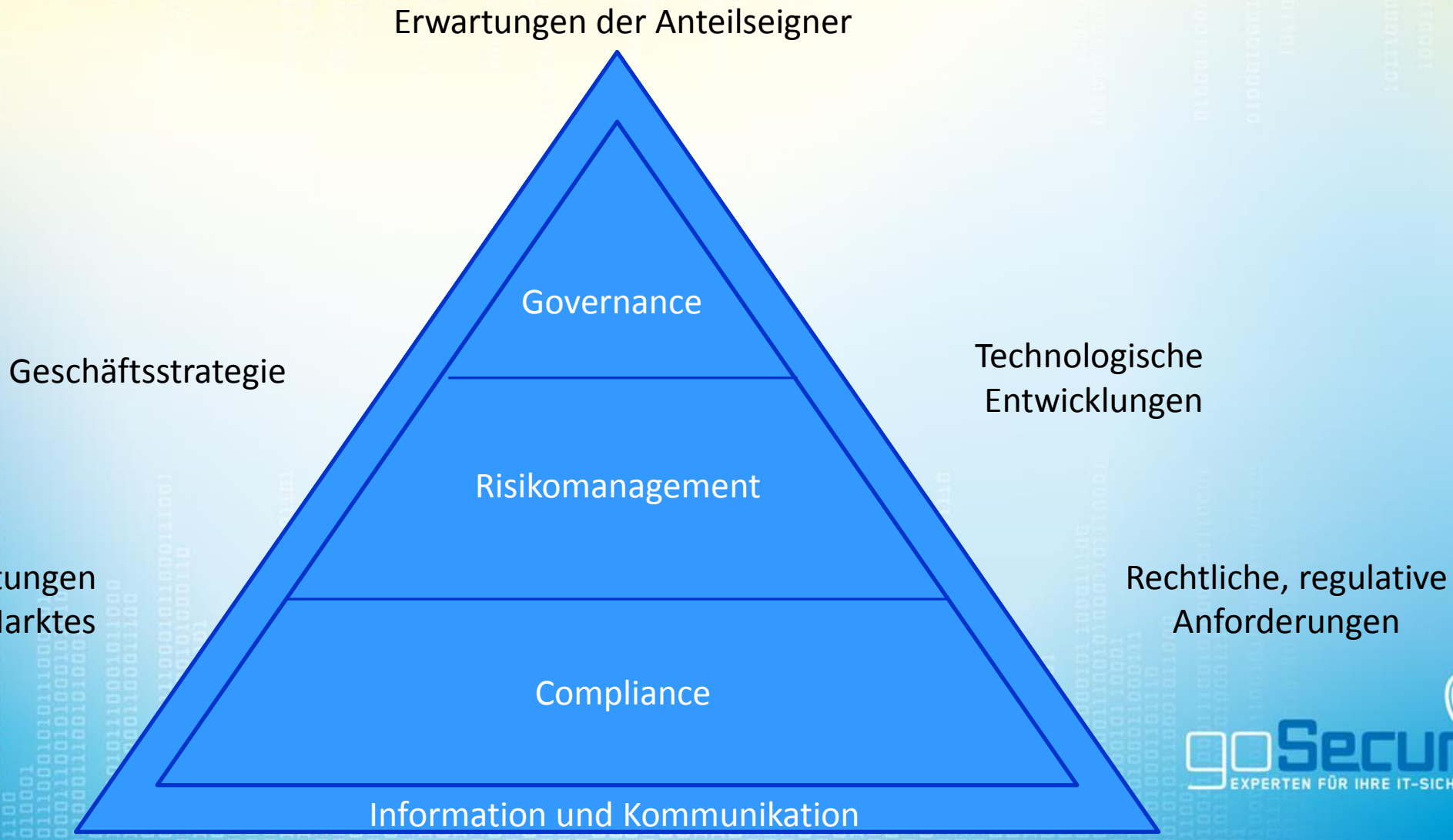
ISMS für KMU

Geldverschwendung oder Mehrwert?

