Informationstag "IT-Sicherheit in der Marktforschung"

Gemeinsame Veranstaltung von

Bundesverband IT-Sicherheit e.V.

Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.

Deutsche Gesellschaft für Online Forschung e.V.

Verband der Marktforscher Österreichs

10.06.2016

Wirtschaftskammer Wien, Blauer Saal, Schwarzenbergplatz 14, 1010 Wien

Informationstag "IT-Sicherheit in der Marktforschung"

Management und Zertifizierung der Informationssicherheit in den Marktforschungsinstituten

Adrian Altrhein

TÜViT®

TÜViT – Ein starker Partner an Ihrer Seite

Sicherheit auf allen Ebenen – objektiv, neutral, unabhängig

Common Criteria

IT-Grundschutz

ISO 27001

Web Application Security

De-Mail

IT Security

Cyber Security

Security Lab

Smart Grid

Biometrie

RZ-Sicherheit

Penetration Testing

FIPS-140-2

ISO 22301

Netzwerksicherheit

Automotive Security

Mobile Security

Vorwort

„Wenn Du tust,

was Du immer getan hast,

wirst Du bekommen,

was Du immer bekommen hast.“

Abraham Lincoln
(1809-1865)
amtierte von 1861 bis 1865 als 16. USA-Präsident

Gliederung

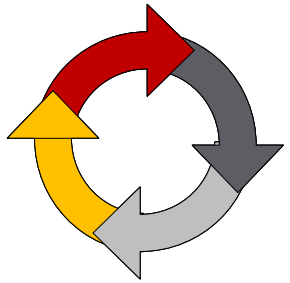
- Informationssicherheit als Prozess, ISMS
- ISO 27000ff.
- BSI-Standards 100 / IT-Grundschutz
- ISMS-Auditierung und Zertifizierung

Gliederung

- Informationssicherheit als Prozess, ISMS
- ISO 27000ff.
- BSI-Standards 100 / IT-Grundschutz
- ISMS-Auditierung und Zertifizierung

Informationssicherheit als Prozess

- **Sicherheit ist kein Produkt!**
  - Sicherheit kann man nicht kaufen, Sicherheit muss man schaffen!
  - Natürlich muss man zum Schaffen von Sicherheit auch auf vorhandene Produkte zurückgreifen.
- **Sicherheit ist kein Projekt!**
  - Es genügt nicht, Sicherheit einmal zu schaffen, sondern Sicherheit muss aufrecht erhalten werden!
  - Natürlich kann man Aufbau und Aufrechterhaltung von Sicherheit auch teilweise in Projekten abwickeln.
- **Sicherheit ist ein Prozess…**
  - der definiert, implementiert, überwacht und überprüft, aufrechterhalten und kontinuierlich verbessert werden muss **(P-D-C-A-Modell)**!



Informationssicherheits-Management

- Informations- und Kommunikationseinrichtungen sind nicht grundsätzlich auf Sicherheit hin ausgelegt.
- Die technisch erzielbare Sicherheit ist begrenzt!

- Notwendig:
  - System von Verfahren, Prozeduren und Regeln zum Management der betrieblichen Informationssicherheit:
  - **Informationssicherheits-Managementsystem (ISMS)**

Informationssicherheits-Management – Definition

- Ein ISMS ist in erster Linie ein Managementsystem
- Dient dem Schutz von Informationen als Werte
- Kombiniert Dokumentenlandschaft, Verhaltensanweisungen, gelebte Praxis

- Der Informationssicherheits-Prozess (IT-Sicherheitsprozess) ist vornehmlich ein („Geschäfts“)prozess, nur untergeordnet ein IT-Prozess

- „[Ein] ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).“

(*Quelle: BSI Standard 100-1)*

Informationssicherheits-Management – Aktivitätsebenen

- Der **Aufbau eines ISMS** erfordert strukturierte und koordinierte Aktivitäten auf mehreren Ebenen:
  - **IS-Prozess** (Ablauforganisation der IS)
  - **IS-Organisation** (Aufbauorganisation der IS)
  - **IS-Konzept** (konkrete Ausgestaltung der IS)

- Ein ISMS kann nur dann im Sinne einer Institution aufgebaut werden, wenn es im Einklang mit den **Anforderungen** an die Institution und seine Sicherheit sowie mit dem konkreten **Risikoumfeld** der Institution aufgebaut ist.

  → **ANFORDERUNGSMANAGEMENT**

  → **RISIKOMANAGEMENT**

Gliederung

- Informationssicherheit als Prozess, ISMS
- ISO 27000ff.
- BSI-Standards 100 / IT-Grundschutz
- ISMS-Auditierung und Zertifizierung

Informationssicherheits-Management nach ISO 27001 – Methodischer Ansatz

- Internationale Norm zur Implementierung von IT-Sicherheitsverfahren
- Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität
- Spezifiziert die Anforderungen an ein dokumentiertes ISMS, hinsichtlich: Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung
- Ein ISMS unterliegt stets der Dynamik relevanter Anforderungen und bedarf einer kontinuierlichen Anpassung und Verbesserung
- Design und Implementierung eines ISMS hängen ab von
  - den Geschäftsbedürfnissen und -Zielen,
  - den daraus resultierenden Verfahren und Prozessen sowie von
  - der Größe und Struktur der Organisation
- Maßnahmen an Gegebenheiten der Organisation adaptieren
- „Einfache Situationen → einfache Lösungen“

Informationssicherheits-Management nach ISO 27001 – Wichtigste Standards der Normenreihe ISO 27000ff.

