Informationssicherheit und Cyber Safety
Beratung mit Weitsicht

Projektleitung, Beratung, Coaching, Umsetzung, Ausbildung
Informationssicherheits-Managementsystem (ISMS)
ISMS Auditing / Review
IS Risikomanagement
ISMS Zertifizierung nach ISO/IEC 27001
IT Notfallhandbuch und Recovery Management
Cyber Krisenmanagement

Sichern Sie Ihre Geschäftserfolge, Datenverfügbarkeit und Know-how

www.information-security-informationssicherheit.com

Risk Management
Security & Risk Management Consultants
Swiss Information Safety

Viele Unternehmen und Institutionen sind nur ungenügend oder gar nicht geschützt

Cyberangriffe werden häuiger, aggressiver, rafinierter. Unternehmen sollten darauf reagieren, Ihre Daten und Ihr Know-how besser schützen und gezielter auf Cyber Security und Forensic setzen. Wir sagen Ihnen, wie Sie aufgestellt sind und helfen Ihnen, auf Nummer sicher zu gehen.

SIND IHRE NETZWERKE, DATEN UND IHR KNOW-HOW AUSREICHEND GESCHÜTZT?

Informationen und Daten sind heute ein wesentlicher Erfolgsfaktor für Unternehmen. Sie zu schützen, wird allerdings immer schwieriger - aufgrund veränderter Infrastruktur, zum Beispiel durch Cloud oder Mobile Computing, Transformationen wie die Vernetzung von Geschäftsprozessen und eine gestiegene Bedrohung durch Cyberattacken. Für einen effizienten Schutz müssen Unternehmen daher gezielte Vorkehrungen treffen und technische und prozessuale Sicherheitsmassnahmen richtig kombinieren.

RM Risk Management AG, als spezialisiertes Beratungsunternehmen für Informationssicherheit, Cyber Safety sowie Know-how Schutz zeigt Ihnen schnell, einfach und nachvollziehbar, wo Sie stehen und in welchen Bereichen Sie handeln sollten.

Kontakt

RM Risk Management AG
Security & Risk Management Consultants
Hertistrasse 25
CH-8304 Wallisellen
Tel. +41 (0)44 360 40 40
rm@rmrisk.ch
www.information-security-informationssicherheit.com

Wissen, wo Ihr Unternehmen verletzbar ist

Sicherung der Unternehmensziele und Erfolge:

Sicherung / Ausbau Wettbewerbsvorteile und Marktpräsenz

Gewinn- und Ertragssicherung

Schadensbegrenzung / Minderung von Imageeinbussen bei Prozess- und Produktionsausfällen

Datendiebstahl
Wettbewerbsspionage
Cyber Crime
IT Ausfall
Telefonieausfall

Blackout
Strommangellage
Ausfall betriebskritischer Anlagen
Ausfall Provider
Ausfall Kühlung

Informatikausfälle
Hacktivisten
Insider
Organisiertes Verbrechen
Spionage / Sabotage

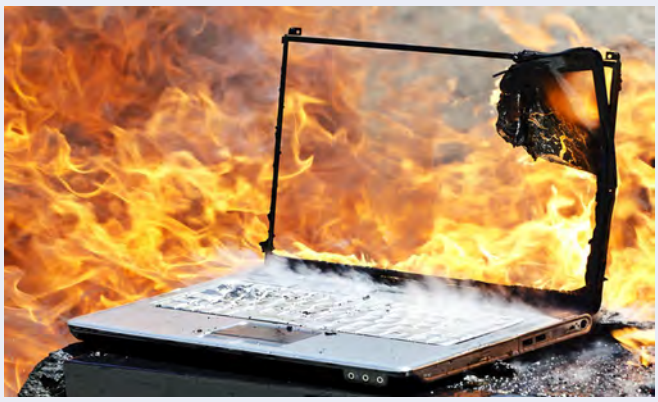
Ausfall Outsourcing Partner
Ausfall Glasfaserkabel
Ausfall Serverräume
Unwetter / Sturm
Brand / Wassereinbruch

Informationssicherheit, Cyber Safety, IS Risikomanagement, Cyber Krisenmanagement

Ermitteln Sie Ihren persönlichen Informationssicherheit / Cyber Security Reifegrad.

IT Ausfälle und Cyber Angriffe passieren immer unerwartet

"Ich hätte nie gedacht, dass so etwas passieren kann".



Informationssicherheit, Cyber Safety, IS Risikomanagement, Cyber Krisenmanagement

Ermitteln Sie Ihren persönlichen Informationssicherheit / Cyber Safety Reifegrad.

