gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Grundlagen eines Audits

Dr. Bernd Schütze, Deutsche Telekom Healthcare and Security Solutions GmbH

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Agenda

- Begriffsbestimmungen
- Warum ein Datenschutzaudit?
- Kompetenz eines Auditors
- Ablauf eines Audits
  1) Vorbereitung des Audits („Auditplan“)
  2) Prüfung der Unterlagen
  3) Durchführung des Audits
  4) Erstellung Abschlussbericht
- Checklisten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

BEGRIFFSBESTIMMUNGEN

Anregungen aus der Welt der Normen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- DIN EN ISO/IEC 19011: „Leitfaden zur Auditierung von Managementsystemen“
  - Keine spezielle Norm für ein Datenschutzaudit
- ISO/IEC 17021 „Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“
  - Anforderungen für eine Drittparteien-Zertifizierung von Managementsystemen
- Grobe Zuweisung
  - Internes Audit: DIN EN ISO/IEC 19011
  - Externes Audit: ISO/IEC 17021
- Bzgl. Begriffsbestimmungen Anlehnung an DIN EN ISO/IEC 19011

Akteure

- Auditor
  - Person, die ein Audit durchführt
- Auditteam
  - ein oder mehrere Auditoren,
  - die ein Audit durchführen,
  - nötigenfalls unterstützt durch Fachexperten
- Fachexperte
  - (Natürliche) Person,
  - die dem Auditteam spezifisches Wissen oder
  - Fachkenntnisse zur Verfügung stellt
- Beobachter
  - Person, die das Auditteam begleitet, aber nicht auditiert
- Betreuer
  - Person, die von der zu auditierenden Organisation benannt wird, um das Auditteam zu unterstützen

Verfahren

- Audit
  - systematischer, unabhängiger und dokumentierter Prozess zur
  - Erlangung von Auditnachweisen und
  - zu deren objektiver Auswertung,
  - um zu ermitteln, inwieweit die Auditkriterien erfüllt sind
- Auditkriterien
  - Verfahren, Vorgehensweisen oder Anforderungen, die als
  - Bezugsgrundlage (Referenz) verwendet werden,
  - anhand derer ein Vergleich mit dem Auditnachweis erfolgt
- Auditnachweis
  - Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen,
  - die für die Auditkriterien zutreffen und
  - verifizierbar sind

Verfahren

- Auditfeststellungen
  - Ergebnisse aus der
  - Bewertung der gesammelten Auditnachweise
  - im Hinblick auf Auditkriterien
- Auditplan
  - Beschreibung der Tätigkeiten und Festlegungen für ein Audit
- Auditumfang
  - Ausmaß und Grenzen eines Audits