- ISO 27000 Management von Informationssicherheit – Übersicht und Begriffe
- ISO 27001 Management von Informationssicherheit – Anforderungen
  → **ausschließliche Grundlage für eine Zertifizierung**
- ISO 27002 Leitfaden zum Management von Informationssicherheit (Umsetzung von Controls)
- ISO 27003 Leitfaden zu Implementierung eines ISMS (Umsetzung des Managementrahmens)
- ISO 27004 Leitfaden zu Messung der Wirksamkeit von ISMS und Controls
- ISO 27005 Leitfaden zum Management von Informationssicherheitsrisiken

Informationssicherheits-Management nach ISO 27001 – Weitere Standards der Normenreihe ISO 27000ff.

ISO 27000 – Management von IS – Übersicht und Begriffe

ISO 27001 - Management von IS – Anforderungen

ISO 27002 - Leitfaden zum Management von IS

ISO 27003 - Leitfaden zu Implementierung eines ISMS

ISO 27004 - Leitfaden zu Messung der Wirksamkeit ISMS, IS

ISO 27005 - Leitfaden zum Management von IS-Risiken

ISO 27006 - Zertifizierungsstellen Anforderungen

ISO 27007 - Auditierung von ISMS (Managementrahmen)

ISO 27008 - Auditierung von ISMS (Maßnahmen des Anhang A)

ISO 27009 - ISO/IEC 27001 für industriespezifische Audits

ISO 27010 - ISM für Kommunikation zwischen Organisationen

ISO 27011 - ISMS für Telekommunikationsunternehmen

ISO 27799 - Leitfaden für das Gesundheitswesen

ISO 27013 – Integriertes MS: ISO 20000-1 u. ISO 27001

ISO 27014 - Steuerung der Informationssicherheit

ISO 27015 - ISMS für den Finanzsektor (Banken etc.)

ISO 27016 - Wirtschaftlichkeit der Informationssicherheit (TR)

ISO 27017 - Leitfaden für Cloud Computing

ISO 27018 - Leitfaden für Informationssicherheit bei Public Cloud Services

ISO 27019 - ISM für Energieunternehmen

ISO 27031 - Business Continuity für Informations- und Kommunikationstechnologie

ISO 27032 - Cybersecurity (Virtuelle Maschinen und Netzwerke, Cloud Computing, ...)

ISO 27033 - IT Netzwerksicherheit

ISO 27034 - Applikationssicherheit

ISO 27035 - Sicherheitsvorfallmanagement

ISO 27036 - Sicherheit beim Outsourcing

ISO 27037 - Digitale Beweisführung

ISO 27038 - Digitale Dokumentenredaktion

ISO 27039 - Auswahl, Implementierung und Betrieb von Intrusion Detection Systemen

ISO 27040 - Speichersicherheit

ISO 27041 - Untersuchungsmethoden

ISO 27042 - Analyse Digitaler Beweise

ISO 27043 - Untersuchungsprozesse

ISO 27044 - SIEM Security Information Event Mgmt.

Informationssicherheits-Management nach ISO 27001 – Gliederung der ISO 27001

Grundlagen

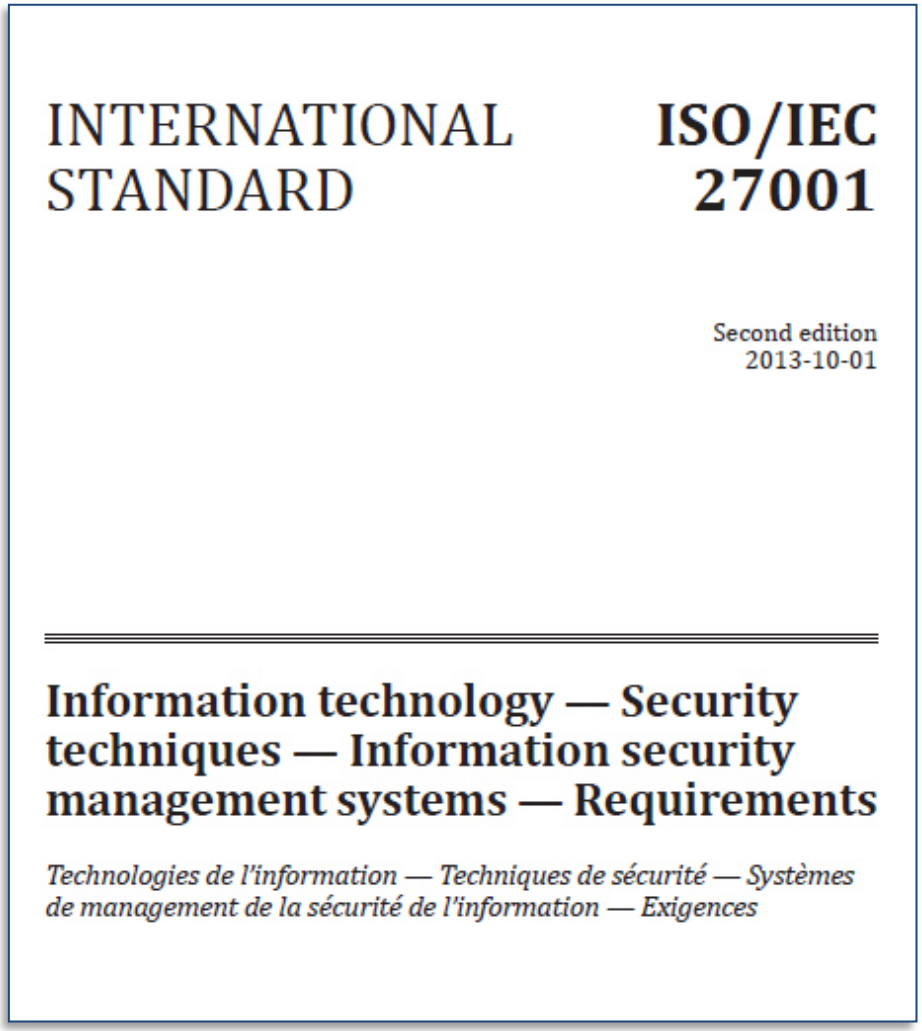
0. Einleitung
1. Anwendungsbereich
2. Normative Referenzen
3. Begriffe und Definitionen

