

IAM Exchange 2024

12. - 13. November 2024

Hotel Ameron Königshof Bonn

IAM im Kontext von Cloud Access & SaaS Governance, AI Analytics, Modernisierung & Dezentralisierung, Identity Theft Prevention, vor dem Hintergrund veränderter Business- und Compliance-Anforderungen durch Remote Working und die Einbindung von Partnern und Kunden.



IAM Insights

- Agile IAM Projects
- Adaptive Access Services
- Zero Trust & Conditional Access
- IAM und SoD (Segregation of Duties)
- IAM Automatisierung & KI
- IAM Compliance & KPI's

Programm

www.iam-exchange.com



FESTO

KFW

LANXESS
Energizing Chemistry



Deutsche Bank

sit schwarz
IT

PFEIFFER VACUUM



huelsenberg holding

KOSTAL

GLENCORE



Partner:



Programm

IAM Exchange 2024

12. – 13. November 2024
Hotel Ameron Königshof Bonn

Themenschwerpunkte

- AI im IAM-Umfeld – Chancen, Risiken, Potenziale
- Angriffstrends im IAM-Bereich – Worauf sollte man vorbereitet sein und welche First Response Maßnahmen sollten beherrscht werden?
- Auswirkungen von DORA und NIS2 auf IAM-Prozesse und Architektur
- IAM Governance im Umfeld von Managed Cloud Services und Datenmanagement in der Cloud
- IAM Intelligence & AI Analytics – IAM im Kontext von AI based Security Analytics zur Verbesserung des IT Risk Managements
- IAM Prozesse im IT-Audit – Einhaltung von Richtlinien und Verbesserung interner Prozesse
- IAM Risk Management – Bewertungskriterien von Risiken und effektive IT-Notfallpläne mit Zero Trust
- Authentifizierungsprozesse und Identitätskontrollen für multiple Identitäten und Devices
- IAM-Architektur als essenzieller Teil der IT-Security Architektur – Wie erreicht man eine optimale Verzahnung?
- Multi-Cloud Identity Management – Sichere Konzepte für Berechtigungen im Multi-Cloud Umgebungen
- Passwortlose Multifaktor Authentifizierung in der Praxis
- SoD (Segregation of Duties) und die Vermeidung problematischer Berechtigungskombinationen
- Identity-Lifecycle Management im Kontext von Usern mit Mehrfach-Identitäten im SaaS Umfeld

Zielgruppe

Verantwortliche und leitende Funktionen aus den Bereichen:

- Identity & Access Management
- User Provisioning
- IT-Security
- IT Risk Management
- IT Compliance
- IT Revision



Programm

IAM Exchange 2024

Referenten und Moderatoren



Thi-Hong-Ha Nguyen

Head of Access Lifecycle Solutions
Deutsche Bank AG



Daniel Werner

HDO2.1 Identity and Access Manager
Leopold Kostal GmbH & Co. KG



Thomas Giebler

Head of Identity and Access Management
Festo SE & Co. KG



Frederik Thorn

Global Information Security Officer
Pfeiffer Vacuum Technology AG



Stefan Bosnjakovic

IAM&GRC Architect
Glencore International AG



Paul Mengele

IT Auditor
Swiss Re



Kevin Pohl

Group Information Security Officer
Huelsenberg Holding GmbH & Co.



Patrick Reich

Leitung IAM
SCHWARZ IT



Friederike Bieber

Abteilungsleiterin Identity and Access Management
KfW Bankengruppe



Christian Egli

IAM-Architekt
SBB AG



Andreas Bender

IDM Domain Lead
LANXESS Deutschland GmbH



Sacha Leemann

IAM-Architekt
SBB AG



Michael Synowczik

Head of Identity Management Solutions
LANXESS Deutschland GmbH

8:50 **Begrüßung und Eröffnung durch den Veranstalter und den Vorsitzenden**

9:00 **Identity and Access Management moving to Cloud**

- Introducing Accessio: program to consolidate onPrem applications of Identity Access Management to a single cloud solution
- Consolidation and Migration plan
- Challenges and Overcomes
- Outlooks



