



# Statement of Applicability

Informationssicherheit, Cybersicherheit und  
Datenschutz -  
Informationssicherheitsmanagementsysteme -  
Anforderungen (ISO/IEC 27001:2022); Deutsche  
Fassung EN ISO/IEC 27001:2023

Das gegenständliche Dokument gilt als vertraulich und ist ausschließlich für den internen Gebrauch bestimmt.  
Es ist nicht gestattet, dieses Dokument oder Teile daraus in irgendeiner Form zum Gebrauch durch Dritte zu vervielfältigen und/oder ganz bzw. auszugsweise zu veröffentlichen.  
Das Dokument im Original, Kopien oder Auszüge daraus müssen auf Verlangen zurückgegeben werden.

# Inhaltsverzeichnis

<b>ISO/IEC 27001:2022</b>	
<b>Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023</b>	<b>1</b>
<hr/>	
<b>Relevanz nach Kapiteln</b>	<b>2</b>
<hr/>	
04 Kontext der Organisation	2
05 Führung	2
06 Planung	2
07 Unterstützung	3
08 Betrieb	4
09 Bewertung der Leistung	4
10 Verbesserung	5
A.5 Organisatorische Maßnahmen	5
A.6 Personenbezogene Maßnahmen	10
A.7 Physische Maßnahmen	11
A.8 Technologische Maßnahmen	12
<hr/>	
<b>Maßnahmen</b>	<b>16</b>
<hr/>	
IS_M_ToEx AG_022 Interne Faktoren mit Einfluss auf den Kontext der Organisation festlegen	16
IS_M_IT_001 Interessierte Parteien, ihre Erwartungen und Anforderungen identifizieren	16
IS_M_ToEx AG_023 Interessierten Parteien, ihre Erwartungen und Anforderungen identifizieren	16
IS_M_SM Edi_001 Determine the scope of the ISMS in the scope document	16
IS_M_SM Edi_003 Create and maintain the ISMS guideline	16
IS_M_ToEx AG_031 IS-Ziele festlegen	16
IS_M_ToEx AG_002 Erforderliche Ressourcen zum Aufbau des ISMS bereitstellen	16
IS_M_SM Edi_002 Provide the necessary resources to establish the ISMS	16
IS_M_ToEx AG_007 Kampagne zur Bewusstseinsbildung im ISMS durchführen	17
IS_M_ToEx AG_025 Kommunikationskonzept/-plan erstellen	17
IS_M_ToEx AG_003 Dokumentenrahmen erstellen	17
IS_M_ToEx AG_004 Leitlinie zur vorgabenkonformen Dokumentation von Informationen erstellen	17
<hr/>	

# Inhaltsverzeichnis

IS_M_ToEx AG_026 Leitlinie zur vorgabenkonformen Lenkung von Dokumenten erstellen	17
IS_M_ToEx AG_001 Pläne zur Erreichung der festgelegten IS-Ziele implementieren	17
IS_M_ToEx AG_005 Planung, Implementierung und Kontrolle der Prozesse zur Aufrechterhaltung der IS einschließlich der festgelegten Maßnahmen erarbeiten	17
IS_M_ToEx AG_006 IS-Risikoeinschätzung initial durchführen	17
IS_M_ToEx AG_030 Plan für die IS-Risikobehandlung implementieren	18
IS_M_ToEx AG_008 Management Reviews inkl. ihrem Aufbau planen	18
IS_M_ToEx AG_042 Vorgehen für die kontinuierliche Verbesserung des ISMS definieren	18
IS_M_ToEx AG_013 Kommunikation der IS-Richtlinie konzipieren	18
IS_M_ToEx AG_024 Verantwortliche und Entscheidungsgremien definieren und nominieren	18
IS_M_ToEx AG_027 Verantwortungsbereiche festlegen	18
IS_M_ToEx AG_028 Trennung widersprüchlicher Aufgaben und Verantwortungsbereiche festlegen	18
IS_M_ToEx AG_014 Relevante Behörden und Überwachungsstellen ermitteln und Umgang mit diesen definieren	19
IS_M_ToEx AG_029 Kontakte zu Interessensvertretungen, Lieferanten, Service-Providern oder anderen spezialisierten Sicherheitsforen und Fachverbänden aufbauen	19
IS_M_ToEx AG_011 Informationsklassifikationsvorgabe erstellen	19
IS_M_IT_002 Zugriffskontrollrichtlinie erstellen	19
IS_M_IT_031 Vorgaben zur Verwaltung der Authentisierungsinformationen von Benutzern festlegen	19
IS_M_IT_029 Prozess zur Sicherstellung von Entzug und Manipulation von Zugriffsrechten einrichten	19
IS_M_IT_030 Prozess zur regelmäßigen Überprüfung von Zugriffsberechtigungen einrichten	19
IS_M_AP Dun_001 Define guidelines for the allocation of access rights	19
IS_M_ToEx AG_012 Richtlinie für Informationssicherheit in Lieferantenbeziehungen erstellen	20
IS_M_ToEx AG_016 Verfahren und Verantwortlichkeiten im IS-Vorfall festlegen	20
IS_M_FICO_003 Equinox assesses IS incidents	20
IS_M_ToEx AG_043 Sammlung von Beweisen für IS Vorfälle definieren	20
IS_M_IT_011 IT-Notfallmanagement planen und konzeptionieren	20
IS_M_IT_012 IT-Notfallmanagement implementieren	20

