Erstes BarCamp 2022 der Fachgruppe IT-Revision

Workshop 3:
Notwendigkeit des IKS und toolgestützte Umsetzung – Erfahrungsaustausch

2. Juni 2022

Torsten Enk, Marc Lorenz

ISACA®
Germany Chapter

Kurze Vorstellung und Erwartungen

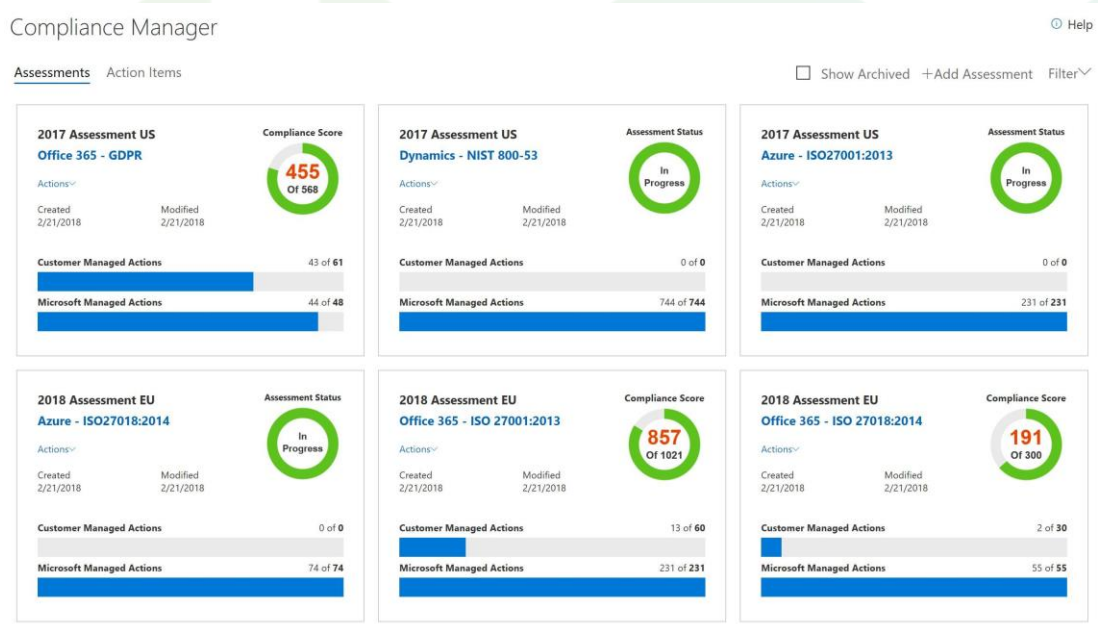
Automatisierung von Kontrollen

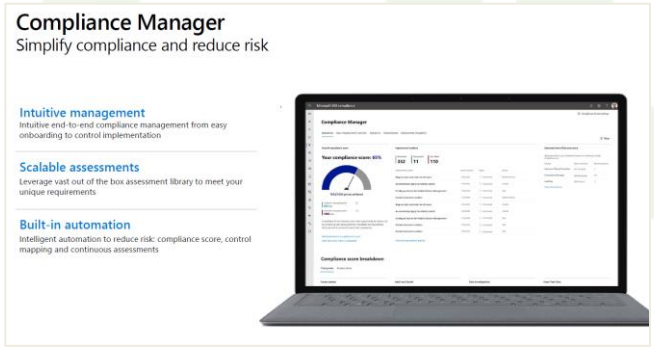
MS Compliance Manager

Microsoft Compliance Manager > auf die Einhaltung von IS/DS fokussiert

- Microsoft Compliance Manager ist ein Feature im Microsoft 365 Compliance Center , mit dem Sie die Compliance-Anforderungen Ihrer Organisation verwalten können. Dieser enthält eine Sammlung vordefinierter Bewertungen, die Sie bei der Skalierung Ihrer Compliance-Aktivitäten unterstützen.
- Unterstützt von der Bestandsaufnahme ihrer Datenschutzrisiken bis hin zur Verwaltung der Komplexität der Implementierung von Steuerelementen, dem aktuellen Stand mit Vorschriften und Zertifizierungen sowie der Berichterstellung an Auditoren.
- Microsoft stellt dazu weitere Services wie das MS Information Governance zur Umsetzung von informationsbasierter Compliance nach den ISO oder DSGVO Standards oder auch das MS Security Compliance Toolkit bereit.

