KOMPETENZGRUPPE SICHERHEIT

ARBEITSKREIS ISMS

PROJEKTPARTNER

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

VdS Schadenverhütung GmbH

AXA Versicherung AG
Kompetenzstelle Cyber - Industriekundengeschäft

Pallas GmbH

Materna GmbH

ARBEITSKREIS MANAGEMENTSYSTEME

Dauerhaft gut fundierte und angemessene IT-Sicherheit erreicht man mit einem Information Security Management System (ISMS). Das ISMS bildet das organisatorische und technische Gerüst, um die Informationssicherheit systematisch zu steuern und auf einem geeigneten, hohen Niveau zu halten. Das dient dem Schutz des Unternehmens und vermeidet Lücken genauso wie Überschneidungen und stellt darüber hinaus die Erfüllung gesetzlicher und vertraglicher Anforderungen sicher.

Für das ISMS nutzt man in der Regel einen eingeführten Standard als Basis, etwa die Norm ISO/IEC 27001 oder den IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Aber es gibt auch einfachere Standards, die mit geringerem Aufwand bei Einführung und ggf. Zertifizierung etwa in kleineren Organisationen ein angemessenes Schutzniveau erreichen lassen, z.B. die Standards VdS 3473 und ISIS12.

Die vorliegende Übersicht stellt diese Standards tabellarisch dar, nennt Vor- und Nachteile sowie Hinweise für Umfang und Aufwand. Außerdem werden nach gleicher Struktur weitere Standard-Systeme behandelt, nämlich Qualitäts-, Risiko- und Business Continuity Management sowie Wirtschaftsprüfer-Standards. Denn diese spielen oft in das ISMS hinein und können zusätzliche Anforderungen stellen.

THEMEN UND BRANCHEN

Datenschutz	**e-health**
Industrie 4.0	**IT-Recht**
Managementsysteme	**Websicherheit**

Literaturhinweise:

Diese Übersicht basiert auf Arbeiten die teilweise auf Basis der untenstehenden Publikationen erarbeitet wurden:

• Kompass der IT-Sicherheitsstandards Bitkom 2013 des Arbeitskreis „Sicherheitsmanagement“: https://www.bitkom.org/Bitkom/Publikationen/Kompass-der-IT-Sicherheitsstandards-2.html

• Handreichung dt. Städtetag / Landkreistag

eco - Verband der Internetwirtschaft e.V.
Lichtstraße 43h, 50825 Köln
fon: +49 (0)221 - 70 00 48-0
fax: +49 (0)221 - 70 00 48-111
info@eco.de, www.eco.de

