Arbeitsrichtlinie Auditmanagement

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Auditmanagement
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	09.12.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	09.12.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.1.	Daniel Fürdauer
20.0	04.12.2020	Redaktionelle Änderungen und in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0: Aktualisierung Bewertungsschema anhand eines Reifegradmodells (Anhang A) und sprachliche Klarstellungen an diversen Stellen.	Daniel Fürdauer
21.0	17.11.2021	Aktualisierung des Kapitels 3.2	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

Inhaltsverzeichnis 3

1. Einleitung 4

2. Auditmanagement 5

2.1. Ziele des Auditmanagements 5

2.2. Prozessdarstellung 5

2.2.1. Prozessauslöser 5

2.2.2. Prozessablauf 5

2.3. Qualifikation 6

2.4. Auditprinzipien 6

3. Teilprozesse des Auditmanagements 7

3.1. Auditprogramm 7

3.2. Auditplanung 7

3.3. Auditdurchführung 9

3.4. Auditnachbereitung 10

1. EINLEITUNG

Das Auditmanagement der Stabstelle Datenschutz und Informationssicherheit dient dazu, Transparenz über die Konformität zu den Datenschutz- und Informationssicherheitsanforderungen herzustellen sowie das Datenschutz- und Informationssicherheitsniveau in der VAV durch geeignete Maßnahmen zu verbessern.
Im Rahmen des Auditprogramms, das auf einen Zeitraum von fünf Jahren angelegt ist, wird geprüft, ob die Umsetzungen mit den Vorgaben zum Datenschutz und zur Informationssicherheit der VAV übereinstimmen. Die Audits der Stabstelle Datenschutz und Informationssicherheit stellen mithin "Überwachungshandlungen" mit Blick auf die internen und externen Anforderungen des Datenschutzes und der Informationssicherheit dar.
Vorrangiges Ziel ist es, Abweichungen von gesetzlichen und regulatorischen Anforderungen, geltenden Datenschutz und Sicherheitsrichtlinien sowie gängigen Sicherheitsstandards frühzeitig zu erkennen und die Behandlung anzustoßen. Weiterhin wird die Leistungsfähigkeit des ISMS und des DSMS durch die Audits überprüft. Damit bilden die Überprüfung der Anforderungen sowie die Planung und Durchführung geeigneter Korrektur- und Verbesserungsmaßnahmen die Grundlagen für einen kontinuierlichen Verbesserungsprozess.
Die Audits (Überwachungshandlungen) der Stabstelle Datenschutz und Informationssicherheit stellen eine Ergänzung zu den unabhängigen Prüfungen der Internen Revision (3rd Linie of Defense) dar.

2. AUDITMANAGEMENT

2.1. Ziele des Auditmanagements

Mit dem Auditmanagement werden die folgenden Ziele verfolgt:

1. Etablierung eines Auditprogramms im Kontext der Sicherheitspolitik und Ziele der VAV auf Basis der DIN ISO/IEC 27001.
2. Überprüfung der Umsetzung auf Konformität zu den internen und externen Anforderungen.
3. Erarbeitung von Handlungsvorschlägen zur Verbesserung des Reifegrades des ISMS und DSMS.

2.2. Prozessdarstellung

Der Auditprozess der Stabstelle Datenschutz und Informationssicherheit mit seinen mitgeltenden Dokumenten wird im Prozessmodell „Auditmanagement“ abgebildet.

2.2.1. Prozessauslöser

Der Auditprozess wird durch ein Ereignis ausgelöst. Ein Ereignis kann in diesem Fall ein regelmäßig wiederkehrender Termin oder eine Reaktion auf sich verändernde Bedingungen (z. B. rechtliche Änderungen oder technische Anpassungen) sein. Ferner können bekannt gewordene Risiken oder aber Sicherheitsvorfälle Auslöser für einen Audit der Stabstelle Datenschutz und Informationssicherheit sein.
Ein Audit zur Prüfung der Einhaltung der Datenschutz- und Informationssicherheitsanforderungen kann im Wesentlichen durch folgende Ereignisse angestoßen werden:
Planmäßig:

- Umsetzung des Auditprogramms / des jährlichen Auditplans

Ad-hoc:

- Empfehlung aus Managementreview
- Erkenntnisse aus dem Schwachstellenmanagement
- Erkenntnisse aus Sicherheitsvorfällen
- Anforderungen des Business Continuity Managements
- Feststellungen und Empfehlungen aus Berichten der Internen Revision
- Maßnahmen, Projekte oder die Einführung neuer Technologien
- Neue regulatorische Anforderungen