- **<u>Der MS Compliance Manager ist in den sogenannten “Plänen” Enterprise, Microsoft 365, Azure und als Zusatzservice über die Security und Protection Pläne lizenziert.</u>**





Quelle: Microsoft GmbH

Automatisierung von Kontrollen

SAP: Enterprise Threat Detection

SAP Enterprise Threat Protection (SAP ETD) > Spezialistentool mit Fokus auf Security

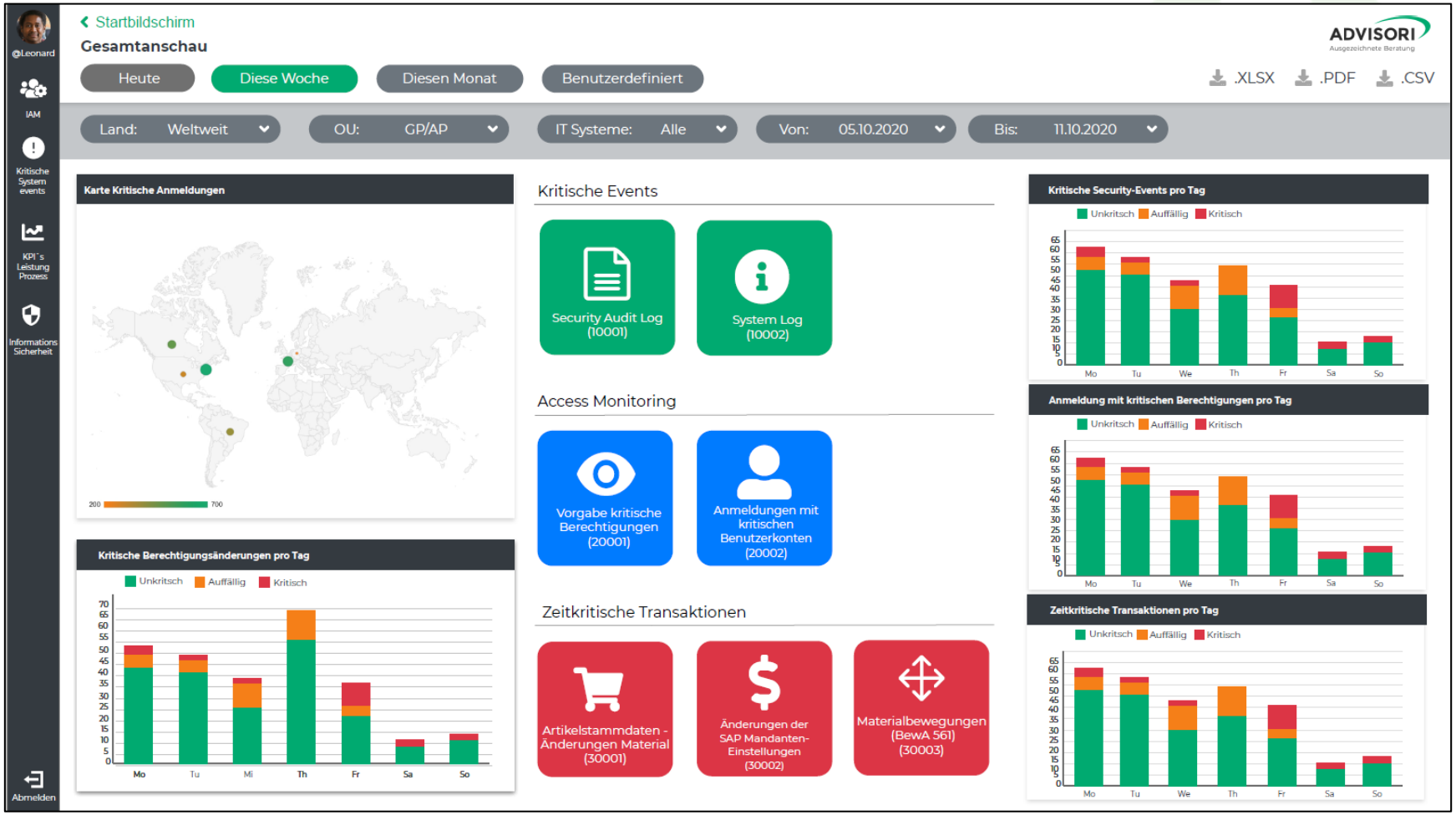
- SAP Enterprise Threat Detection identifiziert Bedrohungen und alarmiert, wenn es zu einem Angriff auf das SAP System kommt. SAP ETD lässt sich als SIEM-Tool (Security Information and Event Management) klassifizieren und ermöglicht die Analyse von Netzwerk- und Sicherheitskomponenten und kann Logs von Betriebssystemen, Datenbanken und Anwendungen erstellen.
- SAP ETD ist auf SAP Systeme spezialisiert und kann ergänzend zu einem SIEM-Tool eingesetzt werden. In kleineren Umgebungen in denen überwiegend nur mit SAP Anwendungen gearbeitet wird, kann die Enterprise Threat Detection auch als alleiniges SIEM genutzt werden.
- Mit **SAP GRC** bietet SAP ergänzend Software-Tools wie das SAP Risk Management, SAP Access Controls, SAP Process Control, SAP Audit Management und SAP Business Integrity Screening.