Managementrahmen

4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Einsatz
9. Leistungsauswertung
10. Verbesserung

Maßn.K.

Anhang A:
Referenz-Maßnahmenziele und Maßnahmen


INTERNATIONAL STANDARD

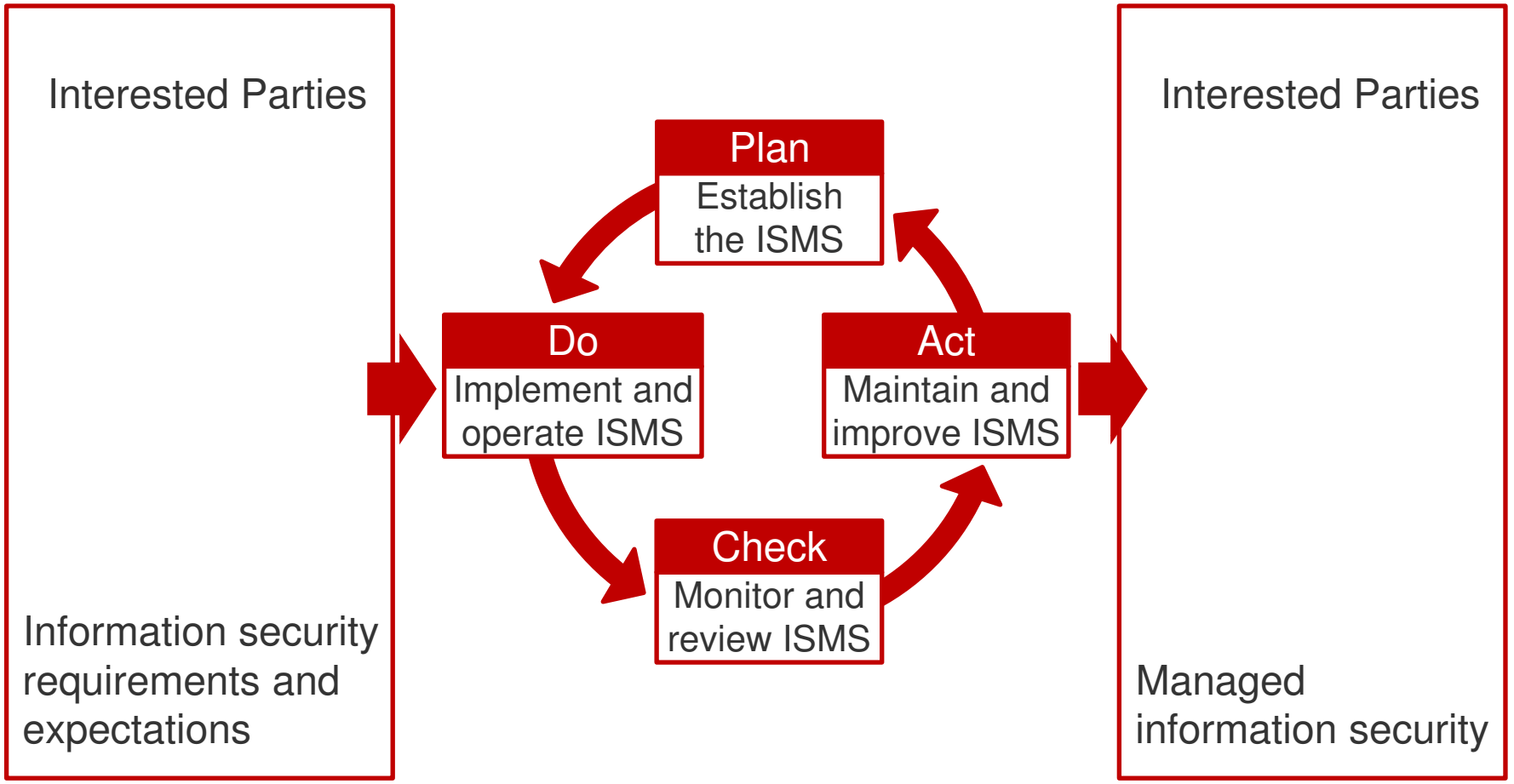
ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