# Inhaltsverzeichnis

IS_M_ToEx AG_010 Anforderungen an IT-Services kritischer Geschäftsprozesse erheben	20
IS_M_ToEx AG_009 Dokumentation für Betriebsverfahren erstellen	20
IS_M_FICO_002 Ensure Equinox introduces security screenings of applicants	21
IS_M_IT_047 Richtlinien für mobiles IT Equipment bei der Telearbeit definieren	21
IS_M_IT_046 Physisches Sicherheitszonenkonzept erstellen und abstimmen	21
IS_M_ToEx AG_015 Leitlinie zur physischen Zugangskontrolle erstellen	21
IS_M_IT_004 Regelungen zu Clear Desk und Clear Screen erstellen	21
IS_M_IT_032 Vorgaben zur Vergabe von Sonderrechten festlegen	21
IS_M_AP Dun_002 Set guidelines for the granting of privileges	21
IS_M_IT_033 Sichere Anmeldung konfigurieren	21
IS_M_IT_022 Kapazitätsmanagement einführen	22
IS_M_IT_010 Konfigurationsmanagement implementieren	22
IS_M_IT_027 Konfigurationen verwalten und überwachen	22
IS_M_IT_006 Trennung Produktiv- und Backupsystem sicherstellen	22
IS_M_IT_007 Backup Überwachung einführen	22
IS_M_AP Dun_003 Protect backup tapes	22
IS_M_IT_005 Ausreichende Redundanzen vorsehen	22
IS_M_IT_003 Ereignisprotokollierung aktivieren	22
IS_M_IT_023 Schutz der Protokollinformationen sicherstellen	23
IS_M_IT_024 Administratoren- und Bedienerprotokolle erstellen und prüfen	23
IS_M_IT_028 Überwachungsmaßnahmen von Aktivitäten in Netzwerken, Systemen und Applikationen festlegen	23
IS_M_IT_025 Zeitsynchronisation sicherstellen	23
IS_M_IT_026 Überwachung von Software im Betrieb einführen	23
IS_M_ToEx AG_044 Awareness Trainings zur Verwendung von Webseiten abhalten	23
IS_M_ToEx AG_017 Richtlinie zur sicheren Entwicklung erstellen	23
IS_M_IT_009 Sicherheitsanforderungen in Applikationen definieren	24
IS_M_IT_008 Änderungsmanagement einführen	24
<b>Kontrollen</b>	<b>25</b>
IS_K_ToEx AG_005 Abgleich Budget und Maßnahmenplanung	25
IS_K_ToEx AG_004 Überprüfung der Aktualität und Angemessenheit der IS Richtlinie	25
IS_K_ToEx AG_006 Wirksamkeitsprüfung der ISMS Awareness Kampagne	25
IS_K_IT_006 Überprüfung geplanter Changes	25

# Inhaltsverzeichnis

IS_K_ToEx AG_003 Management Review	25
IS_K_ToEx AG_007 Überprüfung der Liste der relevanten Behörden und Aufsichtsorganen	25
IS_K_IT_001 Überprüfung der Access Control Richtlinie	25
IS_K_IT_002 Review of the adherence to the Access Control Guideline	25
IS_K_FICO_002 Review of IS incidents at Equinox	26
IS_K_IT_004 Überprüfung der Aktualität und Angemessenheit der Dokumente zum IT Notfallsmanagement	26
IS_K_IT_005 Überprüfung der Aktualität und Angemessenheit des IT Notfallhandbuchs	26
IS_K_ToEx AG_002 IT Notfallsübung	26
IS_K_FICO_001 Verification of the implementation of security screenings of applicants for Equinox	26
IS_K_ToEx AG_001 Überprüfung der Einhaltung der Clear Desk Policy	26
IS_K_IT_003 Review of the backup via Restore Tests	26

