Informatik-Revision 1

Risikoanalyse
- Definition
  - Methodisches Vorgehen zur Beurteilung des Informationssystems und dessen Umfeld
- Aufgaben
  - Ableitung von Risiken aufgrund ermittelter Bedrohungen hinsichtlich möglicher Auswirkungen und Eintretenswahrscheinlichkeit
  - Aufgrund der Schwachstellen Einführung angemessener notwendiger Massnahmen. Verbleibende Restrisiken definieren und Versicherung abwägen
- Vorgehen
  - Initialisierung
  - Systemabgrenzung
  - Erarbeitung IST-Situation
  - Risikoanalyse (Kernthema)
    - Risikoidentifikation
    - Risikobewertung
    - Bewältigungsstrategien
  - Festlegen Sicherheitskonzept
    - Technische, organisatorische, rechtliche Massnahmen etc.
  - Realisierung des Konzeptes
  - Kontrolle und Fortschreibung

Risiken in der Informationsverarbeitung
Zahlen in () entsprechen Gewichtung der Bedeutung

- Fehler
  - Umweltbedrohungen (5)
    - Elementarschäden
  - Hardware (3)
  - Software (2)
    - Instabilität
    - Fehlerhafte Ergebnisse
  - Bedienung (1)
    - Falscheingaben
    - Eingriff in autom. Abläufe
- Missbrauch (4)
  - Computerkriminalität (80% interne Angestellte)
    - Viren
    - Hacker
    - Sabotage
  - Vandalismus
    - Sachbeschädigung
    - Diebstahl
  - Persönlichkeitsverletzung
    - Datenmissbrauch

Anforderungen der Revision an sichere Informations-systeme (Qualitätskriterien)
- Vertraulichkeit
  - IS stellt Informationen und Verarbeitungskapazität nur berechtigten Stellen, zu vorbestimmten Zeiten und in vorbestimmter Form zur Verfügung
- Integrität
  - IS stellt gültige, vollständige, richtige Informationen zur Verfügung
- Verfügbarkeit
  - IS stellt Informationen wann und wo sie benötigt werden zur Verfügung
- Nachvollziehbarkeit/ Nachprüfbarkeit
  - Im IS verarbeitete Informationen und durch das IS getätigte Vorgänge sind im Nachhinein kontrollierbar
- Effektivität
  - IS liefert die Informationen, die von den Empfängern zur Aufgabenerfüllung benötigt werden
- Effizienz
  - IS liefert Resultate auf wirtschaftliche Weise
- Verbindlichkeit
  - Rechtshandlungen welche mittels IS ausgeführt werden, sind für alle Parteien verbindlich und können vor dem Gericht durchgesetzt werden

Hilfsmittel / Prüftechniken
- Ziel
  - Informatikgestützte Prüftechniken sollen Effizienz und Qualität der Revision steigern
- Programmprüfung
  - Vollständigkeit und Funktionstüchtigkeit der programmierten Kontrollen
  - Tatsächliche Anwendung der programmierten Programme
  - Logische Richtigkeit des Programmes (Korrekte Abwicklung, Verhinderung fehlerhafter Daten)
- Datenprüfung
  - Vollständige Erfassung aller gespeicherten Daten
  - Richtigkeitskontrolle durch Kontrollsummen und Zwischentotale
  - Selektive Auszüge und Gruppierung nach Revisionsbedürfnissen
  - Echte Stichprobenauswahl durch Zufallsgenerierung
  - Programmierte Durchführung von Nachrechnungen
  - Nachvollzug der wichtigsten kogischen Entscheide und Vergleiche
  - Dienstprogramme (Utilities) mit Abfragemöglichkeiten
  - Abfragesprachen (Queries) für Auswertungen
  - Listen- und Programmgeneratoren
  - Speziell für Revision codierte Programme
  - Generalized Audit Software Packages (GASP)
  - PC-Standardsoftware zu Analysezwecken
  - PC-Revisionssoftware (ACL, IDEA, CARS etc.)
- Audit-SW

Kontrollmassnahmen
- Physisch
  - Zutrittssicherung
  - Brandschutz
- Logisch
  - Identifikation und Authentifikation
- Organisatorisch
  - Personalpolitik
  - Aufbau- und Ablauforganisation
- Sicherheitsdienste nach ISO 7498-2
- Massnahmen nach Art. 7 Datenschutzgesetz