Vorgehensweise und praktische Umsetzung der Informationssicherheit nach ISO/IEC 27001

Mit ISMS Open Source Tool verinice und OptiRisk Fachdokumente als Vorlagen.

Informationssicherheit / ISMS Umsetzung

8 Phasenmodell

1 Rückhalt im Management

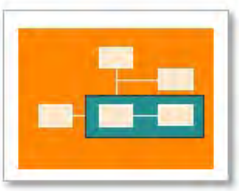
- Projektantrag mit Beschreibung der Ziele
- Abschätzung der Zeitplanung
- Personelle sowie monetäre Ressourcen unter Berücksichtigung eines ersten groben Scopes
- Einsatz externer Experten
- Planungen mit potentiell betroffenen Bereichen abstimmen

2 Self Assessment mit Standardfragebogen und GAP-Analyse

- Ermittlung des Status Quo
- Analyse der vorhandenen relevanten Dokumentationen, Richtlinien und sonstigen Regelwerken
- Erhebung des fachlichen Ist-Zustands mittels strukturierten Interviews, Fragebögen und Workshops
- Gap-Analyse mit Bewertung und Priorisierung auf fachlicher, organisatorischer und prozessualer und technischer Ebene
- Ableitung von high-level Handlungsbedarfen
- Validierung des Status Quo auf Basis der wesentlichen ISO 27001 Anforderungen
- Strukturierte Dokumentation aller Ergebnisse

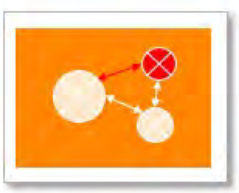
3 Organisation und ISMS Geltungsbereich (Scope) definieren

- Kontext der Organisation analysieren
- Geltungsbereich des ISMS
- Sicherheitsleitlinie und Ziele erstellen
- Dokumentationsrahmenwerk erstellen
- ISMS Pflichtdokumente erstellen



4 Schutzbedürftige Informationen und Assets definieren

- Ermittlung der primären Assets sowie der sekundären, unterstützenden Assets
- Identifizierung der Wirkungskette
- Asset-Register erstellen



OptiRisk®
Knowledge & Templates

5 Durchführung Schutzbedarfs- und Risikoanalyse

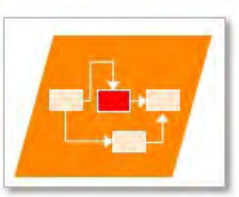
- Risikomanagement-Methodik festlegen
- Risikokategorien und -kriterien festlegen
- Risikomanagement durchführen
- Bestimmung der Risikoeigentümer

6 Risikobehandlungsplan - Massnahmen zur Risikobehandlung

- Risikobehandlungsplan erstellen
- Anhang A der ISO 27001 anwenden
- Massnahmen priorisieren
- Personelle Anforderungen und Kompetenzen festlegen
- Kommunikations-, Trainings- und Awareness-Massnahmen sicherstellen
- Statement of Applicability erstellen

7 ISMS messen, steuern und Verbesserungen umsetzen

- Regelbetrieb mit Monitoring und Reporting etablieren
- Dokumentationsprozesse sicherstellen
- Interne sowie Lieferanten-Audits durchführen
- Kontinuierlicher Verbesserungsprozess leben



8 Ausbildung und Security Awareness

- Ausbildungskonzept im Detail erarbeiten
- Awareness-Konzept im Detail definieren
- Ausbildungen, Trainings und Awareness-Massnahmen durchführen

verinice.
Information Security Management System

Informationssicherheit, Cyber Safety, IS Risikomanagement, Cyber Krisenmanagement

Ermitteln Sie Ihren persönlichen Informationssicherheit / Cyber Safety Reifegrad.

