Gesellschaft für Informatik
Fachgruppe Management von Informationssicherheit (SECMGT)
Workshop: Der Wert von Zertifizierungen

Informationssicherheit
Überblick über Standards und Zertifizierung

07. Juni 2013, Frankfurt

dubois it-consulting gmbh, Holzhofstr. 10, 55116 Mainz, ☎ +49 6131 2150691 oder ☎+49 177 4104045, ✉ ingrid.dubois@dubois-it-consulting.de

dubois it-consulting gmbh

Agenda

- Einleitung
- Überblick über Standards
- Anforderungen aus Standards
- (Zertifizierungs-)Audit
- Zertifikat

Einleitung - Definitionen

- **Standard**
  Ein vereinheitlichtes, i.a. anerkanntes und etabliertes Vorgehen, wie etwas hergestellt oder durchgeführt wird.
  Ein Standard ist ein öffentlich zugängliches Dokument, das unter Beteiligung aller interessierter Parteien entwickelt wird und deren Zustimmung findet.

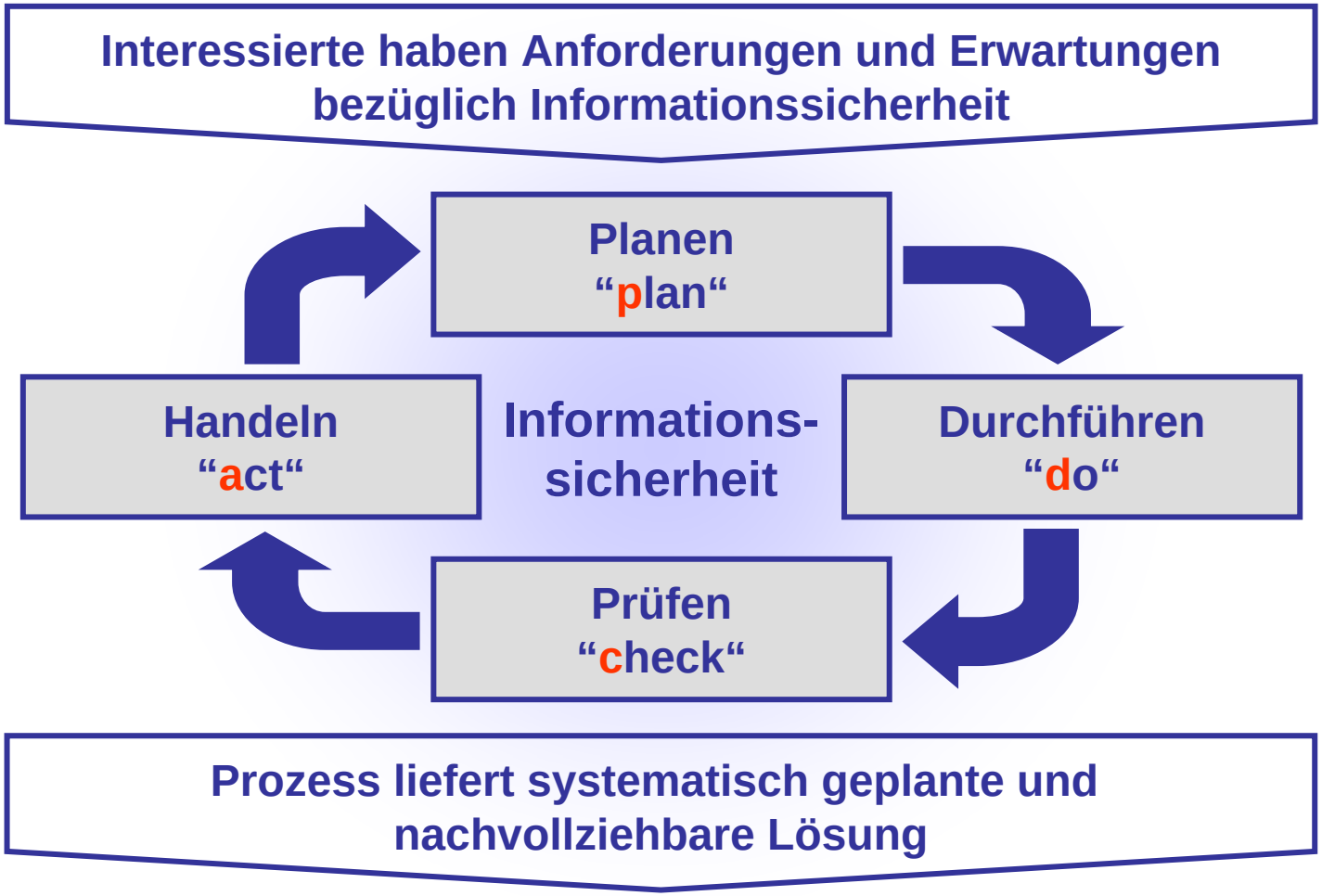
- **Norm**
  Ein anerkanntes Vorgehen bzw. Festlegung, das/die durch ein festgelegtes Normungsverfahren beschlossen wurde.

