


Author	Dipl.-Ing. Daniel Mrskos, BSc
Funktion	CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer
Datum	14. Juni 2024
	
Zertifizierungen	CSOM, CRTL, eCPTXv2, eWPTXv2, CCD, eCTHPv2, CRTE, CRTO, eCMAP, PNPT, eCPPTv2, eWPT, eCIR, CRTP, CARTP, PAWSP, eMAPT, eCXD, eCDFP, BTL1 (Gold), CAPEN, eEDA, OSWP, CNSP, Comptia Pentest+, ITIL Foundation V3, ICCA, CCNA, eJPTv2, Developing Security Software (LFD121), CAP, Checkmarx Security Champion
LinkedIn	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
Website	https://security-mit-passion.at

Richtlinie zum Change Management

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zum Change Management definiert die Anforderungen und Maßnahmen zur Sicherstellung eines strukturierten und kontrollierten Ansatzes für das Management von Änderungen bei [Unternehmen]. Diese Richtlinie basiert auf den Standards ISO 27001:2022, ISO 27002:2022, CIS Controls v8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SZA für KRITIS, dem European Cyber Resilience Act und DORA.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Berater, Zeitarbeitskräfte, Praktikanten und mit Dritten verbundene Personen, die Änderungen an den IT-Systemen von [Unternehmen] planen, durchführen oder verwalten.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zum Change Management mit den relevanten Sicherheitsstandards und -richtlinien zu gewährleisten. Sie zeigt die Zuordnung der einzelnen Policy-Komponenten zu den spezifischen Anforderungen der Standards wie ISO 27001:2022, CIS Controls V8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SZA für KRITIS, dem European Cyber Resilience Act und DORA. Dies erleichtert die Nachverfolgung und Überprüfung, dass alle notwendigen Sicherheitsmaßnahmen implementiert sind und ermöglicht eine klare, transparente Dokumentation unserer Compliance-Verpflichtungen.

Policy-Komponente	ISO 27001:2022 / 27002:2022	TISAX	CIS Controls V8	BSI C5:2020	CCM	NIST CSF	NIS2	OH SzA	European CRA	DORA
Änderungsanforderungen	8.1.1, 8.1.2	1.1.1, 1.2.1	6.1, 6.2, 6.3	ORP1, ORP2, ORP3	AIS- 01, AIS- 02	PR.IP- 1, PR.IP- 2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Änderungsbewertung und -genehmigung	8.2.1, 8.2.2	2.1.1, 2.1.2	7.1, 7.2	ORP4, ORP5	AIS- 03	PR.IP- 3, PR.IP- 4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Änderungsdokumentation	8.3.1, 8.3.2	3.1.1, 3.1.2	8.1, 8.2	OPS1, OPS2	DSI- 01, DSI- 02	PR.DS- 1, PR.DS- 2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Implementierung und Testen von Änderungen	8.4.1, 8.4.2	3.2.1, 3.2.2	9.1, 9.2	OPS3, OPS4	IAM- 01, IAM- 02	PR.DS- 3, PR.DS- 4	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Überwachung und Überprüfung von Änderungen	8.5.1, 8.5.2	4.1.1, 4.1.2	10.1, 10.2	ORP6, ORP7	AIS- 04, AIS- 05	PR.PT- 1, PR.PT- 2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Rückabwicklung von Änderungen	8.6.1, 8.6.2	4.2.1, 4.2.2	11.1, 11.2	ORP8, ORP9	IVS- 01, IVS- 02	PR.IP- 5, PR.IP- 6	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Änderungsanforderungen

Alle Änderungen an IT-Systemen müssen formell angefordert werden (ISO 27001: 8.1.1, 8.1.2). Jede Änderungsanforderung muss die Notwendigkeit und den Umfang der Änderung klar beschreiben und durch die entsprechenden Verantwortlichen genehmigt werden (CIS Controls 6.1, 6.2, 6.3, TISAX 1.1.1, 1.2.1). Die Anforderung muss dokumentiert und nachvollziehbar sein, um eine lückenlose Historie der Änderungen zu gewährleisten (BSI C5: ORP1, ORP2, ORP3, CCM AIS-01, AIS-02).

Änderungsbewertung und -genehmigung

Alle Änderungsanforderungen müssen bewertet und genehmigt werden, bevor sie umgesetzt werden (ISO 27001: 8.2.1, 8.2.2). Dies beinhaltet eine Risikoanalyse und die Überprüfung der potenziellen Auswirkungen auf die IT-Systeme (CIS Controls 7.1, 7.2, TISAX 2.1.1, 2.1.2). Die Genehmigung muss durch die entsprechenden Verantwortlichen erfolgen und dokumentiert werden (BSI C5: ORP4, ORP5, CCM AIS-03).