2.2.2. Prozessablauf

Ausgehend vom Ereignis werden nacheinander die Teilprozesse angestoßen und bearbeitet:

- Auditprogramm
- Auditplanung
- Auditdurchführung

- Auditnachbereitung

2.3. Qualifikation

Die Stabstelle Datenschutz und Informationssicherheit stellt sicher, dass entsprechend qualifizierte, interne Mitarbeiter und externe Spezialisten (bei Bedarf) die Audits durchführen.
Damit wird erreicht, dass

- eine ausreichende Kompetenz vorhanden ist, um die definierten Auditziele unter Berücksichtigung des Auditumfangs, Komplexität und der Kriterien zu erreichen,
- die im Kapitel 3.2 „Auditplanung“ beschriebenen Auditmethoden berücksichtigt werden,
- die Unabhängigkeit der Auditteammitglieder von den zu auditierenden Tätigkeiten sichergestellt ist und etwaige Interessenkonflikte vermieden werden.

2.4. Auditprinzipien

Die Auditierung stützt sich auf eine Reihe von Prinzipien. Diese machen einen Audit zu einem wirksamen und zuverlässigen Werkzeug zur Unterstützung der Informationssicherheits- und Datenschutzstrategie der VAV. Der Auditprozess stellt Informationen bereit, auf deren Grundlage die Geschäftsleitung handeln kann.
Die Auditoren handeln nach den folgenden Prinzipien:

- Ethisches Verhalten
- Sachliche Darstellung
- Unabhängigkeit
- Vorgehensweise, die auf Nachweisen beruht

Die Einhaltung dieser Prinzipien ist eine Voraussetzung dafür, dass die Auditschlussfolgerungen relevant und ausreichend sind. Weiterhin ermöglichen sie, dass Auditoren unabhängig voneinander zu gleichartigen Schlussfolgerungen unter gleichartigen Umständen gelangen. Die Durchführung eines Audits kann durch einen Auditor erfolgen, zur Überprüfung kann ein zweiter Auditor ein Review des Auditberichts durchführen.

3. TEILPROZESSE DES AUDITMANAGEMENTS

3.1. Auditprogramm

Zu Beginn des Auditmanagementprozesses entsteht das Auditprogramm. Das Auditprogramm ist eine Referenzgrundlage, die den Inhalt (Prüfobjekte) der Auditierung vorgibt.
Der ISB ist verantwortlich für die Erstellung eines Auditprogramms, das auf Grundlage des Annexes der DIN ISO/IEC 27001 die Prüfobjekte der Audits über einen Zeitraum von fünf Jahren beinhaltet. Bezüglich der Prüfungsobjekte im Bereich Datenschutz trägt der DSB die Verantwortung. Die Umsetzung des Auditprogramms ist so zu planen, dass in der Regel innerhalb von fünf Jahren alle Prüfobjekte mindestens einmal geprüft worden sind.
Die Ergebnisse aus einzelnen Audits werden durch die Stabstelle Datenschutz und Informationssicherheit überwacht und bewertet. Die Ergebnisse werden im Rahmen der jährlichen Berichterstattung berichtet und dienen als Lessons Learned der Verbesserung oder Erweiterung des Auditprogramms der VAV. Die Stabstelle Datenschutz und Informationssicherheit wird das Auditprogramm anpassen, sofern die Erreichung der Auditziele nicht gewährleitet werden kann.

3.2. Auditplanung

Auf Grundlage des Auditprogramms werden die konkreten Auditthemen im Rahmen der Auditplanung definiert. Der Auditplan beinhaltet u. a. die einzelnen Prüfobjekte nebst kurzer Beschreibung der Prüfungsinhalte, der Prüfungszeiträume und der geprüften Bereiche. Die Auswahl der einzelnen Prüfobjekte erfolgt risikoorientiert. Die Bewertung / Auswahl wird von der Stabstelle Datenschutz und Informationssicherheit dokumentiert. Im Rahmen der Priorisierung werden insbesondere folgende Aspekte berücksichtigt:

- Reifegrad des geprüften Objekts (je geringer dieser ist, desto höher die Priorisierung)
- Prüfobjekt ist eine gesetzliche oder aufsichtsrechtliche Anforderung.