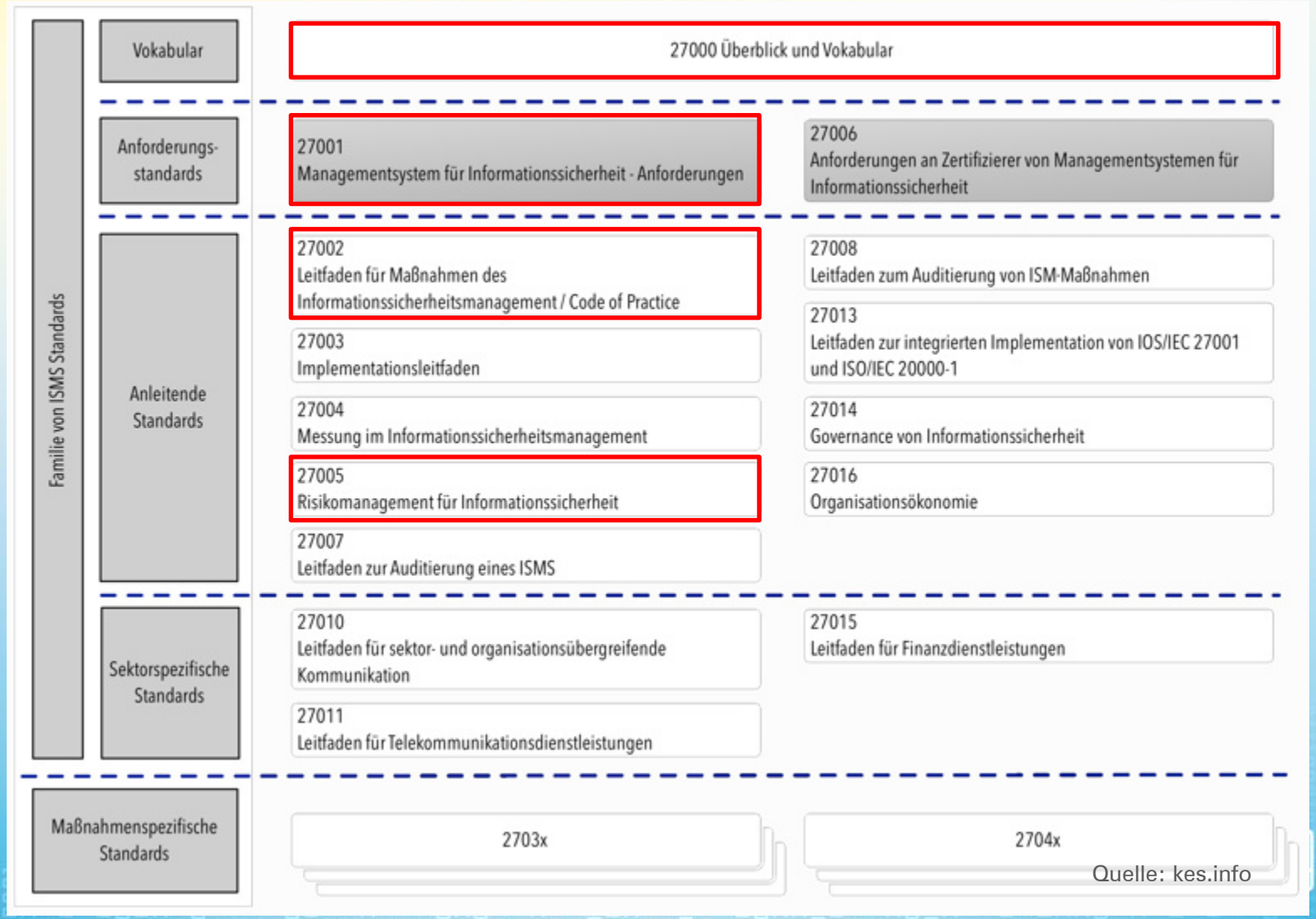
Andreas Wisler
Wisler@goSecurity.ch

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

Standards und Normen



ISO 27000 - Familie



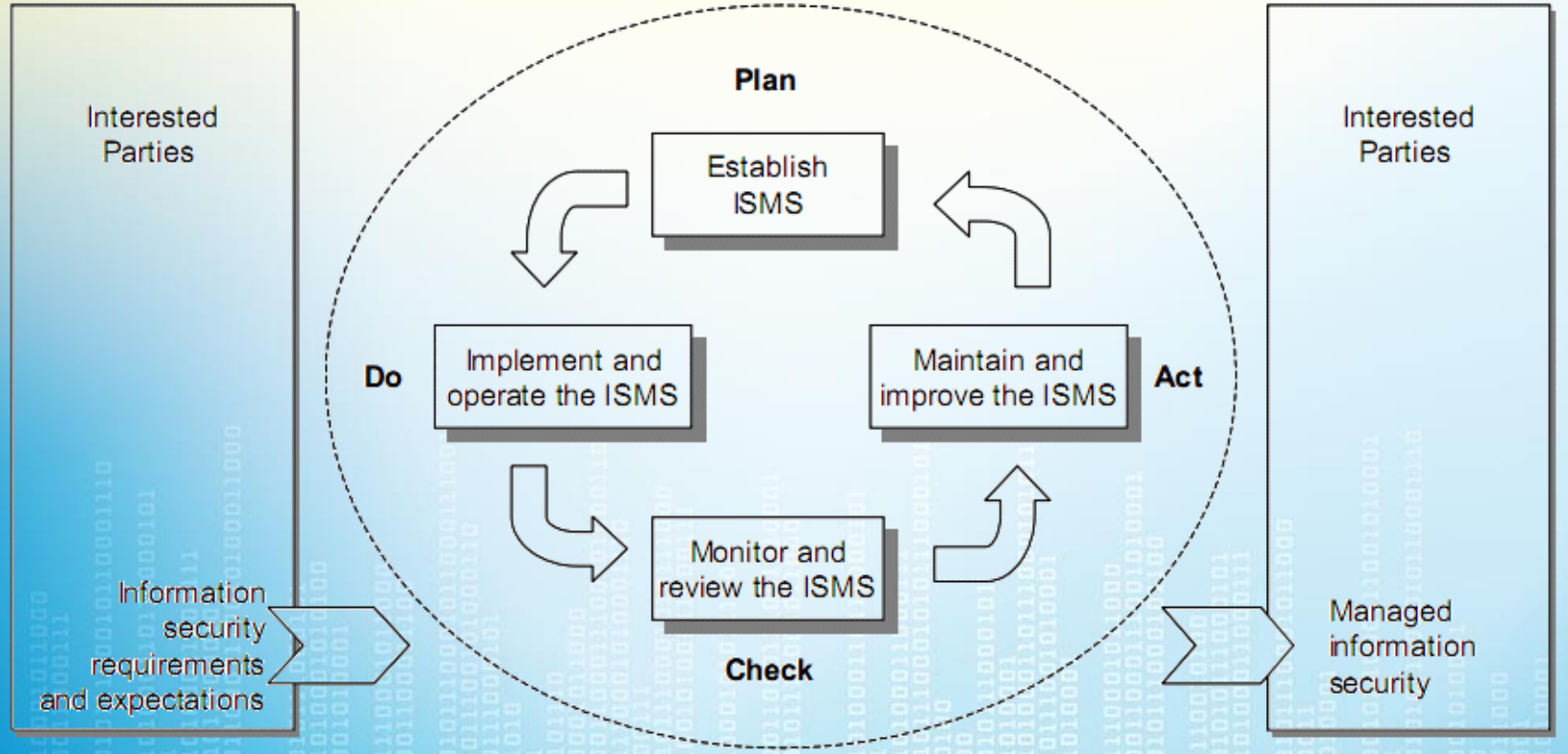
Quelle: kes.info

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.

ISO 27001

- Erfolgreich umgesetzt, wenn



Quelle: ISO 27001

ISO 27001:2013

- 0 Einleitung
- 1 Anwendungsbereich
- 2 Normative Verweisungen
- 3 Begriffe
- 4 Kontext der Organisation
  - 4.1 Verständnis der Organisation und ihres Kontexts
  - 4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien
  - 4.3 Festlegung des Geltungsbereichs des ISMS
  - 4.4 Informationssicherheitsmanagementsystem
- 5 Führung
  - 5.1 Führung und Engagement
  - 5.2 Leitlinie
  - 5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse

ISO 27001:2013

- 6 Planung
  - 6.1 Massnahmen zum Umgang mit Risiken und Chancen
  - 6.2 Informationssicherheitsziele und Pläne für deren Erreichung
- 7 Unterstützung
  - 7.1 Ressourcen
  - 7.2 Kompetenz
  - 7.3 Bewusstsein
  - 7.4 Kommunikation
  - 7.5 Dokumentierte Informationen
- 8 Einsatz
  - 8.1 Einsatzplanung und -kontrolle
  - 8.2 Informationssicherheitsrisikoeinschätzung
  - 8.3 Informationssicherheitsrisikobehandlung

ISO 27001:2013

- 9 Leistungsauswertung
  - 9.1 Überwachung, Messung, Analyse und Auswertung
  - 9.2 Internes Audit
  - 9.3 Prüfung durch die Leitung
- 10 Verbesserung
  - 10.1 Fehler und Korrekturmassnahmen
  - 10.2 Laufende Verbesserung