- **Zertifizierung**
  Ein festgelegtes Verfahren, mit dessen Hilfe die Einhaltung bestimmter Anforderungen nachgewiesen wird.

- **Zertifikat**
  Ein Nachweis einer Qualifikation oder Qualität.

PDCA-Prozessmodell angewandt auf ISO/IEC 27001

Ein System zur Planung, Implementierung, Kontrolle und Steuerung (PDCA). Es umfasst Struktur, Grundsätze, Planungsaktivitäten, Verantwortungen, Verfahren, Prozesse, Ressourcen.



Standards zum Informations-/IT-Sicherheitsmanagement

- **ISO/IEC 27000er-Serie**
  - **ISO/IEC 27000:2012** Overview and vocabulary
  - **ISO/IEC 27001:2005** Information security management systems – Requirements
    Informationssicherheits-Managementsysteme – Anforderungen
  - **ISO/IEC 27002:2005** Code of practice for information security management
    Leitfaden für das Informationssicherheits-Management
  - **ISO/IEC 27003**:2010 ISMS implementation guidance
  - **ISO/IEC 27004**:2009 Information security management - Measurement
  - **ISO/IEC 27005**:2011 Information security risk management
  - **ISO/IEC 27006**:2011 – Accreditation requirements
  - ….
  - **ISO/IEC 27011**:2008 - .. guidelines for telecommunications organizations
  - …
  - **ISO/IEC 27033:2009** – Network security (consists of several parts)
  - …

Weitere Sektor-, Branchen-, und/oder Aufgaben-spezifische Standards sind verfügbar bzw. in Vorbereitung. Z.B:

- Guidelines for ISMS auditing
- ISM guidelines for e-government services
- ICT readiness for business continuity
- Guidelines for application security
- Information security incident management
- …

Die Standards werden in Englisch geschrieben und veröffentlicht. Einige werden von den nationalen Normungsgremien in die Landessprache übersetzt.

Standards zum Informations-/IT-Sicherheitsmanagement

ISO 27001 auf der Basis von IT-Grundschutz (BSI)

- **BSI-Standards**
  - **BSI Standard 100-1**
    Managementsysteme für Informationssicherheit (ISMS)
  - **BSI Standard 100-2**
    IT-Grundschutz-Vorgehensweise
  - **BSI Standard 100-3**
    Risikoanalyse auf der Basis von IT-Grundschutz
  - **BSI Standard 100-4**
    Notfallmanagement

- **IT-Grundschutzkataloge und zugehörige Unterlagen**
  - **IT-Grundschutzkataloge**
    Baustein-, Maßnahmen-, Gefährdungskatalog
  - **Goldene Regeln**
  - **Gefährdungskatalog Elementare Gefährdungen**

Standards mit Bezug zu IT-/Informationssicherheit (Auszug)

- **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002)**
  OECD Richtlinie für die Sicherheit von Informationssystemen und –Netzen (2002)

- **IT Infrastructure Library ITIL**
  Sammlung von “best practices“ für IT-Services (ITSM (IT Service Management))
  Sicherheitsmanagement-Prozess orientiert sich an BS 7799 bzw. ISO/IEC 27001

- **ISO/IEC 20000-x**
  Part 1: Information technology - Service Management – Specification (2011)
  Part 2: Information technology - Service Management - Code of Practice (2012)
  Part x: ….

- **NIST – National Institute of Standards and Technology** (mehr als 250 Dokumente)
  - **FIPS xxx – Federal Information Processing Standards**
    - FIPS 199 Standards for Security Categorization …
    - FIPS 200 Security Controls for Information Systems
    - ...
  - **SP 800-xx – Special Publications**
    - SP 800-41 Guidelines on Firewalls and Firewall Policy
    - SP 800-53 Guide for Assessing the Security Controls
    - ...

Standards mit Bezug zu IT-/Informationssicherheit (Auszug)

- **DIN EN ISO 9001:2008**
  Anforderungen an Qualitätsmanagementsysteme
- **ISACA** (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation)
  - **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology (**CObIT**)
    'IT governance' Richtlinien, um IT und Unternehmensziele zu überwachen
  - IS Auditing Standards, IS Auditing Guidelines, IS Auditing Procedures
- **Prüfungsstandards des IDW** (**I**nstituts für **W**irtschafts**p**rüfer)
  IDW PS 330, IDW PS 951, RS FAIT1, etc.
- **BSI - Informationssicherheitsrevision** (IS-Revision)
  IS-Revision auf der Basis von IT-Grundschutz
- **PCI DSS** (**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard)
- **TIA-942** (**T**elecommunications **I**ndustry **A**ssociation Data Center Standards)
- **WLA – SCS**:2006 (World Lottery Association – Security Control Standard)
- **ISO/IEC 15408-x:2005, C**ommon **C**riteria **(CC)**
- …

