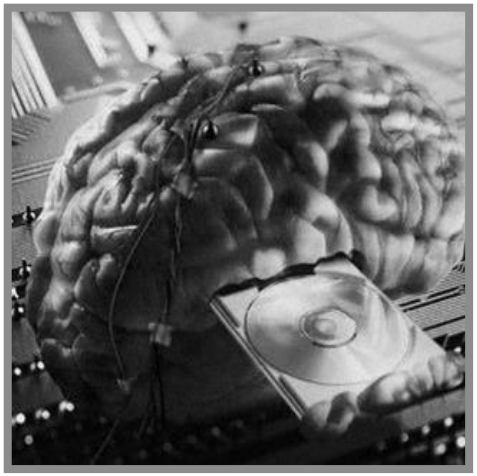
Advanced Aspects of IT-Infrastructures in Healthcare



Standards

Vorlesung
WS 2016

DI Birgit Scholz

INSO - Industrial Software
Institut für Rechnergestützte Automation | Fakultät für Informatik | Technische Universität Wien

Organisatorisches

Vorlesung
Do. 17:00 - 18:30, HS 14

Termine
- 20.10.2016 – Einführung Krankenhausumfeld, IT Strategie
- 27.10.2016 – Standards
- 03.11.2016
- 10.11.2016
- 24.11.2016
- 01.12.2016
- 15.12.2016
- 12.01.2017
- 19.01.2017

Abschlussprüfung
- 26.01.2017

Ziele innerhalb des IT Betriebs und deren Strategie

Abbildung 1: Strategisches Planungsmodell für den IT/MT-Betrieb, Quelle: Becker 1997

Beispiele – Fokus von Zielen

- **Strategische Ziele**
  - Grobkonzeption
  - Im Rahmen der Implementierung werden Feinkonzepte erstellt
- **Einsatzstrategie**
  - Investitions-, Kostenplanung, Budgets
  - Fachliche Ausrichtung
- **Systemstrategie**
  - Konzeption und Implementierung der IT Infrastruktur und der Anwendungslandschaft
  - Risikomanagement und Datenschutz
- **Organisationsstrategie/Ressourcenstrategie**
  - Siehe IT-Strategie, ITIL...

Betriebliche Abläufe vs. Sicherheit

Gibt es dafür Standards?

Normen für Sicherheit

- ISO (International Organization for Standardization)
  - Zentralsekretariat koordiniert in Genf die Normen
  - Gekennzeichnet mit ISO
  - www.iso.org
- IEC (International Electrotechnical Commission)
  - Mitglieder fördern IEC – Normen für Fragen
  - www.iec.ch
- Europäische EN-Normen
  - Werden von europäischen Normungsorganisationen CEN und CENELEC festgelegt
  - Gelten für alle Länder des Europäischen Wirtschaftsraums
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
  - Koordiniert Fragen der IT-Sicherheit in Bonn, zugeordnet der Bundesbehörde im Geschäftsbereich Bundesministerium für Inneres (DE)
    - IT-Grundschutz-Kataloge: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Normen für Sicherheit (Auszug)

- ISO 14001
  - Umweltmanagementnorm, Kontinuierlicher Verbesserungsprozess (Plan-Do-Check-Act, PDCA)
- ISO 15408 CC
  - Information technology – Security techniques – Evaluation criteria for IT security
  - Basiswerk für die Sicherheitsevaluierung von IT-Produkten
- ISO 15446
  - Information technology – Security techniques – Guide for the production of Protection Profiles and Security Target
  - Erstellung von Schutzprofilen und Sicherheitszielen

Normen für Sicherheit (Auszug)

- ISO 13335
  - Basiswerk für Sicherheitsmanagement, Referenz auf weitere Dokumente zum Sicherheitsmanagement
  - Konzepte und Modelle der Sicherheit, Techniken für RM und Sicherheitsmanagement, Auswahl von Sicherheitsmaßnahmen und Netzwerksicherheitsmanagement
- ISO 20000 (BS15000)
  - Servicemanagement und Informationssicherheitsmanagementsysteme (ISMS)
- ISO 27001 – BSI IT Grundschutzkatalog
  - Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Managementsystems für Informationssicherheit (ISMS)
  - Beschreiben damit einhergehende Maßnahmenziele und Maßnahmen
  - Gegenüberstellung: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile

Audits zur Zertifizierung

- Bsp: ISO 27001 - IT Grundschutzkatalog
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile (12.12.2015)
- Rollen beim Audit
  - Antragsteller: Antragsstellung, Beauftragung Auditor
  - Auditor bzw. Autitteamleiter: Durchführung des Audits, Nachweis Unabhängigkeit, Erstellung Auditbericht
  - BSI Zertifizierungsstelle: Verfahrensbeschreibung, Prüfung Auditbericht, Erteilung Zertifikat
- Unabhängigkeitserklärung
  - Um Interessenskonflikt zu vermeiden, z.B. bei
    - Vorhergehende Beratung
    - Geschäftliche Verbindungen
    - Verwandtschaftsverhältnis
- Re-Zertifizierung

Audits zur Zertifizierung

- Bsp: ISO 27001 - IT Grundschutzkatalog
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile (12.12.2016)
- Phasen im Audit
  - Dokumentenprüfung: Referenzdokumente, die von der zu auditierenden Institution erstellt und für die Zertifizierung eingereicht wurden
  - Umsetzungsprüfung vor Ort, ob ISO 27001 und IT-Grundschutz angemessen, korrekt, als auch die ISMS-Wirksamkeit umgesetzt wurde
- Audits:
  - Erst-Audits (ca. 3 Jahre gültig), Überwachungs-Audits (kein neuer Antrag notwendig), Re-Zertifizierungen
  - Bei wesentlichen Änderungen am zertifizierten Informationsverbund, wie Änderungen im Managementsystem, Organisation, Standortwechsel, Tätigkeitsfeldern

Audits zur Zertifizierung

- Bsp: ISO 27001 - IT Grundschutzkatalog
  - Beispiel: Physische und umgebungsbezogene Sicherheit
  - Maßnahmen und Maßnahmenziele sind gesetzt?
    - Sicherheit der Verkabelung
    - Spezifikation in ISO/IEC 27001
    - Umsetzungshinweise in ISO/IEC27002

ISO 27001 – IT Grundschutz: Infrastruktur

Für z.B. Allgemeines Gebäude, Elektronische Verkabelung, Büroraum/Lokaler Arbeitsplatz, Serverraum, Datenträgerarchive, Raum für technische Infrastruktur, Schutzschränke, Häuslicher Arbeitsplatz, Rechenzentrum, Mobiler Arbeitsplatz, Besprechungs-, Veranstaltungs- und Schulungsräume, IT-Verkabelung

- Serverraum Gefährdungslage

ISO 27001 – IT Grundschutz: Infrastruktur

Für z.B. Allgemeines Gebäude, Elektronische Verkabelung, Büroraum/Lokaler Arbeitsplatz, Serverraum, Datenträgerarchive, Raum für technische Infrastruktur, Schutzschränke, Häuslicher Arbeitsplatz, Rechenzentrum, Mobiler Arbeitsplatz, Besprechungs-, Veranstaltungs- und Schulungsräume, IT-Verkabelung

- Serverraum Gefährdungslage
  - Feuer, Wasser, Unzulässige Temperatur, Luftfeuchte, Ausfall von Patchfeldern durch Brand
  - Organisatorische Mängel durch fehlende Regelungen, Unbefugter Zutritt zu schutzbedürftigen Räumen
  - Technisches Versagen durch Ausfall der Stromversorgung, Versorgungsnetzte, Überspannung
  - Vorsätzliche Handlungen durch Manipulation von Geräten, an Informationen oder Software, Diebstahl

ISO 27001 – IT Grundschutz: Infrastruktur

- Serverraum Maßnahmenempfehlungen
  - Planung und Konzeption
    - Technische und organisatorische Vorgaben für Serverräume

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: Infrastruktur

- Serverraum Maßnahmenempfehlungen
  - Planung und Konzeption
    - Technische und organisatorische Vorgaben für Serverräume
    - Angepasste Aufteilung der Stromkreise
    - Handfeuerlöscher

ISO 27001 – IT Grundschutz: Infrastruktur

- Serverraum Maßnahmenempfehlungen
  - Planung und Konzeption
    - Technische und organisatorische Vorgaben für Serverräume
    - Angepasste Aufteilung der Stromkreise
    - Handfeuerlöscher
      - Brand klein halten: Sofortbekämpfung
      - DINEN 3 Tragbare Feuerlöscher in ausrechender Zahl und Größe (max. 20 kg)
      - Regelmäßig geprüft, leicht erreichbar
      - Kennzeichnung durch Schilder

      ? Sind geeignete HF im Brandfall leicht erreichbar?