Thi-Hong-Ha Nguyen

Head of Access Lifecycle Solutions
Deutsche Bank AG

9:40 **SAP IDM Wartungsende 2027 – was nun?**

- Ist Aufnahme – Was nutzen wir aktuell?
- Marktanalyse – Was bietet der Markt?
- Abgleich mit der IT und Teamstrategie – Was wollen wir zukünftig nutzen?
- Auswahlprozess – Welcher Anbieter bietet was wir benötigen?
- Projektstart – Wie setzen wir um?



Michael Synowczik

Head of Identity Management Solutions
LANXESS Deutschland GmbH



Andreas Bender

IDM Domain Lead
LANXESS Deutschland GmbH

10:20 **Erfrischungs- und Networking Pause**

10:50 **Module based cloud native IAM – Warum die SCHWARZ Gruppe komplett neue Wege einschlägt**

- Standardprodukte passen für Standard Firmen und wer will schon Standard sein.
- Wer hohe Anforderung außerhalb der Norm hat braucht individuelle Lösungen.
- Investment in die Anpassung des Standards kann eine hohe Bindung und Abhängigkeit an den Hersteller und die IT Integratoren bedeuten
- Preiserhöhung, breaking Updates, neue Lizenzmodelle - schmeckt mir nicht, aber hab ich die Wahl?
- Wer versteht mein System noch und wie gehe ich mit neuen Anforderungen um?
- Diesen Fragen gehen wir auf den Grund und zeigen Lösungsansätze.



Patrick Reich

Leitung IAM
SCHWARZ IT

11:30 Thema in Abstimmung

IPG

12:10 Business Lunch

13:10 **Interaktive Round Tables**

Round Table 1

IAM Governance – Wie sich Richtlinien effizient umsetzen und kontinuierlich prüfen lassen

*Thema und Moderation
in Abstimmung*

Round Table 2

IAM Architektur und Automatisierung im Umfeld von Multi-Cloud Umgebungen

*Thema und Moderation
in Abstimmung*

14:10 **Präsentation der Ergebnisse aus den Interaktiven Round Tables**

14:25 **SoD im IAM Kontext**

- Segregation of Duties auf Geschäftsprozeßebene (anstatt nur auf IT-Ebene)
- Was ist eine Business Process Taxonomy
- Entwicklung/Herleitung eines org-structure- and IT-landscape-agnostic SoD-Rulesets
- Implementierung eines automatisierten SoD-Subsystems in IAM anhand von Sailpoint
- Analyse der SoD-Violation-Resultsg



Stefan Bosnjakovic
IAM&GRC Architect
Glencore International AG

15:05 **Erfrischungs- und Networking Pause**

15:30 **Definition und Umsetzung einer Zero Trust Strategie im IAM-Umfeld**

- Einführung in Zero Trust
- Zero Trust im IAM-Kontext
- Umsetzung einer Zero Trust Strategie im IAM
- Vorteile von Zero Trust
- Zero Trust vs. Least Privilege



Kevin Pohl

Group Information Security Officer
Huelsenberg Holding GmbH & Co.

16:10 **DORA und IAM: Sicherer Zugriff im Finanzsektor**

- Überblick wichtigsten Anforderungen der DORA-Verordnung
- Prinzipien der rollenbasierten Zugriffskontrolle (RBAC)
- Rolle der Multi-Faktor-Authentifizierung (MFA)
- Anforderungen an die kontinuierliche Überwachung von Zugriffsereignissen
- Notwendigkeit regelmäßiger Überprüfungen der Zugriffsrechte