Standard / Kriterien	ISO 27001 ff.	BSI Grundschutz	VdS 10000	ISIS12	Risikomanagement (ISO 31000)	WP-Standards IDW-PS 951 neue Fassung / ISAE 3402	Business Continuity (BCM) ISO 22301
Zweck des Standards	Erhöhzung der Informationssicherheit	Erhöhung der Informationssicherheit	Erhöhung der Informationssicherheit speziell im KMU Segment und bei Behörden	Erhöhung der Informationssicherheit für den Mittelstand und die öffentliche Verwaltung	Beschreibung und Umsetzung eines Risikomanagement-systems für Unternehmen und Organisationen.	Nachweisfähigkeit gegenüber Dritten bezogen auf die ordnungsgemäße Erbringung der Dienstleistung	a) Nachweisfähigkeit gegenüber Dritten, b) verbesserte Reaktionsfähigkeit im Notfall und Verminderung des Risikos der Bestandsgefährdung durch Eintritt eines Notfalls
Herausgeber des Standards	International Standards Organisation	Bundesamt für Sicherheit in der Informationstechnik	VdS GmbH	Bayerischer IT-Sicherheitscluster e.V.	International Standards Organisation		
Geltungsbereich	Unternehmen bestimmen individuell z. B. im Rahmen eines Scoping Workshops den Geltungsbereich. Ggf. zusätzliche Vorgaben des Gesetzgebers	siehe ISO 27001 Da meist im behördlichen Kontext eingesetzt, gibt es hier auch meist Vorgaben zum Geltungsbereich (z. B. über branchenspezifische Standards B3S).	Office- und Produktions-IT	Scope ist variabel Office- und Produktions-IT bis zur kompletten Organisation	Allgemein anwendbarer, umfassender und offener, generischer Norm-Standard	Dienstleistungsbezogenes internes Kontrollsystem, d. h. im Scope ist eine Dienstleistung, die für ein auslagerndes Unternehmen erbracht wird	vom Unternehmen festzulegen
Unternehmensgröße/-art	Keine Beschränkung Eher größere Unternehmen	Keine Beschränkung Meist behördlicher, öffentlicher Kontext	Keine Beschränkung Sehr gut geeignet für KMU	Keine Beschränkung konzentriert sich aber auf KMUs und die öffentliche Verwaltung	Keine Beschränkung	Keine Beschränkung	keine Beschränkung
internationale Ausrichtung	Ja	Nein	Nein, DACH	Nein, DACH	Ja	Der IDW PS 951 n.F. kommt in D zur Anwendung. Bei internationaler Ausrichtung sollte eine Prüfung nach ISAE 3402 erfolgen.	keine Beschränkung
Branchen/Tätigkeiten	Alle Aber Vorgabe für bestimmte KRITIS-Sektoren (z.B. EVU, Ernährung, usw.) sowie Telekommunikationsunternehmen gem. BNetzA	Alle Verpflichtung zur Orientierung an Standard für Behörden, halböffentliche Institutionen (z.B. IHK, Kassenärztliche Vereinigungen, usw)	Alle	Alle	Alle	Kommt zur Anwendung bei Dienstleistern (Outsourcing) deren Auftraggeber vom WP geprüft werden	keine Beschränkung
Wirksamkeit bzw. Voraussetzung zur Erteilung des Zertifikates/ Testates	Ein wirksames, gelebtes ISMS ist zwingend notwendig, um zertifizierungsfähig zu sein. Reine Dokumentationsverpflichtung ist nur ein Teil.	siehe ISO 27001	siehe ISO 27001	Erfolgreich Einführung im Unternehmen und abgeschlossene Revision (Schritt 12)	Das Unternehmen / die Organisation sollte in regelmäßigen Abständen die Fortschritte im Risikomanagement überprüfen und überwachen, insbesondere ob das Risikomanagement hinsichtlich Rahmenbedingungen, Politik und Planung angesichts des internen und externen Umfeldes noch angemessen ist. Zudem sollte eine Berichterstattung über die Risiken und die Fortschritte erfolgen sowie über den Umsetzungsstand der Risikomanagementpolitik.	Im Rahmen der Typ 2 Prüfung wird die Wirksamkeit der eingerichteten Controls mittels statistisch aussagekräftiger Stichprobenmengen durch den Wirtschaftprüfer geprüft und muss mit Ausstellung des Testats gegeben sein.	ist abhängig von der Art der Umsetzung
Umfang des Standards (groß/mittel/klein)	mittel (ca. 400 Seiten) ca. 150 Maßnahmen	groß (ca. 5.000 Seiten) ca. 1.100 Maßnahmen	klein (ca. 40 Seiten) ca. 100 Maßnahmen	klein bis mittel (ca. 170 Seiten) ca. 400 Maßnahmen	mittel	klein	klein
Bezug des Standards	gegen Kostenerstattung	kostenlos	kostenlos	kostenlos	gegen Kostenerstattung		gegen Kostenerstattung
Beauftragter im Unternehmen	ISB oder CISO	siehe ISO 27001	GF/ ISB	Aufbau eines Informationssicherheitsteams: Ernennung eines für ISIS12 verantwortlichen Sicherheitsteams, z. B. ISB (IT-Sicherheitsbeauftragter)	Sinnvoll, aber nicht zwingend. Die Verantwortung des RM liegt beim Management.	Sinnvoll, aber nicht zwingend: Die Verantwortung für das IKS liegt beim Management.	BCM-Manager