Standards mit Bezug zu IT-/Informationssicherheit (Auszug)

- **ISO/IEC 24762:2008**
  Guidelines for information & communications technology disaster recovery services
- **ISO 22301:2012**
  Societal security – Business continuity management systems - Requirements
- BS 25777 (zurückgezogen), jetzt ISO/IEC 27031
- **PAS 77:2006 IT Service Continuity Management** – Code of practice
- **BCI Good Practice Guidelines**
- **BS 31xxx Risk management**
  - BS ISO 31000:2008 Principles and guidelines on implementation
  - IEC 31010:2008 Risk assessment techniques
  - BS 31100:2008 Code of practice
- **ISIS 12** (**I**nformations**si**cherheitsmanagement**s**ystem in **12** Schritten)
- **NIFIS-Siegel** (**N**ationale **I**nitiative **f**ür **I**nformations- und Internet-**S**icherheit)
- **…**

Zertifizierbare Standards (Auszug)

- **ISO/IEC 27001**
- **ISO 27001 auf der Basis von IT-Grundschutz**
- **ISIS 12**
- **…**

Aufbau der ISO/IEC 27001 und Anforderungen

- Grundlagen, Kapitel 0 – 3
  Einleitung, Anwendungsbereich, Normative Referenzen, Definitionen

- **Managementrahmen, Kapitel 4 – 8** (Verbindlich zu erfüllen für Zertifizierung*)
  - Informationssicherheits-Managementsystem (ISMS)
  - Verantwortung des Managements
  - Interne ISMS-Audits
  - Managementbewertung des ISMS
  - ISMS-Verbesserung

- **Anhang A** (Verbindlich zu erfüllen für Zertifizierung**)
  - Sicherheitsziele und Maßnahmen

- Informativer Teil
  - Anhang B, Gegenüberstellung mit den OECD-Richtlinien
  - Anhang C, Gegenüberstellung mit ISO 9001:2000 und ISO 14001:2004
  - Literaturhinweise

* ➔ Jedes Unternehmen, das eine ISO 27001 Zertifizierung erhalten will, muss nachweisen, dass sie alle diese Anforderungen erfüllt. **Ausschlüsse sind nicht zulässig.** (ISO/IEC 27001, Kapitel 1.2)

** ➔ Alle Anforderungen/Maßnahmen sind vom Unternehmen anzuwenden/umzusetzen, außer wenn die Risikobewertung klar zeigt, das dies nicht notwendig ist. (ISO/IEC 27001, Kapitel 4.2.1.g)

Anforderungskatalog aus ISO/IEC 27001 (Anhang A)

- **Struktur**
  - **11 Bereiche**
  - **39 Kategorien**
  - **133 Maßnahmen**

- **Abschnitte mit Maßnahmen und Maßnahmenzielen**
  - **A.5 Sicherheitsleitlinie**
  - **A.6 Organisation der Informationssicherheit**
  - **A.7 Management von organisationseigenen Werten**
  - **A.8 Personalsicherheit**
  - **A.9 Physische und umgebungsbezogene Sicherheit**
  - **A.10 Betriebs- und Kommunikationsmanagement**
  - **A.11 Zugangskontrolle**
  - **A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen**
  - **A.13 Umgang mit Informationssicherheitsvorfällen**
  - **A.14 Sicherstellung des Geschäftsbetriebs** (Business Continuity Management)
  - **A.15 Einhaltung von Vorgaben** (Compliance)

- **Jeder Abschnitt / jede Sicherheitskategorie enthält**
  - **das Ziel der Maßnahme(n)**
  - **eine oder mehrere Anforderung(en) und Maßnahme(n)**

ISO/IEC 27001 ← → ISO/IEC 27002

Anhang A	Kapitel 5-15
A.5 Sicherheitsleitlinie	5. Sicherheitsleitlinie
A.6 Organisation der Informationssicherheit	6. Organisation der Informationssicherheit
A.7 Management von organisationseigenen Werten	7. Management von organisationseigenen Werten
A.8 Personalsicherheit	8. Personalsicherheit
A.9 Physische und umgebungsbezogene Sicherheit	9. Physische und umgebungsbezogene Sicherheit
A.10 Betriebs- und Kommunikationsmanagement	10. Betriebs- u. Kommunikationsmanagement
A.11 Zugangskontrolle	11. Zugangskontrolle
A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen	12. Beschaffung, Entwicklung und Wartung von Informationssystemen
A.13 Umgang mit Informationssicherheitsvorfällen	13. Umgang mit Informationssicherheitsvorfällen
A.14 Sicherstellen des Geschäftsbetriebs (Business Continuity Management)	14. Sicherstellen des Geschäftsbetriebs (Business Continuity Management)
A.15 Einhaltung von Vorgaben (Compliance)	15. Einhaltung von Vorgaben (Compliance)

