

Identitäts- und Berechtigungsmanagement

Maximilian Heim¹

¹Hochschule Albstadt-Sigmaringen

IT-GRC Seminar, Juni 2024

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- Unterschiedliche Definitionen

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

Identität im Kontext des Identitätsmanagements

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute¹

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute¹
- Wichtig: Digitale Identitäten sind nicht nur Personen

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

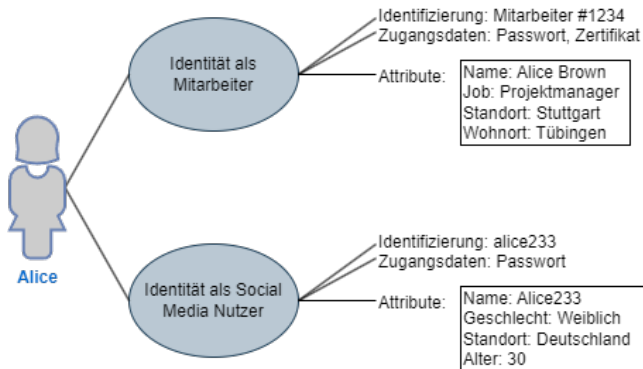


Abbildung: Digitale Identität - Basierend auf Grafik 2.1 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Management von digitalen Identitäten

- Management von digitalen Identitäten
- Gründe: Speicherung, Nutzung und Weitergabe von Identitätsinformationen, Zuordnung von Zutritt und Zugriff zu Entitäten

- Management von digitalen Identitäten
- Gründe: Speicherung, Nutzung und Weitergabe von Identitätsinformationen, Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche: Prozesse (Provisionierung, Änderung . . .), Compliance mit Gesetzen und Standards, Auditierung von Ist vs. Soll . . .

- Management von digitalen Identitäten
- Gründe: Speicherung, Nutzung und Weitergabe von Identitätsinformationen, Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche: Prozesse (Provisionierung, Änderung ...), Compliance mit Gesetzen und Standards, Auditierung von Ist vs. Soll ...
- Grundlegender Prozess: Identitätslebenszyklus

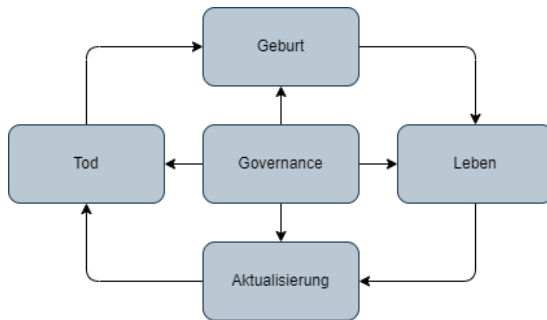


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt:
Datensammlung
und Validierung,
Zugangsdaten

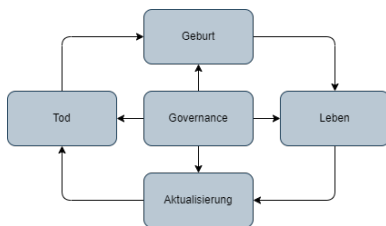
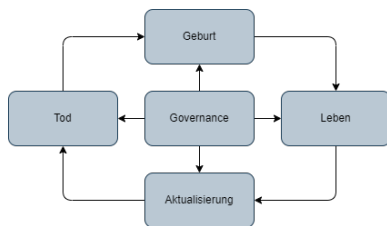
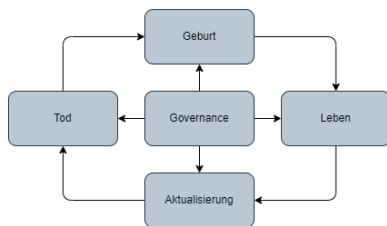


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi



- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi



- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe
- Änderung: Änderungen, Zugangsdaten

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

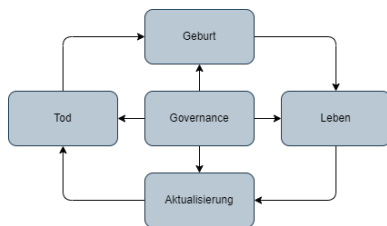


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe
- Änderung: Änderungen, Zugangsdaten
- Tod: Kündigung, Löschung

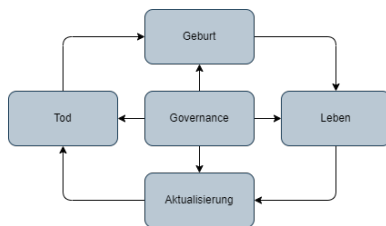


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe
- Änderung: Änderungen, Zugangsdaten
- Tod: Kündigung, Löschung
- Governance: Richtlinien, Audit-Trail^a

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- **Berechtigungsmanagement**
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- Kombination aus Ressource und Operation²

²Alexander Tsoikas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation²
- Beispiele:

²Alexander Tsoikas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?