      ? Werden die HF regelmäßig inspiziert und gewartet?

      ? Sind Mitarbeiter in die Benutzung der Handfeuerlöscher eingewiesen worden?

ISO 27001 – IT Grundschutz: Infrastruktur

- Serverraum Maßnahmenempfehlungen
  - Planung und Konzeption
    - Technische und organisatorische Vorgaben für Serverräume
    - Angepasste Aufteilung der Stromkreise
    - Handfeuerlöscher
      - Brand klein halten: Sofortbekämpfung
      - DINEN 3 Tragbare Feuerlöscher in ausrechender Zahl und Größe (max. 20 kg)
      - Regelmäßig geprüft, leicht erreichbar
      - Kennzeichnung durch Schilder

      ? Sind geeignete HF im Brandfall leicht erreichbar?

      ? Werden die HF regelmäßig inspiziert und gewartet?

      ? Sind Mitarbeiter in die Benutzung der Handfeuerlöscher eingewiesen worden?
    - Sichere Türen und Fenster
    - Gefahrenmeldeanlage
    - Vermeidung von wasserführenden Leitungen
    - Not-Aus-Schalter
    - Klimatisierung der Technikräume
    - Lokale unterbrechungsfreie Stromversorgung
    - Fernanzeige von Störungen
    - Redundanz, Modularität und Skalierbarkeit in der techn. Infrastruktur
    - Technische u. organisatorische Vorgaben für Serverräume
    - Brandschutz von Patchfeldern

ISO 27001 – IT Grundschutz: Infrastruktur

- Serverraum Maßnahmenempfehlungen
  - Umsetzung
    - Zutrittsregelung und – kontrolle
    - Rauchverbot
  - Betrieb
    - Geschlossene Fenster und Türen
    - Abgeschlossene Türen

ISO 27001 – IT Grundschutz: IT-Systeme

Für z.B. Allgemeiner Server, Unix, zSeries-Mainframe, Windows Server 2003, 2008, Allgemeiner Client, Laptop, Client unter Unix, unter Windows, Firewall , Virtualisierung, Terminalserver, Faxgerät, Mobiltelefon, Drucker

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Gefährdungslage
  - Organisatorisch: Unerlaubte Ausübung von Rechten,

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Gefährdungslage
  - Organisatorisch: Unerlaubte Ausübung von Rechten, Unzureichendes Schlüsselmanagement bei Verschlüsselung, Kompromittierung von Anmeldedaten bei Dienstleisterwechsel, Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen, Datenverlust beim Kopieren oder Verschieben von Daten
  - Menschliche: Fehlerhafte Administration von IT-Systemen, Fehlerhafte Zeitsynchronisation, Fehlerhafte Konfiguration, Verlust von BitLocker-verschlüsselten Daten
  - Technisch: Verlust gespeicherter Daten, SW-Schwachstellen oder –Fehler, Datenverlust beim Zurücksetzen des Kennworts
  - Vorsätzliche Handlungen: Abhören von Leitungen, Missbrauch von Administratorrechten, Vertraulichkeitsverlust schützenswerter Informationen, Unberechtigtes Erlangen von Administratorrechten

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Planung und Konzeption

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Planung und Konzeption
    - Planung der Windows Gruppenrichtlinien (XP, Vista, Windows 7)
    - Planung der Administration
    - Planung der Systemüberwachung
    - Planung des Einsatzes von Virtualisierung mit Hyper-V
    - Aktivierung von Windows-Systemen aus einem Volumenlizenzvertrag
    - Einsatz der Windows-Benutzerkontensteuerung
    - Aktivierung des Last Access Zeitstempels ab Windows Vista
    - Überblick über Neuerungen für Active Directory
    - Integritätsschutz ab Windows Vista

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Umsetzung
    - Einrichtung einer eingeschränkten Benutzerumgebung
    - Einsatz von Kommandos und Skripten
    - Nutzung von Rollen und Sicherheitsvorlagen
    - Passwortschutz unter Windows-Systemen
    - Geräteschutz
    - Umgang mit Diensten
    - Einsatz von Netzzugriffsschutz
    - Einsatz von IPSec unter Windows
  - Betrieb
    - Sicheres Löschen unter Windows
    - Patch-Management mit WSUS

