

Inhalt

Vorwort zur 2. Auflage	XI
Vorwort zur 1. Auflage	XIII
1 Richtlinien und Organisation der Informationssicherheit	1
1.1 Richtlinien zur Informationssicherheit	1
1.1.1 Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?	1
1.2 Organisation der Informationssicherheit	4
1.2.1 Inwieweit wird in der Organisation Informationssicherheit gemanagt?	4
1.2.2 Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?	7
1.2.3 Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?	11
1.2.4 Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Dienstleistern 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?	21
1.3.4	Inwieweit wird sichergestellt, dass nur evaluierte und zugelassene Software zum Verarbeiten von Informationswerten der Organisation eingesetzt wird?	24
1.4	Risikomanagement für Informationssicherheit	26
1.4.1	Inwieweit werden Informationssicherheitsrisiken gemanagt?	26
1.5	Assessment	30
1.5.1	Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?	30
1.5.2	Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?	33
1.6	Vorfall- und Krisenmanagement	34
1.6.1	Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?	35
1.6.2	Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?	39
1.6.3	In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?	42
2	Personalabteilung	47
2.1	Personalmanagement	47
2.1.1	Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?	47
2.1.2	Inwieweit werden alle Mitarbeiter vertraglich zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet?	50
2.1.3	Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?	52
2.1.4	Inwieweit ist mobiles Arbeiten geregelt?	54
3	Physische Sicherheit	57
3.1	Physische Sicherheit und Geschäftskontinuität	57
3.1.1	Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?	57
3.1.2	(Ersetzt)	61
3.1.3	Inwieweit ist der Umgang mit Informationsträgern gemanagt? ...	61
3.1.4	Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?	63

4	Identitäts- und Zugriffsverwaltung	65
4.1	Identitätsverwaltung	65
4.1.1	Inwieweit ist der Umgang mit Identifikationsmitteln verwaltet? ..	65
4.1.2	Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?	67
4.1.3	Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?	70
4.2	Zugriffsverwaltung	74
4.2.1	Inwieweit werden Zugriffsrechte vergeben und verwaltet?	74
5	IT-Sicherheit/Cybersicherheit	77
5.1	Kryptografie	77
5.1.1	Inwieweit wird die Nutzung kryptografischer Verfahren verwaltet?	77
5.1.2	Inwieweit werden Informationen während der Übertragung geschützt?	80
5.2	Operations Security	83
5.2.1	Inwieweit werden Änderungen verwaltet?	83
5.2.2	Inwieweit sind die Entwicklungs- und Testumgebungen von Produktivumgebungen getrennt?	85
5.2.3	Inwieweit werden IT-Systeme vor Schadsoftware geschützt?	86
5.2.4	Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?	89
5.2.5	Inwieweit werden Schwachstellen erkannt und behandelt?	92
5.2.6	Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?	95
5.2.7	Inwieweit wird das Netzwerk der Organisation verwaltet?	98
5.2.8	Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?	100
5.2.9	Inwieweit werden die Sicherung und die Wiederherstellung von Daten und IT-Diensten sichergestellt?	104
5.3	Systemanschaffung, Anforderungsmanagement und Entwicklung	107
5.3.1	Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?	107
5.3.2	Inwieweit sind Anforderungen an Netzwerkdienste definiert?	110
5.3.3	Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?	112
5.3.4	Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?	114

6	Lieferantenbeziehungen	115
6.1	Lieferantenbeziehungen	115
6.1.1	Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?	115
6.1.2	Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?	119
7	Compliance	123
7.1	Unternehmen an Gesetzen und Richtlinien ausrichten	123
7.1.1	Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?	123
7.1.2	Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?	129
8	Prototypenschutz	131
8.1	Physische und umgebungsbezogene Sicherheit	131
8.1.1	Inwieweit ist ein Sicherheitskonzept vorhanden, das Mindestanforderungen zur physischen und umgebungsbezogenen Sicherheit für den Prototypenschutz beschreibt?	132
8.1.2	Inwieweit ist Perimeterschutz vorhanden, der den unberechtigten Zutritt zu geschützten Objekten der Liegenschaften verhindert?	134
8.1.3	Inwieweit ist die Außenhaut der geschützten Gebäude in einer Form ausgeführt, die das Entfernen oder Öffnen von Außenhautkomponenten mit handelsüblichen Werkzeugen verhindert?	135
8.1.4	Inwieweit wird der Sicht- und Einblickschutz in definierte Sicherheitsbereiche sichergestellt?	137
8.1.5	Inwieweit ist der Schutz vor unbefugtem Betreten in Form einer Zugangskontrolle geregelt?	138
8.1.6	Inwieweit werden die zu sichernden Räumlichkeiten auf Einbruch überwacht?	139
8.1.7	Inwieweit ist ein dokumentiertes Besuchermanagement vorhanden?	140
8.1.8	Inwieweit ist eine Mandantentrennung vor Ort gegeben?	142
8.2	Organisatorische Anforderungen	143
8.2.1	Inwieweit liegen vertragsrechtlich gültige Geheimhaltungsvereinbarungen/-verpflichtungen vor?	143
8.2.2	Inwieweit sind Vorgaben für die Beauftragung von Unterauftragnehmern bekannt und erfüllt?	144

8.2.3	Inwieweit werden Mitarbeiter und Projektbeteiligte bezüglich des Umgangs mit Prototypen nachweislich geschult und sensibilisiert?	145
8.2.4	Inwieweit sind die Sicherheitseinstufungen des Projekts und die daraus resultierenden Maßnahmen zur Absicherung bekannt? ..	146
8.2.5	Inwieweit ist ein Prozess zur Zutrittsvergabe in Sicherheitsbereiche definiert?	147
8.2.6	Inwieweit sind Regelungen zur Bildaufzeichnung und zum Umgang mit erstelltem Bildmaterial vorhanden?	148
8.2.7	Inwieweit ist ein Prozess für das Mitführen und die Nutzung von mobilen Video- und Fotogeräten in definierten Sicherheitsbereichen etabliert?	149
8.3	Umgang mit Fahrzeugen, Komponenten und Bauteilen	150
8.3.1	Inwieweit werden Transporte von als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen nach den Vorgaben des Auftraggebers abgewickelt?	150
8.3.2	Inwieweit ist sichergestellt, dass als schutzbedürftig klassifizierte Fahrzeuge, Komponenten und Bauteile den Vorgaben des Auftraggebers entsprechend abgestellt/gelagert werden?	153
8.4	Anforderungen für Versuchsfahrzeuge	154
8.4.1	Inwieweit werden die vorgegebenen Regelungen zur Tarnung von den Projektbeteiligten umgesetzt?	154
8.4.2	Inwieweit werden Maßnahmen für den Schutz von freigegebenem Test- und Erprobungsgelände eingehalten/umgesetzt?	155
8.4.3	Inwieweit werden die Schutzmaßnahmen für freigegebene Test- und Erprobungsfahrten in der Öffentlichkeit eingehalten/umgesetzt?	155
8.5	Anforderungen für Veranstaltungen und Shootings	156
8.5.1	Inwieweit sind die Sicherheitsvorgaben für Ausstellungen und Veranstaltungen mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt?	156
8.5.2	Inwieweit sind die Schutzmaßnahmen für Film- und Fotoshootings mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt?	157
Die Autoren		159
Index		161