²Alexander Tolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?

²Alexander Tsoikas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?
 - Wer darf in AWS Zertifikate erstellen?

²Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?
 - Wer darf in AWS Zertifikate erstellen?
 - Wer darf das Wohnzimmer in der Poststraße 22 betreten?

²Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung
- Aufgaben:

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...
 - Technische Umsetzung (Authorisierung)

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...
 - Technische Umsetzung (Authorisierung)
 - Umsetzung von Complianceanforderungen, methodische Standards

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...
 - Technische Umsetzung (Authorisierung)
 - Umsetzung von Complianceanforderungen, methodische Standards
 - Auditierung der Berechtigungsvergabe, kritischen Zugriffen

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe: PoLP (Sicherheit vs. Produktivität/), SoD/Funktionstrennung
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...
 - Technische Umsetzung (Authorisierung)
 - Umsetzung von Complianceanforderungen, methodische Standards
 - Auditierung der Berechtigungsvergabe, kritischen Zugriffen
 - Gewährleistung der Rückverfolgbarkeit

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- Identitäts- und Berechtigungsmanagement = Identity access management (IAM)

- Identitäts- und Berechtigungsmanagement = Identity access management (IAM)
- Unterscheidung: IAM vs CIAM

Identitäts- und Berechtigungsmanagement-Systeme

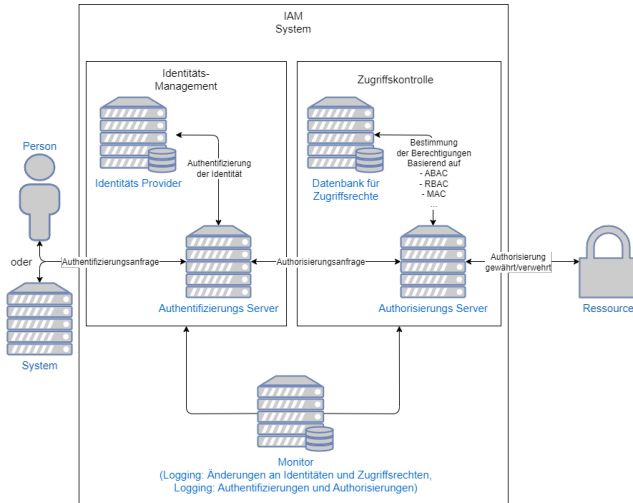


Abbildung: IAM System - Basierend auf Grafik 1 aus „Identity and access management using distributed ledger technology: A survey“ von Fariba Ghaffari, Komal Gilani, Emmanuel Bertin und Noel Crespi

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- CIO: Verantwortlich für Prozesse und Technologien

³Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁴Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

⁵Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...³

³Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁴Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

⁵Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb.* 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...³
- IT-Betrieb: Implementierung und Wartung der involvierten Technik

³Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁴Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

⁵Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb.* 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...³
- IT-Betrieb: Implementierung und Wartung der involvierten Technik
- Personalabteilung: Identity-Lifecycle Management⁴

³Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁴Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

⁵Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb.* 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...³
- IT-Betrieb: Implementierung und Wartung der involvierten Technik
- Personalabteilung: Identity-Lifecycle Management⁴
- Helpdesk: Hilfe bei Authentifizierung und Authorisierung⁵

³Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁴Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

⁵Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb.* 2004.

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- **Technische Aspekte**
- Compliance Aspekte

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On
 - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On
 - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management
 - Integration von Service Providern: Active Directory, Microsoft Office, AWS, HR Anwendungen

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On
 - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management
 - Integration von Service Providern: Active Directory, Microsoft Office, AWS, HR Anwendungen
 - ...

Technische Aspekte

The screenshot displays the Microsoft Entra admin center for the 'Contoso' tenant. The left sidebar contains navigation links: Home, Favorites, Identity, Overview (selected), Users, Groups, Devices, Applications, Protect & secure, Identity Governance, External Identities, Show more, Protection, Identity governance, Permissions Management, Verifiable credentials, Global Secure Access, and Learn & support. The main content area shows the 'Overview' tab with a search bar for the tenant. Below this is the 'Basic information' section, which includes a table of tenant details:

Property	Value
Name	Contoso
Organization ID	7918d4b5-0442-4a87-bc3d8-...
Primary domain	contoso.com
License	Microsoft Entra ID P2
My roles	Global administrator, Global...
Users	434,500
Groups	805,546
Applications	10,234
Devices	55,054

Below the basic information, there are two alert boxes: 'TLS 1.0, 1.1 and 3DES deprecation' and 'Consent required'. The 'My feed' section shows three items: 'Sign ins' (2341 sign ins today, 23% increase), 'Secure Score for Identity' (83.71%, updates every 48 hours), and 'Preview features' (21 private previews, 5 public previews). The 'Recommendations' section shows 24 total recommendations. The bottom right corner displays the user profile for 'Corrie Wilson' (Global Administrator).