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Aussonderung

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Aussonderung
    - Geregelte Deaktivierung und Löschung ungenutzter Konten
      - Benutzerkonto soll deaktiviert oder gelöscht werden
      - Anhand Dokumentation der Zugriffsberechtigungen muss überprüft werden, welche Berechtigungen das Konto in der IT-Umgebung hat und für welchen Authentisierungsvorgänge es benötigt wird

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Aussonderung
    - Geregelte Deaktivierung und Löschung ungenutzter Konten
      - Benutzerkonto soll deaktiviert oder gelöscht werden
      - Anhand Dokumentation der Zugriffsberechtigungen muss überprüft werden, welche Berechtigungen das Konto in der IT-Umgebung hat und für welchen Authentisierungsvorgänge es benötigt wird
      - Ungenützte Benutzerkonten, Benutzer- und administrative Konten
      - Rechte: z.B. Dateifreigaben – Windows Lauffähigkeit darf nicht eingeschränkt werden (Ersatzkonto) – sonst ggf. nicht mehr lesbar, Testdurchlauf
      - Konto muss aus Zugriffsberechtigungslisten (Access Control List) entfernt worden sein
      - Dokumentation zur geregelten Deaktivierung und Löschung von Benutzerkonten

      ? Werden Windows-Systeme regelmäßig auf ungenutzte administrative und Benutzerkonten überprüft?
      ? Werden bei Windows Systemen ungenutzte Benutzerkonten sofort deaktiviert?
      ? Wird bei Windows-Systemen vor dem Löschen von Benutzerkonten überprüft, auf welche Objekte die Berechtigung gesetzt sind?
    - Geregelte Außerbetriebnahme eines Verzeichnisdienstes

ISO 27001 – IT Grundschutz: IT-Systeme

- Windows Server 2008 Maßnahmenempfehlungen
  - Aussonderung
    - Geregelte Deaktivierung und Löschung ungenutzter Konten
      - Benutzerkonto soll deaktiviert oder gelöscht werden
      - Anhand Dokumentation der Zugriffsberechtigungen muss überprüft werden, welche Berechtigungen das Konto in der IT-Umgebung hat und für welchen Authentisierungsvorgänge es benötigt wird
      - Ungenützte Benutzerkonten, Benutzer- und administrative Konten
      - Rechte: z.B. Dateifreigaben – Windows Lauffähigkeit darf nicht eingeschränkt werden (Ersatzkonto) – sonst ggf. nicht mehr lesbar, Testdurchlauf
      - Konto muss aus Zugriffsberechtigungslisten (Access Control List) entfernt worden sein
      - Dokumentation zur geregelten Deaktivierung und Löschung von Benutzerkonten

      ? Werden Windows-Systeme regelmäßig auf ungenutzte administrative und Benutzerkonten überprüft?
      ? Werden bei Windows Systemen ungenutzte Benutzerkonten sofort deaktiviert?
      ? Wird bei Windows-Systemen vor dem Löschen von Benutzerkonten überprüft, auf welche Objekte die Berechtigung gesetzt sind?
    - Geregelte Außerbetriebnahme eines Verzeichnisdienstes
  - Notfallversorge
    - Erstellen eines Notfallplans für den Ausfall von Windows-Systemen
    - Regelmäßige Sicherung wichtiger Systemkomponenten für Win-Server