Quelle: SAP SE

ISACA Germany Chapter

Kontrollautomatisierung mit SPLUNK

Überwachung von Events, Zugriff und kritischen Transaktionen



Quelle: Rödl & Partner, ADVISORI GmbH

ISACA Germany Chapter

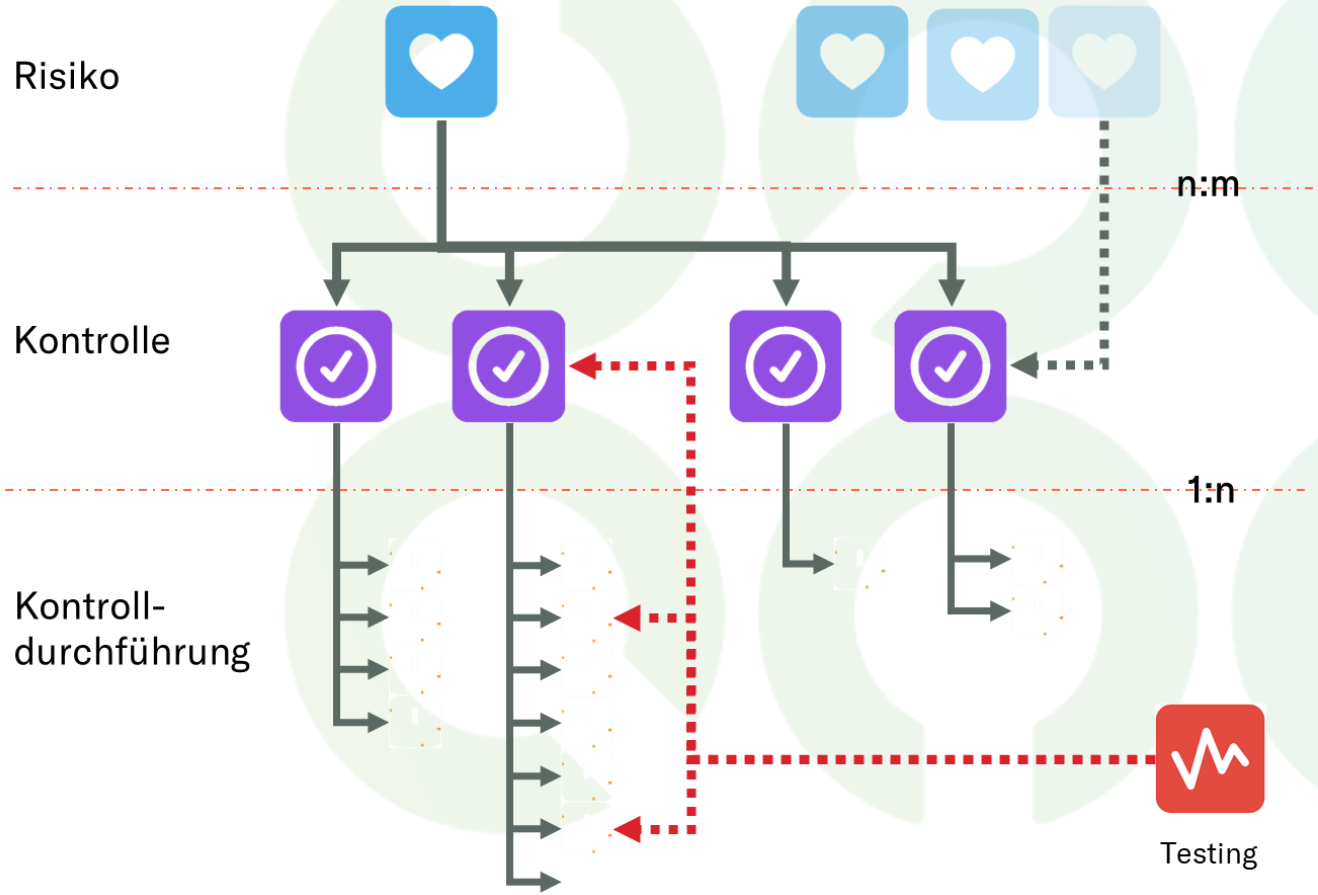
Risiko- und Kontrolldokumentation in JIRA