Frederik Thorn

Global Information Security Officer
Pfeiffer Vacuum Technology AG

16:50 **Raumwechsel**

Programm

IAM Exchange 2024

1. Konferenztag: Dienstag, 12. November 2024

16:55

Working Groups

Working Group 1

Dezentralisierung im Enterprise IAM
Umfeld

*Thema und Moderation
in Abstimmung*

Working Group 2

Mit KI und maschinellem Lernen,
Anomalien und ungewöhnliches
Nutzerverhalten erkennen

*Thema und Moderation
in Abstimmung*

17:55

Präsentation der Ergebnisse aus den Working Groups

18:10

Ende des 1. Konferenztages

18:30

Abendempfang

8:50 **Begrüßung und Eröffnung durch den Vorsitzenden**

9:00 **IAM in Multi-Cloud Umgebungen**

- Alle Hyperscaler haben ihre eigenen Identitätsdienste - wie bekommen wir die in der Praxis vereint?
- Identity Federation als Brücke zwischen Cloud Diensten und auch On-premise
- Provisionierung von Identitäten und Entitlements
- Access Requirements und MFA über Platform-Grenzen hinweg
- Wie greifen Mitarbeiter auf Angebote für Kunden zu?



Thomas Giebler

Head of Identity and Access Management
Festo SE & Co. KG

9:40 **IAM Prozesse im IT-Audit – Einhaltung von Richtlinien und Verbesserung interner Prozesse**

- Grundlagen - Auf was wird im IT Audit geachtet?
- Risiken und Kontrollen - Effektivität und Effizienz
- Fallstricke und Probleme - Ein Auge fürs Detail
- Beispiel anhand Swiss Re Prozesslandschaft und/oder Diskussionsrunde/Fragen



Paul Mengele

IT Auditor
Swiss Re

10:20 **Erfrischungs- und Networking Pause**

10:50 **Aktuelle Trends in der IT – Wie lassen sich neue Tools, Skriptautomatisierung und KI für ein effizientes und effektives IAM nutzen?**

- Immer mehr Tools, Skript- bzw. Prozessautomatisierung und künstliche Intelligenz sind verfügbar und versprechen enorme Effizienzsteigerungen
- Wie lassen sich diese Trends in der Realität sinnvoll nutzen?
- Welche Voraussetzungen müssen dafür erfüllt sein?
- Und wo sind die Grenzen der Nutzbarkeit?
- Was ist vereinbar mit unserer Regulatorik?
- Eigenen Erfahrungen und Gedankenexperimenten über die Zukunft des IAM



Friederike Bieber

Abteilungsleiterin Identity and Access Management
KfW Bankengruppe

11:30

IAM der Zukunft: Automatisierung und Self-Services als Schlüsselfaktoren für integrierte Sicherheit und Skalierbarkeit in der Cloud

- Self-Services zum Bestellen von Cloud-Ressourcen sind heute eine Selbstverständlichkeit, welche wir im IAM-Umfeld häufig noch nicht bieten können.
- Mit Zero Trust und Microservice Architekturen steigt der Druck, immer feingranularer zu autorisieren. Das verlangt eine weitgehende Automatisierung auch im Bereich von Policies und Berechtigungen.
- Wir zeigen, wie sich viele Prinzipien aus dem Cloud Computing auch auf IAM-Ressourcen anwenden lassen und wie wir damit die Sicherheit und Skalierbarkeit massiv erhöhen.
- Die Automatisierung der Prozesse führt zudem zu einer höheren Sichtbarkeit der relevanten Kenngrößen: Daten können als KPIs ausgewiesen werden und sind vorbereitet für weitere Analysen mit KI.
- Mit der Adoption von Self-Services und Automatisierung transformieren wir unsere IAM-Landschaft mehr und mehr in eine "Identity Fabric".