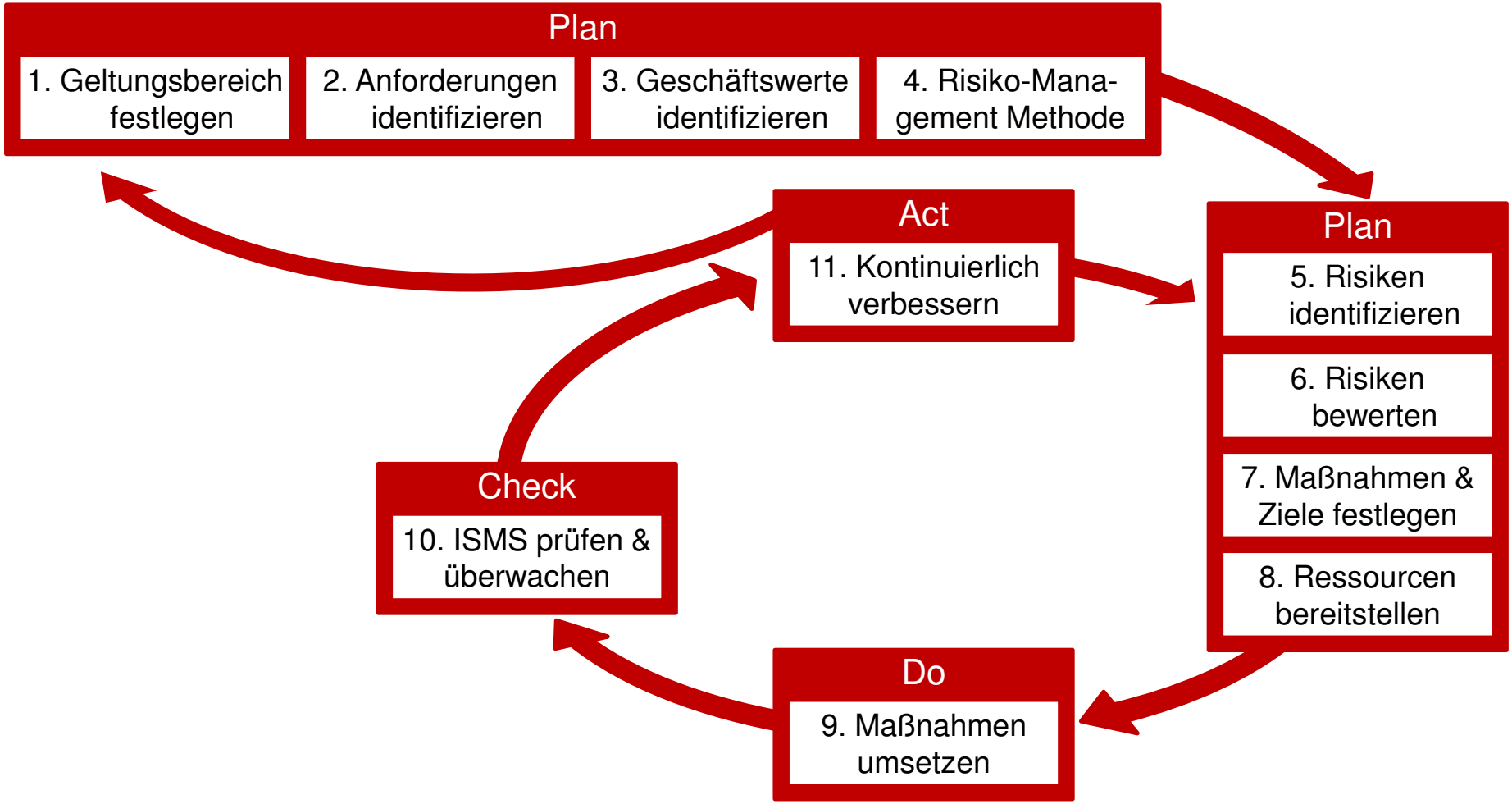
Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Informationssicherheits-Management nach ISO 27001 – Prozessansatz der ISO 27001



Grafik nicht mehr in der 2013er-Version enthalten

Informationssicherheits-Management nach ISO 27001 – Erweiterter PDCA-Zyklus



Informationssicherheits-Management nach ISO 27001 – Maßnahmenkatalog: ISO 27001, Anhang A

- A.5 Sicherheitsleitlinie
- A.6 Organisation der Informationssicherheit
- A.7 Personalsicherheit
- A.8 Management von organisationseigenen Werten
- A.9 Zugriffskontrolle
- A.10 Kryptographie
- A.11 Physische und umgebungsbezogene Sicherheit
- A.12 Betriebssicherheit
- A.13 Kommunikationssicherheit
- A.14 Systembeschaffung, -entwicklung und -wartung
- A.15 Lieferantenverhältnis
- A.16 Umgang mit Informationssicherheitsvorfällen
- A.17 Sicherstellung des Business Continuity Management
- A.18 Einhaltung von Vorgaben (Compliance)

Informationssicherheits-Management nach ISO 27001 – Formulierung der Controls in ISO 27001, Anhang A (Beispiel)

A.5	**Information security policies**	
A.5.1	**Management direction for information security**	
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6	**Organization of information security**	
A.6.1	**Internal organization**	
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Informationssicherheits-Management nach ISO 27001 – Formulierung der Controls in ISO 27002 (Beispiel)

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

Gliederung

- Informationssicherheit als Prozess, ISMS
- ISO 27000ff.
- BSI-Standards 100 / IT-Grundschutz
- ISMS-Auditierung und Zertifizierung

Informationssicherheits-Management nach IT-Grundschutz – Methodischer Ansatz

- Interpretation einer bewährten Methode für die Planung und Überprüfung von Informationssicherheit in Organisationen jeder Größe
- Im Kern steht die effektive und effiziente Umsetzung eines ISMS sowie dessen überprüfbare Wirksamkeit
- BSI-Standards enthalten Sicherheits-Empfehlungen des BSI zu Methoden, Verfahren und Prozessen
- Grundschutz-Kataloge enthalten konkrete Hinweise zur Umsetzung bewährter Standardsicherheitsmaßnahmen
- Trotz sehr detaillierten Vorgaben zur Umsetzung besteht in der Praxis immer Gestaltungsspielraum, der auch genutzt werden sollte!