Auditarten

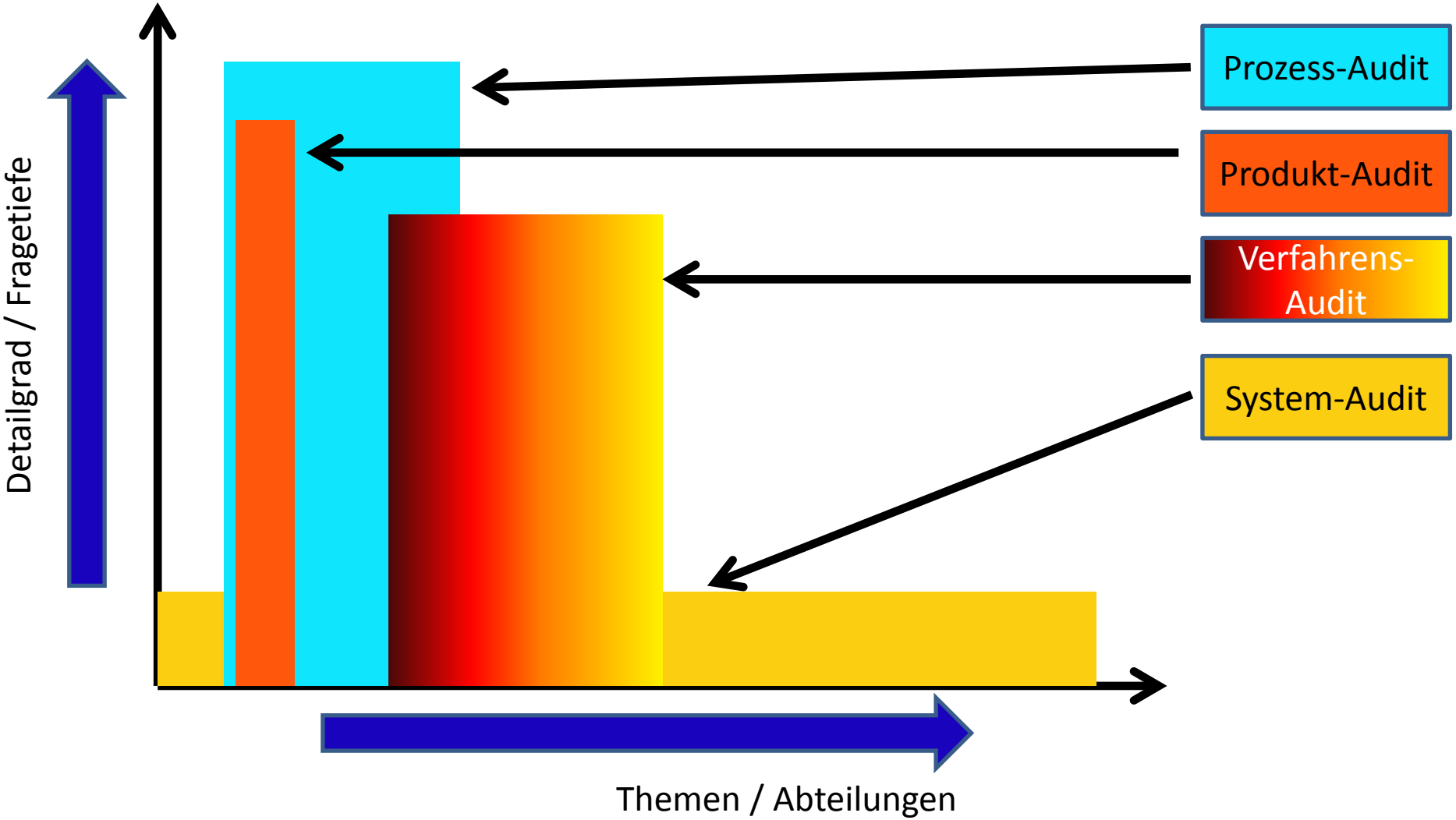
- Systemaudit
  - Datenschutzsystem wird auf Vollständigkeit, Zweckmäßigkeit und praktische Umsetzung überprüft und beurteilt
- Produktaudit
  - (End-)Produkte und Dokumentation(en) werden unter Berücksichtigung datenschutzrelevanter Aspekte überprüft und beurteilt
- Verfahrensaudit
  - Eingesetzte Datenverarbeitungsverfahren werden bzgl. richtiger Umsetzung der Vorgaben seitens Verantwortlichen sowie auf Einhaltung der rechtlichen Vorgaben geprüft
- Prozessaudit
  - Ein oder mehrere festgelegte Prozesse werden bzgl. Compliance zu datenschutzrechtlichen Vorgaben untersucht
- Konformitätsaudit
  - Prüfung erfolgt auf Grundlage eines vorgegebenen Katalogs, z. B. Verhaltensregeln oder eines Code of Conduct, der für den zu prüfenden Bereich gilt