Wortwahl innerhalb der Maßnahmentexte	
… muss … (… shall …)	… sollte … (… should …)

Zertifizierbare Standards (Auszug)

- ISO/IEC 27001

➔ • ISO 27001 auf der Basis von IT-Grundschutz

- ISIS 12

- …

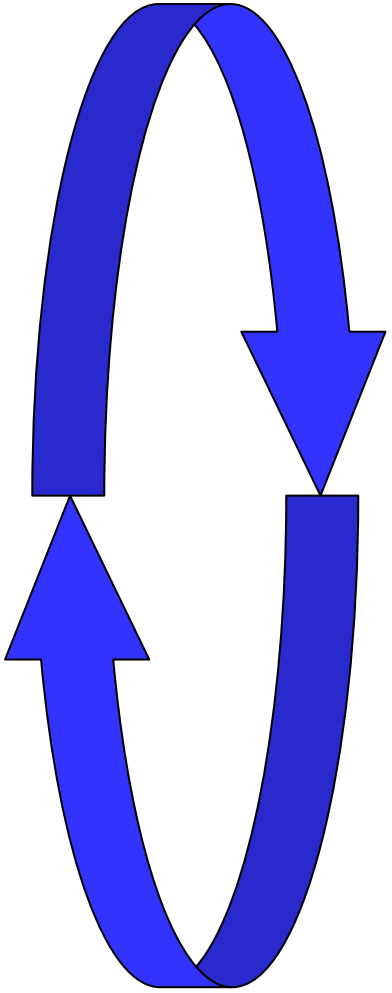
BSI-Standard 100-1, ISMS (Managementsysteme für Informationssicherheit)

- **Ziele**
  1. **Etablieren eines angemessenen Sicherheitsmanagements**
     Integration des IT-Sicherheitsmanagements in Organisationsstrukturen und Prozesse
  2. **Umsetzen von technischen und organisatorischen Maßnahmen**

- **Inhalt und Aufbau**
  - **Überblick über Standards zur Informationssicherheit**
  - **Komponenten eines Managementsystems**
    Managementprinzipien, Mitarbeiter, Sicherheitsprozess, Ressourcen
  - **Prozessbeschreibung und Lebenszyklus**
    Planung, Umsetzung, Kontrolle, Verbesserung und Beschaffung … Aussonderung
  - **Management-Prinzipien**
    Verantwortung, Überwachung, Steuerung, Kommunikation/Dokumentation
  - **Ressourcen**
  - **Einbinden der Mitarbeiter**
  - **Festlegen und Einführen eines Informationssicherheitsprozesses**
    Geltungsbereich, Organisation, Leitlinie, Umsetzung, Erfolgskontrolle,
  - **Sicherheitskonzept**
    nach der IT-Grundschutz-Vorgehensweise

BSI-Standard 100-2, IT-Grundschutz Vorgehensweise

- Initiierung des Sicherheitsprozesses
  - Verantwortung der Leitungsebene
  - Konzeption und Planung
  - Aufbau einer Sicherheitsorganisation
  - Erstellen der IT-Sicherheitsleitlinie
  - Bereitstellen der Ressourcen zur IT-Sicherheit
  - Einbinden aller Mitarbeiter
- IT-Sicherheitskonzeption
  - Festlegen des Geltungsbereichs
  - IT-Strukturanalyse
  - Schutzbedarfsfeststellung
  - Auswahl der Maßnahmen (Modellierung)
  - Basis Sicherheits-Check
  - Ergänzende Sicherheitsanalyse
  - Umsetzung des IT-Sicherheitskonzeptes
- Aufrechterhaltung und kontinuierliche Verbesserung



Aufbau der IT-Grundschutzkataloge

- **IT-Grundschutz-Kataloge** (> 4.500 Seiten (Stand: 12te Ergänzungslieferung))
  - **IT-Grundschutz: Ziel, Idee, Konzeption**
  - **Schichtenmodell und Modellierung** (Seiten 24 bis 33)
    - kurze Beschreibung der 5 Schichten
    - Kurze Beschreibung der Modellierung
  - **Rollen** (Seiten 34 bis 38)
    >45 Rollen (z.B. Administrator, Bauleiter, Entwickler, Fachverantwortlicher, IT-Sicherheitsbeauftragter, ….)
  - **Glossar und Begriffsdefinitionen** (Seiten 39 bis 51)
  - **Bausteinkatalog** (Seiten 52 – 317)
    Bausteine aufgeteilt auf 5 Schichten (B1.x – B5.x)
  - **Gefährdungskatalog** (Seiten 318 – 1022)
    Bereiche von Gefährdungen in 6 Gruppen (G1 – G6) zusammengefasst
  - **Maßnahmenkatalog** (Seiten 1023 – 4067)
    Maßnahmen sind in 7 Bereichen (M1 – M7) gruppiert
  - **Index** (Seiten 4073 – 4101)