ISO 27002:2013

- ISO 27002 enthält diverse Kontrollmechanismen:
  - 14 Überwachungsbereiche
  - 114 Sicherheitsmassnahmen
- Bereiche:
  - A.5 Informationssicherheitsleitlinien
    - A.5.1 Vorgaben der Leitung zur Informationssicherheit
      - A.5.1.1 Informationssicherheitsleitlinien
      - A.5.1.2 Prüfung der Informationssicherheitsleitlinien

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.6 Organisation der Informationssicherheit
    - A.6.1 Interne Organisation
      - A.6.1.1 Aufgaben und Zuständigkeiten im Bereich der IS
      - A.6.1.2 Aufgabentrennung
      - A.6.1.3 Kontakt zu Behörden
      - A.6.1.4 Kontakt mit Interessengruppen
      - A.6.1.5 Informationssicherheit im Projektmanagement
    - A.6.2 Mobilgeräte und Telearbeit
      - A.6.2.1 Leitlinie zu Mobilgeräten
      - A.6.2.2 Telearbeit

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.7 Personalsicherheit
    - A.7.1 Vor der Einstellung
      - A.7.1.1 Überprüfung
      - A.7.1.2 Arbeitsvertragsklauseln
    - A.7.2 Während der Anstellung
      - A.7.2.1 Verantwortung des Managements
      - A.7.2.2 Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit
      - A.7.2.3 Disziplinarverfahren
    - A.7.3 Beendigung und Wechsel der Anstellung
      - A.7.3.1 Zuständigkeiten bei Beendigung oder Wechsel der Anstellung

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.8 Management von organisationseigenen Werten
    - A.8.1 Verantwortung für organisationseigene Werte
      - A.8.1.1 Inventar der organisationseigenen Werte
      - A.8.1.2 Eigentum von organisationseigenen Werten
      - A.8.1.3 Zulässiger Gebrauch von organisationseigenen Werten
      - A.8.1.4 Rückgabe von organisationseigenen Werten
    - A.8.2 Klassifizierung von Informationen
      - A.8.2.1 Klassifizierung von Informationen
      - A.8.2.2 Kennzeichnung von Informationen
      - A.8.2.3 Handhabung von organisationseigenen Werten
    - A.8.3 Handhabung von Speicher- und Aufzeichnungsmedien
      - A.8.3.1 Verwaltung von Wechselmedien
      - A.8.3.2 Entsorgung von Medien
      - A.8.3.3 Transport physischer Medien

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.9 Zugriffskontrolle
    - A.9.1 Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle
      - A.9.1.1 Leitlinie zur Zugangskontrolle
      - A.9.1.2 Zugang zu Netzwerken und Netzwerkdiensten
    - A.9.2 Benutzerverwaltung
      - A.9.2.1 An- und Abmeldung von Benutzern
      - A.9.2.2 Zugangsbereitstellung für Benutzer
      - A.9.2.3 Verwaltung von Sonderzugangsrechten
      - A.9.2.4 Verwaltung geheimer Authentifizierungsdaten von Benutzern
      - A.9.2.5 Überprüfung von Benutzerberechtigungen
      - A.9.2.6 Entziehung oder Anpassung von Zugangsrechten
    - A.9.3 Benutzerverantwortung
      - A.9.3.1 Verwendung geheimer Authentifizierungsdaten von Benutzern

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.9.4 Kontrolle des Zugangs zu Systemen und Anwendungen
    - A.9.4.1 Beschränkung des Zugangs zu Informationen
    - A.9.4.2 Sichere Anmeldeverfahren
    - A.9.4.3 Kennwortmanagementsystem
    - A.9.4.4 Verwendung von Systemwerkzeugen
    - A.9.4.5 Kontrolle des Zugriffs auf Software-Quellcode
  - A.10 Kryptographie
    - A.10.1 Kryptographische Massnahmen
      - A.10.1.1 Leitlinie zur Nutzung von kryptographischen Massnahmen
      - A.10.1.2 Verwaltung kryptographischer Schlüssel