Der Geschäftsleitung steht es frei, neben den Prüfungen ad-hoc Prüfungen durch die Stabstelle Datenschutz und Informationssicherheit zu beauftragen.
Dies kann z.B. dann der Fall sein, wenn Sicherheitsvorfälle, externe Prüfungen, Beschwerden o. Ä. auf Schwächen oder hohe Risiken hinweisen, so dass eine kurzfristige Überprüfung aus Datenschutz- und Informationssicherheit angezeigt ist.
Die Prüfungsplanung wird mit der Auditplanung der Internen Revision abgestimmt, um Doppelprüfungen zu vermeiden.
Die Stabstelle Datenschutz und Informationssicherheit stimmt die Auditplanung (insbesondere den Zeitpunkt und den Inhalt der Prüfung sowie die notwendigen Zugriffe auf Systeme und Daten) mit dem betroffenen Risikoverantwortlichen rechtzeitig vor der geplanten Prüfung ab.
Eine auditbedingte Einschränkung von Systemverfügbarkeiten soll nach Möglichkeit verhindert werden. Zu den Aufgaben von der Stabstelle Datenschutz und Informationssicherheit zählt die Auswahl der Auditoren. Auditoren können intern und extern (in Abstimmung mit der Geschäftsleitung) berufen werden.
Das Auditteam sollte nach Möglichkeit aus mindestens zwei Auditoren bestehen. Bei der Zusammenstellung des Auditteams sollten folgende Kriterien berücksichtigt werden:

- Ziele, Umfang, Kriterien und geschätzte Dauer des Audits
- Gesamtqualifikation des Auditteams, um die Ziele des Audits zu erreichen
- Unabhängigkeit des Auditteams von den zu auditierenden Tätigkeiten, um Interessenskonflikte zu vermeiden.

Ferner sind die Auditmethoden im Auditplan festzulegen und zu dokumentieren. Hierbei können die nachfolgenden Audit-Methoden zum Einsatz kommen:
Dokumentenprüfung: Bei der Dokumentenprüfung handelt es sich um eine Überprüfung von Dokumenten und Aufzeichnungen. Die Dokumentenprüfung erfolgt i. d. R. auf Basis von Stichproben. Die Durchsicht erfolgt durch die Auditoren anhand der bereitgestellten Dokumente. Für die Auditoren besteht keine Holschuld, falls die Dokumente unzureichend bzw. unvollständig sind. Die Auditoren können nur auf der Basis der ihnen gelieferten Informationen ihre Bewertung vornehmen. Identifizierte Mängel werden im Audit in den Fachbereichen angesprochen, um diesen die Möglichkeit der Erläuterung bzw. zur Nachlieferung zu geben.
Interview: Interviews werden mit ausgewählten Mitarbeitern der VAV geführt um Informationen zu den Themen im zu überprüfenden Bereich zu erhalten. Weiterhin folgen Interviews mit ausgewählten Mitarbeitern um bereits erhobene Informationen zu verifizieren und einen Eindruck für die Sensibilisierung zu sicherheitsrelevanten Themen zu erhalten. Interviews werden nach Möglichkeit immer durch mindestens zwei Auditoren durchgeführt.
Begehung: Beobachtungen finden im Rahmen von Standort-Begehungen oder beim Ausführen von Verfahren an konkreten IT-Systemen oder Prozessen statt. Die erhaltenen Erkenntnisse werden aufgezeichnet und eine Bewertung erfolgt in Abstimmung mit dem auditierten Fachbereich.
Technische Prüfungen: Bei technischen Prüfungen handelt es sich um Audits an definierten Systemen, wie zum Beispiel bei einem Penetrationstest. Die Prüfungen werden mit Unterstützung aus den Fachbereichen durchgeführt und die Ergebnisse in einem Auditbericht zusammengefasst. Zugriffe der Auditoren auf Systeme werden überwacht und protokolliert.
Alle Auditmethoden sind auch kombinierbar.