IT-GSHB: Schichtenmodell und Inhalt des Bausteinkatalogs

- **Übergeordnete Aspekte**
  Strategie, Richtlinien, grundsätzliche Maßnahmen
  Sicherheitsmanagement, Datensicherung, Virenschutz, Personal, Outsourcing, Sensibilisierung/Schulung, Archivierung, Hardware- und Softwaremanagement, …

- **Infrastruktur**
  Physische und umgebungsbezogene Sicherheit, Haustechnik
  Gebäude, Rechenzentrum, Serverraum, häuslicher Arbeitsplatz, …

- **IT-Systeme**
  Systeme, Administration, Anwender
  UNIX-System, PC, TK-Anlage, Mobiltelefon, Storage

- **Netze**
  Netz-Topologie, -Protokolle, -Management
  Firewall, Remote Access, WLAN, …

- **IT-Anwendungen**
  Installation, Konfiguration, Betrieb von Anwendungen
  Groupware/E-Mail, Web-Server, Faxserver, Datenbank, Verzeichnisdienste, …

BSI IT-Grundschutzkataloge, 12te Ergänzungslieferung (2011)

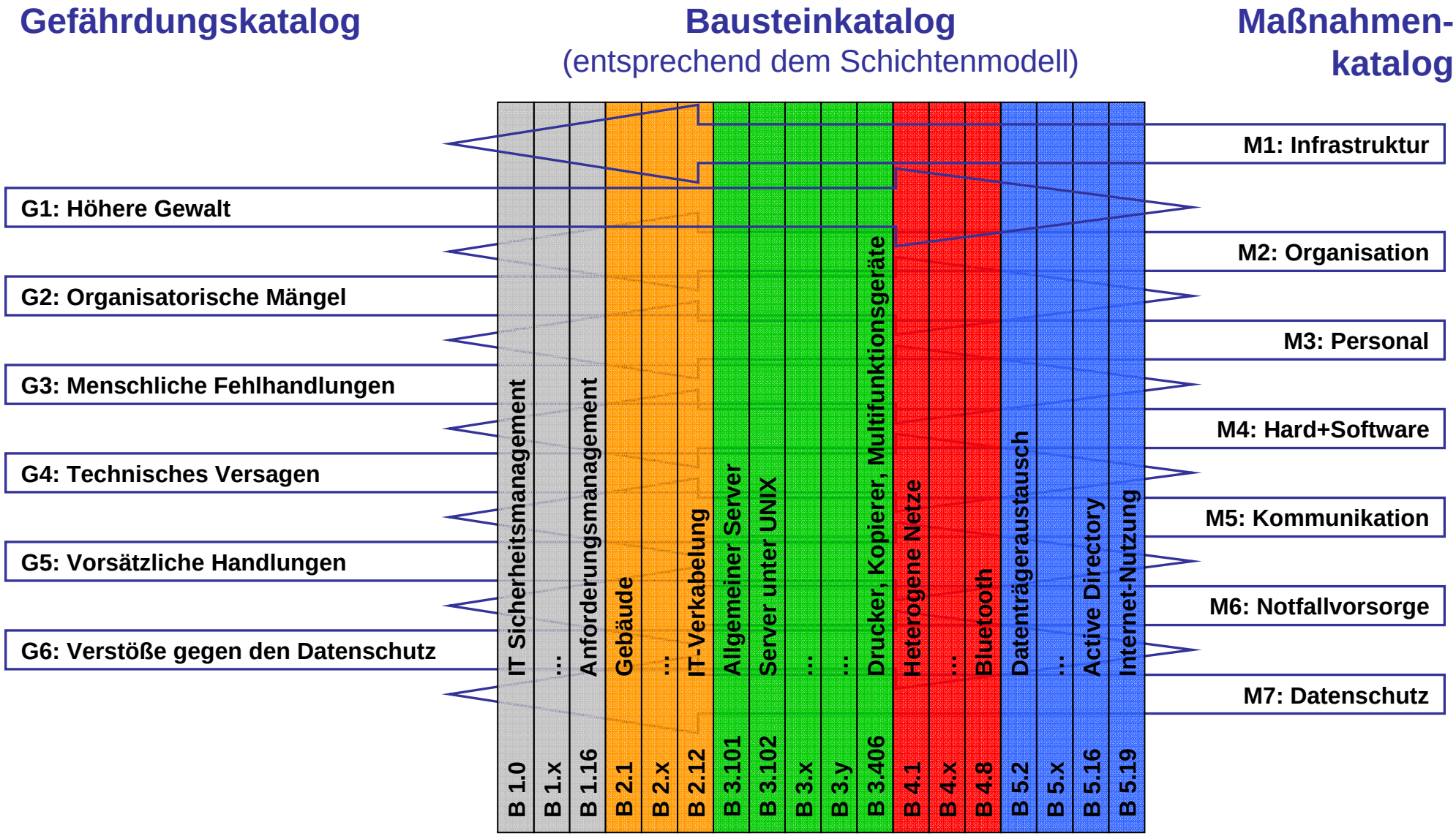
Übergreifende Sicherheitsaspekte	Baulich-technische Sicherheit	Sicherheit der IT-Systeme		Sicherheit im Netz	Sicherheit in Anwendungen
Sicherheits-management	Gebäude	Allgemeiner Server	Sicherheitsgateway (Firewall)	Heterogene Netze	Datenträgeraustausch
Organisation	Elektrotechnische Verkabelung	Server unter UNIX	Router und Switches	Netz- und System-management	Groupware
Personal	Büroraum	Server unter Novell Netware 4.x	Speichersysteme und Speichernetze	Modem	Webserver
Notfallmanagement	Serverraum	Server unter Windows 2000	Virtualisierung	VPN	Lotus Notes
Daten-sicherungskonzept	Datenträgerarchiv	S/390 und zSeries-Mainframe	Terminalserver	LAN-Anbindung eines IT-Systems über ISDN	Faxserver
Datenschutz	Raum für technische Infrastruktur	Server unter Windows 2003	TK-Anlage	WLAN	Datenbanken
Schutz vor Schadprogrammen	Schutzschränke	Allgemeiner Client	Faxgerät	VoIP	Telearbeit
Kryptokonzept	Häuslicher Arbeitsplatz	Allgemeines nicht vernetztes System	Mobiltelefon	Bluetooth	Novell eDirectory
Behandlung von Sicherheitsvorfällen	Rechenzentrum	Laptop	PDA		Exchange 2000, Outlook 2000
Hard- und Software-Management	Mobiler Arbeitsplatz	Client unter UNIX	Drucker, Kopierer, Multifunktionsgeräte		SAP System
Standardsoftware	Besprechungs-, Veranstaltungsraum	Client unter Windows 2000			Mobile Datenträger
Outsourcing	IT-Verkabelung	Internet-PC			Allgemeiner Verzeichnisdienst
Archivierung		Client unter Windows XP			Active Directory
Sicherheitssensibili-sierung & -schulung		Client unter Windows Vista			Samba
Patch- & Änderungs-management					DNS-Server
Löschen und Vernichten von Daten					Internet-Nutzung
Anforderungs-management					