Auditarten

- Einzelaudit
  - Es erfolgt genau ein Audit in einem Unternehmen
- Kombiniertes Audit
  - Zwei oder mehr Managementsysteme unterschiedlicher Ausrichtungen werden zugleich geprüft
  - Beispiel:
    - Qualitätsmanagementsystem, Umweltmanagementsystem, Datenschutzmanagementsystem, IT-Sicherheitsmanagementsystem werden zugleich gerüft
- Gemeinschaftliches Audit
  - Zwei oder mehrere Organisationen werden gleichzeitig auditiert
  - Beispiel: Auftragsverarbeiter und Sub-Auftragsverarbeiter werden an Hand der Vereinbarungen aus dem Auftragsverarbeitungsvertrag bzgl. deren Einhaltungen auditiert

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Detailtiefe des Audits



gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

WARUM EIN DATENSCHUTZAUDIT?

Interesse der datenverarbeitenden Stelle

- Gewährleistung der Rechtsicherheit der Verarbeitung personenbezogener Daten
- Ergebnis erlaubt interne Verbesserungen bzgl. Datenschutz oder Datensicherheit
- Ergebnis kann in der Außendarstellung zur Verbesserung der Außenwahrnehmung eingesetzt werden
- Audit liefert vergleichbare Ergebnisse in Bezug auf Marktmitbewerber
  - Unterschiede können der Öffentlichkeit vermittelt werden
- Ergebnis darf nicht zu Wettbewerbsverzerrungen führen
  - Kein Zwang zu deutlich höherem Ressourcenverbrauch, so dass Angebot Mitbewerber unverhältnismäßig günstiger erscheinen
- Kosten für Audit müssen im Verhältnis zum Ergebnis im vertretbaren Rahmen liegen
  - Audit darf nicht bürokratisch „überbläht“ sein
  - Dokumentationsaufwand muss im Rahmen liegen

Interesse betroffener Personen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Interesse an Datenschutz/Datensicherheit nimmt in der Globalisierung zu
- Transparenz zwischen unterschiedlichen vergleichbaren Angeboten wichtig
- Bei gleicher Qualität und vergleichbarem Preis ist Datensparsamkeit gegenüber „Datenkraken“ ein wichtiges Argument
- Begrenzung der Risiken der Verarbeitung der eigenen Daten, d.h. Fortschritte bei Datenschutz und Sicherheit der Verarbeitung
  - (Nachvollziehbare) Reaktion auf neue Risiken
  - Nutzung neuer Möglichkeiten zur Gewährleistung der Sicherheit
- Audit muss von neutraler Stelle ausgeführt werden, d.h. Gewährleistung
  - Objektivität und Korrektheit der Überprüfung
  - Glaubwürdigkeit der Ergebnisse

Interesse der Allgemeinheit

- Gesellschaftliche wie auch individuelle Gefährdungs- und Schadenspotential in der Verarbeitung personenbezogener Daten reduzieren
  - Nur öffentliche Prämierung der „Besten“ führt zum Nachahmungseffekt
  - → Kontinuierliche Verbesserung des Datenschutzes
  - Cave: „Prangerwirkung“ kein Nachahmungseffekt; Abschreckung zur Prozess-Verbesserung eher ungeeignet
- Unterstützung und Entlastung der Datenschutz-Aufsichtsbehörden durch
  - Verbesserte Umsetzung von Datenschutzanforderungen
  - Unabhängige Kontrolle von Verarbeitungsvorgängen
- Öffentliche Darstellung, dass ergriffene Datenschutzmaßnahmen belohnt werden,
  - führt bei Datenverarbeitern zu einem höheren Bedarf an entsprechenden Maßnahmen
  - führt in der Bevölkerung zu mehr Datenschutz-Bewußtsein und erhöht so langfristig die Nachfrage

→ Politik gefordert, hier entsprechende Anreizsysteme zu schaffen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

KOMPETENZ EINES AUDITORS

Grundlegende Anforderungen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Ethisches Verhalten
  - Vertrauen, Integrität, Diskretion
- Unabhängigkeit
  - Unparteilichkeit und Objektivität bzgl. Audit sowie daraus resultierender Schlussfolgerungen muss gewährleistet sein
- Sorgfältigkeit
  - Anwendung von Sorgfalt beim Auditieren
- Zuverlässigkeit
  - Pflicht, wahrheitsgemäß und genau zu berichten