Christian Egli

IAM-Architekt
SBB AG



Sacha Leemann

IAM-Architekt
SBB AG

12:10

Business Lunch

13:10

IAM Designphase - Anforderungen und Tool-Auswahl für ein internationales, produzierendes Unternehmen

- Kurze Vorstellung des Unternehmens (über 20 Standorte und über 20.000 Mitarbeiter weltweit)
- Ist-Situation in Bezug auf Quellsystem (HR-Data Cube) und Zielsysteme (Active Directory, etc.)
- Vorstellung des Projekts in Bezug auf Prozessanalyse und Zusammenführung der Onboarding-Prozesse
- Überführung in Anforderungskatalog und Software-Evaluationsmatrix
- Learnings und Takeaways



Daniel Werner

HDO2.1 Identity and Access Manager
Leopold Kostal GmbH & Co. KG

14:10

Raumwechsel

Programm

IAM Exchange 2024

2. Konferenztag: Mittwoch, 13. November 2024

14:15

Interaktive Round Tables

Round Table 1

Sichere Automatisierung identitätsbezogener Kontrollen in physischen, virtuellen und Cloud-basierten Umgebungen

*Thema und Moderation
in Abstimmung*

Round Table 2

Bring your own Identity – Einbindung externer Authentifizierungsmethoden für Partner Dienstleister und Kunden

*Thema und Moderation
in Abstimmung*

15:15

Präsentation der Ergebnisse aus den Interaktiven Round Tables

15:30

Ende der Konferenz

IAM Exchange 2024

Lebensläufe der Referenten und Moderatoren

Paul Mengele

in Deutschland aufgewachsen, Erfahrungen im Public und Governmental Affairs in Berlin gesammelt und nun seit knapp 5 Jahren als IT Auditor in Zürich tätig, sowohl bei PwC in der externen Prüfung als auch bei Swiss Re in der Internen Revision.

Daniel Werner

hat nach seinem Studium der Wirtschaftsinformatik acht Jahre in einer Unternehmensberatung in den Themengebieten SAP Berechtigungen und SAP GRC Access Control gearbeitet. Danach wechselte er als Application Manager für das IAM System zur Postbank Systems AG nach Bonn. Seit Mitte 2022 verantwortet er bei der Leopold Kostal GmbH & Co. KG als Identity und Access Manager die IAM-System- und Prozesseinführung.

Andreas Bender

arbeitet seit 2015 im Bereich des Identity and Access Management bei LANXESS. Als globaler Solution Architect verantwortet er seitdem die IAM Prozesse und hat die nun abzulösende SAP IDM Landschaft & Prozesse initial mit aufgesetzt und über die Jahre weiter ausgebaut.

Vor seiner aktuellen Position bekleidete er diverse Funktionen im Rahmen von IT HR bezogenen Projekten.

Die derzeit größte Herausforderung des Bereichs liegt in der Implementierung einer neuen IDM Lösung.

Michael Synowczik

verantwortet seit März 2023 das Thema Identity Management bei LANXESS. Vor seiner aktuellen Position verbrachte er sieben Jahre in verschiedenen Funktionen; insbesondere in dem Bereich Compliance Management des Konzerns. Bevor er zu LXS kam, arbeitete Michael sechs Jahre lang in der Beratungsbranche. Die derzeit größte Herausforderung des Bereichs liegt in der Implementierung einer neuen IDM Lösung.

Stefan Alexander Bosnjakovic

The emphasis of my professional activity during the last twenty years was on IdAM (Identity and Access Management) and GRC (Governance, Risk and Compliance) projects, driven by the clients' needs to comply with regulatory demands and close audit findings in a timely manner, complemented by related project activities incl. SoD (Segregation of Duties) methodology development, RE (Requirement Engineering), RM (role modelling and design of standardised access- and role-models), onboarding and full integration of complex business application suits into the corporate IdAM-frameworks, WM (workflow- and associated process modelling) and BPAM (business process analysis and modelling), applying relevant security norms (ISO27000, Cobit, MaRisk, IT-Grundschutz, etc.) and regulatory requirements (EU (GDPR), ECB, SOx, UKCR, MAS, FFIEC, BaFin (BAIT, VAIT, KAIT), BuBa, FinMa, BoE, etc.). In addition to pure IAG issues I am also integrating related IT-Security related topics like HPAM (High Privilege Access Management), SSO (Single-Sign On), MFA/Passwordless Technologies, CM

(Cloud Migration), Firewall and VPN/SD-WAN into my architecture solutions to complete the overall end-to-end IAG framework. Rounded-up by communication, coordination and setting up train-the-trainer schemes with HR, relevant business and specialist departments.