IT-GSHB: Inhalte von Gefährdungs- und Maßnahmenkatalog

- **Gefährdungskatalog** (insgesamt > 450 Gefährdungen enthalten)
  - **G1: Höhere Gewalt**
  - **G2: Organisatorische Mängel**
  - **G3: Menschliche Fehlhandlungen**
  - **G4: Technisches Versagen**
  - **G5: Vorsätzliche Handlungen**
  - **G6: Missbrauch personenbezogener Daten**

- **Maßnahmenkatalog** (insgesamt mehr als 1.250 Maßnahmen enthalten)
  - **M1: Infrastruktur**
  - **M2: Organisation**
  - **M3: Personal**
  - **M4: Hard- und Software**
  - **M5: Kommunikation**
  - **M6: Notfallvorsorge**
  - **M7: Datenschutz**

Grundschutzkataloge (Schematische Darstellung des Zusammenspiels der Kataloge)



(Zertifizierungs)Audit

- **Definition**
  Systematischer, unabhängiger und dokumentierter Prozess, um zu überprüfen, in wie weit festgelegte Kriterien erfüllt sind.

- **Ziel**
  Nachweis, dass die Prozesse (ISMS) überwacht, überprüft und verbessert werden

- **Rahmenbedingungen**
  - Aufzeichnungen als Nachweis für die Konformität (Produkte/Systeme, Verfahren, etc. erfüllen die Anforderungen)
  - Das Audit ist unabhängig und objektiv
  - Die Ergebnisse des Audits sind nachweisbar und wiederholbar
  - Die Bewertung des Auditors stützt sich nur auf nachweisbare Fakten

- **Sonstiges**
  - Ein Audit (insbesondere ein Zertifizierungsaudit) ist ein formaler Prozess
  - Der formale Prozess ist Voraussetzung für Objektivität und Verfahrenstreue
  - Das ISMS wird so lange als ‘compliant‘ angesehen, bis das Gegenteil bewiesen ist (factual evidence of failure/non-conformity)

Internes Audit (First party audit)

- **Initiator**
  Das eigene Unternehmen

- **Ziele**
  - Erfüllen einer Anforderung aus dem Standard (z.B. ISO/IEC 27001, Kapitel 6)
  - Nachweis der Wirksamkeit des ISMS