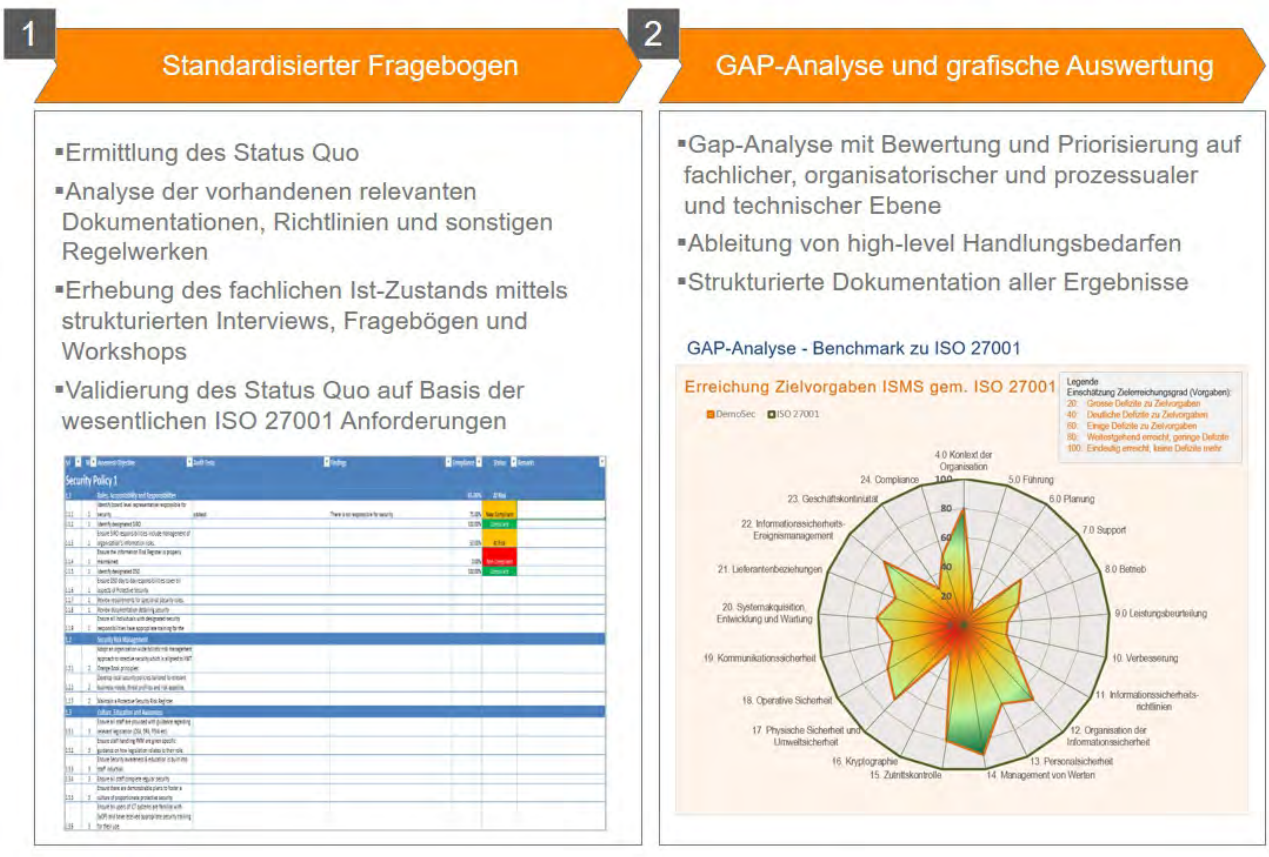
ISMS Umsetzung - 8 Phasenmodell

1. Rückhalt im Management

Für Unternehmen gibt es zahlreiche Motive, sich mit einer Ausrichtung oder sogar Zertifizierung nach der ISO/ IEC 27001 auseinanderzusetzen. Die Gesetzgebung sendet die notwendigen Signale, welchen Stellenwert derzeit das Thema Informationssicherheit und Cyber Security einnimmt. Die Industrie beispielsweise ist auf den Schutz ihres Know-hows und damit ihrer Wettbewerbsvorteile aber auch infolge der hohen Automatisierungsgrade auf die hohe Verfügbarkeit der IT Services angewiesen. Es empfiehlt sich daher, die bestehenden Umsetzungsgesetze aufmerksam zu verfolgen und bei sich frühzeitig die notwendigen Vorbereitungen für eine ISMS-Implementierung einzuleiten. Ein Management Committment ist von grosser Bedeutung, damit die ISMS Umsetzung hinsichtlich Qualität, Zeit, Budget möglichst reibungslos erfolgt. Der Projektantrag soll neben den Zielen die Zeitplanung und die personellen sowie finanziellen Ressourcen unter Berücksichtigung des Projektrahmens (Scope) definieren, in dem das ISMS künftig betrieben werden soll. Gegebenenfalls ist auch der Einsatz externer Experten mitzuberücksichtigen. Das Management muss zudem mit potentiell betroffenen Fachbereichen die Planungen abstimmen.

