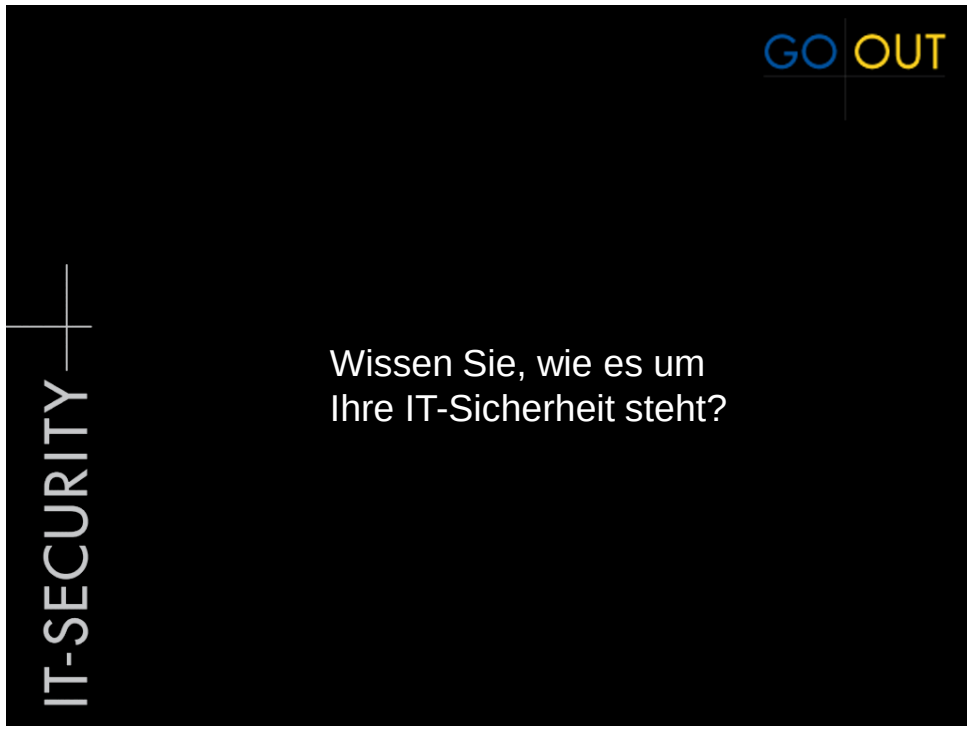

GO OUT
IT-SECURITY
Wissen Sie, wie es um
Ihre IT-Sicherheit steht?


GO OUT
IT-SECURITY
Aktuelles zu ISO 27001/2
Andreas Wisler
GO OUT Production GmbH
Dipl. Ing FH, CISSP, CISA, ISO 27001 Lead Auditor
www.goSecurity.ch / wisler@goout.ch