- **Aufgabe**
  Überprüfung des eigenen Unternehmens(bereichs) für eigene Zwecke

- **Prüfgrundlage**
  Das eigene, dokumentierte ISMS und der Standard

- **Auditoren**
  Eigenes Personal oder Externe im Auftrag des Unternehmens.
  Aber: Die Auswahl der Auditoren und die Durchführung der Audits müssen Objektivität und Unparteilichkeit des Auditprozesses sicherstellen.
  Auditoren dürfen nicht ihre eigene Tätigkeit auditieren. (ISO/IEC 27001, Kap. 6)

- **Auditbericht**
  Auditierter Bereich, Umfang, Ziele, Feststellungen, (Aktivitätenplan), Auditor, Datum

Fremdfirmenaudit (Externes Audit, Second party audit)

- **Initiator**
  Ein fremdes Unternehmen, das mit dem auditierten Unternehmen eine Geschäftsbeziehung als Kunde oder Lieferant hat bzw. ggf. aufnehmen will

- **Ziele**
  Nachweis, dass Verträge erfüllt werden bzw. Anforderungen erfüllt werden können

- **Aufgabe**
  Überprüfung des Auftragnehmers bzw. potentiellen Auftragnehmers

- **Prüfgrundlage**
  Üblicherweise der Vertrag bzw. Vertragsentwurf

- **Auditoren**
  Personen der Fremdfirma oder Dritte im Auftrag der Fremdfirma

- **Auditbericht**
  Art und Umfang werden von der Fremdfirma bestimmt

Zertifizierungsaudit (Externes Audit, Third party audit)

- **Initiator**
  Das eigene Unternehmen
- **Ziele**
  - Zertifikat - Nachweis durch eine unabhängigen Stelle
  - Positionierung gegenüber Geschäftspartnern, Mitarbeitern, etc.
  - Vermeiden oder Reduzieren des Aufwands, der durch andere Audits verursacht wird
    (z.B. Wirtschaftsprüfer, Fremdfirmenaudit, Kontrollen aufgrund Auftragsdatenverarbeitung (§11 BDSG))
- **Aufgabe**
  Überprüfen, ob und wie die Anforderungen aus dem Standard erfüllt sind
- **Prüfgrundlage**
  Der Standard (z.B. ISO/IEC 27001, ISO 27001 auf der Basis von IT-Grundschutz, etc.)
- **Auditoren**
  Unabhängige, von einer (akkreditierten) Zertifizierungsstelle lizenzierte Auditoren
- **Auditbericht**
  Formales Dokument, in dem Prüfgegenstand und Feststellungen beschrieben sind und der Auditor ein zusammenfassendes Urteil zu den Ergebnissen des Audits im Hinblick auf das Zertifikat abgibt ((nicht/unter Auflagen) erteilen, (temporär) aussetzen, entziehen, o.ä.)

(Zertifizierungs)Audit - Voraussetzungen

- **Prüfstandards**
  - **ISO/IEC 17021:2011** Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren
  - **ISO/IEC 27006:2011** Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten
  - **DIN EN ISO 19011:2011** Leitfaden zur Auditierung von Managementsystemen

  - Zusätzlich bei Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Zertifizierungs - und Prüfschema, Gültigkeit der Prüfgrundlagen

- **(akkreditierte) Zertifizierungsstelle** (beispielhafte Auswahl)
  - **Bundesamt für Sicherheit in der Informationstechnik (BSI), British Standards Institution (bsi), DQS, SQS, diverse TÜV-Gesellschaften, diverse Wirtschaftprüfungsgesellschaften, Bureau Veritas, etc.**

- **Prüfer / Auditor(en) / Revisor(en)**
  - **Fachkunde und Erfahrung**
  - **Prüfung(en) für den Standard erfolgreich abgelegt**
  - **Von einer Zertifizierungsstelle zugelassen für**
    - **Normenwerk**
    - **Branchen/Fachbereiche**

(Zertifizierungs)Audit

- **Organisatorisches**
  - **Auswahl der Zertifizierungsstelle**
  - **Vertrag**
  - **Auswahl der Auditoren**
  - **Dauer und Kosten** (abhängig von Komplexität, # Standorte, # Mitarbeiter, uam.)