2. Self-Assessment mit Standardfragebogen und GAP-Analyse

Um die Parameter des Projektrahmens für die Informationssicherheit sowie den Projektumfang bestmöglichst einschätzen zu können, hat sich die Ermittlung des Status Quo, einer sogenannten „Gap-Analyse“ (Lückenanalyse) als „Best-Practice“ besonders bewährt. Innerhalb eines Vorprojektes wird dafür der personelle, prozessorientierte und organisatorische Reifegrad des Unternehmens möglichst objektiv identifiziert und beurteilt. Dies geschieht anhand standardisierter Fragebögen, basierend auf ISO-Standards, Best-Practices, rechtlich und regulatorischen sowie technisch-organisatorischen Anforderungen. Der ermittelte Status Quo (Ergebnis des Self-Assessments bzw. der GAP-Analyse) hilft die Detailplanungen für das ISMS-Projekt auszuarbeiten. Die dazu notwendigen Arbeitsschritte werden anhand des Phasenmodells zur ISMS Umsetzung Schritt für Schritt dargestellt. Es wird in acht aufeinander aufbauende Projektphasen dargestellt. Dieses Phasenmodells zur ISMS Umsetzung dienen dazu, die notwendigen Arbeitspakete und eine Detailplanung sowie die Projektsteuerung zu definieren.



Informationssicherheit, Cyber Safety, IS Risikomanagement, Cyber Krisenmanagement

Ermitteln Sie Ihren persönlichen Informationssicherheit / Cyber Safety Reifegrad.

Informationssicherheits-Managementsystem (ISMS)

3. Organisation und ISMS Geltungsbereich (Scope) definieren

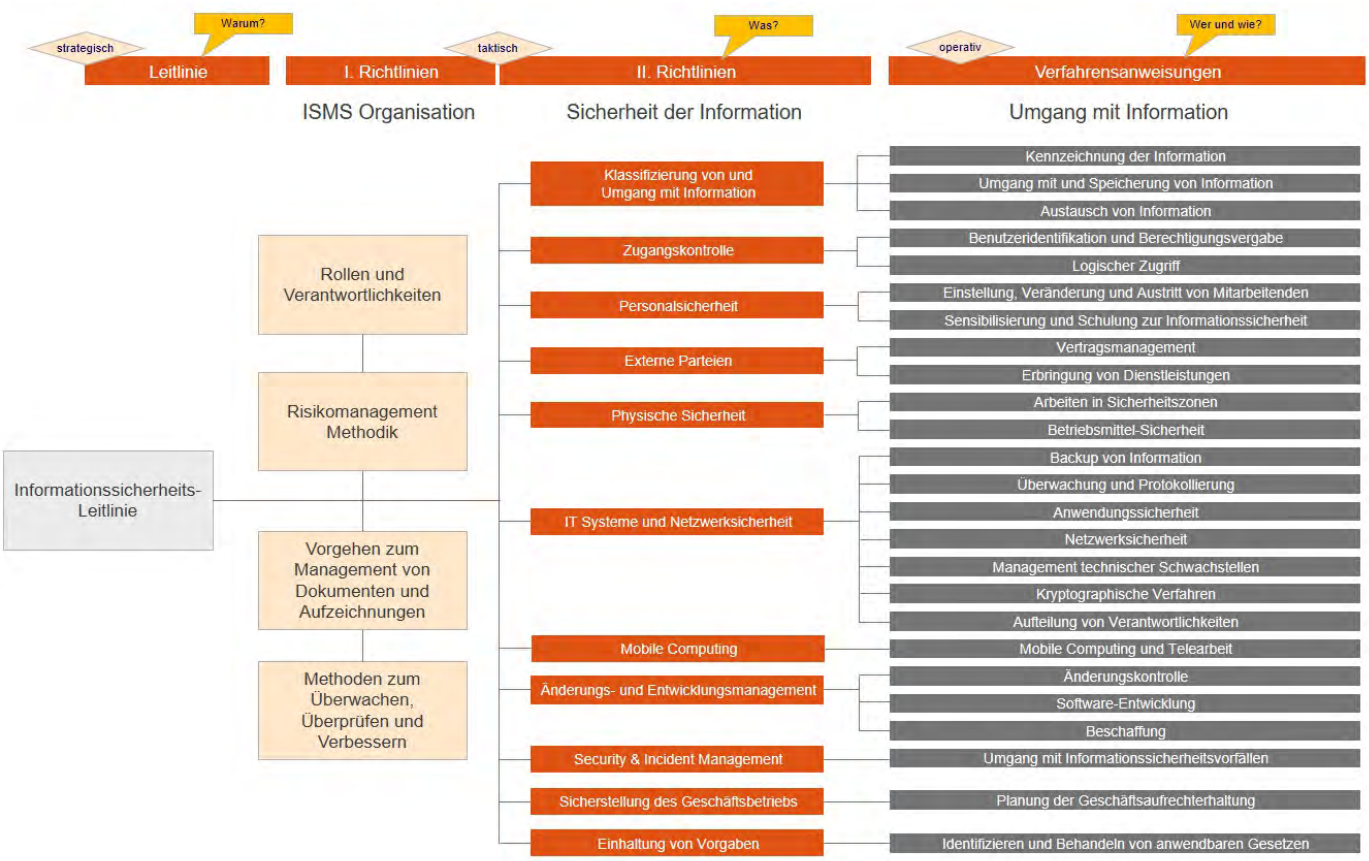
In diesem Arbeitsschritt wird die Organisation analysiert, in der das ISMS betrieben werden soll. Dies geschieht zielführend auch anhand einer Checkliste. Die zu untersuchenden Punkte werden mittels Interviews oder Workshops zusammengetragen. Dabei sollen folgende Fragestellungen geklärt werden:

- Welche Organisationseinheiten im Unternehmen sollen vom ISMS künftig abgedeckt werden und welche nicht (Grenzen)?
- Welches sind die informationsverarbeitenden Prozesse und die dazu gehörigen Datenflüsse? Wo liegen diese?
- Welche externen Parteien (Drittunternehmen) sind zu berücksichtigen (Kunden, Mitarbeiter, Dienstleister, Lieferanten, Behörden, ...)
- Welche expliziten und impliziten Anforderungen und Erwartungen stellen diese Drittfirmen an die Organisation bzw. das ISMS?
- Welche externen Einflussfaktoren (u. a. rechtlich-regulatorische Vorgaben, Wettbewerbssituation, Marktstellung, Branchenspezifika) sind zu berücksichtigen?

Ein Dokumentationsrahmenwerk sollte schon frühzeitig geplant und erstellt werden. Die Dokumentationsregeln müssen Anforderungen an die Prozesse zur Erstellung, Veröffentlichung, Speicherung, Änderung, Versionierung und Entsorgung erfüllen (Revisionssicherheit). Es können dafür Content Management Systeme wie WIKIs oder strukturierte Dateiablagen genutzt werden. Auch das Tool verinice (Open Source Lösung als Einzelplatz oder Web Server Lösung) sind für die Dokumentation sehr gut geeignet.

Organisation und ISMS Geltungsbereich (Scope) definieren

Struktur eines Rahmenwerks



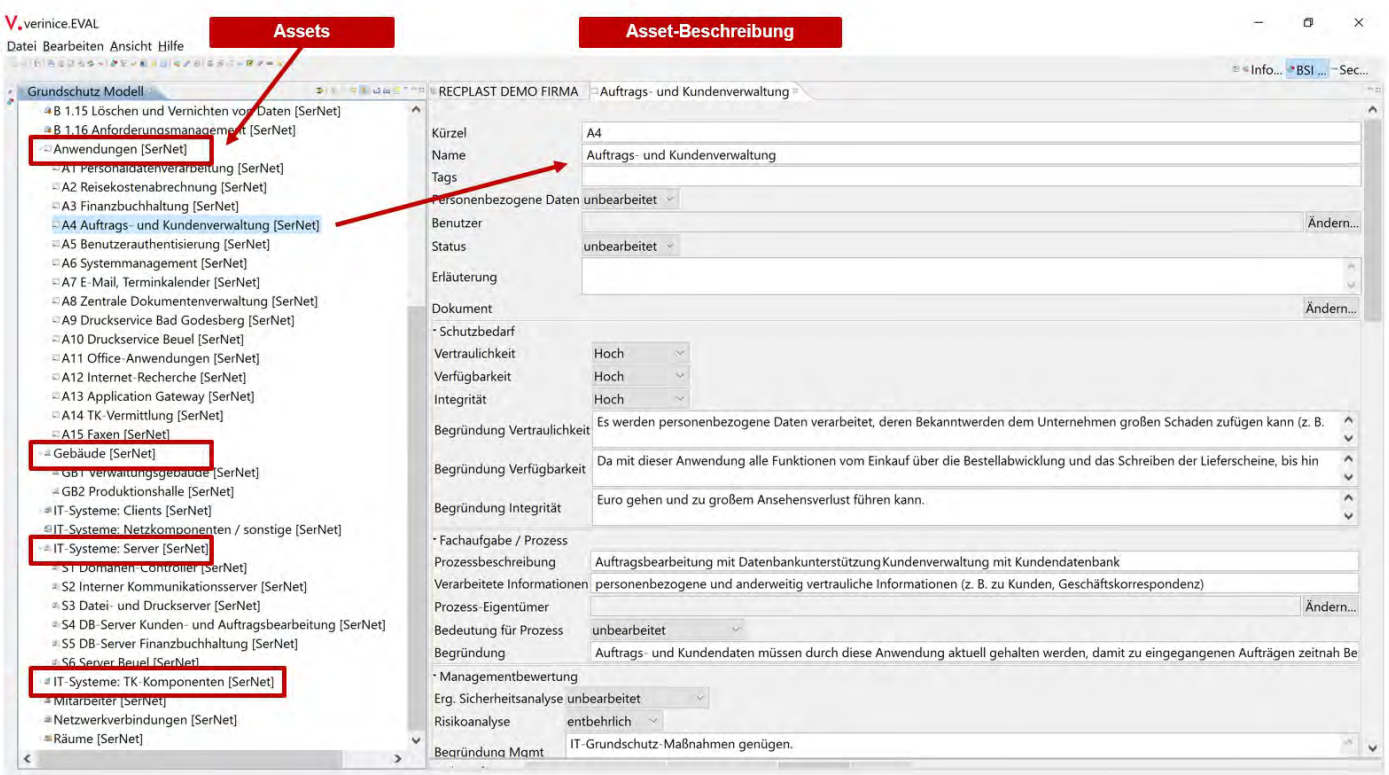
Schutzbedürftige Informationen und Assets