Änderungsdokumentation

Alle genehmigten Änderungen müssen dokumentiert werden (ISO 27001: 8.3.1, 8.3.2). Die Dokumentation muss eine detaillierte Beschreibung der durchgeführten Änderungen, die beteiligten Personen und die durchgeführten Tests enthalten (CIS Controls 8.1, 8.2, TISAX 3.1.1, 3.1.2). Diese Dokumentation muss in einem zentralen Repository gespeichert und regelmäßig überprüft werden (BSI C5: OPS1, OPS2, CCM DSI-01, DSI-02).

Implementierung und Testen von Änderungen

Änderungen müssen in einer kontrollierten Umgebung implementiert und getestet werden, bevor sie in die Produktionsumgebung überführt werden (ISO 27001: 8.4.1, 8.4.2). Dies beinhaltet die Durchführung von Tests, um sicherzustellen, dass die Änderungen wie erwartet

funktionieren und keine neuen Risiken einführen (CIS Controls 9.1, 9.2, TISAX 3.2.1, 3.2.2). Die Ergebnisse der Tests müssen dokumentiert und überprüft werden (BSI C5: OPS3, OPS4, CCM IAM-01, IAM-02).

Überwachung und Überprüfung von Änderungen

Alle implementierten Änderungen müssen überwacht und regelmäßig überprüft werden, um sicherzustellen, dass sie den erwarteten Nutzen bringen und keine negativen Auswirkungen haben (ISO 27001: 8.5.1, 8.5.2). Die Überwachung muss kontinuierlich erfolgen und alle relevanten Metriken erfassen (CIS Controls 10.1, 10.2, TISAX 4.1.1, 4.1.2). Die Ergebnisse der Überwachung müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren (BSI C5: ORP6, ORP7, CCM AIS-04, AIS-05).

Rückabwicklung von Änderungen

Für den Fall, dass eine Änderung nicht wie erwartet funktioniert oder unerwartete Probleme verursacht, muss ein Plan zur Rückabwicklung der Änderung vorhanden sein (ISO 27001: 8.6.1, 8.6.2). Dieser Plan muss detaillierte Schritte zur Wiederherstellung des vorherigen Zustands enthalten und von den entsprechenden Verantwortlichen genehmigt werden (CIS Controls 11.1, 11.2, TISAX 4.2.1, 4.2.2). Alle Rückabwicklungen müssen dokumentiert und analysiert werden, um zukünftige Probleme zu vermeiden (BSI C5: ORP8, ORP9, CCM IVS-01, IVS-02).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Change Management Teams. Alle Mitarbeiter sind verpflichtet, sich an diese Richtlinie zu halten und jegliche Verstöße umgehend zu melden.

Quellen und Referenzen

Quelle	Zweck	Link
ISO27001:2022	Aufbau und Implementierung eines ISMS	ISO 27001:2022
CIS Controls v8	Sicherheitsmaßnahmen gegen Cyberangriffe	CIS Controls v8
BSI C5:2020	Cloud Security Standard	BSI C5:2020
Cloud Controls Matrix (CCM)	Sicherheitskontrollen für Cloud-Dienste	Cloud Controls Matrix
NIST Cybersecurity Framework	Rahmenwerk zur Verbesserung der Cybersicherheit	NIST CSF
NIS2 Draft	EU-Richtlinie zur Netz- und Informationssicherheit	NIS2 Draft
OH SzA für KRITIS	Orientierungshilfe Angriffserkennung für Kritische Infrastrukturen	OH SzA
European Cyber Resilience Act	EU-Verordnung zur Cyber-Resilienz	European CRA
Digital Operational Resilience Act (DORA)	EU-Verordnung zur digitalen operationellen Resilienz	DORA

Diese Quellen und Referenzen bieten umfassende Leitlinien und Best Practices für die Entwicklung und Implementierung von Sicherheitsmaßnahmen sowie für die Einhaltung der relevanten Standards und Richtlinien. Sie dienen als Grundlage und Unterstützung bei der Implementierung und Aufrechterhaltung eines strukturierten und sicheren Change Management Prozesses bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie zum Change Management
Version: 1.0
Datum: [Heutiges Datum]
Verantwortlich: IT-Sicherheitsbeauftragter
Genehmigt von: [Name der genehmigenden Person]
Nächste Überprüfung: [Datum der nächsten Überprüfung]