3.3. Auditdurchführung

Nach der Erstellung der Auditplanung erfolgt die Auditdurchführung. Die Auditdurchführung wird durch das Auditteam vorgenommen.
Bevor das Audit durchgeführt wird, sollte in der Regel eine Eröffnungsbesprechung mit den Verantwortlichen des zu auditierenden Bereichs stattfinden. In der Eröffnungsbesprechung sollen die folgenden Punkte behandelt werden:

- Vorstellung der Teilnehmer, Kurzdarstellung ihrer Rollen im Prozess und im Audit
- Ziel des Audits
- Kurze Erläuterung der geplanten Audittätigkeiten, Methoden und Verfahren, die für die Durchführung des Audits zur Anwendung kommen sollen
- Klären von Fragen des auditierten Bereichs
- Bestätigung des Auditzeitplans und anderer relevanter Regelungen mit der zu auditierenden Organisation

Phase 1: Im ersten Schritt wird die im Prüfungsfokus stehende Dokumentenlage hinsichtlich der Verwendbarkeit für die zu auditierenden Objekte überprüft. Ausgehend von der Dokumentenlage und den daraus geschlossenen Informationen werden Prüfdokumente erstellt.
Arbeitsdokumente einschließlich Aufzeichnungen müssen aufbewahrt werden. Die Dokumente, die vertrauliche oder streng vertraliche Informationen enthalten, müssen von den Mitgliedern des Auditteams in geeigneter Weise geschützt werden.
Phase 2: Im nächsten Schritt erfolgt die inhaltliche Prüfung. Werden bei der Prüfung besonders gravierende Mängel festgestellt, müssen diese von der Stabstelle Datenschutz und Informationssicherheit als ad-hoc Meldung an die IT oder an den Risikoverantwortlichen (bei Non-IT-Feststellungen) weitergeleitet werden (Sofortmeldung).
Die Auditnachweise werden gegenüber den von der Stabstelle Datenschutz und Informationssicherheit festgelegten Auditkriterien bewertet, um die Auditfeststellungen zu erarbeiten. Bei der Prüfung sind die internen Vorgaben (Konzernrichtlinien und Arbeitsrichtlinien) zugrunde zu legen.
Auditfeststellungen sind anhand des im Anhang A dargestellten Reifegradmodells zu bewerten.
Sämtliche Ergebnisse werden in einem Abschlussbericht zusammengestellt. Um die Auditergebnisse abstimmen zu können, muss eine Abschlussbesprechung mit den Beteiligten festgelegt, koordiniert und durchgeführt werden.
Der Abschlussbericht sollte folgendes beinhalten:

- Zielsetzung des Audits mit Auditumfang, besonders die Organisations- und Funktionseinheiten oder die Prozesse, die auditiert wurden und Angabe des betrachteten Zeitraums
- Benennung des Prüfers in der Stabstelle Datenschutz und Informationssicherheit
- Termine, Orte und Ansprechpartner vor Ort, wo Audittätigkeiten durchgeführt wurden
- Die Auditkriterien, die Auditfeststellungen, deren Klassifikation, ein mögliches Risiko sowie die Korrekturmaßnahmen

Die Stabstelle Datenschutz und Informationssicherheit übermittelt den vollständigen Auditbericht zur Abstimmung an den Risikoverantwortlichen. Die Auditfeststellungen und –schlussfolgerungen sind so darzulegen, dass sie für den auditierten Bereich nachvollziehbar sind. Zudem muss dem auditierten Bereich ein angemessener Zeitraum für die Vorlage eines Korrektur- und Verbesserungsmaßnahmenplans gewährt werden.
Der Vorstand erhält die Zusammenfassung der Audits im Rahmen der regelmäßigen Berichterstattung von der Stabstelle Datenschutz und Informationssicherheit.

3.4. Auditnachbereitung

Die im Audit identifizierten Maßnahmen werden durch den geprüften Fachbereich/Risikoverantwortlichen geplant und ihre Umsetzung eingeleitet. Die Umsetzung der jeweiligen Maßnahme ist durch den entsprechenden Risikoverantwortlichen zu überwachen und die Erledigung an die Stabstelle Datenschutz und Informationssicherheit zu melden. Die Stabstelle Datenschutz und Informationssicherheit aggregiert die Informationen über Behebungs- und Verbesserungsmaßnahmen auf Basis des Risikobehandlungsplans und erstellt daraus jährlich einen Bericht für die Geschäftsleitung.
Der Abschluss und die Wirksamkeit der Korrekturmaßnahmen müssen durch die Stabstelle Datenschutz und Informationssicherheit überprüft und verifiziert werden. Diese Verifizierung kann Bestandteil eines nachfolgenden Audits sein. Die Ergebnisse des Audits sollen genutzt werden, um das Auditprogramm und den Auditplan auf notwendige Anpassungen und Verbesserungen zu prüfen.