Informationssicherheits-Management nach IT-Grundschutz – BSI-Standards und Regelwerke

BSI-Standards zur Informationssicherheit
Informationssicherheit und IT-Grundschutz

BSI-Standard 100-1
Managementsysteme zur generellen Initiierung uns Steuerung der Informationssicherheit

BSI-Standard 100-2
IT-Grundschutz-Vorgehensweise mit konkreter methodischer Hilfestellung zur ISMS-Einführung

BSI-Standard 100-3
Vereinfachte Vorgehensweise zur Risikoanalyse auf Basis der Gefährdungskataloge

BSI-Standard 100-4
Notfallmanagement
(Business Continuity Management)

IT-Grundschutzkataloge
Loseblattsammlung und Internet

Kapitel 1 Einleitung
Kapitel 2 Schichtenmodell und Modellierung

Bausteinkataloge
- Übergreifende Aspekte
  - B 1.0 Sicherheitsmanagement
  - ...
- Infrastruktur
- IT-Systeme
- Netze
- Anwendungen

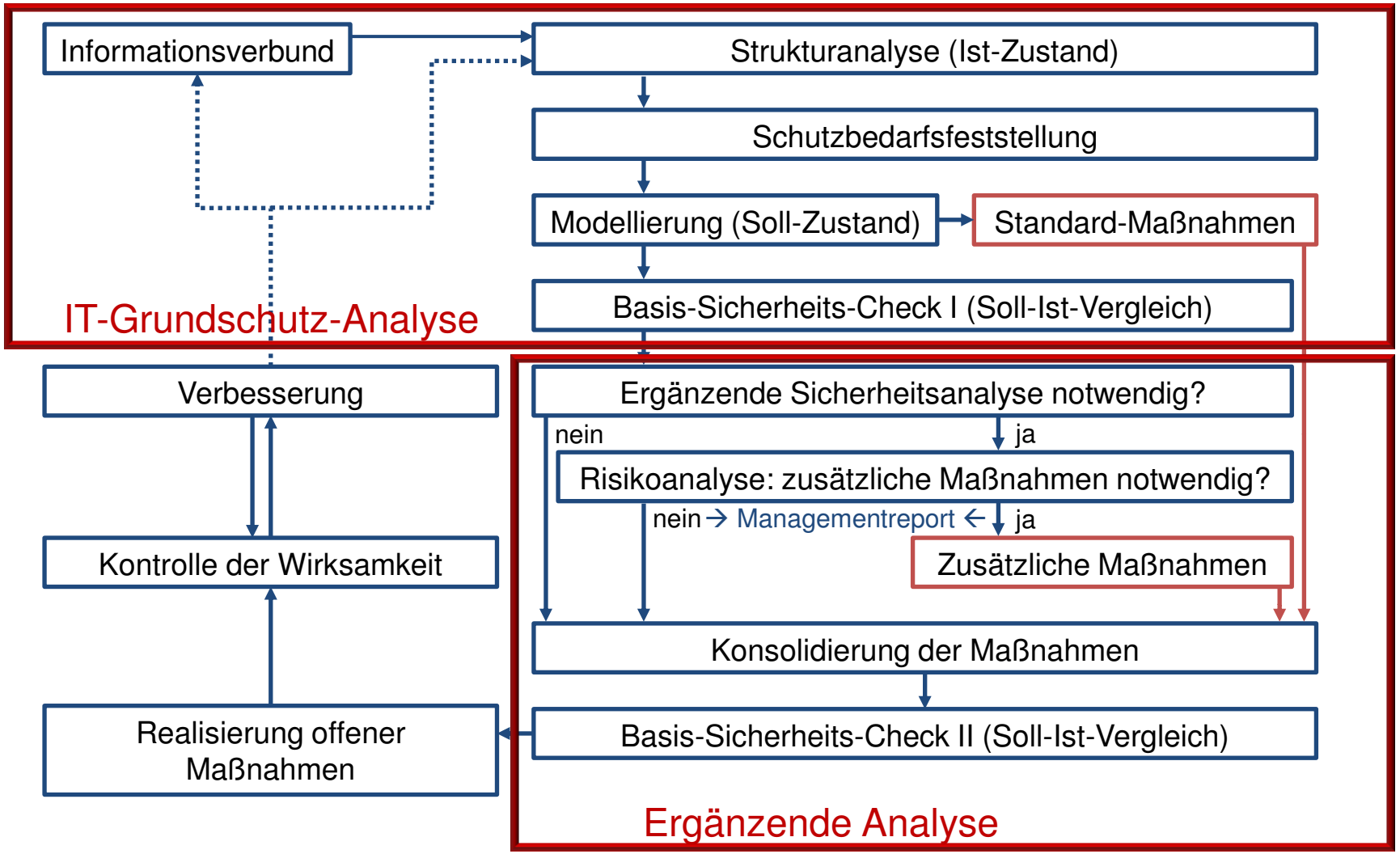
Gefährdungskataloge

Maßnahmenkataloge

Informationssicherheits-Management nach IT-Grundschutz – Bausteinkataloge

- Kern der IT-Grundschutzkataloge, sind alle gleich gegliedert:
  - Kurzbeschreibung:
    Beschreibung und Abgrenzung des betrachteten Gegenstandes
  - Gefährdungslage:
    Gefährdungen, denen der beschriebene Gegenstand ausgesetzt ist
    (ohne Berücksichtigung von Eintrittswahrscheinlichkeiten)
  - Maßnahmenempfehlungen (orientiert am Lebenszyklusmodell)
    Erläuterung von Maßnahmen, um den Gefährdungen zu begegnen
- Bausteine gegliedert in Schichtenmodell
  - B1: Übergreifende Aspekte → organisatorische Aspekte ges. Inf.-Verb.
  - B2: Infrastruktur → baulich-technisch, physischer Schutz
  - B3: IT-Systeme → Sicherheitsaspekte von IT-Systemen
  - B4: Netze → Hinweise zur Netz-Administration
  - B5: Anwendungen → Sicherheitsaspekte von Anwendungen