GO OUT

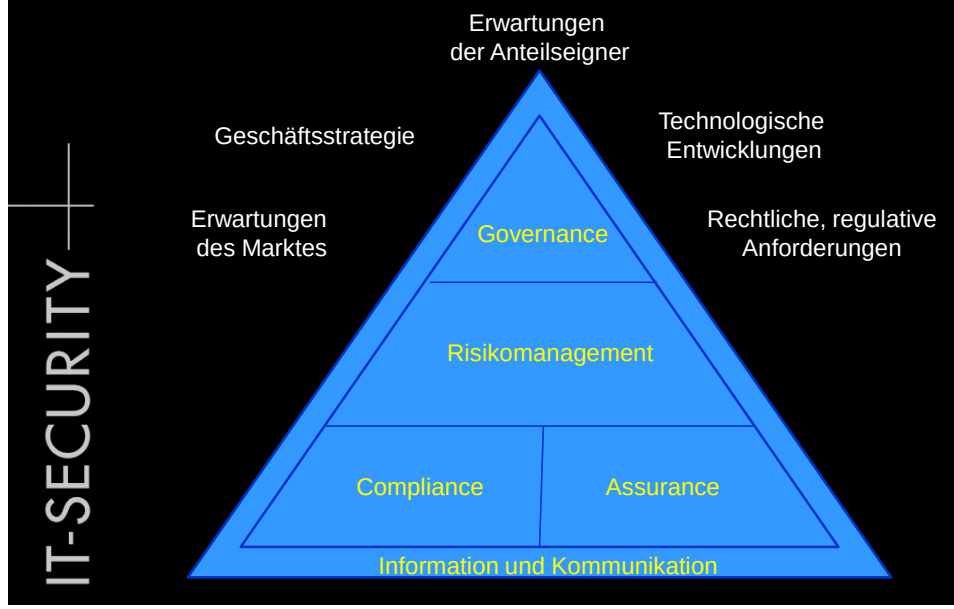
Standards und Normen

- Ziel von Standards:
  - beschreiben Modelle, anhand derer ein Sicherheits-management systematisch Bedeutung aufgebaut und weiterentwickelt werden kann,
  - zeigen auf, welche organisatorischen und technischen Massnahmen für Informationssicherheit erforderlich sind, und
  - liefern Kriterien, anhand derer überprüft werden kann, ob die umgesetzten Massnahmen angemessen sind und weithin anerkannten Massstäben genügen.

IT-SECURITY

GO OUT

Standards und Normen



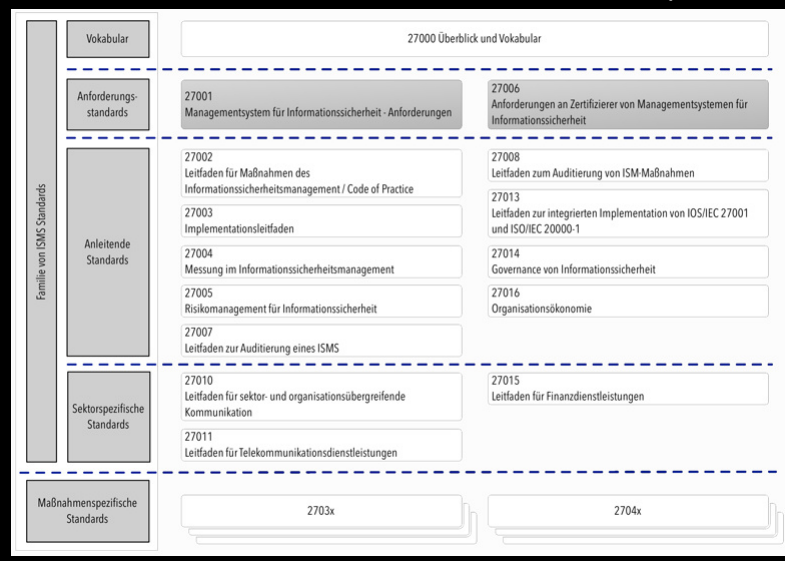
IT-SECURITY

GO OUT

IT-SECURITY

ISO 27000 - Familie

Quelle: kes.info



GO OUT

IT-SECURITY

ISO 27001

- Aufbau **I**nformations**S**icherheits**M**anagement**S**ystem
  - Festlegung und Abgrenzung des Bereichs
  - Erstellen einer Leitlinie, die auf die Werte, Prozesse, Aufgaben und technischen Gegebenheiten bezogen ist,
  - Auswahl einer Risikoanalysemethode zur systematischen Beurteilung der Risiken und Sicherheitsanforderungen. Entwicklung von Kriterien für die Behandlung der Risiken (einschliesslich für deren Akzeptanz),
  - Identifizieren und Bewerten der Sicherheitsrisiken,
  - Auswahl von effektiven und wirtschaftlich angemessenen Massnahmen zur Abwehr der Risiken,
  - Auswahl von Methoden zur Überprüfung der Wirksamkeit der Massnahmen.

