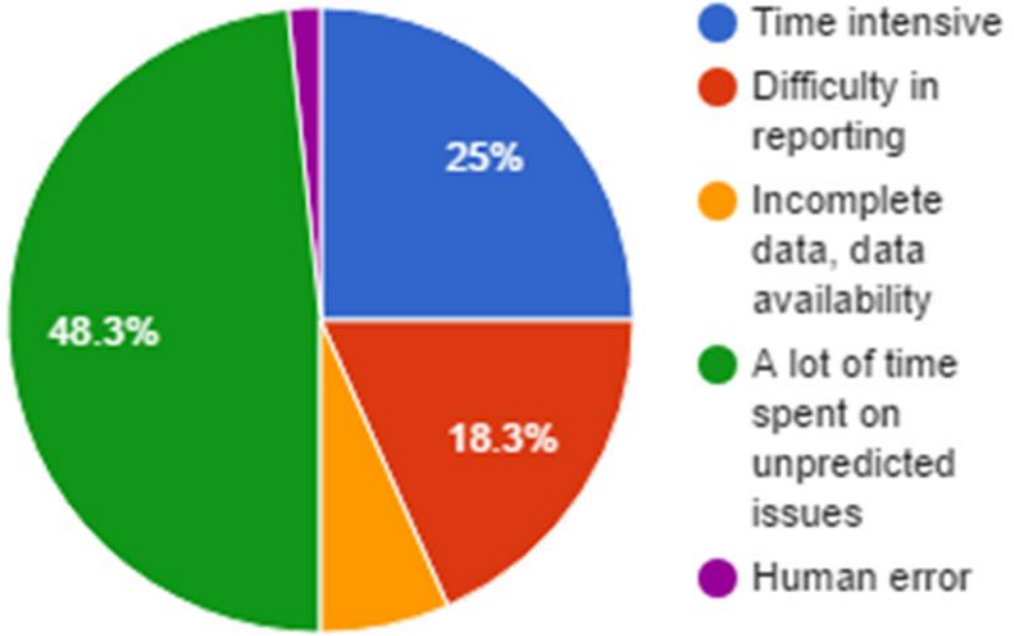
- **Qualifications**
  Bachelor's degree, Proven experience in project management or a related role, Strong leadership and team management skills, Excellent communication and interpersonal skills, Problem-solving and critical-thinking abilities, Knowledge of project management methodologies, ... , Attention to detail and a focus on quality, Ability to work under pressure and meet deadlines.

Mitspieler / Stakeholders

- **Betrieb/Operations**
- **User Access Management / Helpdesk**
- **Change Management / Development / Interne Modulexperten and externe Consultants / Problemlösung / FireFighting**
- **Internes und externes Audit / Compliance Verantwortlicher / Legal**
- **Nicht zuletzt … Fachbereichs-Verantwortliche und Geschäftsleitung**
- **Ups … nicht zu vergessen … SAP Benutzer**

Betrieb / Operations

- Fachkräftemangel
- Koordination von Ressourcen
- Zeitverbrauchender / langsamer Betrieb
- Komplexität / hohes Risikopotential
- System Downtime beeinträchtigt Produktivität
- Kostenreduktion
- Schnelle Reaktion
- Schlanke Prozesse