## **Anhang**

**27**



# ISO/IEC 27001:2022

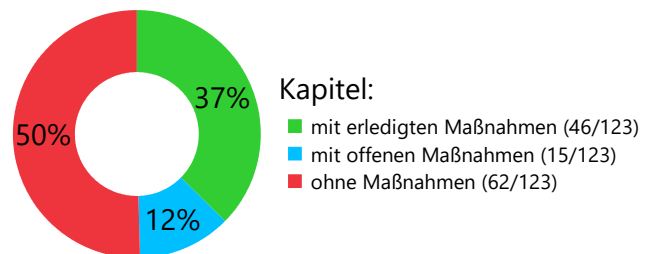
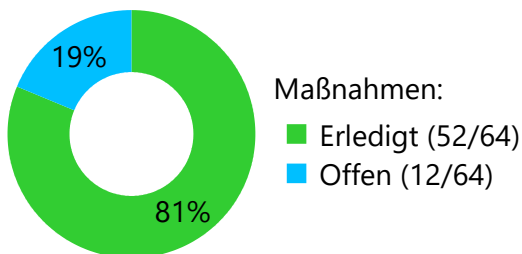
Informationssicherheit, Cybersicherheit und Datenschutz -

Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023

Stand:	30.11.2024
Beschreibung:	<p>Diese Norm ist für alle Organisationsarten anwendbar und legt die Anforderungen an Aufstellen, Umsetzen, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung von dokumentierten Informationssicherheit-Managementsystemen in Bezug auf die allgemeinen Geschäftsrisiken einer Organisation fest.</p> <p>Sie legt außerdem die Anforderungen an die Einführung von Sicherheitskontrollen fest, die auf die Bedürfnisse einer Organisation oder Teilen davon zugeschnitten sind. Das Informationssicherheits-Managementssystem ist dafür entwickelt worden, die Auswahl ausreichender und angemessener Sicherheitskontrollen zu gewährleisten, die den Informationsbestand sichern und interessierten Partnern Vertrauenswürdigkeit vermitteln.</p>