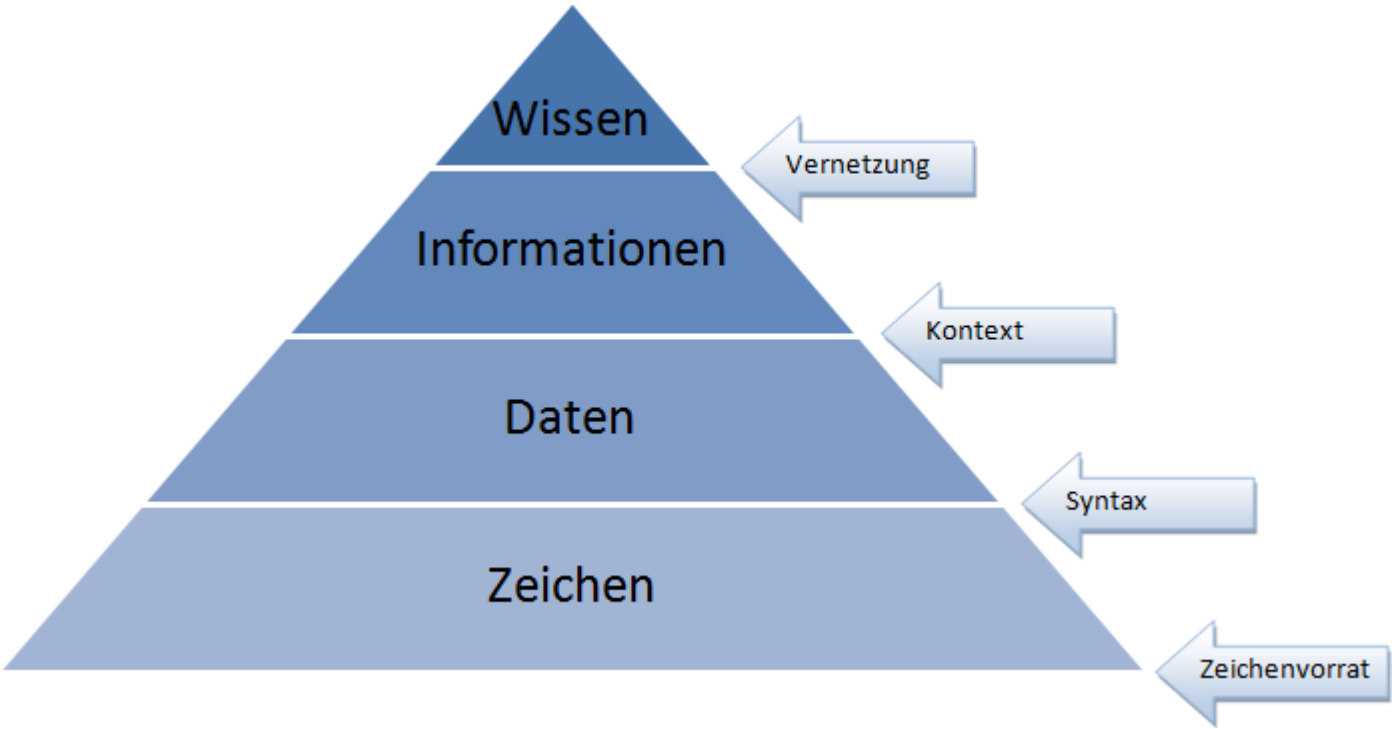
Informationen im Betrieb

Welche Informationen habe ich im Betrieb?

Warum muss ich das wissen?

Informationen im Betrieb

- Informationen unterschiedlichster Art im Betrieb zu finden
  - Zeichen
  - Daten
  - Informationen
  - Wissen



Source: https://vawiwm.wikispaces.com/Wissen

Sicherheitsbedürfnisse

- Verfügbarkeit
  - auch bei Systemausfall, kostenintensiv
- Integrität
  - Korrektheit, Manipulationsfreiheit und Unversehrtheit
- Verbindlichkeit
  - Rechtsverbindliche Kommunikation
- Überprüfbarkeit
  - Vlg. doppelte Buchführung
- Vertraulichkeit
  - Personenkreis, der auf die Daten zugreifen kann
- Anonymität
  - Selbsthilfegruppen vs. elektronischen Zahlungen
- Authentifikation
  - Passwort: password, 123456

ISO 27001 – IT Grundschutz: Anwendungen

Für z.B. Datenträgeraustausch, Webserver, Lotus Notes, Faxserver, Datenbanken, Telearbeit, SAP System, Mobile Datenträger, Active Directory, DNS-Server, Internet-Nutzung, OpenLDAP, Webanwendungen, Protokollierung, Cloud Management, Web-Services, Allgemeine Anwendungen

ISO 27001 – IT Grundschutz: Anwendungen

- Webanwendungen Gefährdungslage
  - Organisatorisch: Unzureichende Kontrolle der Sicherheitsmaßnahmen,