Offenes Datenmodell

JIRA / CONFLUENCE ist in der Anschaffung günstig.

JIRA wird im IT-Bereich meist für die Ticketbearbeitung, agile Entwicklung, IT-Asset- oder das Change Management genutzt .

Das RM und IKS kann in JIRA durch Anpassung des Datenmodells umgesetzt werden.



Quelle: Mit freundlicher Genehmigung der ISPICIO GmbH

ISACA Germany Chapter

Risiko- und Kontrolldokumentation in JIRA

Risiko- und Kontrollübersicht

Risk Management

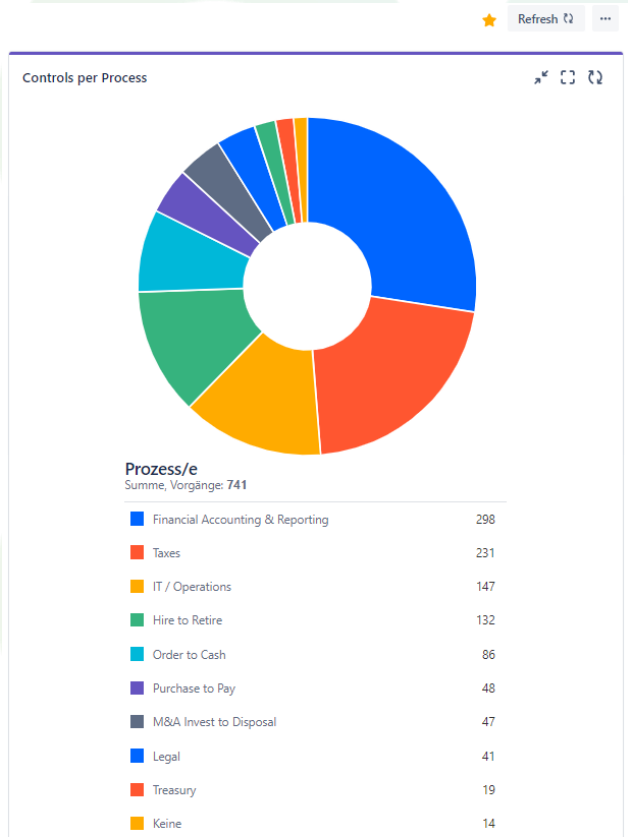
Risk Register

S	Schlüssel	Zusammenfassung	Prozess/e
	RISK-531	Inventory value not correct	Purchase to Pay
	RISK-481	Cash forecast incomplete, not correct or not done	Financial Accounting & Reporting
	RISK-480	Cash Risk: Financial year not fully funded	Financial Accounting & Reporting
	RISK-479	Information and numbers are incorrect	Financial Accounting & Reporting
	RISK-468	IT/systems risk (no system integration: Excel, ERP, bookkeeping system)	Financial Accounting & Reporting, ... (1)
	RISK-452	Workload or wrong organisation delayes closing process.	Financial Accounting & Reporting
	RISK-450	Employees in accounting department are not trained or not familiar with bookkeeping	Financial Accounting & Reporting
	RISK-444	Closing process: Problems regarding external data or documents.	Financial Accounting & Reporting, ... (1)

Internal Controls

Internal Controls

S	Schlüssel	Zusammenfassung
	CTRL-890	Handling and control of bulk transfers
	CTRL-889	Approval process for invoices
	CTRL-885	Inventory value correct
	CTRL-884	Prüfungsausschuß reviewed financial information before disclosure
	CTRL-883	Online access to Bilanz-, IFRS-Kommentaren (Haufe, Beck'scher Bilanzkomm and learning sessions (Lucanet)
	CTRL-881	Back up (IT/ERP) of financial data
	CTRL-880	Standard reporting template for all consolidated companies applied
	CTRL-879	New developments and legal requirements: Report to Management Board Supervisory Board
	CTRL-878	Comprehensive calendar with all actions and deadlines for the financial yea quarterly reportings...)