Bewertungskriterien

- Qualitativ, z. B.
  - Nachgewiesenes persönliches Verhalten
  - Wissen oder die Leistungsfähigkeit in Bezug auf benötigte Fertigkeiten
  - Ausbildung
- Quantitativ, z. B.
  - Jahre an Berufserfahrung
  - Anzahl durchgeführten Audits
  - Stunden an Auditschulungen

Benötigte Kompetenz beim Datenschutz-Audit

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Insbesondere

- Gute Kenntnisse in Bezug auf Gesetze und Vorschriften, die sich mit Datenschutz und Informationssicherheit befassen
  - Eigene Ausbildung zum geprüften Datenschutzbeauftragten sollte vorhanden sein
- Wissen und Fertigkeiten in Bezug auf die Branche, die auditiert wird
  - Insbesondere branchenspezifische normative Regelungen
  - Kenntnisse der spezifischen Anforderungen der interessierten Parteien
- Untersuchung und Bewertung von Aufzeichnungsverfahren durch Befragung, Beobachtung und Validierung
- Beurteilung von Verfahren zur Informationsgewinnung und -überwachung
- Sicherheitsmanagement-relevante Terminologie
  - Beurteilung der Angemessenheit und Leistungsfähigkeit von Protokollierungssystemen
  - Risikobewertung und Beurteilung der Risikominderung
  - Kenntnis von Methoden und Praktiken zur Untersuchung von Vorfällen
  - Kenntnis von Methoden und Praktiken zur Überwachung der Sicherheitsleistung
- Beurteilung menschliches Verhalten und Interaktion, insbesondere
  - Analyse der menschlichen Faktoren in Bezug auf Sicherheitsmanagement
  - Interaktion von Menschen, Maschinen, Prozessen und der Arbeitswelt
- Entwicklung proaktiver und reaktiver Leistungsgrößen und -indikatoren

Benötigte Kompetenz beim Datenschutz-Audit

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Beispiel

- Bundeswehrkrankenhaus: Kenntnisse Landeskrankenhausgesetze uninteressant, aber dafür Soldatengesetz & Co. relevant
- Nicht-kirchliches Krankenhaus: Regelungen der Kirchen uninteressant, aber ggf. entsprechendes Landesrecht
- Cave:
  - Überall Kenntnisse bzgl. Patientenversorgung unerlässlich
  - Ansonsten kann Erfordernis zur Patientendatenverarbeitung nicht geprüft werden

  → Ohne hinreichende Kenntnis muss Auditor Erfordernis der Verarbeitung glauben

  → D.h. es findet keine Prüfung mehr statt

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

ABLAUF EINES AUDITS

Wie häufig ist ein internes Audit erforderlich?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Abhängig von verschiedenen Faktoren
- Insbesondere sind zu berücksichtigen
  - Art, Umfang und Komplexität der Verarbeitung
  - Bedeutung der Verarbeitung hinsichtlich Datenschutzaspekten
  - Rechtliche Anforderungen
  - Externe Anforderungen, z. B. durch Kunden
  - Status und Bedeutung der Einhaltung datenschutzrechtlicher Vorgaben für de jeweiligen Bereiche
  - Risikostatus der auditierten Organisation
  - Prüfergebnisse von Aufsichtsbehörden
  - Ergebnisse vorhergehender Audits

1) Vorbereitung des Audits

Erstellen eines Auditplans

- Definition der Audit-Zielsetzungen
- Festlegung des Auditumfangs
- Festlegung des Auditteams
- Erstellung einer Checkliste
- Bereitstellung der Mittel
- Prüfung der Autorisierung
- Kontaktaufnahme mit zu auditierenden Bereich

2) Prüfung der Unterlagen

Auswertung bereitgestellter Unterlagen, z. B.