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: Anwendungen

- Webanwendungen Gefährdungslage
  - Organisatorisch: Unzureichende Kontrolle der Sicherheitsmaßnahmen, Unerlaubte Ausübung von Rechten, Fehlende Auswertung von Protokolldaten, Fehlende Dokumentation, Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten, Verwendung von unsicheren Protokollen, Unzureichende Schulung der Mitarbeiter, Mängel bei der Entwicklung der Webanwendung und Web-Services
  - Menschlich: Konfiguration- und Bedienungsfehler, Ungeeigneter Umgang mit Passwörter
  - Technisch: SW-Schwachstellen, Schlechte Authentikation, Unsichere kryptographische Algorithmen
  - Vorsätzlicher Handlungen: Ausprobieren von Passwörtern, Missbrauch von Benutzerrechten, Verhinderung von Diensten, Web-Spoofing, SQL-Injection, Fehler in der Logik, Unzureichendes Session-Management, Cross-Site Scripting (XSS), Injection-Angriffe, Clickjacking

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Planung und Konzeption

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Planung und Konzeption
    - Regelung des Passwortgebrauchs
    - Einrichten der Zugriffsrechte
    - Erstellung eines Anforderungskatalogs für Standardsoftware
    - Schutz gegen SQL-Injection
    - Dokumentation der Architektur von Webanwendungen und Web-Services
    - Web-Tracking
    - Auswahl einer Authentisierungsmethode für Webangebote
    - Systemarchitektur einer Webanwendung
    - Serverseitige Verwendung von SSL/TLS

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Umsetzung
    - Authentisierung bei Webanwendungen
    - Sichere Konfiguration von Webanwendungen
    - Schutz vertraulicher Daten bei Webanwendungen
    - Zugriffskontrolle
    - Verhinderung Cross-Site Request Forgery (Angreifer führt eine Transanktion in einer Webanwendung durch, obwohl Anwender angemeldet ist)

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Vergabe von Zugriffsrechten
    - Dokumentation der zugelassenen Benutzer und Rechteprofile
    - Dokumentation der Veränderungen an einem bestehenden System
    - Informationsbeschaffung über Sicherheitslücken des Systems
    - Kontrolle der Protokolldateien
    - Schulung von Sicherheitsmaßnahmen
    - Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests
      - Gibt die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System wieder
      - Ansatzpunkte: Netzkoppelelemente (Router, Switches), Server (Datenbanken, Webserver), Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop), Web-Services (REST-Interface, SOAP-API, SOA),…
      - Sollten regelmäßig durchgeführt werden
      - Typische Angriffstechniken:
        Netzwerk- und Portscanning um genutzte Dienste (Ports) zu identifizieren,
        Denial-of-Service-Angriffe (DoS): Ziel ist es einen oder mehrere Dienste außer Betrieb zu setzen (z.B. vermehrte Anfragen durch E-Mails)
        Passwort-Attacken
        Information Gathering: Sammlung von pot. Nützlichen Informationen, z.B. verwendete Nummerierungsschema für Verzeichnisse oder Server
        SQL-Injection auf Datenbankebene Manipulation

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests
      - Gibt die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System wieder
      - Ansatzpunkte: Netzkoppelelemente (Router, Switches), Server (Datenbanken, Webserver), Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop), Web-Services (REST-Interface, SOAP-API, SOA),…
      - Sollten regelmäßig durchgeführt werden
      - Typische Angriffstechniken:
        Netzwerk- und Portscanning um genutzte Dienste (Ports) zu identifizieren,
        Denial-of-Service-Angriffe (DoS): Ziel ist es einen oder mehrere Dienste außer Betrieb zu setzen (z.B. vermehrte Anfragen durch E-Mails)
        Passwort-Attacken
        Information Gathering: Sammlung von pot. Nützlichen Informationen, z.B. verwendete Nummerierungsschema für Verzeichnisse oder Server
        SQL-Injection auf Datenbankebene Manipulation

      ? Wird für Penetrationtests ausschließlich zuverlässiges und qualifiziertes Personal eingesetzt?
      ? Wurde im Vorfeld der Penetrationstests das Einverständnis aller zuständigen Stellen eingeholt?
      ? Wurden die Ansprechpartner und deren Erreichbarkeit für den Zeitraum der Durchführung von Penetrationstests verbindlich festgelegt?
      ? Werden Abschlussberichte den IT-Sicherheitsbeauftragten und den verantwortlichen Führungskräften vorgelegt?