Vorteile	Sehr hoher Nutzen, gutes Invest-/ Nutzenverhältnis, wenn der Geltungsbereich geschickt gewählt wird. Vorteile eines risikobasierten Ansatzes, der betriebswirtschaftlich angemessene Maßnahmen forciert. Gestaltbar Hoher, internationaler Bekanntheitsgrad und Anerkennung / akkteditierte Zertifizierungsstelle	Über Grundschutzkataloge hoher Nutzen, wenn man diese Orientierung sucht. Sehr detailliert, festgelegte Vorgehensweise, klare Führung des Anwenders. Umfangreiche vorhandene Dokumentationen. Hohe Anerkennung - insbesondere im Behördenbereich.	Handhabbarer IT-Sicherheitsstandard für KMU Pragmatischer Ansatz, schneller Einstieg möglich Hohe Durchdringung bei Versicherern (Cyber-Versicherung) Breite Anerkennung im Umfeld von Versicherungen	Schneller, einfacher und kostengünstiger Einstieg in die Informationssicherheit - 12 aufbauenden Verfahrensschritten - Klar formulierte Anweisungen auch zur IT-Dokumentation und zum IT-Service-Management - Sensibilisierung der Mitarbeiter und Stärkung des Sicherheitsbewusstseins im Unternehmen - Fokussierung auf unternehmenskritische Anwendungen und verbundene IT-Systeme - Radikale Reduzierung des Maßnahmenkatalogs gegenüber BSI-Grundschutz	Internationale Anwendbarkeit bzw. Bezug auf eine internationale Norm. a) Risiken effektiv, nachvollziehbar und dokumentiert in einem Unternehmen bewältigen b) Verbesserung der Corporate Governance und des Chancen-/Risiken-Profils c) Erfüllung rechtlicher und behördlicher Bestimmungen	Nachweisfähigkeit gegenüber Dritten bezogen auf die ordnungsgemäße Erbringung der Dienstleistung	a) Nachweisfähigkeit gegenüber Dritten, b) verbesserte Reaktionsfähigkeit im Notfall und Verminderung des Risikos der Bestandsgefährdung durch Eintritt eines Notfalls
Nachteile	komplex und manchmal abstrakt Ggf. nur positive Seiten des Unternehmens in den Geltungsbereich einbezogen	Wenig flexibel, um sich auf spezielle Anforderungen einstellen zu können. Detailverliebt. Sehr hoher Dokumentationsaufwand - mindert das Invest-/ Nutzenverhältnis. Kein risikoorientierter Ansatz (Mindestniveau Sicherheit über Alles), daher betriebswirtschaftlich nicht optimal. Dokumentationen teilweise nicht immer auf aktuellem Stand der Technik oder für neuere Systeme nicht vorhanden - hier fehlt dann eine klare Anleitung	Noch keine breite Anerkennung insb. im internationalen Umfeld - allerdings auch nur auf deutsche Unternehmen abgestellt!	Keine Akkreditierung für Zertifizierungsstelle	administrativer Aufwand durch die unternehmensweite Erhebung und Aktualisierung von Risikodaten	jährlich Kosten für die WP-Prüfung und interne Aufwände für die Pflege des IKS sowie Vor-/Nachbereitung und Begleitung der Wirtschaftsprüfung	jährlich Kosten für die Zertifizierung und interne Aufwände für die Pflege des BCM-Systems sowie Vor-/ Nachbereitung und Begleitung der Zertifizierer
Aufwand der Installation	30 - 300 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit; Interner Aufwand Faktor 1,5 - 2	30 - 300 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit; Interner Aufwand Faktor 2 - 4	70% Ergebnis der ISO 27001 bei 30% des Aufwandes	extern: 5-40 PT Berateraufwand. Intern: abhängig vom gewähltem Scope und Ist-Zustand	Aufwand variiert nach Unternehmensgröße und Geschäftsmodell und -prozesse sowie Fokus	Im Falle der ISAE 3402 muss die IKS-Dokumentation auf Englisch vorgelegt werden. 20-40 PT + interner Aufwand	Der Aufwand für Aufbau und Implementierung eines BCM-Systems ist von verschiedenen Faktoren abhängig. Wenn es z.B schon ein zertifiziertes Managementsystem nach ISO 27001 gibt, ist der Aufbauaufwand deutlich geringer. Auch eine vorhandenes Notfallmanagment wirkt sich positiv auf den Aufwand aus.
Zertifizierungsmöglichkeit	ISO-Zertifizierung ISO/IEC 27001:2013 + ggf. Branchenstandards (z. B. 27018 für Clouddienstleister)	ISO-Zertifizierung nach BSI-Grundschutz BSI-Standards (100-1, 100-2, 100-3,100-4) inklusive der BSI-Grundschutzkataloge	VdS 10000 Testat (Vorstufe zum Zertifikat) VdS 10000 Zertifikat	DQS-Zertifizierung	keine Zertifizierung möglich	keine Zertifizierung, WP-Testat (Typ 1 und 2)	ISO-Zertifizierung
Dauer der Gültigkeit der Zertifizierung/Testate	3 Jahre, jährlich Monitorings	3 Jahre, jährlich Monitorings	3 Jahre, jährlich Monitorings	3 Jahre, jährlich Monitorings	Entfällt	Das Testat wird üblicherweise für einen Zeitraum von vorausgehenden 12 Monaten ausgestellt. Die Prüfung muss daher jährlich erfolgen.	nach einem Jahr ist eine Rezertifizierung erforderlich
Zertifizierungsaufwand (Personentage)	Abhängig von Anzahl Mitarbeiter im Scope; Feste Kalkulationstabelle; Aufwand ist im Vergleich zur Vorbereitung sehr gering. ISO 27006 zeigt den zu erwartenden Aufwand an	Abhängig von Anzahl Mitarbeiter im Scope; Feste Kalkulationstabelle. Aufwand ist im Vergleich zur Vorbereitung sehr gering.	1-2 Tage je nach Unternehmensgröße	Abhängig von Anzahl Mitarbeiter im Scope; Feste Kalkulationstabelle. Aufwand ist im Vergleich zur Vorbereitung gering.	Entfällt	abhängig vom Scope (u.a. Anzahl der zu prüfenden Standorte) wird vom Wirtschaftsprüfer festgelegt. (Die Typ 1-Prüfung ist vom Aufwand geringer als die nachfolgende Typ 2-Prüfung, da hier noch keine umfangreichen Stichproben gezogen werden.)	abhängig vom Scope (u.a. Anzahl der zu prüfenden Standorte), wird vom Zertifizierer festgelegt