- Datenschutzunterlagen
- Verfahrens-, Prozessbeschreibungen
- Auftragsverarbeitungen
- Funktionsübertragungen

3) Durchführung des Audits

- Einsicht in Unterlagen vor Ort
- Interviews
- Verfolgung von Vorgängen
  - Inkl. Stichproben bzgl. Einhaltung von Verfahrens- und Prozessbeschreibungen
- Verifizierung Ergebnisse der Verfahren mit Verfahrensbeschreibung
- Beobachtungen und Bewertung der Abläufe
- Ergebnisdiskussion
- Abschlussbericht

4) Erstellung Abschlussbericht

- Zusammenfassung der Auditergebnisse
- Bewertung der Auditergebnisse
- Zusammenstellung festgestellter Abweichungen
- Ggf. Vorschläge für Korrekturen/Verbesserungen

1) VORBEREITUNG DES AUDITS

Auditplan

- Umfang des Auditprogramms festlegen
  - Geltungsbereich, z.B.
    - Personalabteilung
    - Abrechnungsabteilung
    - IT-Abteilung
    - Station xy
    - Vollständiges Krankenhaus
  - Inhaltlicher Umfang, z.B.
    - In Personalabteilung
      - Nur Rekruiting
      - Ausschließlich Gehaltsabrechnung
    - In IT-Abteilung
      - Nur Fernwartungsvorgänge
  - Ergebnisse bzw. Schlussfolgerungen aus früheren internen bzw. externen Audits berücksichtigen

→ Merke: Audit immer nur eine Stichprobe aus dem Tagesgeschäft, d.h. Festlegung der Themen der Stichprobe entscheidet über Effektivität und Ergebnisse des Audits

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
  - Wer leitet das Audit?
  - Welche Fachexperten werden benötigt?
  - Wer betreut das Auditteam?
  - Wer beobachtet die Auditierung?
    - Hinweis: zur Beurteilung der Qualität des Audits durch den Auftraggeber ist die Begleitung des Auditors durch fachkundige Personen nahezu unerlässlich
  - Liegen für das Audit notwendige Autorisierungen vor?
    - Z. B. Betreten von Serveräumlichkeiten, OP, … oder Einblick in Geschäftsbücher/Geschäftsgeheimnisse

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
- Erforderliche Ressourcen prüfen
  - Sind alle benötigten Fachexperten sind vorhanden?
  - Ist ein Betreuer benannt worden?
  - Welche Unterlagen werden benötigt? Ist ein Einblick vor dem Audittermin möglich?
  - Benötigte Autorisierungen vorhanden?
  - Existieren ggf. Kontaktmöglichkeiten (Mobiltelefonnummer, Durchwahl, …) mit Unternehmensleitung, um Fragen bzgl. Autorisierung direkt beim Audit klären zu können?
  - Sind vor Ort alle benötigten Interviewpartner vorhanden?
    - Ggf. Urlaub beachten; nicht für jede Person existiert Stellvertreter

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
- Erforderliche Ressourcen prüfen
- Bei Konformitätsaudit
  - Katalog zur Prüfung vorgegeben und vorhanden?
  - Passt Katalog zum zu auditierenden (Fach-)Bereich?
  - Beachtet Katalog alle relevanten rechtlichen und fachlichen Vorgaben?
    - Wenn nicht: Auftraggeber bzgl. Lücken informieren!