- **Audit**
  - Vor-Audit (optional; nur einmal vor der Erst-Zertifizierung möglich)
  - **Phase 1** (Prüfung des ISMS und der zugrunde liegenden Dokumentation)
  - **Phase 2** (Prüfung der Umsetzung – Vor-Ort-Prüfung)
  - Nach-Audit (wenn gravierende Abweichungen festgestellt wurden)
  - **Überwachungsaudit(s)**

Ein Zertifizierungszyklus dauert üblicherweise 3 Jahre und besteht zumindest aus dem Zertifizierungs- und zwei Überwachungsaudits.
Nach drei Jahren kann der Zyklus mit einem so genannten Re-Zertifizierungs-Audit erneut gestartet werden.
Die Zeiträume, die zwischen den einzelnen Aktionen liegen dürfen, sind aufgrund von Anforderungen aus den Prüfstandards i.a. streng terminiert (Mindest- und Maximallaufzeiten).
Alle Bereiche, Prozesse und Lokationen, für die das ISMS gilt, müssen von einem Auditor innerhalb eines Zertifizierungszyklus mindestens einmal geprüft werden.

(Zertifizierungs)Audit

- **Ablauf**
  - **Auditplan**
  - **Prüfen der Unterlagen**
    - **vor Ort beim Auditee? oder vor Ort beim Auditor?**
    - **Überlassen von Unterlagen** (teils im Prüfschema gefordert)
  - **Prüfung vor Ort**
    - **Interviews mit Mitarbeitern aller Hierarchiestufen, ggf. auch mit Externen**
    - **Begehungen**
    - **Prüfen von Systemen und Konfigurationen**
  - **Umgang mit Prüfergebnissen**
    - **Feedback an den Gesprächspartner, bei Bedarf an Vorgesetzte**
    - **Notizen und Auditbericht**
  - **Auditbericht**
    - **Auditor schreibt den Auditbericht und verteilt ihn an festgelegten Adressatenkreis**
    - **Gestaltung und Umfang hängen vom Standard und Prüfverfahren ab**

- **Weitere Hinweise**
  - **Informieren Sie den Auditor über Sicherheitsvorschriften und sonstige Besonderheiten** (Dolmetscher, Terminengpässe von Interviewpartnern, etc.)
  - **Begleitung der Auditoren**

(Zertifizierungs)Audit

- **Feststellungen**
  - **Schwerwiegende Abweichung / major non-conformity**
    Eine oder mehrere Anforderungen des Standards sind nicht erfüllt (Versagen, Fehler, o.ä.) oder eine Situation löst Zweifel aus, dass das Managementsystem funktioniert.
  - **Abweichung / non-conformity / minor non-conformity**
    ein einzelnes festgestelltes Versäumnis, das allein noch nicht die Wirksamkeit des Managementsystems in Frage stellt
  - **Empfehlung, Verbesserungspotential / opportunity for improvement**
  - **Beobachtung / observation**

Der Auditor muss jede Abweichung begründen können (mit Referenz auf die Anforderung aus der Norm, die nicht angemessen erfüllt wurde).
Die geprüfte Organisation hat ein Widerspruchsrecht, wenn sie die Sachlage anders beurteilt. Wird kein Konsens gefunden, entscheidet die Zertifizierungsstelle.

Wird eine schwerwiegende Abweichung festgestellt, kann das dazu führen, dass das Zertifikat entzogen oder zeitweise ausgesetzt wird.

Zertifikat

- **Zertifizierungsstelle entscheidet über Vergabe/Entzug/Aussetzen**
  - **Entscheidung auf Grundlage des Auditberichtes**
    bei ISO 27001 auf Basis von IT-Grundschutz auch auf Grundlage der Referenzdokumente

- **Das Zertifikat**
  - **Zertifizierungstelle informiert das auditierte Unternehmen**
  - **‘Übergabe‘ kann elektronisch, per Post oder persönlich erfolgen**
  - **Layout ist von der Zertifizierungsstelle vorgeben**
  - **Individuelle Ergänzungen sind ggf. möglich**

- **Rechte und Pflichten im Zusammenhang mit dem Zertifikat**
  - **Umgang mit Zertifikats-‘Logo‘ ist reglementiert (Prüfstandards, Vertrag)**
  - **Interessenten müssen erfahren können, für welchen Anwendungsbereich (Scope, Informationsverbund) das Zertifikat gilt.**
  - **Missbrauch kann zum Entzug des Zertifikates führen**

Weiterführende Informationen und Links

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  - www.bsi.bund.de (homepage)
  - BSI-Standards: www.bsi.bund.de/literat/bsi_standard
  - Grundschutzkataloge: www.bsi.bund.de/gshb/deutsch
  - Tools und Hilfsmittel: www.bsi.bund.de/IT-Grundschutz/IT-Grundschutz GSTOOL/...
  - Gültige Zertifikate und Testate und über von BSI zugelassene Auditoren www.bsi.bund.de/IT-Grundschutz/IT-Grundschutz-Zertifikat

- **Normen und Standards**
  - ISO: www.iso.org
  - Beuth-Verlag: www.beuth.de

- **Informationen über aktuell gültige ISO/IEC 27001-Zertifikate**
  - Certificate register: www.iso27001certificates.com/Register%20Search.htm
  - Additional information: www.iso27001certificates.com/Taxonomy/CertificateSearch.htm