Patrick Reich

übernahm als Entwickler ein gescheitertes IDM Projekt bei dem seine Naivität nur noch durch seine Motivation getoppt werden konnte. Es folgten diversen IDM Migrationen in verschiedenen Rollen bei großen Unternehmen. Beste Technik und elegante Prozesse sind aber nicht der Garant für den Erfolg - sondern es braucht auch organisatorische Rahmenbedingungen, die eine komplexe IAM Welt beherrschbar machen.

Christian Egli

is a senior IAM architect at SBB AG, the leading Swiss transport company. As an IT professional with more than 20 years of experience in various areas, he has been with SBB since 2010. Notably, he played an instrumental role as a founder of the SBB Cloud Stack, establishing the company's first cloud infrastructure. Christian believes that Identity and Access Management stands as a reservoir of untapped potential for cyber security, automation, and business value, and thus has long been among his favourite topics. Currently, he is on a mission to reshape SBB's Enterprise IAM infrastructure with an emphasis on identity first, everything-as-code, and an overarching policy framework that spans SBB's entire IT landscape. Besides his role at SBB, Christian lends his expertise to shape the Swiss E-ID.

Sacha Leemann

ist IAM-Architekt bei der SBB AG. Er konzentriert sich auf die Entwicklung von Konzepten und Integrationen rund um Workload-Identitäten, um feingranulare Just-in-Time-Zugriffe zu ermöglichen.

Sacha glaubt, dass es notwendig ist, IAM nahtlos mit den heutigen Cloud-zentrierten Entwicklerumgebungen zu verbinden.

Als leidenschaftlicher Software-Ingenieur taucht Sacha in DevSecOps-Prozesse ein, um die betriebliche Effizienz zu steigern und die Ausfallsicherheit zu erhöhen - und das alles bei gleichzeitiger Aufrechterhaltung der Sicherheit auf höchstem Niveau.

Frederik Thorn

agiert als Information Security Officer bei Pfeiffer Vacuum. Neben seiner Expertise für Informationssicherheit auf globaler Ebene kann er mehrjährige Projekterfahrung bei Banken und Versicherungen vorweisen. Sein Master in IT Sicherheits- und Risikomanagement, sowie gängige Zertifizierungen wie DORA Certified Compliance Specialist (DCCS) bekräftigen seine Methodenkompetenz. Er ist bekannt als Mentor für Neueinsteiger in der Informationssicherheit und hält Keynotes zu Cybersicherheitsthemen.

Programm

IAM Exchange 2024

Lebensläufe der Referenten und Moderatoren

Thomas Giebler

25 Jahre Praxiserfahrung in der Unternehmens IT - mehr als 10 Jahre im Identity & Access Management. Verantwortlich für die globalen Aktivitäten des Identity & Access Management der Festo Gruppe. Dazu gehören der sichere Betrieb der Identity Infrastruktur (AD, AAD, AD FS), das SAP Berechtigungsmanagement sowie die Prozesse und Tools der Identity Governance.

Friederike Bieber

kam 2015 von PwC zur KfW. Nach dem Einstieg in der aufsichtsrechtliche Compliance, war sie die persönliche Referentin der Vorständin für das inländische Fördergeschäft. Ab 2019 war sie als Abteilungsdirektorin für das Neukunden Zuschuss- und Kreditgeschäft der wohnwirtschaftlichen Finanzierung zuständig. Seit 2022 verantwortet sie in der IT das zentrale Identity and Access Management für die KfW Bankengruppe