4. Schutzbedürftige Informationen und Assets identifizieren

In diesem Arbeitsschritt werden die schutzbedürftigen Geschäftsinformationen (primäre Assets) und die zugehörigen sekundären Assets identifiziert und erfasst. Zu den sekundären Assets zählen die informationsverarbeitenden IT-Anwendungen, Server- und Speichersysteme, Netzwerke und infrastrukturelle Einrichtungen sowie Arbeitsmittel oder auch Mitarbeiterrollen. Zum Beispiel mittels dem Tool verinice können für jedes Asset die Wirkungsketten zusammengestellt und dokumentiert werden. Welche Geschäftsinformationen im definiertem Projektrahmen (Scope) der Organisation von Bedeutung sind, ergibt sich durch Interviews mit den verantwortlichen Führungskräften.

Schutzbedürftige Informationen und Assets definieren

Open Source ISMS Tool verinice



Information Security Risikomanagement

5. Durchführung Schutzbedarfs- und Risikoanalyse

Prozesse und Assets müssen zunächst bewertet werden, damit man bestimmen kann, welches Schutzniveau für einen bestimmten Geschäftsprozess inklusive seiner zugehörigen IT-Services und sekundären Assets angemessen ist. Damit dieses Ziel erreicht werden kann, wird eine **Business Impact Analyse (BIA)** (vgl. BSI-Standard 100-4: Notfallmanagement) durchgeführt. Die Zielsetzung der Business Impact Analyse ist, die maximale Schadenshöhe durch Verletzungen der Schutzziele der Informationssicherheit innerhalb der einzelnen Geschäftsprozesse zu identifizieren. Die Schadenspotentiale müssen für jedes der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) konkretisiert werden. Die Schadenausmasse werden in den folgenden vier Kategorien ausgewiesen:

- Finanzielle Auswirkungen,
- Compliance-Auswirkungen,
- Operative Auswirkungen,
- Aussen- und Innenwirkung.

Gleichzeitig wird auch die allgemeine Risikotoleranz ermittelt, um darauf basierend die Anforderungen an den Schutzbedarf ableiten zu können.

Die Gefährdungsanalyse (Bedrohungen / Schwachstellen)

Die systematische Gefährdungsanalyse ermöglicht eine umfassende Sicht auf Bedrohungen und Schwachstellen von Assets und deren Eintrittswahrscheinlichkeit. Ausgewählte Bedrohungen und Schwachstellen werden zu Gefährdungen zusammengeführt, um eine vereinfachte Bewertungsmöglichkeit zu schaffen. Eine umfangreiche Gefährdungsliste liefern das BSI (vgl. BSI-Gefährdungskataloge) oder die ISO 27005. Für die fundierte Gefährdungsanalyse empfiehlt es sich, diese zusammen mit Experten durchzuführen, um schwierige Fragestellung durch auskunftsfähige Sicherheitsspezialisten klären zu können.

6. Risikobehandlungsplan - Massnahmen zur Risikobehandlung

Nach der Risikoanalyse wird festgelegt, wie diese Risiken zu bewältigen sind. Es erfolgt die Zuordnung der Sicherheitsmassnahmen zu Umsetzungsverantwortlichen (Risikoeigner). Es entsteht somit ein Risikobehandlungsplan. Dieser umfasst die noch zu erledigenden Sicherheitsmassnahmen, um das ISMS zu etablieren. Der Risikoeigner steuert und überwacht die Umsetzung der Sicherheitsmassnahmen bis zur Fertigstellung. Zusammen mit der Umsetzung der Sicherheitsmassnahmen kann auch das für die Zertifizierung erforderliche Statement of Applicability (SOA) fertiggestellt werden.