Informationssicherheits-Management nach IT-Grundschutz – Prozessschritte der Implementierung



Informationssicherheits-Management
ISO 27001 vs. Grundschutz

	ISO 27001	Grundschutz
Regulatorischer Umfang	relevante Normen < 100 Seiten	Grundschutz-Kataloge > 4.000 Seiten
Anforderungen	Abstrakte und generische Rahmenbedingungen	Konkrete Vorgaben praktischer Maßnahmen
Risikoanalyse	Vollständige Analyse jedes Zielobjektes	Vereinfachte Analyse bei erhöhtem Schutzbedarf
Maßnahmen	ca. 150 konzeptionelle Anforderungen	> 1.100 konkrete Maßnahmen
Zertifizierung	Zertifizierung	Auditor-Testate + Zertifizierung
Gültigkeit	3 Jahre, jährliche Überwachungsaudits	3 Jahre, jährliche Überwachungsaudits

Gliederung

- Informationssicherheit als Prozess, ISMS
- ISO 27000ff.
- BSI-Standards 100 / IT-Grundschutz
- ISMS-Auditierung und Zertifizierung

Definition und Ziele eines Audits

Definition

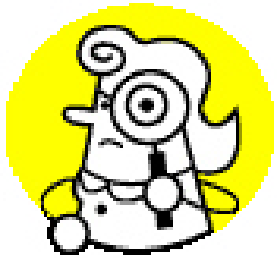
- Analyse des Ist-Zustandes des ISMS

Ziele

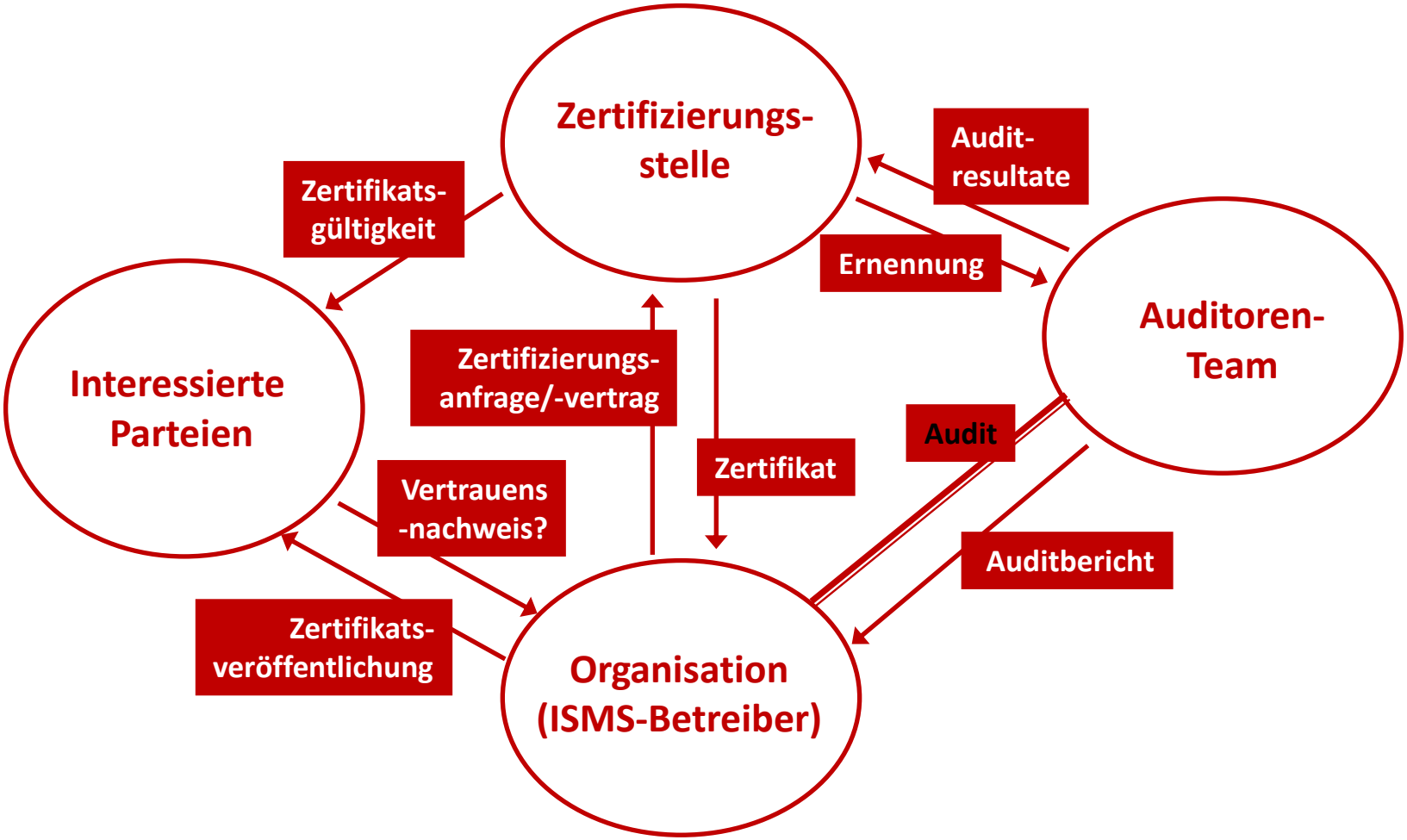
- Prüfung des Fortschritts der Implementierung des ISMS
- Ermittlung des Grades der Erfüllung anwendbarer Anforderungen an das ISMS
- Prüfung der Anwendung und Wirksamkeit des ISMS
- Identifikation von Sicherheitsschwachstellen
- Feststellung von Verbesserungspotenzial für das ISMS