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.11 Schutz vor physischem Zugang und Umwelteinflüssen
    - A.11.1 Sicherheitsbereiche
      - A.11.1.1 Physische Sicherheitszonen
      - A.11.1.2 Physische Zugangskontrollen
      - A.11.1.3 Sicherung von Büros, sonstigen Räumen und Einrichtungen
      - A.11.1.4 Schutz vor externen und umweltbedingten Bedrohungen
      - A.11.1.5 Arbeit in Sicherheitsbereichen
      - A.11.1.6 Anlieferungs- und Ladezonen

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.11.2 Sicherheit von Betriebsmitteln
    - A.11.2.1 Platzierung und Schutz von Betriebsmitteln
    - A.11.2.2 Versorgungseinrichtungen
    - A.11.2.3 Sicherheit der Verkabelung
    - A.11.2.4 Instandhaltung von Betriebsmitteln
    - A.11.2.5 Entfernung von Werten
    - A.11.2.6 Sicherheit von Betriebsmitteln und Werten ausserhalb der Betriebsgebäude
    - A.11.2.7 Sichere Entsorgung oder Wiederverwendung von Betriebsmitteln
    - A.11.2.8 Unbeaufsichtigte Endgeräte
    - A.11.2.9 Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.12 Betriebssicherheit
    - A.12.1 Betriebsverfahren und Zuständigkeiten
      - A.12.1.1 Dokumentierte Betriebsverfahren
      - A.12.1.2 Änderungsmanagement
      - A.12.1.3 Kapazitätsmanagement
      - A.12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen
    - A.12.2 Schutz vor Malware
      - A.12.2.1 Kontrollmassnahmen gegen Malware
    - A.12.3 Backup
      - A.12.3.1 Datensicherungen

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.12.4 Protokollierung und Überwachung
    - A.12.4.1 Ereignisprotokollierung
    - A.12.4.2 Schutz von Protokollinformationen
    - A.12.4.3 Administrator- und Betreiberprotokolle
    - A.12.4.4 Zeitsynchronisation
  - A.12.5 Kontrolle von Betriebssoftware
    - A.12.5.1 Installation von Software auf betrieblichen Systemen
  - A.12.6 Technisches Schwachstellenmanagement
    - A.12.6.1 Management technischer Schwachstellen
    - A.12.6.2 Beschränkungen der Software-Installation
  - A.12.7 Auswirkungen von Audits auf Informationssysteme
    - A.12.7.1 Kontrollen für Audits von Informationssystemen

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.13 Sicherheit in der Kommunikation
    - A.13.1 Netzwerksicherheitsmanagement
      - A.13.1.1 Netzwerkkontrollen
      - A.13.1.2 Sicherheit von Netzwerkdiensten
      - A.13.1.3 Trennung in Netzwerken
    - A.13.2 Informationsübertragung
      - A.13.2.1 Leitlinien und Verfahren für die Informationsübertragung
      - A.13.2.2 Vereinbarungen zur Informationstransfer
      - A.13.2.3 Elektronische Nachrichtenübermittlung
      - A.13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen
    - A.14.1 Sicherheitsanforderungen für Informationssysteme
      - A.14.1.1 Analyse und Spezifikation von Sicherheitsanforderungen
      - A.14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzen
      - A.14.1.3 Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen
    - A.14.2.1 Leitlinie für sichere Entwicklung
    - A.14.2.2 Änderungskontrollverfahren
    - A.14.2.3 Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform
    - A.14.2.4 Beschränkung von Änderungen an Software-Paketen
    - A.14.2.5 Leitlinien zur sicheren Systementwicklung
    - A.14.2.6 Sichere Entwicklungsumgebung
    - A.14.2.7 Ausgelagerte Entwicklung
    - A.14.2.8 Systemsicherheitsprüfungen
    - A.14.2.9 Systemabnahmeprüfung
  - A.14.3 Prüfdaten
    - A.14.3.1 Schutz von Prüfdaten

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.15 Lieferantenbeziehungen
    - A.15.1 Informationssicherheit bei Lieferantenbeziehungen
      - A.15.1.1 Informationssicherheitsleitlinie für Lieferantenbeziehungen
      - A.15.1.2 Sicherheitsthemen in Lieferantenverträgen
      - A.15.1.3 Lieferkette für Informations- und Kommunikationstechnologie
    - A.15.2 Management der Dienstleistungserbringung durch Lieferanten
      - A.15.2.1 Überwachung und Prüfung von Lieferantendienstleistungen
      - A.15.2.2 Management von Änderungen an Lieferantendienstleistungen