Anhang A Bewertungsschema

Das Bewertungsschema besteht aus einer Bewertung der vorhandenen Dokumentation und der Umsetzung der Anforderungen. Durch die Einwertung der Dokumentation und Umsetzung in die Abstufungen „keine“, „teilweise“ und „vollumfänglich“ ergibt sich ein Reifegrad.
Hinweis:

- Eine „vollumfängliche“ Dokumentation beinhaltet die Anforderungen zur Lenkung dokumentierter Informationen und unterliegt einem regelmäßigen Review.
- Eine „vollumfängliche“ Umsetzung“ beinhaltet einen Prozess zur Verbesserung.

		Dokumentation		
		keine	teilweise	vollumfänglich
Umsetzung	vollumfänglich	2	4	5
	teilweise	1	2	3
	keine	0	1	1

Tabelle 1: Reifegradmodell

Anhang B: Auditprogramm Datenschutz und Informationssicherheit

In der folgenden Tabelle sind die Prüfobjekte für den Datenschutz und die Informationssicherheit anhand der DIN ISO 27001 aufgelistet:

A.5.1	Vorgaben der Leitung für Informationssicherheit	A.5.1.1	Informationssicherheitsrichtlinien
		A.5.1.2	Überprüfung der Informationssicherheitsrichtlinien
A.6.1	Interne Organisation	A.6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten
		A.6.1.2	Aufgabentrennung
		A.6.1.3	Kontakt zu Behörden
		A.6.1.4	Kontakt mit speziellen Interessensgruppen
		A.6.1.5	Informationssicherheit im Projektmanagement
A.6.2	Mobilgeräte und Telearbeit	A.6.2.1	Richtlinie zu Mobilgeräten
		A.6.2.2	Telearbeit
A.7.1	Vor der Beschäftigung	A.7.1.1	Sicherheitsüberprüfung
		A.7.1.2	Beschäftigungs- und Vertragsbedingungen
A.7.2	Während der Beschäftigung	A.7.2.1	Verantwortlichkeit der Leitung
		A.7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung
		A.7.2.3	Maßregelungsprozess
A.7.3	Beendigung und Änderung der Beschäftigung	A.7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
A.8.1	Verantwortlichkeit für Werte	A.8.1.1	Inventarisierung der Werte
		A.8.1.2	Zuständigkeit für Werte
		A.8.1.3	Zulässiger Gebrauch von Werten
		A.8.1.4	Rückgabe von Werten
A.8.2	Informationsklassifizierung	A.8.2.1	Klassifizierung von Informationen
		A.8.2.2	Kennzeichnung von Informationen
		A.8.2.3	Handhabung mit Werten
A.8.3	Handhabung von Datenträgern	A.8.3.1	Handhabung von Wechseldatenträgern
		A.8.3.2	Entsorgung von Datenträgern
		A.8.3.3	Transport von Datenträgern
A.9.1	Geschäftsanforderungen an die Zugangssteuerung	A.9.1.1	Zugangssteuerungsrichtlinie
		A.9.1.2	Zugang zu Netzwerken und Netzwerkdiensten
A.9.2	Benutzerzugangsverwaltung	A.9.2.1	Registrierung und Deregistrierung von Benutzern
		A.9.2.2	Zuteilung von Benutzerzugängen
		A.9.2.3	Verwaltung privilegierter Zugangsrechte

		A.9.2.4	Verwaltung geheimer Authentisierungsinformation von Benutzern
		A.9.2.5	Überprüfung von Benutzerzugangsrechten
		A.9.2.6	Entzug oder Anpassung von Zugangsrechten
A.9.3	Benutzerverantwortlichkeiten	A.9.3.1	Gebrauch geheimer Authentisierungsinformation
A.9.4	Zugangssteuerung für Systeme und Anwendungen	A.9.4.1	Informationszugangsbeschränkung
		A.9.4.2	Sichere Anmeldeverfahren
		A.9.4.3	System zur Verwaltung von Kennwörtern
		A.9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten
		A.9.4.5	Zugangssteuerung für Quellcode von Programmen
A.10.1	Kryptographische Maßnahmen	A.10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen
		A.10.1.2	Schlüsselverwaltung
A.11.1	Sicherheitsbereiche	A.11.1.1	Physischer Sicherheitsperimeter
		A.11.1.2	Physische Zutrittssteuerung
		A.11.1.3	Sichern von Büros, Räumen und Einrichtungen
		A.11.1.4	Schutz vor externen und umweltbedingten Bedrohungen
		A.11.1.5	Arbeit in Sicherheitsbereichen
		A.11.1.6	Anlieferungs- und Ladebereiche
A.11.2	Geräte und Betriebsmittel	A.11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln
		A.11.2.2	Versorgungseinrichtungen
		A.11.2.3	Sicherheit der Verkabelung
		A.11.2.4	Instandhalten von Geräten und Betriebsmitteln
		A.11.2.5	Entfernen von Werten
		A.11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten
		A.11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
		A.11.2.8	Unbeaufsichtigte Benutzergeräte