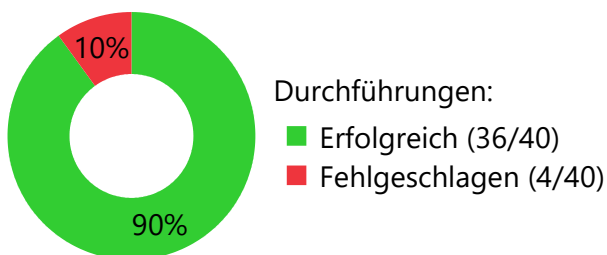
## Maßnahmen Übersicht

64 Maßnahmen sind diesem Standard bzw. dieser Norm zugewiesen.



## Kontrollübersicht

15 Kontrollen sind diesem Standard bzw. dieser Norm zugewiesen.





## Relevanz nach Kapiteln

Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
<b>04</b>	<b>Kontext der Organisation</b>		ISO Website	Ja	
4.1	Verstehen der Organisation und ihres Kontextes	IS_M_ToEx AG_022 Interne Faktoren mit Einfluss auf den Kontext der Organisation festlegen		Ja	
4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien	IS_M_IT_001 Interessierte Parteien, ihre Erwartungen und Anforderungen identifizieren, IS_M_ToEx AG_023 Interessierten Parteien, ihre Erwartungen und Anforderungen identifizieren		Ja	
4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystem	IS_M_SM Edi_001 Determine the scope of the ISMS in the scope document	ISMS_Scope.pdf	Ja	
4.4	Informationssicherheitsmanagementsystem		Definition of an ISM	Ja	
<b>05</b>	<b>Führung</b>		ISO Website	Ja	
5.1	Führung und Verpflichtung	IS_K_ToEx AG_005 Abgleich Budget und Maßnahmenplanung		Ja	
5.2	Politik	IS_M_SM Edi_003 Create and maintain the ISMS guideline, IS_K_ToEx AG_004 Überprüfung der Aktualität und Angemessenheit der IS Richtlinie	ISMS_Politik.pdf	Ja	
5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation			Ja	
<b>06</b>	<b>Planung</b>		ISO Website	Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
6.1	Maßnahmen zum Umgang mit Risiken und Chancen			Ja	
6.1.1	Allgemeines		PBS_SecurityIncidentMgmt.pdf	Ja	
6.1.2	Informationssicherheitsrisikobeurteilung			Ja	
6.1.3	Informationssicherheitsrisikobehandlung			Ja	
6.2	Informationssicherheitsziele und Planung zu deren Erreichung	IS_M_ToEx AG_031 IS-Ziele festlegen		Ja	
6.3	Planning of changes			Ja	
<b>07</b>	<b>Unterstützung</b>		ISO Website	Ja	
7.1	Ressourcen	IS_M_SM Edi_002 Provide the necessary resources to establish the ISMS, IS_M_ToEx AG_002 Erforderliche Ressourcen zum Aufbau des ISMS bereitstellen		Ja	
7.2	Kompetenz			Ja	
7.3	Bewusstsein	IS_M_ToEx AG_007 Kampagne zur Bewusstseinsbildung im ISMS durchführen, IS_K_ToEx AG_006 Wirksamkeitsprüfung der ISMS Awareness Kampagne	Awarenessprogramm_Übersicht.pdf	Ja	
7.4	Kommunikation	IS_M_ToEx AG_025 Kommunikationskonzept/-plan erstellen	Awarenessprogramm_Übersicht.pdf	Ja	
7.5	Dokumentierte Information			Ja	
7.5.1	Allgemeines	IS_M_ToEx AG_003 Dokumentenrahmen erstellen		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
7.5.2	Erstellen und Aktualisieren	IS_M_ToEx AG_004 Leitlinie zur vorgabenkonformen Dokumentation von Informationen erstellen		Ja	
7.5.3	Lenkung dokumentierter Information	IS_M_ToEx AG_026 Leitlinie zur vorgabenkonformen Lenkung von Dokumenten erstellen		Ja	
<b>08</b>	<b>Betrieb</b>		ISO Website	Ja	
8.1	Betriebliche Planung und Steuerung	IS_M_ToEx AG_001 Pläne zur Erreichung der festgelegten IS-Ziele implementieren, IS_M_ToEx AG_005 Planung, Implementierung und Kontrolle der Prozesse zur Aufrechterhaltung der IS einschließlich der festgelegten Maßnahmen erarbeiten, IS_K_IT_006 Überprüfung geplanter Changes		Ja	
8.2	Informationssicherheitsrisikobeurteilung	IS_M_ToEx AG_006 IS-Risikoeinschätzung initial durchführen		Ja	
8.3	Informationssicherheitsrisikobehandlung	IS_M_ToEx AG_030 Plan für die IS-Risikobehandlung implementieren		Ja	
<b>09</b>	<b>Bewertung der Leistung</b>		ISO Website	Ja	
9.1	Überwachung, Messung, Analyse und Bewertung			Ja	
9.2	Internes Audit			Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
9.2.1	Allgemeines			Ja	
9.2.2	Internes Auditprogramm			Ja	
9.3	Managementbewertung	IS_M_ToEx AG_008 Management Reviews inkl. ihrem Aufbau planen, IS_K_ToEx AG_003 Management Review		Ja	
9.3.1	Allgemeines	IS_M_ToEx AG_008, IS_K_ToEx AG_003		Ja	
9.3.2	Inputs der Managementbewertung	IS_M_ToEx AG_008, IS_K_ToEx AG_003		Ja	
9.3.3	Ergebnisse der Managementbewertung	IS_M_ToEx AG_008, IS_K_ToEx AG_003		Ja	
<b>10</b>	<b>Verbesserung</b>		ISO Website	Ja	
10.1	Fortlaufende Verbesserung	IS_M_ToEx AG_042 Vorgehen für die kontinuierliche Verbesserung des ISMS definieren		Ja	
10.2	Nichtkonformität und Korrekturmaßnahmen			Ja	
<b>A.5</b>	<b>Organisatorische Maßnahmen</b>			Ja	