Quelle: Rödl & Partner

ISACA Germany Chapter

Risiko- und Kontrolldokumentation in JIRA

Adressatengenaue Live-Dashboards

Head of ICS / C-Level

Risks per Process and Status

Prozess/e	OFFEN	APPROVED	S:
Financial Accounting & Reporting	157	25	**182**
Hire to Retire	41	5	**46**
IT / Operations	49	4	**53**
Legal	35	17	**52**
M&A Invest to Disposal	32	4	**36**
Order to Cash	76	13	**89**
PMI (Onboarding Companies)	10	3	**13**
Purchase to Pay	43	15	**58**
Strategy	21	13	**34**
Taxes	138	4	**142**
Treasury	13	5	**18**
n/a	8	2	**10**
Summe, Vorgänge:	**421**	**53**	**474**

Gruppiert durch: Status

Zeigt **12** von **12** Statistiken an.

Controls per Process and Status

Prozess/e	OFFEN	APPROVED	S:
Financial Accounting & Reporting	277	21	**298**
Hire to Retire	132	0	**132**
IT / Operations	144	3	**147**
Legal	41	0	**41**
M&A Invest to Disposal	47	0	**47**
Order to Cash	84	2	**86**
PMI (Onboarding Companies)	9	0	**9**
Purchase to Pay	45	3	**48**
Strategy	12	0	**12**
Taxes	227	4	**231**
Treasury	19	0	**19**
n/a	1	0	**1**
Keine	14	0	**14**
Summe, Vorgänge:	**719**	**22**	**741**

Gruppiert durch: Status

Zeigt **13** von **13** Statistiken an.

Quelle: Rödl & Partner

ISACA Germany Chapter

Mögliche Fragestellungen (zur Diskussion)

1. In welchem Umfang werden bereits ähnliche Technologien in den Unternehmen der Workshop Teilnehmer genutzt oder der Einsatz geplant?

2. Welche Erfahrungen haben Sie über die Zeit damit gesammelt?

3. Wurden geplante Prozesskosten für das IKS Management eingespart und hat sich die Transparenz erhöht?

ISACA Germany Chapter

Ergebnisse

Themenwünsche:

- Toolunterstützung über die 3LoD
- Netze und Produktions-IT
- Synergie zwischen IAM- und IKS-Systemen bzw. Policies
- Zusammenarbeit/Integration über verschiedene Ebenen
- Automatisierung und Erwartung der Banken-Aufsicht
- Zusammenarbeit/Übergang zum Risikomanagement bzw. der 2. Line

ISACA Germany Chapter

Ergebnisse

- Tools für die Digitalisierung des IKS wurden anhand von Beispielen gezeigt und diskutiert wie JIRA, Phython für das Cont. Controls Monitoring.
- Fragestellungen waren auch:
  - Wer pflegt das IKS und Risikomanagement mit Bezug auf das 3LoD Modell?
  - Wie sieht der Projektweg aus?
  - Welches Profil braucht die Interne Revision zukünftig?
  - Wichtige Voraussetzung für datenbasierte Kontrollen und ein digitales IKS ist das tiefe Verständnis der verfügbaren Daten und des Datenmodells > in welcher Tabelle und welchem Feld stehen welche Daten.
  - Ist ein SIEM schon eine Art des digitalen IKS?
  - Eignet sich ein SIEM System auch als Basis für ein digitales IKS genutzt werden.

ISACA Germany Chapter

Vielen Dank!

Torsten Enk
Rödl & Partner
Digital GRC

Straße des 17. Juni 106
10623 Berlin

T 0151-19443137
M torsten.enk@roedl.com

Marc Lorenz
QMS, Methoden & Prozesse (K-GRG-1)
Konzernrevision

Volkswagen Aktiengesellschaft
Brieffach 011/18860
38436 Wolfsburg

Tel. +49 5361 9-89831
Mobil +49 1520 1662038

ISACA Germany Chapter

ISACA®

Germany Chapter