Quelle: SAP

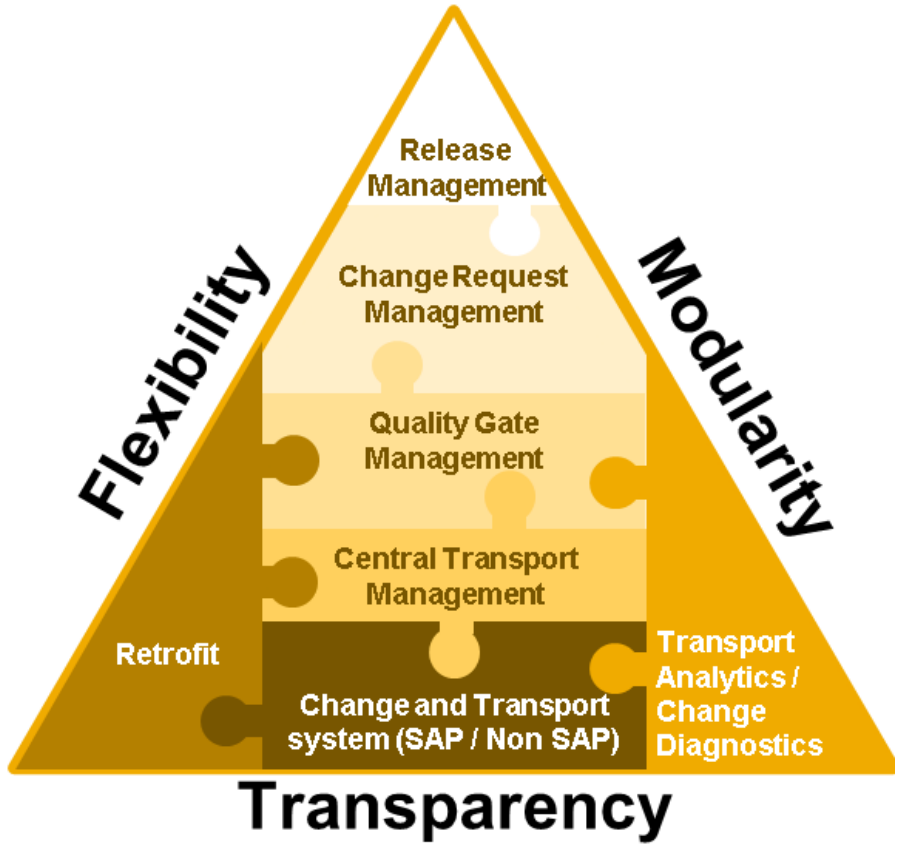
Management Board/Business Line Managers

- **Erlös-/ Gewinnsteigerung**
- **Steigende Kundenzufriedenheit**
- **On-time Lieferungfähigkeit verbessern**
- **Durchlaufzeit reduzieren (Vendor Invoicing, Period end Closing, ...)**
- **Prozesskosten/ TCO reduzieren (Logistics, Customer Support, ...)**
- **Risiko- und Compliance-Kosten reduzieren**

User Access Management/ Helpdesk

- **Fehlender zentraler Überblick**
- **Fehler im User Lifecycle Management. Manuelle Zuweisungen und Abgrenzungen plus Rollenmutation**
- **Unklarer Beantragungsprozess**
- **Sicherstellen der Applikations-Integration**
- **Dritt-Anbieter-Tools Compliance (auch SaaS)**
- **Weitreichende Zugriffsrechte**
- **Konfigurations-Fehler**
- **Compliance/ Audit Herausforderung**
- **Multicloud Risiken**
- **Insider Threats And Privilege Abuse**
- **Schwache Management Policies / Practices**
- **Data Access Risiken**