A.5.1	Informationssicherheitsrichtlinien	IS_M_SM Edi_003 Create and maintain the ISMS guideline, IS_M_ToEx AG_013 Kommunikation der IS-Richtlinie konzipieren, IS_K_ToEx AG_004 Überprüfung der Aktualität und Angemessenheit der IS Richtlinie		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	IS_M_ToEx AG_024 Verantwortliche und Entscheidungsgremien definieren und nominieren, IS_M_ToEx AG_027 Verantwortungsbereiche festlegen		Ja	
A.5.3	Aufgabentrennung	IS_M_ToEx AG_028 Trennung widersprüchlicher Aufgaben und Verantwortungsbereiche festlegen		Ja	
A.5.4	Verantwortlichkeiten der Leitung	IS_M_ToEx AG_013 Kommunikation der IS-Richtlinie konzipieren		Ja	
A.5.5	Kontakt mit Behörden	IS_M_ToEx AG_014 Relevante Behörden und Überwachungsstellen ermitteln und Umgang mit diesen definieren, IS_K_ToEx AG_007 Überprüfung der Liste der relevanten Behörden und Aufsichtsorganen		Ja	
A.5.6	Kontakt mit speziellen Interessensgruppen	IS_M_ToEx AG_029 Kontakte zu Interessensvertretungen, Lieferanten, Service-Providern oder anderen spezialisierten Sicherheitsforen und Fachverbänden aufbauen		Ja	
A.5.7	Bedrohungsintelligenz			Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.5.8	Informationssicherheit im Projektmanagement			Ja	
A.5.9	Inventar der Informationen und anderen damit verbundenen Werten			Ja	
A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten			Ja	
A.5.11	Rückgabe von Werten			Ja	
A.5.12	Klassifizierung von Information	IS_M_ToEx AG_011 Informationsklassifikationsvorgabe erstellen		Ja	
A.5.13	Kennzeichnung von Information			Ja	
A.5.14	Informationsübertragung			Ja	
A.5.15	Zugangssteuerung	IS_M_IT_002 Zugriffskontrollrichtlinie erstellen, IS_K_IT_001 Überprüfung der Access Control Richtlinie, IS_K_IT_002 Review of the adherence to the Access Control Guideline		Ja	
A.5.16	Identitätsmanagement			Ja	
A.5.17	Informationen zur Authentifizierung	IS_M_IT_031 Vorgaben zur Verwaltung der Authentisierungsinformationen von Benutzern festlegen		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.5.18	Zugangsrechte	IS_M_AP Dun_001 Define guidelines for the allocation of access rights, IS_M_IT_029 Prozess zur Sicherstellung von Entzug und Manipulation von Zugriffsrechten einrichten, IS_M_IT_030 Prozess zur regelmäßigen Überprüfung von Zugriffsberechtigungen einrichten		Ja	
A.5.19	Informationssicherheit in Lieferantenbeziehungen	IS_M_ToEx AG_012 Richtlinie für Informationssicherheit in Lieferantenbeziehungen erstellen		Ja	
A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen			Ja	
A.5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette			Ja	
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen			Ja	
A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten			Ja	
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	IS_M_ToEx AG_016 Verfahren und Verantwortlichkeiten im IS-Vorfall festlegen		Ja	
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	IS_M_FICO_003 Equinox assesses IS incidents		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.5.26	Reaktion auf Informationssicherheitsvorfälle	IS_K_FICO_002 Review of IS incidents at Equinox		Ja	
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen			Ja	
A.5.28	Sammeln von Beweismaterial	IS_M_ToEx AG_043 Sammlung von Beweisen für IS Vorfälle definieren		Ja	
A.5.29	Informationssicherheit bei Störungen	IS_M_IT_011 IT-Notfallmanagement planen und konzeptionieren, IS_M_IT_012 IT-Notfallmanagement implementieren, IS_K_IT_004 Überprüfung der Aktualität und Angemessenheit der Dokumente zum IT Notfallsmanagement, IS_K_IT_005 Überprüfung der Aktualität und Angemessenheit des IT Notfallhandbuchs, IS_K_ToEx AG_002 IT Notfallsübung		Ja	
A.5.30	IKT-Bereitschaft für Business Continuity	IS_M_ToEx AG_010 Anforderungen an IT-Services kritischer Geschäftsprozesse erheben		Ja	
A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen			Ja	
A.5.32	Geistige Eigentumsrechte			Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.5.33	Schutz von Aufzeichnungen	IS_M_ToEx AG_011 Informationsklassifikationsvorgabe erstellen		Ja	
A.5.34	Datenschutz und Schutz personenbezogener Daten (pbD)			Ja	
A.5.35	Unabhängige Überprüfung der Informationssicherheit			Ja	
A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	IS_M_ToEx AG_013 Kommunikation der IS-Richtlinie konzipieren		Ja	
A.5.37	Dokumentierte Betriebsabläufe	IS_M_ToEx AG_009 Dokumentation für Betriebsverfahren erstellen		Ja	
<b>A.6</b>	<b>Personenbezogene Maßnahmen</b>			Ja	