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
- Erforderliche Ressourcen prüfen
- Bei Konformitätsaudit
- Termin und Dauer des Audit
  - Wann findet das Audit statt?
  - Gesamtdauer als auch Dauer für Interviews festlegen

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
- Erforderliche Ressourcen prüfen
- Bei Konformitätsaudit
- Termin und Dauer des Audit
- Weitere Rahmenbedingungen beachten, z.B.
  - Ggf. Sprache, kulturelle und soziale Belange berücksichtigen
  - Anliegen interessierter Parteien, wie z. B. Kundenbeschwerden
  - Geplante Absprachen bezüglich der relevanten Managementnormen, der rechtlichen und vertraglichen Anforderungen
  - Verfügbarkeit von Informations- und Kommunikationstechnologien zur Unterstützung der
  - Audittätigkeiten, insbesondere die Verwendung von Remote-Auditmethoden

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
- Erforderliche Ressourcen prüfen
- Bei Konformitätsaudit
- Termin und Dauer des Audit
- Weitere Rahmenbedingungen beachten
- Erstellen von Arbeitsdokumenten, z.B.
  - Checklisten
  - Formblätter zur Aufzeichnung von Informationen wie z.B.
    - Nachweise
    - Auditfeststellungen
    - Sitzungsprotokollen

Auditplan

- Umfang des Auditprogramms festlegen
- Verantwortlichkeiten für das Audit festlegen
- Erforderliche Ressourcen prüfen
- Bei Konformitätsaudit
- Termin und Dauer des Audit
- Weitere Rahmenbedingungen beachten
- Erstellen von Arbeitsdokumenten
- Ggf. Erstellung von Empfehlungen basierend auf Auditergebnis (Je nach Auftrag)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

2) PRÜFUNG DER UNTERLAGEN

Benötigte Unterlagen

- Neben rechtlichen Vorgaben sind insbesondere unternehmensinterne Regelungen von Bedeutung; Vorgaben z.B. aus
  - QM (Verfahrensanweisungen, Prozessbeschreibungen, …)
  - IT (z.B. Backup-Konzept, Protokollierungskonzept, Berechtigungskonzept)
  - Medizinischer Versorgungsbereich (z.B. „Best-Practice“-Regelungen der Fachgesellschaften, Kammervorgaben)
- Für Datenschutz-Audit unabdingbar: Zugriff auf Datenschutz-Unterlagen, insbesondere
  - Datenschutzkonzept
  - ADV-Verträge
  - Schulungsunterlagen, d.h. Schulungskonzept, Schulungsinhalte, Frequenz und Teilnehmerbereich (z.B. IT-Beschäftigte, Pflegepersonal) der Schulungen
- Idealerweise alle Unterlagen vor Audit erhalten
  - Nur so optimale Möglichkeit zur Vorbereitung
  - Hierzu angemessener Zeitraum zur Prüfung (insbesondere der Vollständigkeit) der Dokumente unabdingbar

→ Aus Unterlagen ergeben sich ggf. Hinweise bzgl. im Audit zu prüfender Themen!

3) DURCHFÜHRUNG

Durchführung des Audits

- Eröffnungsbesprechung; Zweck
  - Zustimmung aller am Audit beteiligten Parteien bestätigen
  - Auditteam vorstellen einschließlich der Beobachter und Betreuer, sowie eine Kurzdarstellung ihrer Rolle
  - Gewährleisten, dass alle geplanten Audittätigkeiten durchgeführt werden können

Durchführung des Audits

- Eröffnungsbesprechung
- Prüfen von Dokumenten während der Durchführung des Audits
  (soweit nicht vorher erfolgt)
  - Prüfung der Dokumentation bzgl.
    - Konformität des Systems, soweit dokumentiert, mit den Auditkriterien
    - Informationen zur Unterstützung der Audittätigkeiten sammeln

Durchführung des Audits

- Eröffnungsbesprechung
- Prüfen von Dokumenten während der Durchführung des Audits
- Kommunikation während des Audits
  - Regelmäßige Darstellung des Stands des Audits durch Auditteamleiter gegenüber Auditteam
  - (Kurze) Darstellung der Ziele gegenüber Interviewpartner: Was wird speziell mit diesem Interview bezweckt?
    - Transparenz im Audit unerlässlich für optimale Zusammenarbeit
    - Interviewpartner muss Ziele kennen, um bestmöglich alle relevanten Informationen darstellen zu können