7. ISMS messen, steuern und Verbesserungen umsetzen

Ein für den kontinuierlichen Verbesserungsprozess (KVP) im Rahmen des ISMS anerkannter und bewährter Prozess ist der PDCA-Zyklus (mit den Phasen: Plan, Do Check, Act), der seitens der ISO hier methodisch herangezogen wird. Aus der Praxiserfahrung sei angemerkt, dass ein Zertifizierer nicht erwartet, dass alle initial ermittelten Sicherheitsmassnahmen zu einer Erstzertifizierung bereits zu 100 Prozent umgesetzt worden sind. Jedoch sind ausstehende Arbeiten nachvollziehbar zu steuern, und es sollten sich darunter keine signifikanten Sicherheitsmassnahmen befinden, die Zweifel an der systemischen Funktionsfähigkeit des ISMS aufkommen lassen (beispielsweise fehlendes oder nicht angewendetes IT Risikomanagement).

8. Ausbildung und Information Security Awareness

Die Akzeptanz und Unterstützung von Information Security Awareness bzw. IT Sicherheit durch Mitarbeitende ist keine universelle Voraussetzung. Man muss auch damit rechnen, dass sich Mitarbeiter nicht für dieses Thema interessieren. Bei Security Awareness gehen die Meinungen über die Nützlichkeit stark auseinander: Von lobenswert und nützliche Sicherheitsmassnahme bis schlichtweg Zeit- und Geld- Verschwendung. Wie schwer es ist, den Menschen zu Veränderungen im eigenen Verhalten zu bewegen kann jeder an sich selbst beurteilen. Ungeachtet dieser Tatsache, sind aber viele Unternehmen bzw. Branchen auch verpflichtet, Mitarbeitende in der sicheren und korrekten Nutzung der IT zu schulen.

RM Risk Management AG
Services Informationssicherheit und Cyber Safety

Projektleitung, Beratung, Coaching, Ausbildung

BERATUNG SEIT 1988 - NATIONAL UND INTERNATIONAL

RM Risk Management AG berät Sie integral bei der Realisierung der gewünschten Informationssicherheits- und Cyber Saftey Lösung. Wir unterstützen Sie von Anfang an durch die Weitergabe unseres in vielen Projekten und Trainings in unterschiedlichsten Branchen gewonnenen Know-hows. Sie erhalten hierbei keine Konzepte aus der Schublade, sondern individuell auf Ihr Unternehmen und Ihre Projekte abgestimmte Lösungen.

UNSERE DIENSTLEISTUNGEN FÜR VERSCHIEDENE BRANCHEN, UNTERNEHMEN UND INSTITUTIONEN

ISMS Projektleitung / Beratung

- Beratung / Coaching und Umsetzungsbegleitung zum Thema Informationssicherheit / Cyber Safety
- Projektleitung Umsetzung Informationssicherheit / Cyber Safety
- Konzeption und Organisation Informationssicherheit
- Funktionsbeschreibungen mit Aufgaben und Verantwortung
- Definition Führungskultur Informationssicherheit

ISMS AUDIT / REVIEW

- Audit / Review zum Informationssicherheit / Cyber Safety mit Optimierungsmassnahmen
- ISMS Audit / Review
- Aufzeigen der Hauptrisiken, welche zu Informationsdiebstahl, Produktions- und Business-Prozessausfällen führen können
- Unterstützung bei der Management-Motivation für die Implementierung eines Informationssicherheits-Managementsystems
- Aufbereitung und Präsentation aller notwendigen Entscheidungsgrundlagen für das Management

BERATUNG / EINFÜHRUNG ISMS OPEN SOURCE TOOL VERINICE

- Fachliche Beratung - Umsetzung Informationssicherheit mit verinice.
- Beratung / Einführungsunterstützung Open-Source ISMS-Tool verinice für das Informationssicherheits-Managementsystem
- Unterstützung bei der Umsetzung von Informations-sicherheit und Datensicherheit Projekten im Zusammenhang mit der Zertifizierung nach ISO 27001
- Beratung / Unterstützung bei der Erarbeitung der notwendigen ISMS Dokumente.