A.6.1	Sicherheitsüberprüfung	IS_M_FICO_002 Ensure Equinox introduces security screenings of applicants, IS_K_FICO_001 Verification of the implementation of security screenings of applicants for Equinox		Ja	
A.6.2	Beschäftigungs- und Vertragsbedingungen			Ja	
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	IS_M_ToEx AG_013 Kommunikation der IS-Richtlinie konzipieren		Ja	
A.6.4	Maßregelungsprozess			Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung			Ja	
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen			Ja	
A.6.7	Telearbeit	IS_M_IT_047 Richtlinien für mobiles IT Equipment bei der Telearbeit definieren		Ja	
A.6.8	Meldung von Informationssicherheitsereignissen			Ja	
<b>A.7</b>	<b>Physische Maßnahmen</b>			Ja	
A.7.1	Physische Sicherheitsperimeter	IS_M_IT_046 Physisches Sicherheitszonenkonzept erstellen und abstimmen		Ja	
A.7.2	Physischer Zutritt	IS_M_ToEx AG_015 Leitlinie zur physischen Zugangskontrolle erstellen		Ja	
A.7.3	Sichern von Büros, Räumen und Einrichtungen			Ja	
A.7.4	Physische Sicherheitsüberwachung			Ja	
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen			Ja	
A.7.6	Arbeiten in Sicherheitsbereichen			Ja	
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	IS_M_IT_004 Regelungen zu Clear Desk und Clear Screen erstellen, IS_K_ToEx AG_001 Überprüfung der Einhaltung der Clear Desk Policy		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln			Ja	
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	IS_M_IT_047 Richtlinien für mobiles IT Equipment bei der Telearbeit definieren		Ja	
A.7.10	Speichermedien			Ja	
A.7.11	Versorgungseinrichtungen			Ja	
A.7.12	Sicherheit der Verkabelung			Ja	
A.7.13	Instandhaltung von Geräten und Betriebsmitteln			Ja	
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln			Ja	
<b>A.8</b>	<b>Technologische Maßnahmen</b>			Ja	
A.8.1	Endpunktgeräte des Benutzers			Ja	
A.8.2	Privilegierte Zugangsrechte	IS_M_AP Dun_002 Set guidelines for the granting of privileges, IS_M_IT_032 Vorgaben zur Vergabe von Sonderrechten festlegen		Ja	
A.8.3	Informationszugangsbeschränkung	IS_M_AP Dun_001 Define guidelines for the allocation of access rights		Ja	
A.8.4	Zugriff auf den Quellcode			Ja	
A.8.5	Sichere Authentifizierung	IS_M_IT_033 Sichere Anmeldung konfigurieren		Ja	
A.8.6	Kapazitätssteuerung	IS_M_IT_022 Kapazitätsmanagement einführen		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.8.7	Schutz gegen Schadsoftware			Ja	
A.8.8	Handhabung von technischen Schwachstellen			Ja	
A.8.9	Konfigurationsmanagement	IS_M_IT_010 Konfigurationsmanagement implementieren, IS_M_IT_027 Konfigurationen verwalten und überwachen		Ja	
A.8.10	Löschung von Informationen			Ja	
A.8.11	Datenmaskierung			Ja	
A.8.12	Verhinderung von Datenlecks			Ja	
A.8.13	Sicherung von Information	IS_M_AP Dun_003 Protect backup tapes, IS_M_IT_006 Trennung Produktiv- und Backupsystem sicherstellen, IS_M_IT_007 Backup Überwachung einführen, IS_K_IT_003 Review of the backup via Restore Tests		Ja	
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	IS_M_IT_005 Ausreichende Redundanzen vorsehen		Ja	
A.8.15	Protokollierung	IS_M_IT_003 Ereignisprotokollierung aktivieren, IS_M_IT_023 Schutz der Protokollinformationen sicherstellen, IS_M_IT_024 Administratoren- und Bedienerprotokolle erstellen und prüfen		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.8.16	Überwachung von Aktivitäten	IS_M_IT_028 Überwachungsmaßnahmen von Aktivitäten in Netzwerken, Systemen und Applikationen festlegen		Ja	
A.8.17	Uhrensynchronisation	IS_M_IT_025 Zeitsynchronisation sicherstellen		Ja	
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten			Ja	
A.8.19	Installation von Software auf Systemen im Betrieb	IS_M_IT_026 Überwachung von Software im Betrieb einführen		Ja	
A.8.20	Netzwerksicherheit			Ja	
A.8.21	Sicherheit von Netzwerkdiensten			Ja	
A.8.22	Trennung von Netzwerken			Ja	
A.8.23	Webfilterung	IS_M_ToEx AG_044 Awareness Trainings zur Verwendung von Webseiten abhalten		Ja	
A.8.24	Verwendung von Kryptographie			Ja	
A.8.25	Lebenszyklus einer sicheren Entwicklung	IS_M_ToEx AG_017 Richtlinie zur sicheren Entwicklung erstellen		Ja	
A.8.26	Anforderungen an die Anwendungssicherheit	IS_M_IT_009 Sicherheitsanforderungen in Applikationen definieren		Ja	
A.8.27	Sichere Systemarchitektur und technische Grundsätze	IS_M_IT_009 Sicherheitsanforderungen in Applikationen definieren		Ja	
A.8.28	Sicheres Coding	IS_M_ToEx AG_017 Richtlinie zur sicheren Entwicklung erstellen		Ja	