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests – Kriterien eines Dienstleisters

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests – Kriterien eines Dienstleisters
      - Programmiersprachen
      - Schwachstellenscanner
      - Administration von Betriebssystemen und Anwendungen
      - Netzwerkprotokolle und Auswertung von Netzwerkverkehr
      - Sicherheitsprodukte (z.B. Sicherheitsgateways, Intrusion Detection Systeme)

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests - Vorgehensweise
      - Vereinbarung über die Verschwiegenheitspflichten
      - Vereinbarungen über den Einsatz von Hard- und Software

Source: https://vawiwm.wikispaces.com/Wissen

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests - Vorgehensweise
      - Vereinbarung über die Verschwiegenheitspflichten
      - Vereinbarungen über den Einsatz von Hard- und Software
      - Vereinbarungen über die zu testenden IT-Systeme und IT-Anwendungen
      - Festlegung von erlaubten und unerlaubten Aktivitäten der Penetrationstester, um Schäden möglichst zu vermeiden
      - Festlegung über den Ort der Durchführung sowie zur Auswertung und Berichterstellung für den Penetrationstest
      - Festlegung eines Terminplans einschließlich Wartungsfenster für die Durchführung der Tests
      - Detaillierte Vereinbarung über den Zugang zum Internet beziehungsweise den Anschluss von Testsystemen an das Internet
      - Vereinbarung über Zuständigkeiten und die Erreichbarkeit von Ansprechpartnern sowie zur Notfallversorge

ISO 27001 – IT Grundschutz: Infrastruktur

- Webanwendungen Maßnahmenempfehlungen
  - Betrieb
    - Durchführung von Penetrationtests – Kriterien eines Dienstleisters
      - Programmiersprachen
      - Schwachstellenscanner
      - Administration von Betriebssystemen und Anwendungen
      - Netzwerkprotokolle und Auswertung von Netzwerkverkehr
      - Sicherheitsprodukte (z.B. Sicherheitsgateways, Intrusion Detection Systeme)
    - Durchführung von Penetrationtests - Vorgehensweise
      - Vereinbarung über die Verschwiegenheitspflichten
      - Vereinbarungen über den Einsatz von Hard- und Software
      - Vereinbarungen über die zu testenden IT-Systeme und IT-Anwendungen
      - Festlegung von erlaubten und unerlaubten Aktivitäten der Penetrationstester, um Schäden möglichst zu vermeiden
      - Festlegung über den Ort der Durchführung sowie zur Auswertung und Berichterstellung für den Penetrationstest
      - Festlegung eines Terminplans einschließlich Wartungsfenster für die Durchführung der Tests
      - Detaillierte Vereinbarung über den Zugang zum Internet beziehungsweise den Anschluss von Testsystemen an das Internet
      - Vereinbarung über Zuständigkeiten und die Erreichbarkeit von Ansprechpartnern sowie zur Notfallversorge

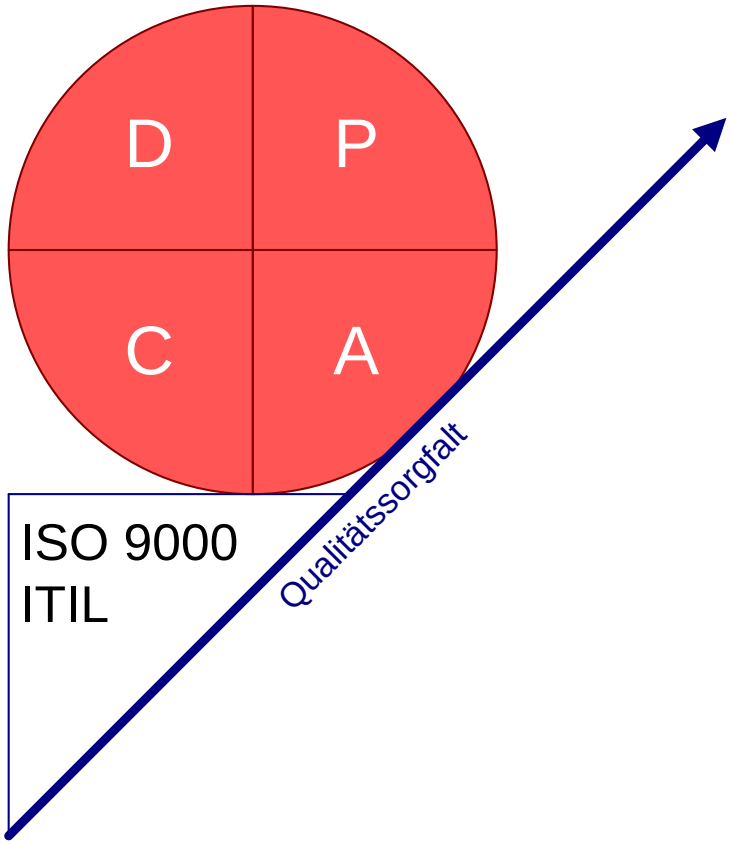
Betriebliche Leistungen

Wie halte ich die Qualität bzw. die Sicherheit?