Durchführung des Audits

- Eröffnungsbesprechung
- Prüfen von Dokumenten während der Durchführung des Audits
- Kommunikation während des Audits
- Sammeln und Verifizieren von Informationen
  - Methoden zum Sammeln von Informationen schließen insbesondere ein
    - Befragungen
    - Beobachtungen
    - Überprüfung von Dokumenten einschließlich Aufzeichnungen

Durchführung des Audits

- Eröffnungsbesprechung
- Prüfen von Dokumenten während der Durchführung des Audits
- Kommunikation während des Audits
- Sammeln und Verifizieren von Informationen
- Erarbeiten von Auditfeststellungen
  - Auditnachweise werden anhand der Auditkriterien eingeschätzt
  - Nichtkonformitäten sowie deren unterstützende Auditnachweise werden aufgezeichnet
    - Bewertung erfolgt gemeinsam mit der auditierten Organisation

Durchführung des Audits

- Eröffnungsbesprechung
- Prüfen von Dokumenten während der Durchführung des Audits
- Kommunikation während des Audits
- Sammeln und Verifizieren von Informationen
- Erarbeiten von Auditfeststellungen
- Erarbeiten von Auditschlussfolgerungen
  - Bewertung der Auditfeststellungen sowie alle weiteren geeigneten Informationen, die während des Audits gesammelt wurden, anhand der Auditziele
  - Auditteam erlangt Einigkeit über die Auditschlussfolgerungen unter Berücksichtigung der mit dem Auditprozess verbundenen Unsicherheit
  - Empfehlungen werden erarbeitet (falls dies im Auditplan festgelegt ist)
  - Auditfolgemaßnahmen, soweit zutreffend, erörtert

Durchführung des Audits

- Eröffnungsbesprechung
- Prüfen von Dokumenten während der Durchführung des Audits
- Kommunikation während des Audits
- Sammeln und Verifizieren von Informationen
- Erarbeiten von Auditfeststellungen
- Erarbeiten von Auditschlussfolgerungen
- Audit-Abschlussbesprechung
  - Auditierte Abteilung erhält kurzen Bericht über erfolgtes Audit sowie gewonnener Erkenntnisse
    - Cave: Detailtiefe zuvor mit Auftraggeber besprechen; nicht immer ist eine vollständige Information über alle Auditergebnisse gegenüber allen Beschäftigten erwünscht
  - Dank des Auditteams wird ausgesprochen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

4) ERSTELLUNG ABSCHLUSSBERICHT

Erstellen des Auditberichts

- Auditbericht = kurzgefasste und klare Aufzeichnung des Audits
- Inhalt
  - Auditziele
  - Auditumfang, insbesondere die Nennung der Organisations- und Funktionseinheiten bzw. der auditierten Prozesse
  - Nennung des Auditauftraggebers
  - Nennung des Auditteams sowie der Teilnehmer am Audit der auditierten Organisation
  - Termine und Orte, an denen die Audittätigkeiten durchgeführt wurden
  - Auditkriterien
  - Auditfeststellungen sowie zugehörige Nachweise
  - Auditschlussfolgerungen
  - Angabe, in welchem Umfang die Auditkriterien erfüllt wurden

Erstellen des Auditberichts

- Auditbericht = kurzgefasste und klare Aufzeichnung des Audits
- Inhalt
- Optionale Ergänzungen
  - Benennung all jener Bereiche, die vom Auditumfang nicht erfasst wurden
  - Alle nicht beigelegten Meinungsverschiedenheiten zwischen dem Auditteam und der auditierten Organisation
  - Bestätigung, dass die Auditziele innerhalb des Auditumfangs in Übereinstimmung mit dem Auditplan erreicht wurden
  - Identifizierte bewährte Praktiken
  - Vereinbarte Pläne für Nachfolgemaßnahmen, falls zutreffend
  - Verbesserungsmöglichkeiten, falls im Auditplan angegeben
  - Verteilerliste für den Auditbericht
  - Eine Aussage zum vertraulichen Charakter der Inhalte