Change Management

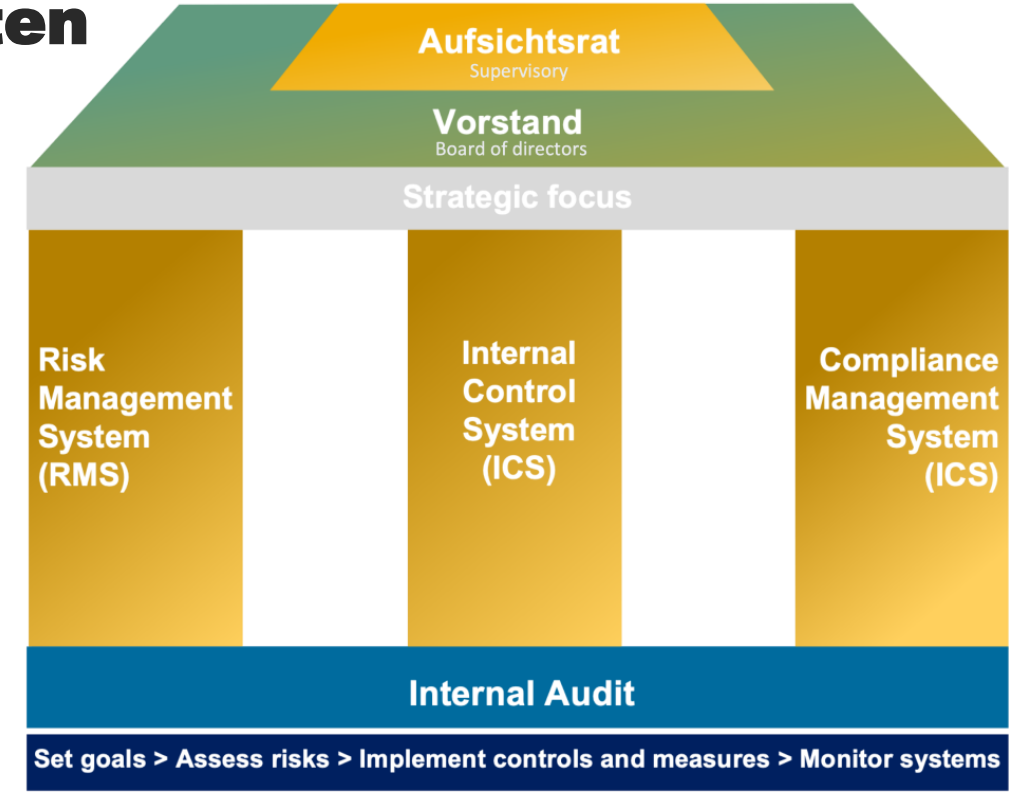


Quelle: SAP

Internes und externes Audit/ Compliance Board

- **Geschäftsprozesse**
- **Funktions-Trennung und kritische Daten**
- **Kontroll-Auswahl**
- **Kontroll-Typen**
- **Konfigurierbare Kontrollen**
- **Prozess-Risiken**
- **Rotation**
- **Risiko-basierter Ansatz**

House of Governance



Quelle: SAP

SAP Benutzer

- **Benutzer-Eintritt/ SAP-Zugriff/ Initial onboarding**
- **Typische Benutzerklagen/ pain points**
- **Nur periodisch ausgeführte Aktivitäten und Prozesse**
- **Datenqualität**
- **Missbrauch, Zugriffsverletzungen, einfach nur simple Fehleingaben**

Conflicting interests: The Challenge

Quelle: Uderzo Coscinny

Grundlage: 4 Ebenen-Modell Compliance in SAP

Ein effektives internes Kontrollsystem muss auf allen risikobehafteten Schichten eines Unternehmens implementiert werden. Bei der Umsetzung eines solchen ganzheitlichen IKS in einem SAP-gestützten Prozess gehören hierzu:

- **die Kontrollen auf Geschäftsprozessebene,**
- **die Kontrollen auf SAP Anwendungsebene (prozessbezogen und applikationsübergreifend),**
- **die Kontrollen für die SAP Basissysteme und**
- **die Kontrollen für die SAP-Infrastruktur.**

Perimeter Layer/ Basis Layer

Kontroll-ebene	Kontrollart	Kontrollziele	SAP Funktionalität (Beispiele zur Umsetzung der Kontrollen)
SAP Basis-systeme	Generelle IT Kontrollen (ITGC)	Software-entwicklung IT-Änderungen IT-Betrieb Zugriffskontrolle Systemsicherheit Datensicherheit Überwachung	SAP Berechtigungen
			SAP Change Management Prozesse
			SAP Transport Management System
			SAP Support Packages
			SAP Security Notes
			SAP Passwort- und Anmeldeparameter
			Schutz der SAP Standardbenutzer (SAP*, DDIC, SAPCPIC, …)
			Zugriffskontrollen für Datenbanken
			Change Management für Datenbanken
			Patching für Datenbanken
			Passwort- und Anmeldeparameter für Datenbanken
SAP Infra-struktur	Generelle IT Kontrollen (ITGC)		Zugriffskontrollen auf Infrastruktur
			Change Management Kontrollen für Infrastruktur
			Patching auf Betriebssystemebene
			Passwort- und Anmeldeparameter für Infrastruktur (SAP Server, Betriebssysteme, Netzwerk)
			Physische Sicherheit
			System Hardening
			Backup Procedures
			Disaster Recovery Pläne für SAP Systeme