GO OUT

ISO 27001

- Erfolgreich umgesetzt, wenn
  - es eine definierte Leitlinie gibt, Ziele und Massnahmen an den Geschäftszielen orientiert sind und das Vorgehen zum Management der Informationssicherheit der Unternehmenskultur angepasst ist,
  - für Informationssicherheitsmanagement ein Budget zugeteilt wurde und die Aktivitäten zur Informationssicherheit von der Leitung (Topmanagement) unterstützt werden,
  - in der Organisation das Verständnis für die Anforderungen an Informationssicherheit verbreitet ist, Risikoanalysen durchgeführt und Notfallvorsorge betrieben wird,
  - die Benutzer hinreichend für Informationssicherheit sensibilisiert und geschult sind und die geltenden Sicherheitsvorgaben und Regelungen kennen sowie
  - ein Sicherheitsprozess mit einer regelmässig wiederholten Beurteilung und Verbesserung des ISMS abläuft.

IT-SECURITY

GO OUT

ISO 27001

- Erfolgreich umgesetzt, wenn

IT-SECURITY

GO OUT

ISO 27001:2013

- 4 Context of the organization
  - 4.1 Understanding the organization and its context
  - 4.2 Understanding the needs and expections of interested parties
  - 4.3 Determining the scope of the ISMS
  - 4.4 ISMS
- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities and authorities
- 6 Planning
  - 6.1 Actions to address risks and opportunities
  - 6.2 Information security objectives and planning to achieve them

IT-SECURITY

GO OUT

ISO 27001:2013

- 7 Support
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- 8 Operation
  - 8.1 Operational planning and control
  - 8.2 Information security risk assessment
  - 8.3 Information security risk treatment

IT-SECURITY

GO OUT

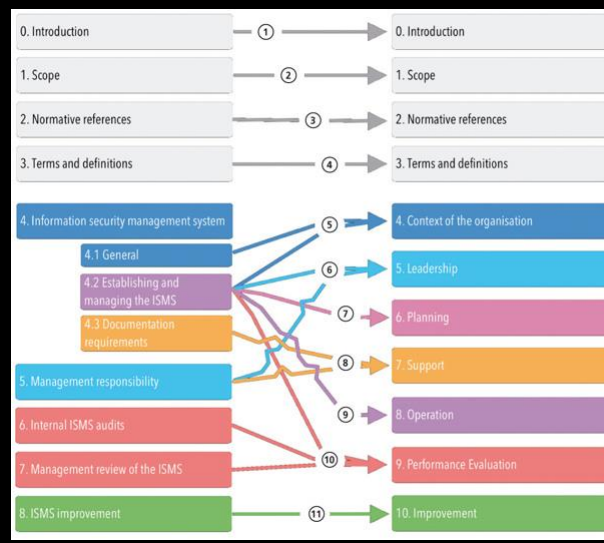
ISO 27001:2013

- 9 Performance evaluation
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.2 Internal audit
  - 9.3 Management review
- 10 Improvement
  - 10.1 Nonconformity and corrective action
  - 10.2 Continual improvement

IT-SECURITY

GO OUT

ISO 27001 : 2005 zu 2013



Quelle: kes.info

IT-SECURITY

GO OUT

IT-SECURITY

ISO 27002:2013

- ISO 27002 enthält diverse Kontrollmechanismen:
  - 14 Überwachungsbereiche (11)
  - 114 Sicherheitsmassnahmen (133)
- Bereiche:
  - 5 Information security policies
    - 5.1 Management direction for information security
  - 6 Organization of information security
    - 6.1 Internal organization
    - 6.2 Mobile devices and teleworking
  - 7 Human resource security
    - 7.1 Prior to employment
    - 7.2 During employment
    - 7.3 Termination and change of employment

GO OUT

IT-SECURITY

ISO 27002:2013

- Bereiche (Fortsetzung)
  - 8 Asset management
    - 8.1 Responsibility for assets
    - 8.2 Information classification
    - 8.3 Media handling
  - 9 Access control
    - 9.1 Business requirements of access control
    - 9.2 User access management
    - 9.3 User responsibilities
    - 9.4 System and application access control
  - 10 Cryptography
    - 10.1 Cryptographic controls