Klassifizierung von Audits hinsichtlich der Unabhängigkeit des Auditors

- 1st Party Audit (intern)
  Auditierende Instanz gehört zur Organisation, in der das Audit durchgeführt wird
- 2nd Party Audit (extern)
  von Kunden-, Partner- oder Beratungsunternehmen durchgeführt
- 3rd Party Audit (unabhängig, neutral, objektiv)
  von einer unabhängigen Auditierungsinstanz durchgeführt (bspw. von den Auditoren einer akkreditierten Zertifizierungsstelle, im Rahmen eines regulären Zertifizierungsverfahrens)

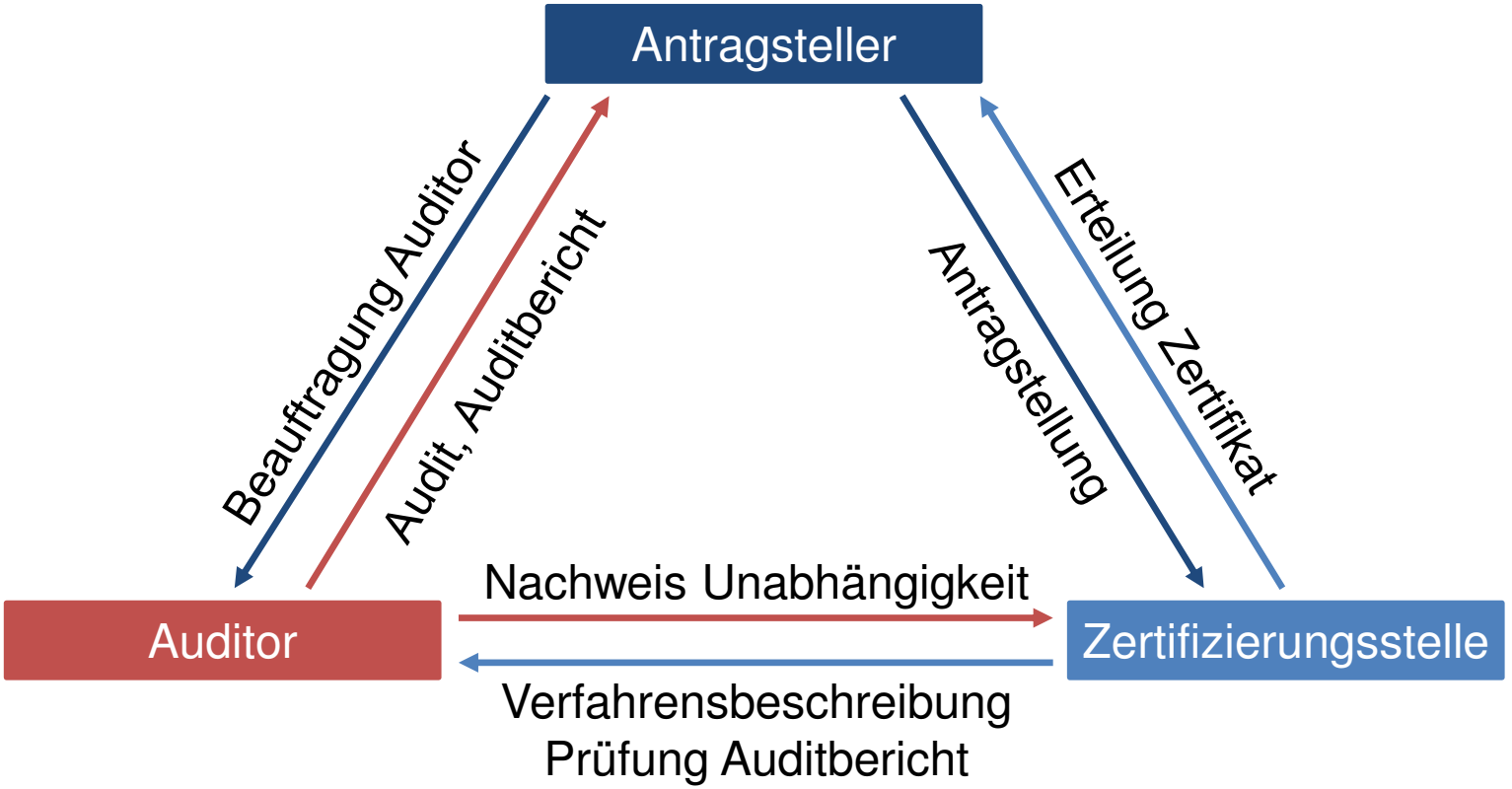


ISO/IEC 27001 – Zertifizierungsverfahren



ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsverfahren

Bundesamt für Sicherheit in der Informationstechnik



ISMS – Kritische Erfolgsfaktoren

- Verankerung in der Business Perspektive des Unternehmens
- Klare und verbindliche Unterstützung durch die Geschäftsführung (als Auftraggeber und Förderer des ISMS)
- Einführung in Übereinstimmung mit der Unternehmenskultur
- Angemessene Sensibilisierung und Know-how-Bildung
- Durchsetzung der „Spielregeln“ gegenüber allen leitenden Angestellten, Mitarbeitern und Geschäftspartnern
- Gut funktionierende Anforderungs- und Risikomanagement
- Verfahren und Metriken zur Bewertung der Leistungsfähigkeit des Informationssicherheits-Managementsystems (ISMS)
- Tool-Unterstützung