Revision Begriff / Abgrenzung
- Revision: Systematisches Nachvollziehen, Analysieren und Beurteilen von Gegenständen, Sachverhalten oder abgeschlossenen Vorgängen
- Periodische oder einmalige Untersuchung. Durchgeführt von unabhängigen Personen, die im Betriebsablauf nicht integriert sind
- Revisoren haben keine Weisungsbefugnis. Sie nehmen Stellung zu den Prüfobjekten und geben allenfalls Empfehlungen ab

Interne/Externe Revision
- Interne Revision
  - Den obersten Organen der zu prüfenden Unternehmung unterstellt
  - Aufgaben
    - Prüfung Buchführung und Jahresrechnung, Berichterstattung an Generalversammlung
    - Prüfung Finanzielles IKS
    - Prüfungen im Auftrag der Unternehmungleitung wie Systemprüfung, Beurteilung internes Kontrollsystem IKS
- Externe Revision
  - Wahrnehmung durch Personen oder Unternehmen welche vom geprüften Unternehmen unabhängig sind
  - Aufgaben
    - Prüfung Buchführung und Jahresrechnung
    - Prüfung Finanzielles IKS
- Informatik Revision
  - Sowohl in der internen als auch externen Revision vertreten; prüft einerseits aus Blickwinkel des Abschlussprüfers als gesetzliches Prüfungsorgan und andererseits als Bestandteil der Führungskontrolle im Unternehmen

Aufgaben
- Die IS Revision hat zur Aufgabe, IS auf ihre Ordnungsmässigkeit zu prüfen
  - Sicherheitsaspekte
  - Funktionsfähigkeit
  - Wirtschaftlichkeit
- Vorgehen
  - Aufnahme IST-Zustand (Beobachtungen, Messungen, Gespräche)
  - Ableitung Soll-Zustand aus allgemeingültigen Normen (Gesetze, Vorgaben)
  - Interpretation und Gewichtung von Abweichungen Soll/Ist in ihren Auswirkungen und Bedeutung sowie Berichterstattung darüber

Vorgehen/ Arbeitschritte
- Prüfungsvorbereitung
- Prüfungsplanung
  - Funktionen, Objekte, Zeit, Personal, Hilfsmittel
- Prüfungsdurchführung
  - Soll-Ist-Sachverhalt feststellen, analisieren, bewerten, beurteilen
- Arbeitspapiere
  - Handlungen in Prüfpapieren festhalten
- Qualitätskontrolle
  - Kompetenz Revisoren, Urteilsbildung, Prüfhandlungen und Dokumentation
- Berichterstattung

Prüfungsmethoden
- Ergebnisorientierte Prüfung
  - Revisor geht von einem finanziellen Ergebnis aus. Basiert i.d.R. auf Stichproben
- Verfahrensorientierte Prüfung oder Systemprüfung
  - Untersuchung der Wirksamkeit des IKS
- Führungsprüfung
  - Zukunftsorientierte Beurteilung der Tätigkeit aller Führungsstufen
- Projektprüfung
  - Überprüfung der Abwicklung laufender und abgeschlossener Projekte und Vergleich der Resultate mit den Zielsetzungen, Untersuchungen der Ursachen der Abweichungen
- Sonderaufgaben
  - Z.B. Veruntreuungsuntersuchungen, Delikte, Gutachten usw.

Kontrollgegenstand
- Computergestützte Informations-Systeme (IS)

Kontrollziele
- Vollständigkeit und Richtigkeit
  - Datenerfassung und -eingabe
  - Datenverarbeitung
  - Datentransport
  - Datenspeicherung
  - Datenausgabe
- Gültigkeit der Geschäftsvorfälle
  - Identität und Autorisierung des Auftraggebers
- Vollständigkeit und Gültigkeit der automatisch generierten Daten
  - Richtigkeit und Integrität der Programme
- Massnahmen zur Sicherstellung der Verarbeitung
  - Nachvollziehbarkeit
  - Abstimmbarkeit
  - Unterstützung der Fehlersuche