GO OUT

ISO 27002:2013

- Bereiche (Fortsetzung)
  - 11 Physical and environmental security
    - 11.1 Secure areas
    - 11.2 Equipment
  - 12 Operations security
    - 12.1 Operational procedures and responsibilities
    - 12.2 Protection from malware
    - 12.3 Backup
    - 12.4 Logging and monitoring
    - 12.5 Control of operational software
    - 12.6 Technical vulnerability management
    - 12.7 Information systems audit considerations

IT-SECURITY

GO OUT

ISO 27002:2013

- Bereiche (Fortsetzung)
  - 13 Communications security
    - 13.1 Network security management
    - 13.2 Information transfer
  - 14 System acquisition, development and maintenance
    - 14.1 Security requirements of information systems
    - 14.2 Security in development and support processes
    - 14.3 Test data
  - 15 Supplier relationships
    - 15.1 Information security in supplier relationships
    - 15.2 Supplier service delivery management

IT-SECURITY

GO OUT

ISO 27002:2013

- Bereiche (Fortsetzung)
  - 16 Information security incident management
    - 16.1 Management of information security incidents and improvements
  - 17 Information security aspects of BCM
    - 17.1 Information security continuity
    - 17.2 Redundancies
  - 18 Compliance
    - 18.1 Compliance with legal and contractual requirements
    - 18.2 Information security reviews

IT-SECURITY

GO OUT

ISMS 27001 : Anpassungen

- Mehraufwand bei:
  - ISMS-Measurement und -Improvement werden intensiv formuliert und gefordert und sind für eine Zertifizierung definitiv nachzuweisen.
  - Die Beteiligung des Managements wird stärker eingefordert und geht über einen "Letter of Intent" hinaus.
  - Neben negativen Risiken sind nun auch positive Risiken (bzw. Chancen) zu betrachten.
  - Nunmehr müssen alle Personen im Anwendungsbereich Gegenstand von klaren Rollenbeschreibungen und Awareness-Massnahmen sein (zuvor genügte es, nur die Rolleninhaber der ISMS-Organisation zu betrachten).

IT-SECURITY

GO OUT

IT-SECURITY

BSI-Standard 100-1

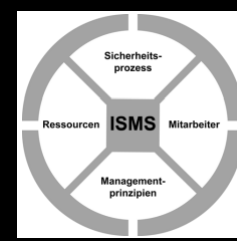
- Vollständig kompatibel zu ISO 27001:2005
- leicht verständliche und systematische Anleitung, unabhängig davon, mit welcher Methode die Anforderungen umgesetzt werden
- Kostenlos Downloadbar

GO OUT

IT-SECURITY

BSI-Standard 100-1

- ISMS-Komponenten:
  - Management-Prinzipien
  - Ressourcen
  - Mitarbeiter
  - Sicherheitsprozess
    - Leitlinie zur Informationssicherheit, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind
    - Sicherheitskonzept
    - Informationssicherheitsorganisation



BSI-Standard 100-1

- Aufgaben und Pflichten des Managements
  - Übernahme der Gesamtverantwortung für Informationssicherheit
  - Informationssicherheit integrieren
  - Informationssicherheit steuern und aufrechterhalten
  - Erreichbare Ziele setzen
  - Sicherheitskosten gegen Nutzen abwägen
  - Vorbildfunktion

BSI-Standard 100-1

- Aufrechterhaltung der Informationssicherheit und kontinuierliche Verbesserung
  - Pflicht für «interne» Audits
  - Durchführung von Übungen und Sensibilisierungsmassnahmen
  - Einbindung bei Änderungen
- Kommunikation und Wissen
  - Berichte an die Leitungsebene
  - Informationsfluss
  - Dokumentation
    - Techn. Doku, Anleitungen, Reporte für Mgmt-Aufgaben, Aufzeichnungen von Entscheiden

BSI-Standard 100-1

- Ressourcen für IS
  - finanzielle, personelle und zeitliche Ressourcen
  - «Wenn Zielvorgaben aufgrund fehlender Ressourcen nicht erreichbar sind, sind hierfür nicht die mit der Umsetzung betrauten Personen verantwortlich, sondern die Vorgesetzten, die unrealistische Ziele gesetzt bzw. die erforderlichen Ressourcen nicht bereitgestellt haben.»
  - Grundvoraussetzung für einen sicheren IT-Betrieb ist ein gut funktionierender IT-Betrieb. Für den IT-Betrieb müssen daher ausreichende Ressourcen zur Verfügung gestellt werden.

