

# Inhalt

<b>Vorwort</b>	<b>IX</b>
<b>1 IS Policies and Organization</b>	<b>1</b>
1.1 Information Security Policies	1
1.1.1 Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?	1
1.2 Organization of Information Security	4
1.2.1 Inwieweit wird in der Organisation Informationssicherheit gemanagt?	5
1.2.2 Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?	8
1.2.3 Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?	11
1.2.4 Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Service-Anbietern und der eigenen Organisation definiert?	13
1.3 Asset Management	16
1.3.1 Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?	16
1.3.2 Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?	19
1.3.3 Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?	22
1.4 IS Risk Management	24
1.4.1 Inwieweit werden Informationssicherheitsrisiken gemanagt?	24

1.5	Assessment .....	28
1.5.1	Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt? .....	28
1.5.2	Inwieweit wird das ISMS von einer unabhängigen Instanz überprüft? .....	31
1.6	Incident Management .....	32
1.6.1	Inwieweit werden Informationssicherheitsereignisse verarbeitet? .....	32
<b>2</b>	<b>Human Resources .....</b>	<b>37</b>
2.1	Personalmanagement .....	37
2.1.1	Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt? .....	37
2.1.2	Inwieweit werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet? .....	40
2.1.3	Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert? .....	42
2.1.4	Inwieweit ist mobiles Arbeiten geregelt? .....	44
<b>3</b>	<b>Physical Security and Business Continuity .....</b>	<b>47</b>
3.1	Physische Sicherheit und Geschäftskontinuität .....	47
3.1.1	Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt? .....	47
3.1.2	Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt? .....	52
3.1.3	Inwieweit ist der Umgang mit Informationsträgern gemanagt? ..	54
3.1.4	Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt? .....	55
<b>4</b>	<b>Identity and Access Management .....</b>	<b>57</b>
4.1	Identity Management .....	57
4.1.1	Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt? ..	57
4.1.2	Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert? .....	59
4.1.3	Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt? .....	61

4.2	Access Management .....	65
4.2.1	Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt? .....	65
<b>5</b>	<b>IT Security/Cyber Security .....</b>	<b>69</b>
5.1	Cryptography .....	69
5.1.1	Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt? .....	69
5.1.2	Inwieweit werden Informationen während der Übertragung geschützt? .....	72
5.2	Operations Security .....	75
5.2.1	Inwieweit werden Änderungen gesteuert? .....	75
5.2.2	Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt? .....	77
5.2.3	Inwieweit werden IT-Systeme vor Schadsoftware geschützt? .....	78
5.2.4	Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert? .....	81
5.2.5	Inwieweit werden Schwachstellen erkannt und behandelt? .....	84
5.2.6	Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)? .....	87
5.2.7	Inwieweit wird das Netzwerk der Organisation gemanagt? .....	89
5.3	System Acquisitions, Requirement Management and Development ....	91
5.3.1	Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt? .....	91
5.3.2	Inwieweit sind Anforderungen an Netzwerkdienste definiert? ...	93
5.3.3	Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt? .....	96
5.3.4	Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt? .....	97
<b>6</b>	<b>Supplier Relationships .....</b>	<b>99</b>
6.1	Lieferantenbeziehungen .....	99
6.1.1	Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt? .....	99
6.1.2	Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart? .....	101

**7 Compliance ..... 105**

7.1 Unternehmen an Gesetzen und Richtlinien ausrichten ..... 105

7.1.1 Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt? ..... 105

7.1.2 Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt? ..... 110

**Die Autoren ..... 113**

**Index ..... 115**