Abbildung: Microsoft Entra ID - von

<https://www.microsoft.com/de-de/security/business/microsoft-entra>

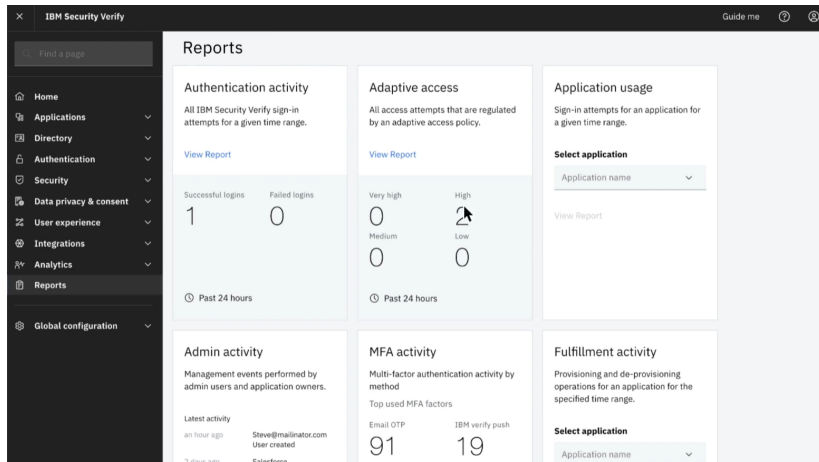


Abbildung: IBM Security Verify - von <https://www.ibm.com/de-de/products/verify-saas>

Technische Aspekte

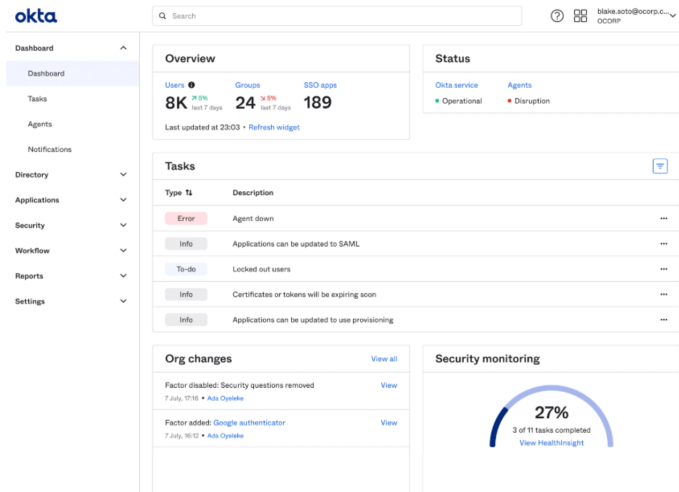


Abbildung: Okta Workforce Identity Cloud - von <https://thectoclub.com/tools/best-identity-and-access-management-solutions/>

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- ISO 27001: Annex A.9 definiert Zugangssteuerung

- ISO 27001: Annex A.9 definiert Zugangssteuerung
- IT-Grundschutz: BSI-Standard 200-1, ORP.4

- ISO 27001: Annex A.9 definiert Zugangssteuerung
- IT-Grundschutz: BSI-Standard 200-1, ORP.4
- NIST 800-53A: Kapitel Access Control Family (AC) und Identification and Authentication Family (IA)

- ISO 27001: Annex A.9 definiert Zugangssteuerung
- IT-Grundschutz: BSI-Standard 200-1, ORP.4
- NIST 800-53A: Kapitel Access Control Family (AC) und Identification and Authentication Family (IA)
- ...

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem
- GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff): Berechtigungskontrolle, Nachvollziehbarkeit von Änderungen

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem
- GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff): Berechtigungskontrolle, Nachvollziehbarkeit von Änderungen
- EU-DSGVO (EU- Datenschutzgrundverordnung) und BDSG (Bundesdatenschutzgesetz): Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem
- GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff): Berechtigungskontrolle, Nachvollziehbarkeit von Änderungen
- EU-DSGVO (EU- Datenschutzgrundverordnung) und BDSG (Bundesdatenschutzgesetz): Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten
- ...

- Vielen Dank für eure Aufmerksamkeit!

- Vielen Dank für eure Aufmerksamkeit!
- Fragen?

- [1] Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.
- [2] Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.
- [3] Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.
- [4] Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- [5] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.