BSI-Standard 100-1

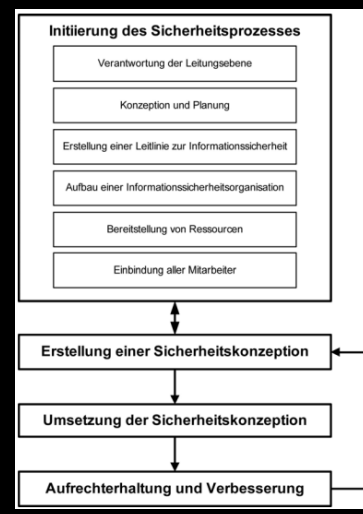
- Einbindung der Mitarbeiter
  - Sensibilisierung für Informationssicherheit und entsprechende Schulungen der Mitarbeiter sowie aller Führungskräfte.
  - Dazu gehört neben den Kenntnissen, wie Sicherheitsmechanismen bedient werden müssen, auch das Wissen über Sinn und Zweck von Sicherheitsmassnahmen. Auch Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeiter beeinflussen die Informationssicherheit entscheidend.

GO OUT

IT-SECURITY

BSI-Standard 100-2

- IT-Grundschutz
  - Sicherheits-prozess



GO OUT

IT-SECURITY

BSI-Standard 100-2

- Konzeption und Planung des Sicherheitsprozesses
  - Ermittlung von Rahmenbedingungen
    - Welche Geschäftsprozesse gibt es in der Organisation und wie hängen diese mit den Geschäftszielen zusammen?
    - Welche Geschäftsprozesse hängen von einer funktionierenden Informationstechnik ab?
    - Welche Informationen werden für diese Geschäfts-prozesse verarbeitet?
    - Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum?

BSI-Standard 100-2

- Konzeption und Planung des Sicherheitsprozesses
  - Ermittlung von Rahmenbedingungen
    - gesetzliche Rahmenbedingungen (nationale und internationale Gesetze und Bestimmungen),
    - Umwelteinflüsse, beispielsweise aufgrund der geografischen Lage oder aufgrund von sozialen und kulturellen Rahmenbedingungen,
    - Anforderungen von Kunden, Lieferanten und Geschäftspartnern, aktuelle Marktlage, Wettbewerbssituation und weitere relevante marktspezifische Abhängigkeiten,
    - branchenspezifische Sicherheitsstandards.

BSI-Standard 100-2

- Konzeption und Planung des Sicherheitsprozesses
  - Formulierung von allgemeinen IS-Zielen
  - Bestimmung des angemessenen Niveaus
    - **Sehr hoch**: Der Schutz vertraulicher Informationen muss unbedingt gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen.
    - **Hoch**: Der Schutz vertraulicher Informationen muss hohen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein.
    - **Normal**: Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.

GO OUT

BSI-Standard 100-2

- Organisation des Sicherheitsprozesses
  - Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
  - Aufbau der Informationssicherheitsorganisation, Beispiele für
    - Kleine Institution
    - Mittelgrosse Institution
    - Grosse Institution

IT-SECURITY

GO OUT

BSI-Standard 100-2

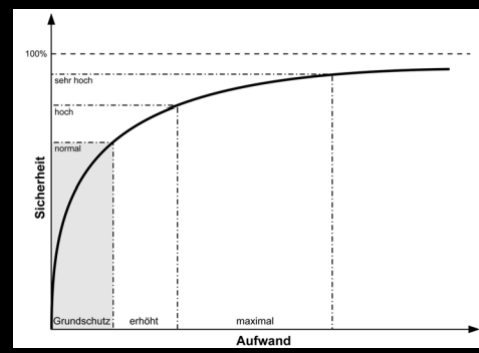
- Organisation des Sicherheitsprozesses

IT-SECURITY

GO OUT

BSI-Standard 100-2

- Bereitstellung von Ressourcen für die IS
  - Kosteneffiziente Sicherheitsstrategie