Application Layer

Kontroll-ebene	Kontrollart	Kontrollziele	SAP Funktionalität (Beispiele zur Umsetzung der Kontrollen)
SAP Anwen-dungen	Automatische Prozess- / Applikations-kontrollen (ITAC)	Vollständigkeit Nachvollzieh-barkeit Unveränderbarkeit Genauigkeit Gültigkeit Berechtigungen Funktions-trennung	Prozessmonitoring, z.B. - Aufzeigen von Zahlungen ohne Referenzdokument - Identifizieren von ausgehenden Zahlungen > Betrag x - Identifizieren von Lieferanten, die zum Löschen vorgemerkt, aber noch nicht gesperrt sind - Identifizieren von Lieferanten mit Zahlungsbedingung "Zahlbar sofort" oder Zahlungsmethode "Barzahlung" - Monitoring von Änderungen sensibler Felder im Lieferantenstamm wie "alternativer Zahlungsempfänger" - Aufdecken von Fällen wo die Bestellung am Tag des Rechnungseingangs oder danach erstellt wurde - Identifizieren gesplitteter Bestellungen (zum Umgehen definierter Bestell- und Genehmigungslimits)
	Prozessüberg reifende Applikations-kontrollen (ITAC)		Monitoring der Datenverarbeitung und der Benutzeraktivitäten in SAP: - Änderungsbelege - Tabellenprotokollierung - Belegnummernvergabe - AuditLog, - SystemLog - Überwachung von Batch-Input-Verarbeitungen, von IDocs

Business on non-SAP Layer

Kontroll-ebene	Kontrollart	Kontrollziele	SAP Funktionalität (Beispiele zur Umsetzung der Kontrollen)
Geschäfts-prozesse	Manuelle Prozess-kontrollen	Vollständigkeit Nachvollzieh-barkeit Unveränder-barkeit Genauigkeit Gültigkeit Berechtigungen Funktions-trennung	NICHT in SAP: - Unterschriftenregelungen - Lieferantenauswahl (Lieferantenzertifizierung, Vergleich mit „Schwarzer Liste“ der EU / US, …) - Anbieterverfahren (Mindestanzahl, Selektionskriterien, …) - Lieferantenbewertung (Kriterien, Periodizität, …)
SAP Anwen-dungen	Automatische Prozess- / Applikations-kontrollen (ITAC)	Vollständigkeit Nachvollzieh-barkeit Unveränder-barkeit Genauigkeit Gültigkeit Berechtigungen Funktions-trennung	SAP Funktionstrennungen (SoD), z.B. - Stammdatenpflege und Rechnungsverbuchung - Bestellung und Wareneingang - Anlegen und Freigabe der Bestellung SAP Applikationskontrollen, z.B. - 3-Way-Match (Bestellung, Wareneingang, Rechnung) - Freigabestrategie im Bestellwesen (Vier-Augen-Prinzip) - Pflege kritischer Felder von Kreditoren im 4-Augen-Prinzip - Nutzung von Toleranzgruppen für Preisabweichungen - Rechnungssperren bei Mengen- und Preisabweichungen

Solution: Compliance Cockpit

Das Compliance-Cockpit zeigt, inwiefern die Vorgaben für bestimmte Prozesse und Zustände im System eingehalten wurden

Das Cockpit erlaubt eine Einschätzung der Compliance

Es dient zur Herausstellung von Handlungsbedarf / Korrekturbedarf

Das Cockpit wird einmal monatlich zu Händen der Geschäftsleitung erstellt und von der Geschäftsleitung formell zur Kenntnis genommen

Schwerpunkte:

- **User Account und Access Review**
- **Firefighter**
- **Change Monitoring**

Solution: Compliance Cockpit

#		Indikator	Zielwert	Wert im Bezugszeitrum	
Config	1.1	Anonyme Dialognutzer (SUIM)	0	0	●
	1.2	Anzahl gültige Dialogbenutzer mit hohen Berechtigungen (SUIM, Benutzer nach komplexen Selektionskriterien, Z_DIALOG_01)	0	0	●
	1.3	Firefighter-Berechtigte Konten (MESAFORTE Mandant 001 / 002)	n/a	x / xx Benutzer	Info
	1.4	Technische Benutzer mit hohen Berechtigungen (SUIM , Z_TECH_001)	n/a	x / xy	●
	1.5	Systemkonfiguration, Befunde aus MESAFORTE	keine Befunde	Keine kritischen Tätigkeiten	Info
	1.6	Vollständige Konfiguration Secure Audit Log (SM19, Profile Z100ALL)	Ja	Durchgeführt, zuletzt im 25. Mai 2022 geändert	●
	1.7	Servicebenutzer (SUIM)	n/a	Anzahl Servicebenutzer mit hohen Berechtigungen 0	Info
Usage	2.1	Zugriffe durch anonyme Dialognutzer (SE16, CDHDR)	n/a	0 (keine anonymen Benutzer)	●
	2.2	Zugriffe durch Benutzer mit hohen Berechtigungen	0	0	●
	2.3	Zugriffe auf das System durch Firefighter-Berechtigte	n/a	FF-Benutzungen im Berichtsmonat: Benutzungen: x Total: X Anwender Jane Doe, John Doe Tickets: 1234, 5678 (2x)	Info
	2.3.1	Längste zugewiesene Berechtigung für Firefighter (MESAFORTE)	YTage	X Tage	●
	2.3.2	Konsistenzprüfung Tätigkeiten SAP SAL <-> Mesaforte		Oktober	
	2.5	Anzahl der ungenehmigten Systemöffnungen (SE16, T000)	0	0	●
	2.6	Unverarbeitete Batch-Input-Mappen (SM35, 6 Wochen max. alt)	0	0/3 (Mail an Jane Doe für Bereinigung)	●
	2.7	Prüfung verschiedene abgebrochener Jobs (SM37)	n/a	XX/XY Total ZZ	Info
	2.8	Prüfung inaktiver Konten (kein Login > 90 Tage) SUIM (nach Anmeldedatum und Kennwortänderung)	n/a	XX	Info

Solution: Compliance Cockpit

#		Indikator	Zielwert	Wert im Bezugszeitrum	
Changes	3.0	Anzahl der Transporte in Produktion	n/a	Transporte: Gesamt: XX, Workbench: XY, Customizing: Z	Info
	3.1	Anzahl der unvollständigen Changes (Test/Doku/SOD) , P. Althaus	0	(XX/XX/XX)	●
Controls	4.0	User Account & Access Right Reviews	n/a	offen	Info
	4.1	Datum des letzten abgeschlossenen Zyklus	< 1 Jahr	31.12.2022	●
	4.2	Offene Reviews	2	2 (neue Reviews für 2023 durchzuführen)	Info
	4.3	Anzahl der kontrollierten Nutzungen (2.3 und 2.1, siehe oben)	100%	100%	●
	4.4	Anzahl der Befunde aus der Kontrolle (2.3 und 2.1, siehe oben)	0	Keine	●
	4.5	Kontrolle (Freigabe und Aktionen) Systemöffnungen	100%	0 (Keine Systemöffnungen)	●
	4.6	Review der Firefighter Tätigkeiten auf ungewöhnliche Aktionen	n/a	Durchgeführt und protokolliert, keine kritischen Auffälligkeiten	●
	4.7	Review der A_ User , SAP_OSS* , UCES_RFC-Tätigkeiten auf ungewöhnliche Aktionen (SM20 Ereignisse Stufe 9)	n/a	UCES_RFC V_T001 lesen Zugriff	●
	4.8	Review Aktualität definierte Key Benutzer + update	100%	Beauftragt	●
	4.9	Review Modifikation und Exits Mitarbeiter und Externe	n/a	Durchgeführt, Details siehe unten	●
	5.0	Review ungenehmigte Rollen- und Rechteänderungen	n/a	Ok	●

Cloud-Lösungen (SaaS) und Externalized Services (EaaS)

- **Compliance Engine and Compliance Services**
- **Firefighter Access and Monitoring**
- **Forensic Analyses and Audit Process Services**
- **Role Maintenance Services**
- **...**

Nächste Schritte … fighting the Black Box

- **Automatisiertes Audit … The Auditor**
- **Access Control weiter gedacht: Process Control Monitoring**
- **Continuous Monitoring: Echtzeit-Überwachung und Maschine Learning**

Schlussfolgerungen und Lessons Learnt

- **Compliance technisch implementieren wo immer möglich!**
- **Best-practise Lösungen (Cloud) zur Unterstützung einsetzen!**
- **Leistungen ent-personalieren und externalieren wo immer sinnvoll!**

Mission accomplished ... ;)

Quelle: Uderzo Coscinny

Dankeschön / Fragerunde

Besuchen Sie uns an
unserem Stand Q2

… wir freuen uns auf
einen regen Austausch.