Gliederung	Bezeichnung	Maßnahmen/Kontrollen	Verknüpfte Dokumente	Anw.	Begründung
A.8.29	Sicherheitsprüfung in Entwicklung und Abnahme			Ja	
A.8.30	Ausgegliederte Entwicklung			Ja	
A.8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen			Ja	
A.8.32	Änderungssteuerung	IS_M_IT_008 Änderungsmanagement einführen		Ja	
A.8.33	Prüfinformationen			Ja	
A.8.34	Schutz der Informationssysteme während der Überwachungsprüfung			Ja	



## Maßnahmen

### IS\_M\_ToEx AG\_022 Interne Faktoren mit Einfluss auf den Kontext der Organisation festlegen

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_IT\_001 Interessierte Parteien, ihre Erwartungen und Anforderungen identifizieren

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_ToEx AG\_023 Interessierten Parteien, ihre Erwartungen und Anforderungen identifizieren

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_SM Edi\_001 Determine the scope of the ISMS in the scope document

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_SM Edi\_003 Create and maintain the ISMS guideline

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_ToEx AG\_031 IS-Ziele festlegen

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_ToEx AG\_002 Erforderliche Ressourcen zum Aufbau des ISMS bereitstellen

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_M\_SM Edi\_002 Provide the necessary resources to establish the ISMS

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac.



Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_007 Kampagne zur Bewusstseinsbildung im ISMS durchführen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_025 Kommunikationskonzept/-plan erstellen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_003 Dokumentenrahmen erstellen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_004 Leitlinie zur vorgabenkonformen Dokumentation von Informationen erstellen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_026 Leitlinie zur vorgabenkonformen Lenkung von Dokumenten erstellen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_001 Pläne zur Erreichung der festgelegten IS-Ziele implementieren**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_005 Planung, Implementierung und Kontrolle der Prozesse zur Aufrechterhaltung der IS einschließlich der festgelegten Maßnahmen erarbeiten**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_M\_ToEx AG\_006 IS-Risikoeinschätzung initial durchführen**



Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_030 Plan für die IS-Risikobehandlung implementieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_008 Management Reviews inkl. ihrem Aufbau planen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_042 Vorgehen für die kontinuierliche Verbesserung des ISMS definieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_013 Kommunikation der IS-Richtlinie konzipieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_024 Verantwortliche und Entscheidungsgremien definieren und nominieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_027 Verantwortungsbereiche festlegen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_028 Trennung widersprüchlicher Aufgaben und Verantwortungsbereiche festlegen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

**IS\_M\_ToEx AG\_014 Relevante Behörden und Überwachungsstellen ermitteln und Umgang mit diesen definieren**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_ToEx AG\_029 Kontakte zu Interessensvertretungen, Lieferanten, Service-Providern oder anderen spezialisierten Sicherheitsforen und Fachverbänden aufbauen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_ToEx AG\_011 Informationsklassifikationsvorgabe erstellen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_IT\_002 Zugriffskontrollrichtlinie erstellen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_IT\_031 Vorgaben zur Verwaltung der Authentisierungsinformationen von Benutzern festlegen**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_IT\_029 Prozess zur Sicherstellung von Entzug und Manipulation von Zugriffsrechten einrichten**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_IT\_030 Prozess zur regelmäßigen Überprüfung von Zugriffsberechtigungen einrichten**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

**IS\_M\_AP Dun\_001 Define guidelines for the allocation of access rights**



---

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_ToEx AG\_012 Richtlinie für Informationssicherheit in Lieferantenbeziehungen erstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_ToEx AG\_016 Verfahren und Verantwortlichkeiten im IS-Vorfall festlegen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_FICO\_003 Equinox assesses IS incidents**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_ToEx AG\_043 Sammlung von Beweisen für IS Vorfälle definieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_011 IT-Notfallmanagement planen und konzeptionieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_012 IT-Notfallmanagement implementieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_ToEx AG\_010 Anforderungen an IT-Services kritischer Geschäftsprozesse erheben**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_ToEx AG\_009 Dokumentation für Betriebsverfahren erstellen**



---

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_FICO\_002 Ensure Equinox introduces security screenings of applicants**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_IT\_047 Richtlinien für mobiles IT Equipment bei der Telearbeit definieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_IT\_046 Physisches Sicherheitszonenkonzept erstellen und abstimmen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_ToEx AG\_015 Leitlinie zur physischen Zugangskontrolle erstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_IT\_004 Regelungen zu Clear Desk und Clear Screen erstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_IT\_032 Vorgaben zur Vergabe von Sonderrechten festlegen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_AP\_Dun\_002 Set guidelines for the granting of privileges**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