IT-SECURITY

GO OUT

BSI-Standard 100-2

- Einbindung aller Mitarbeiter in den Sicherheitsprozess
  - Schulung und Sensibilisierung
  - Kommunikation, Einbindung und Meldewege
  - Aufgabenwechsel oder Weggang von Mitarbeitern

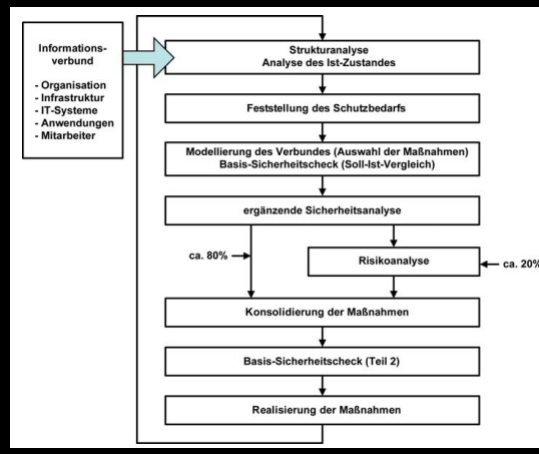
IT-SECURITY

GO OUT

IT-SECURITY

BSI-Standard 100-2

- Erstellung einer Sicherheitskonzeption

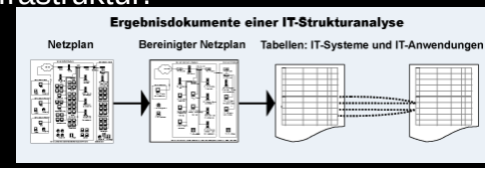


GO OUT

IT-SECURITY

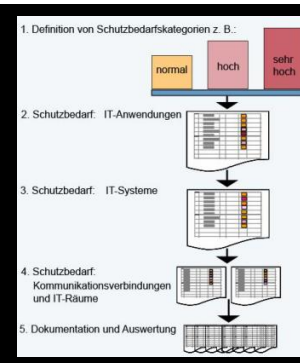
BSI-Standard 100-2

- Strukturanalyse umfasst:
  - im Informationsverbund betriebene Anwendungen und gestützten Geschäftsprozesse,
  - die org. und personellen Rahmenbedingungen,
  - im Informationsverbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,
  - die Kommunikationsverbindungen zwischen den IT-Systemen und nach aussen,
  - die vorhandene Infrastruktur.



IT-SECURITY

BSI-Standard 100-2



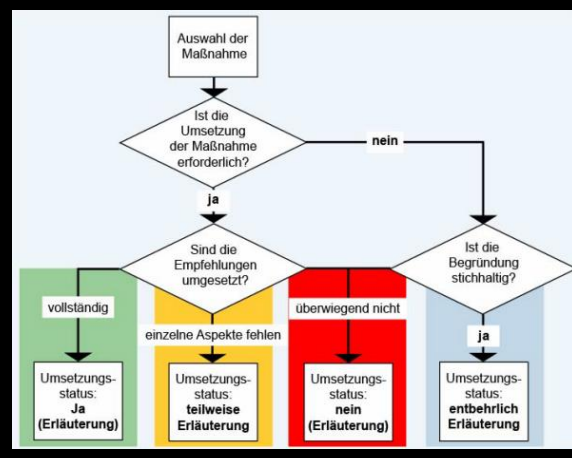
- Schutzbedarfsfeststellung
  - Anwendungen
  - IT-Systeme
  - Räume
  - Kommunikationsverbindungen
- Auswahl und Anpassung von Massnahmen
  - Basis-Sicherheitscheck
  - Massnahme «entbehrlich», «ja», «teilweise», «nein»
- Weiterführende Sicherheitsmassnahmen