ISO 27001 INFORMATIONSSICHERHEIT ZERTIFIZIERUNG / COACHING

- Beratung / Umsetzungsbegleitung Informationssicherheits-Management bis zur Zertifizierungsreife nach ISO 27001
- Coaching Informationssicherheits-Management bis zur Zertifizierungsreife nach ISO 27001
- Überprüfung / Standortbestimmung der noch fehlenden Elemente bis zur Zertifizierungsreife nach ISO 27001

IT RISIKOMANAGEMENT / IT RISIKOANALYSE

- Überprüfung/ Review der bestehenden IT Risikomanagement / IT Risikoanalyse Methodik
- Aufzeigen von Optimierungspotentialen für das IT Risikomanagement
- Vorbereitung und Einführung einer optimierten Methode / Verfahren zur systematischen und einheitlichen IT Risikobewertung
- Neutrale Beratung / Coaching und Umsetzungsbegleitung im Umgang mit IT Sicherheits- und Risikoinvestitionen
- Aufzeigen der Hauptrisiken für das IT Management als Basis für künftige Sicherheitsinvestitionen
- Coaching der Geschäftsleitung in Fragen der IT Sicherheitsstrategie

Informationssicherheit, Cyber Safety, IS Risikomanagement, Cyber Krisenmanagement

Ermitteln Sie Ihren persönlichen Informationssicherheit / Cyber Safety Reifegrad.

Wir bringen Ihre Informationen in Sicherheit

Sytematisch, effizient und professionell

CYBER KRISENMANAGEMENT IT NOTFALLHANDBUCH UND RECOVERY MANAGEMENT

- Beratung / Coaching bei der Integration des Cyber Krisenmanagements in das Krisenmanagement des Unternehmens
- Erarbeitung Cyber Krisenmanagement (Konzeption und Organisation mit allen notwendigen Führungsdokumenten)
- Grundausbildung / Schulung der Mitglieder im Cyber Krisenmanagement
- Vorbereitung, Durchführung und Auswertung von IT Krisenstabsübungen
- IT Notfallhandbuch und Recovery Management

KRITISCHE INFRASTRUKTURSYSTEME - BUSINESS CONTINUITY MANAGEMENT UND RESILIENZ

- Unterstützung KRITIS-Betrieber im Rahmen Betriebskontinuitätsfragen
- Asset Risikoanalyse
- Business Impact Analyse
- Standort-Audits mit Fokus Ausfallrisiken (baulich, technisch, organisatorisch)
- Business Continuity Management
- Business Continuity Strategien
- Business Continuity Pläne
- Wiederanlaufverfahren für kritische Anlagen

IT SICHERHEITSGESETZ - IDENTIFIZIERUNG UND UMSETZUNG VERPFLICHTENDER MASSNAHMEN

- KRITIS-Betroffenheitsanalyse
- Identifizierung und Umsetzung verpflichtender Massnahmen
- Umsetzung Branchenstandards
- IT Risikomanagement
- Informationssicherheitsmanagementsystem (ISMS)
- Begleitung bis zur Zertifizierung

SCADA / ICS SECURITY / BUSINESS CONTINUITY UND RESILIENZ

- Audit / Review ICS Security
- Beratung / Coaching und Umsetzungsbegleitung zum Thema Business Continuity Management
- OptiRisk Business Continuity Management (Tool Umsetzung)
- Konzept Business Continuity Management
- Organisation Business Continuity Management (BCM)
- BCM Funktionsbeschreibungen mit Aufgaben und Verantwortung
- Definition BCM Führungskultur und Strategie
- Business Continuity Pläne (PCP) für die Prozess Eigner
- Erstellung aller notwendigen BCM Führungsdokumente für die Prozess Eigner
- Integration des Krisenmanagements in das Business Continuity Management

Kontakt

RM Risk Management AG
Security & Risk Managment Consultants
Hertistrasse 25
CH-8304 Wallisellen
Tel. +41 (0)44 360 40 40
rm@rmrisk.ch
www.information-security-informationssicherheit.com

Informationssicherheit, Cyber Safety, IS Risikomanagement, Cyber Krisenmanagement

Ermitteln Sie Ihren persönlichen Informationssicherheit / Cyber Safety Reifegrad.

Risk Management

Security & Risk Management Conultants

RM Risk Management AG
Security & Risk Management Consultants
Hertistrasse 25
CH-8304 Wallisellen
Tel. +41 (0)44 360 40 40
rm@rmrisk.ch
www.information-security-informationssicherheit.com

innovation & consistency | since 1988

Mitglied SSI Schweizerische Vereinigung von unabhängigen Sicherheitsingenieuren und -beratern