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.16 Management von Informationssicherheitsvorfällen
    - A.16.1 Management von Informationssicherheitsvorfällen und Verbesserungen
      - A.16.1.1 Zuständigkeiten und Verfahren
      - A.16.1.2 Meldung von Informationssicherheitsereignissen
      - A.16.1.3 Meldung von Informationssicherheitsschwachstellen
      - A.16.1.4 Bewertung von und Entscheidung über Informationssicherheitsereignisse
      - A.16.1.5 Reaktion auf Informationssicherheitsvorfälle
      - A.16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen
      - A.16.1.7 Sammeln von Beweismaterial

ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.17 Informationssicherheitsaspekte des Betriebskontinuitätsmanagements
    - A.17.1 Aufrechterhaltung der Informationssicherheit
      - A.17.1.1 Planung der Aufrechterhaltung der Informationssicherheit
      - A.17.1.2 Implementierung von Verfahren zur Aufrechterhaltung der Informationssicherheit
      - A.17.1.3 Überprüfung, Überarbeitung und Auswertung von Maßnahmen zur Aufrechterhaltung der Informationssicherheit
    - A.17.2 Redundanzen
      - A.17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen

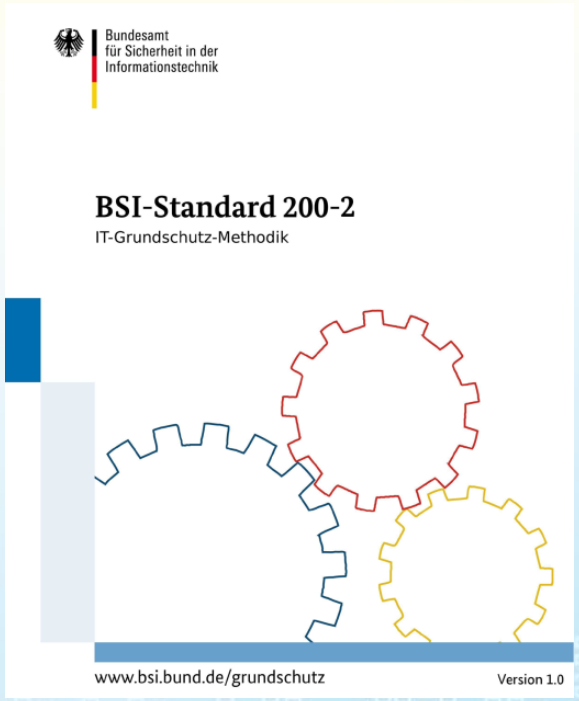
ISO 27002:2013

- Bereiche (Fortsetzung)
  - A.18 Richtlinienkonformität
    - A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen
      - A.18.1.1 Feststellung anwendbarer Gesetze und vertraglicher Anforderungen
      - A.18.1.2 Rechte an geistigem Eigentum
      - A.18.1.3 Schutz von Aufzeichnungen
      - A.18.1.4 Privatsphäre und Schutz von personenbezogenen Informationen
      - A.18.1.5 Regulierung kryptographischer Kontrollmassnahmen
    - A.18.2 Informationssicherheitsprüfungen
      - A.18.2.1 Unabhängige Prüfung der Informationssicherheit
      - A.18.2.2 Einhaltung der Sicherheitsleitlinien und -normen
      - A.18.2.3 Technische Konformitätsprüfung

Wie umsetzen?

- BSI-Standards 200-1 / 200-2 / 200-3

Aufbau ISMS



ISMS Methodik

Risiko-Analyse

Aufwand?

- Notwendiges Wissen erarbeiten
  - Kurse, Videos, Literatur
- Erstellen der notwendigen Dokumente
  - Vorlagen im Internet vorhanden, jedoch grosser Aufwand zur Anpassung
  - Evtl. externe Unterstützung
- Etablieren der Prozesse
- Regelmässige Kontrollen durchführen

- Kosten für Mitarbeiterzeit, technische Erweiterungen, externe Unterstützung, allfällige Zertifizierung

Nutzen?

- Management-Verbindlichkeit
- Klare Vorgaben für alle
- Nachvollziehbare Prozesse
- Risiken werden regelmässig bewertet und behandelt
- Informationssicherheit ist keine einmalige Sache

- (noch) Wettbewerbsvorteil
- Verbindlichkeit gegenüber Partner und Lieferanten

Fazit

Mit einem ISMS kann die Sicherheit definiert und erhöht werden.

Klare Prozesse und Vorgaben helfen allen.

Die Initialkosten sind hoch, aber auf die Dauer kann damit Geld gespart werden.