IT-SECURITY

GO OUT

BSI-Standard 100-2

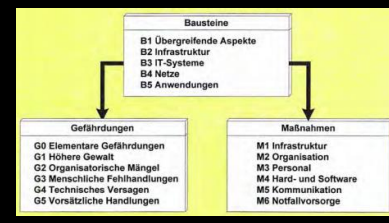
- Umsetzungsgrad



GO OUT

BSI-Standard 100-2

- Grundschutzkataloge
  - Bausteine
    - B 1: Übergreifende Aspekte
    - B 2: Infrastruktur
    - B 3: IT-Systeme
    - B 4: Netze
    - B 5: Anwendungen
  - Gefährdungen
    - G 0: Elementare Gefährdungen
    - G 1: Höhere Gewalt
    - G 2: Organisatorische Mängel
    - G 3: Menschliche Fehlhandlungen
    - G 4: Technisches Versagen
    - G 5: Vorsätzliche Handlungen



www.bsi.de/gshb

IT-SECURITY

GO OUT

BSI-Standard 100-2

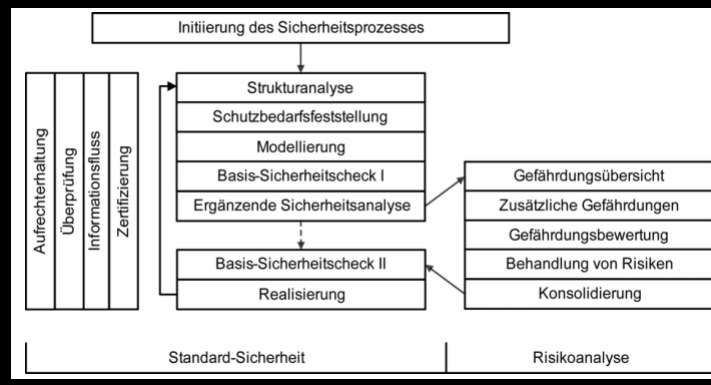
- Grundschutzkataloge
  - Massnahmen
    - M 1: Infrastruktur
    - M 2: Organisation
    - M 3: Personal
    - M 4: Hard- und Software
    - M 5: Kommunikation
    - M 6: Notfallvorsorge

IT-SECURITY

GO OUT

BSI-Standard 100-3

- Einbindung Risiko-Analyse in den Grundschutz

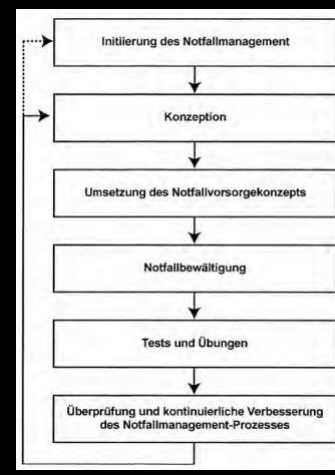


IT-SECURITY

GO OUT

BSI-Standard 100-4

- Notfallmanagement
  - BCM / ISO 22301
  - BS 25999
  - Leitlinie
  - BIA
  - Notfallhandbuch
  - Übungen



IT-SECURITY

GO OUT

Fazit

- ISO 27001 und 27002 sind ein idealer «Ratgeber»
- Vorgehen nach BSI 100-1 und 100-2 erleichtert die Arbeit massiv
- Alle Geschäftsprozesse müssen berücksichtigt werden
- Management-Unterstützung essentiell

IT-SECURITY

GO OUT

Mit uns wissen Sie,
wie es um Ihre IT-Sicherheit steht!


A. Wisler


Th. Furrer


S. Müller


E. Kauth


A. Kulhanek


S. Walser


C. Wehrli


A. Zlateva


N. Rasstrigina


J. Kappeler

IT-SECURITY


Dienstleistungen …
GO OUT
IT-Security Audit
Quick Audit
Penetration Test
Review
IT-SECURITY
QSEC
Projekt - Begleitung
IT-Security Konzepte