Verteilen des Auditberichts

- Verteilung erfolgt innerhalb eines mit dem Aufraggeber vereinbarten Zeitraums
- Verteilung erfolgt an alle zuvor bestimmten Empfänger
- Wenn möglich und vom Auftraggeber genehmigt:

  ➔ Autitierte Einheiten der Organisation erhalten ebenfalls Bericht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

CHECKLISTEN

Checklisten

- Checklisten sollten individuell für Audit erstellt/angepasst werden
- Gebrauch von Checklisten und Formblättern darf Umfang von Audittätigkeiten nicht einschränken
  - Insbesondere muss Inhalt des Audits ggf. entsprechend Interview angepasst werden
- Checklisten und Fragebögen sollten immer unter Beteiligung der zu auditierenden Abteilung ausgefüllt werden
  - Niemals nach dem Audit
  - Hinweis: gilt nicht zwingend für Gedächnisnotizen

Checklisten Datenschutz

- Ergänzende Checklisten zum Muster-ADV-Vertrag für das Gesundheitswesen (https://gesundheitsdatenschutz.org/doku.php/adv-mustervertrag-2015)
- Checkliste GDD
  - GDD Ratgeber „Datenschutz-Prüfung von Rechenzentren“ (https://www.gdd.de/downloads/praxishilfen/GDD-Ratgeber_Datenschutz-Pruefung_von_Rechenzentren_2015.pdf)
  - Datenschutz im Unternehmen (https://www.gdd.de/downloads/praxishilfen/datenschutz-im-unternehmen-2)
- Checkliste Datenschutz-Wiki (https://www.datenschutz-wiki.de/Checkliste_TOM_Auftragskontrolle oder https://www.datenschutz-wiki.de/Checkliste_TOM_Verf%C3%BCgbarkeitskontrolle)
- Baustein B 1.5 Datenschutz BSI (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html sowie Tabelle http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/ErgaenzendeDoks/MassnahmeGS-Kat.pdf?__blob=publicationFile)
- Anhang A der ISO 27001
- Checklisten der Aufsichtsbehörden
  - Bayern (https://www.inte.de/BayLDA.pdf)
  - Niedersachsen (http://www.lfd.niedersachsen.de/download/32309/Orientierungshilfe_Fremd-_und_Fernwartung_LfD_Niedersachsen_.pdf)
  - Orientierungshilfen der Aufsichtsbehörden, insbesondere
    - Orientierungshilfe Krankenhausinformationssysteme https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html)
- …

Checklisten: IT-Sicherheit

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - IT-Grundschutz-Kataloge (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html)
  - BSI-Standards (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html;jsessionid=A4BD6A096C0F99008DA28B8D96A81D11.1_cid091)
- ISIS12-InformationsSIcherheitsmanagementSystem (https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html)
- DIN ISO/IEC 27002 „Leitfaden für Informationssicherheits-Maßnahmen“
- DIN EN ISO 27799 „Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002“
- IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie
  - Institut der Wirtschaftsprüfer (https://shop.idw-verlag.de/product.idw?product=20068)
  - IDW Prüfungsnavigator Grundversion (https://www.idw.de/idw/im-fokus/idw-pruefungsnavigator/idw-pruefungsnavigator-grundversion---zip-datei/28246)
  - IT-Auditor IDW – Richtlinie (https://www.idw.de/blob/87038/eac3b57db3b9a8c8a8bb1417fa1ba1bc/down-it-au-richtlinie-data.pdf)
- COBIT-Campus (http://www.isaca.org/Education/on-demand-learning/Pages/default.aspx bzw. https://www.isaca.org/ecommerce/Pages/vCampusLogin.aspx?returnurl=/ecommerce/Pages/ProcessLogin.aspx?vt=2)

Diskussion