**IS\_M\_IT\_033 Sichere Anmeldung konfigurieren**



---

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_022 Kapazitätsmanagement einführen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_010 Konfigurationsmanagement implementieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_027 Konfigurationen verwalten und überwachen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_006 Trennung Produktiv- und Backupsystem sicherstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_007 Backup Überwachung einführen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_AP\_Dun\_003 Protect backup tapes**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_005 Ausreichende Redundanzen vorsehen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_003 Ereignisprotokollierung aktivieren**



Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_IT\_023 Schutz der Protokollinformationen sicherstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_IT\_024 Administratoren- und Bedienerprotokolle erstellen und prüfen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_IT\_028 Überwachungsmaßnahmen von Aktivitäten in Netzwerken, Systemen und Applikationen festlegen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_IT\_025 Zeitsynchronisation sicherstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_IT\_026 Überwachung von Software im Betrieb einführen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_044 Awareness Trainings zur Verwendung von Webseiten abhalten**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

### **IS\_M\_ToEx AG\_017 Richtlinie zur sicheren Entwicklung erstellen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---



---

### **IS\_M\_IT\_009 Sicherheitsanforderungen in Applikationen definieren**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---

---

### **IS\_M\_IT\_008 Änderungsmanagement einführen**

Beschreibung:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.
---------------	---



## Kontrollen

### IS\_K\_ToEx AG\_005 Abgleich Budget und Maßnahmenplanung

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_ToEx AG\_004 Überprüfung der Aktualität und Angemessenheit der IS Richtlinie

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_ToEx AG\_006 Wirksamkeitsprüfung der ISMS Awareness Kampagne

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_IT\_006 Überprüfung geplanter Changes

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_ToEx AG\_003 Management Review

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_ToEx AG\_007 Überprüfung der Liste der relevanten Behörden und Aufsichtsorganen

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_IT\_001 Überprüfung der Access Control Richtlinie

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### IS\_K\_IT\_002 Review of the adherence to the Access Control Guideline

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac.



Pellentesque vitae consequat nibh.

### **IS\_K\_FICO\_002 Review of IS incidents at Equinox**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_K\_IT\_004 Überprüfung der Aktualität und Angemessenheit der Dokumente zum IT Notfallsmanagement**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_K\_IT\_005 Überprüfung der Aktualität und Angemessenheit des IT Notfallhandbuchs**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_K\_ToEx AG\_002 IT Notfallsübung**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_K\_FICO\_001 Verification of the implementation of security screenings of applicants for Equinox**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_K\_ToEx AG\_001 Überprüfung der Einhaltung der Clear Desk Policy**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.

### **IS\_K\_IT\_003 Review of the backup via Restore Tests**

Beschreibung: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus nec lectus ac leo maximus vehicula et in ex. Nullam molestie mattis ex, ac faucibus nibh pulvinar ac. Pellentesque vitae consequat nibh.



## Anhang

Donut-Diagramme zeigen die Anzahl und den Status zugewiesener Maßnahmen & Kontrollen. Die Gesamtzahl der Kapitel in der Auswertung entspricht der Anzahl der Kapitel auf der untersten Kapitelebene. Wurde eine Maßnahme bzw. Kontrolle einem Kapitel zugewiesen, so wird sie auch allen seinen Unterkapiteln zugerechnet. Hat also ein Überkapitel eine Maßnahme oder Kontrolle zugeteilt, verhält es sich genauso, als würden alle Unterkapitel diese Maßnahme oder Kontrolle zugeteilt haben.

### Maßnahmen Übersicht

Das linke Donut-Diagramm stellt dar, wie viele Maßnahmen im Status „geplant“, „offen“, „erledigt“ und „ausgesetzt“ dem Auswertungsbereich zugeordnet sind. Das rechte Donut-Diagramm bringt zum Ausdruck wie viel Prozent der auszuwertenden Kapitel des Standards bzw. der Norm mit offenen, mit erledigten bzw. ohne Maßnahmen belegt sind. Sind einem Kapitel sowohl offene als auch erledigte Maßnahmen zugewiesen, wird das Kapitel unter „offene Maßnahmen“ gezählt.

### Kontrollen Übersicht

Das linke Donut-Diagramm stellt dar, wie viele Kontrollen erfolgt sind und wie viele davon erfolgreich waren oder fehlgeschlagen sind. Berücksichtigt werden dabei nur Kontrollen von Kontrolldefinitionen, die Kapiteln des Anwendungsbereichs zugeordnet sind. Das rechte Donut-Diagramm bringt zum Ausdruck wie viel Prozent der auszuwertenden Kapitel des Standards bzw. der Norm mit aktiven bzw. ausgesetzten Kontrollen belegt sind.