Qualität

Quality Management

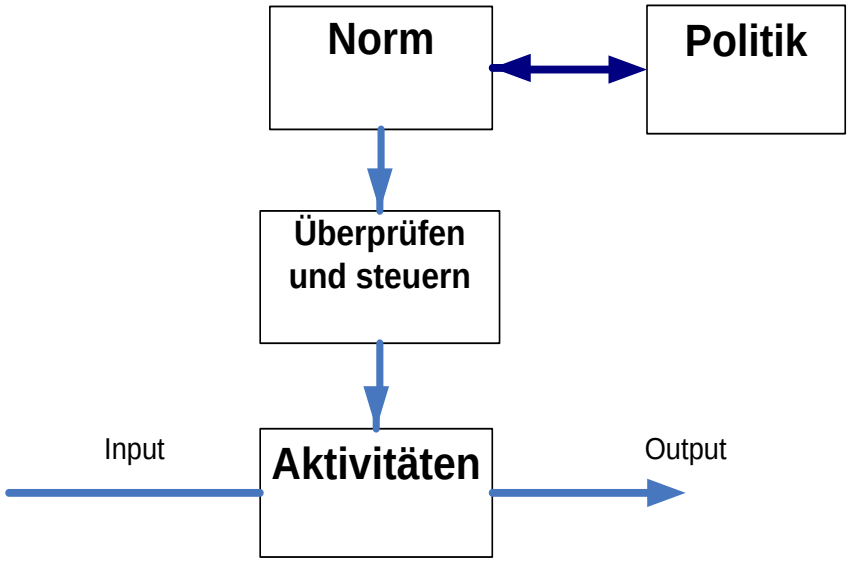
- Plan
- Do
- Check
- Act



Prozess

Prozess

- ist eine logische Reihenfolge von Aktivitäten um ein gewisses Ziel zu erreichen



IT Service Management Lifecycle

- IT Infrastructure Library (ITIL) is the most widely accepted approach to IT Service Management. It provides a best-practice framework for identifying, planning, delivering and supporting IT services to the business.

ITIL V3 Components

ITIL – im Detail

- ITIL – IT Infrastructure Library
- Publikationen
- Best Practices für IT Service Management
- Worldwide Industry standards
  - Processes
  - Guidelines
  - Checklisten
- Management Philosophy

Source: https://vawiwm.wikispaces.com/Wissen

ITIL – Service Lifecycle

- **Service Strategy**
  - Financial management
  - Service portfolio management
  - Demand management
- **Service Design**
  - Service catalogue management
  - Service level management
  - Availability management
  - Capacity management
  - IT Service continuity management
  - Information security management
  - Supplier management
- **Service Transition**
  - Release and deployment management
  - Transition planning and support
  - Service validation and testing
  - Service asset and configuration management
  - Change management
  - Knowledge management
- **Service Operation**
  - Problem management
  - Incident management
  - Request fulfilment
  - Event management
  - Access management
- **Continual Service Improvement**
  - Service measurement & reporting
  - 7-step improvement process

ITIL – Service Lifecycle

- **Service Strategy**
  - Financial management
  - Service portfolio management
  - Demand management
- **Service Design**
  - Service catalogue management
  - Service level management
  - Availability management
  - Capacity management
  - IT Service continuity management
  - Information security management
  - Supplier management
- **Service Transition**
  - Release and deployment management
  - Transition planning and support
  - Service validation and testing
  - Service asset and configuration management
  - Change management
  - Knowledge management
- **Service Operation**
  - Problem management
  - Incident management
  - Request fulfilment
  - Event management
  - Access management
- **Continual Service Improvement**
  - Service measurement & reporting
  - 7-step improvement process

→ Auch für Analysen nützlich!
z.B: Strukturanalyse für Betrieb, Disaster Recovery Pläne

Danke für Ihre Aufmerksamkeit!