		A.11.2.9	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren
A.12.1	Betriebsabläufe und -verantwortlichkeiten	A.12.1.1	Dokumentierte Bedienabläufe
		A.12.1.2	Änderungssteuerung
		A.12.1.3	Kapazitätssteuerung
		A.12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen
A.12.2	Schutz vor Schadsoftware	A.12.2.1	Maßnahmen gegen Schadsoftware
A.12.3	Datensicherungen	A.12.3.1	Sicherung von Information
A.12.4	Protokollierung und Überwachung	A.12.4.1	Ereignisprotokollierung
		A.12.4.2	Schutz der Protokollinformation
		A.12.4.3	Administratoren- und Bedienerprotokolle
		A.12.4.4	Uhrensynchronisation
A.12.5	Steuerung von Software im Betrieb	A.12.5.1	Installation von Software auf Systemen im Betrieb
A.12.6	Handhabung technischer Schwachstellen	A.12.6.1	Handhabung von technischen Schwachstellen
		A.12.6.2	Einschränkung von Softwareinstallation
A.12.7	Audit von Informationssystemen	A.12.7.1	Maßnahmen für Audits von Informationssystemen
A.13.1	Netzwerksicherheitsmanagement	A.13.1.1	Netzwerksteuerungsmaßnahmen
		A.13.1.2	Sicherheit von Netzwerkdiensten
		A.13.1.3	Trennung in Netzwerken
A.13.2	Informationsübertragung	A.13.2.1	Richtlinien und Verfahren zur Informationsübertragung
		A.13.2.2	Vereinbarungen zur Informationsübertragung
		A.13.2.3	Elektronische Nachrichtenübermittlung
		A.13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen
A.14.1	Sicherheitsanforderungen an Informationssysteme	A.14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen
		A.14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken
		A.14.1.3	Schutz der Transaktionen bei Anwendungsdiensten
A.14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	A.14.2.1	Richtlinie für sichere Entwicklung
		A.14.2.2	Verfahren zur Verwaltung von Systemänderungen
		A.14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform

		A.14.2.4	Beschränkung von Änderungen an Softwarepaketen
		A.14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme
		A.14.2.6	Sichere Entwicklungsumgebung
		A.14.2.7	Ausgegliederte Entwicklung
		A.14.2.8	Testen der Systemsicherheit
		A.14.2.9	Systemabnahmetest
A.14.3	Testdaten	A.14.3.1	Schutz von Testdaten
A.15.1	Informationssicherheit in Lieferantenbeziehungen	A.15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen
		A.15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen
		A.15.1.3	Lieferkette für Informations- und Kommunikationstechnologie
A.15.2	Steuerung der Dienstleistungserbringung von Lieferanten	A.15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen
		A.15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen
A.16.1	Handhabung von Informationssicherheitsvorfällen und Verbesserungen	A.16.1.1	Verantwortlichkeiten und Verfahren
		A.16.1.2	Meldung von Informationssicherheitsereignissen
		A.16.1.3	Meldung von Schwächen in der Informationssicherheit
		A.16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse
		A.16.1.5	Reaktion auf Informationssicherheitsvorfälle
		A.16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen
		A.16.1.7	Sammeln von Beweismaterial
A.17.1	Aufrechterhalten der Informationssicherheit	A.17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit
		A.17.1.2	Umsetzen der Aufrechterhaltung der Informationssicherheit
		A.17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit
A.17.2	Redundanzen	A.17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen

A.18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	A.18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen
		A.18.1.2	Geistige Eigentumsrechte
		A.18.1.3	Schutz von Aufzeichnungen
		A.18.1.4	Privatsphäre und Schutz von personenbezogener Information
		A.18.1.5	Regelungen bezüglich kryptographischer Maßnahmen
A.18.2	Überprüfungen der Informationssicherheit	A.18.2.1	Unabhängige Überprüfung der Informationssicherheit
		A.18.2.2	Einhaltung von Sicherheitsrichtlinien und -standards
		A.18.2.3	Überprüfung der Einhaltung von technischen Vorgaben