ISMS – Integrationspotenzial mit weiteren Managementsystemen

- ISO 9001 Qualitätsmanagementsysteme
- ISO 14001 Umweltmanagementsysteme
- OHSAS 18001 Arbeits- und Gesundheitsschutz
- ISO 20000-1 IT-Service-Managementsysteme
- ISO 22301 Business Continuity Managementsysteme
- ISO 28000 Sicherheitsmanagementsysteme für Lieferketten
- ISO 31000/ ÖNR 49001 Risikomanagementsysteme
- …

Lessons learned – Use case 1
ISMS als tatsächlich wahrgenommene Chance

Wenn die Botschaft der ISO (P–D–C–A, Prozessdenken, starke Managementeinbindung) in einer Organisation einmal angekommen ist, ergeben sich:

- systematische und wirtschaftlich ausgelegte Informationssicherheit → Risikobegrenzung
- Kontinuität im Umgang sowie Optimierung der Informationssicherheit
- erhöhte Konformität mit
  - Informationssicherheitszielen und –politik
  - Anforderungen und Erwartungen → Compliance
- Entlastung der Leitungsebene sowie der Mitarbeitern in IS-relevanten Positionen von Haftungsrisiken!

Lessons learned – Use case 2
ISMS als Alibi (so tun als ob…)

Wenn nicht:

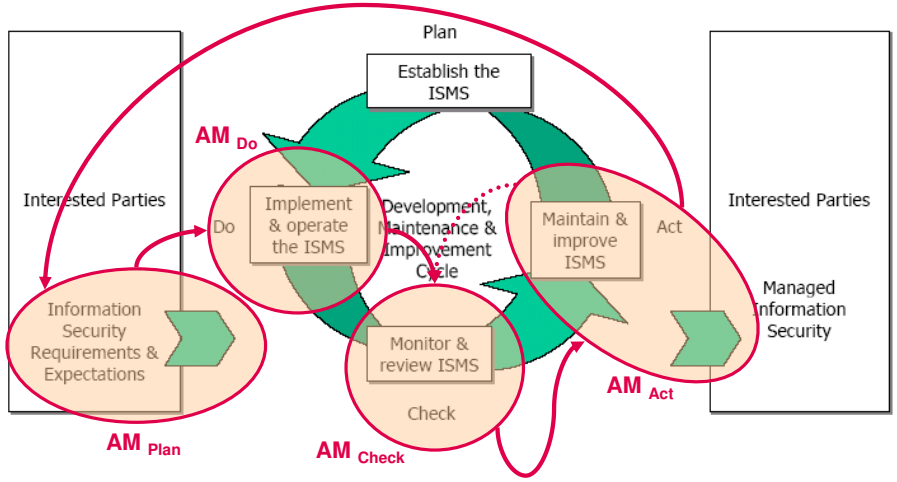
- Fatale Missachtung der Gegebenheiten (Ziele, Anforderungen, Risiken usw.) der Organisation
- keine Bewertung der Notwendigkeit & Angemessenheit
- Anforderungen und Risiken höchstens „pro forma“ betrachtet
- Chancen durch Verzahnung von Sicherheit und Geschäft/Aufgabe kaum wahrgenommen
- Identität der Organisation (Unternehmen/Behörde) mit ihren tatsächlichen Zielen, Aufgaben, Prozessen, Geschäftsmodell, Anforderungen, Erwartungen und Risiken ist im ISMS kaum erkennbar → ISMS der Marke „08/15“ (nicht „authentisch“)
- Compliance bleibt meistens eine Worthülse… ☹

So nicht!

Fazit

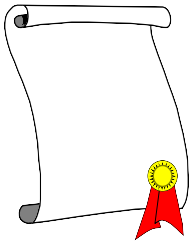
Nur gewollte, gekonnte und gelebte ISMSs garantieren

- die Beherrschung von Informationsrisiken und
- ein ausreichendes Maß an eCompliance



Zertifikate helfen nur dann wirklich,

- wenn sie kein Selbstzweck sind und
- wenn die damit verbundenen Anstrengungen Ihrem Unternehmen auf Dauer dienen.



TÜViT – Einfach durchstarten!
Unterstützung auf allen Ebenen

Trainings für Führungskräfte und Mitarbeiter

Überwachung und Unterstützung in allen ISMS-Phasen

Vertrauensbildung durch externe Überprüfungen

informationen aus erster Hand zu aktuellen Entwicklungen

Transfer von Know-how für den IT-Sicherheitsbeauftragten

Alles klar? Noch offene Fragen?

Vielen Dank für Ihre Aufmerksamkeit…
… und viel Erfolg!

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD

Dipl.-Ing. Adrian Altrhein
Senior Director Business Consulting

Langemarckstr. 20
45141 Essen

Telefon: +49 271 3378 – 195 / +49 1608885195
E-Mail: a.altrhein@tuvit.de
URL: www.tuvit.de