

Handlungszielorientierte

Zusammenfassung WI2

Informationssicherheit

von Richard Degonda

Inhalt:

Datenschutz und Datensicherheit

HZ 131-30 Datenschutz und Datensicherheit anwendungsbezogen sicherstellen **S. 2**

Systemberechtigungen, Zugriffsschutzsysteme

HZ 131-20 Einrichtung und Verwaltung von Systemberechtigungen organisieren,
Zugriffsschutzsysteme, Sicherheitsanforderungen an Zugriffsschutzsysteme **S. 6**

HZ 131-30 Datenschutz und Datensicherheit anwendungsbezogen sicherstellen

Definitionen:

Definitionen: Ein Index aller sicherheitsrelevanten Definitionen befindet sich im Manuskript Bitterli auf S. x (Index). Hier werden nur die in den HZ erfordernten Definitionen behandelt.

Datenschutz: Schutz von personenbezogenen Informationen (Angaben über eine natürliche od. juristische Person) vor Missbrauch, unberechtigter Einsicht oder Verfälschung und damit Schutz des Betroffenen vor Verletzung seiner Privatsphäre. (S. 5 Bitterli)
Rechtsbegriff, der im engeren Sinne den Schutz personenbezogener Daten vor Missbrauch beinhaltet (S. 8 Bürkli)

Datensicherheit: Umfasst die Gesamtheit aller technischer/organisatorischer Massnahmen zum Schutze der Daten, Programme und Datenverarbeitungsanlagen gegen Verlust, Verfälschung und unberechtigten Zugriff aufgrund von Katastrophen, technischen Ursachen (Pannen), menschlichen Versagens oder mutwilligen Eingriffen. (S. 5 Bitterli)

Kontrollziel: Aussage zum gewünschten Resultat (Zweck) das mit der Implementierung von Kontrollen (Kontrolltechnik, Verfahren, Methode) erreicht werden soll.

Kontrollen: Der Begriff Kontrollen (controls) ist definiert als die Konzepte, Verfahren, Praktiken und Organisationsstrukturen, welche eine angemessene Gewissheit verschaffen, dass die Geschäftsziele erreicht und dass unerwünschte Ereignisse verhindert oder erkannt und korrigiert werden. (S. 7 Bitterli)

Sicherheit: Qualitätskriterien sichere und ordnungsmässige Informationssysteme
- COBIT: (S. 9 und S. 6 Bitterli, sowie S12 Bitterli)

Vertraulichkeit: Schutz sensibler Informationen vor unberechtigte Kenntnisnahme.

Verfügbarkeit: Informationen sind verfügbar, wenn durch Geschäftsprozess benötigt, auch in Zukunft. Daher Schutz notwendiger Ressourcen (Daten, Anwendungen, Technologien, Anlagen und Personal) und Kenntnisse.

Integrität: Schutz der Richtigkeit und Vollständigkeit von Informationen und ihrer Uebereinstimmung mit betriebswirtschaftlichen Werten und Erwartungen.

Effektivität: (Wirksamkeit) Für Geschäftsprozess relevante Informationen sind rechtzeitig, fehlerfrei, konsistent und in verwendbarer Form abrufbar.

Effizienz: (Wirtschaftlichkeit) Bereitstellung von Informationen mit optimaler (produktivster und wirtschaftlichster) Verwendung von Ressourcen.

Rechtl. Erfordernisse: (Compliance) Erfüllung extern auferlegter Geschäftskriterien: Gesetze, Verträge, Regulative.

Zuverlässigkeit:(Ordnungsmässigkeit) Alle erheblichen Tatbestände und Ereignisse sind erfasst (Vollständigkeit), laufend nachgeführt (Aktualität) und verständlich (Klarheit), sowie sachlich geordnet (Systematik), zeitgemäss organisiert und zusammenhängend von der Erfassung bis zum Schlussergebnis (Prüfpfad od. Prüfspur)

Sicherheitsrisiken werden nach bestimmten Kriterien durch sog. Kontrollziele (Schutzanforderungen) resp. Kontrolltechniken (Verfahren/Methoden) minimiert

Vgl. auch:

CobIT Framework S.12 – 22 Bitterli : Ausformulierte und systematisch geordnete Kontrollziele für den IT-Prozess. Control Objectives for IT , international, Information Systems Audit and Control Association. 1998

CoP S. 129 – 134 Bitterli: Sicherheitsstandard (Mustersicherheitskonzept S135- 146 Bitterli) 'Code of Practice' for Information Security Management (CoP) aus UK.

Sicherheitskonzept: Mustersicherheitskonzept S135- 146 Bitterli 'Code of Practice' for Information Security Management (CoP)

HZ 131-30 **Datenschutz / Datensicherheit anwendungsbezogen sicherstellen in Phasen der Informationsverarbeitung**

Risiken – Kontrollziele (Schutzanforderungen) – Massnahmen (Kontrolltechniken)

Kriterien:

- Vollständigkeit
- Richtigkeit
- Gültigkeit der Daten
- Nachvollziehbarkeit Ueberprüfbarkeit Ordnungsmässigkeit

Phasen 1-8:

- 1 Datenerfassung / -eingabe
- 2 Verarbeitung
- 3 Datentransport / Uebermittlung
- 4 Datenspeicherung
- 5 Datenausgabe
- 6 Gültigkeit Geschäftsvorfälle
- 7 generierte Daten

Bedrohungen der logischen Sicherheit: real / vermutet (S.122 Bitterli)

- Anzapfen von Leitungen 1 / 40
- Hacking 3 / 60
- Computerbetrug 4 / 65
- Interner Zugriff 6 / 65
- Operatorfehler 12 / 70
- Benutzerfehler 25 / 75
- Computermissbrauch 25 / 75
- ungetestete Software 30 / 80
- Viren 35 / 85

vgl auch Kontrollgrafik zum **Finden von anwendungsbezogenen Risiken** (S. 75 Bitterli) und Zusammenstellung (S. 76 Bitterli)

1 Datenerfassung / - eingabe

Risiken: (S. 60)

- Geschäftsvorfälle werden nicht ins System eingegeben
- doppelte Erfassung / Eingabe
- fehlerhafte Erfassung
- nicht autorisierte Geschäftsvorfälle (fiktive Transakt)
- fehlerhafte Geschäftsvorfälle nicht bereinigt
- Datenerfassung nicht zeitnah

Kontrollziele: (S. 61)

- Erfassungsformulare (Minimierung Fehler Auslassung)
- Quelldokumente vollständig, richtig erfasst und zeitnah weitergeleitet
- Quelldokumente innerhalb best. (gesetzl) Fristen auffindbar und rekonstruierbar aufbewahrt
- Quelldokumente entsprechend gesetzlicher Fristen und ges. vorgeschr. Form aufbewahrt
- Autorisierung der Geschäftsvorfälle ist sichergestellt; die Erfassung erfolgt durch berechnigte Personen
- Ueberprüfung Erfassungskontrolle Gültigkeit Felder
- Fehler und Unregelmässigkeiten werden erkannt, gemeldet und zeitgerecht korrigiert
- Korrektur von Fehlern durch unabhängige Person

Kontrolltechniken: (S 61 –65)

- Einzelpostenvergleich
- Stapelkontrollsummen
- Reihenfolgekontrolle
- Datenabgleich
- Kontrollerfassung
- Kritische Durchsicht (visuelle Kontrolle)
- Format- und Plausibilitätskontrollen
 - Mischsumme je Eingabebeleg
 - Grenzwertkontrolle
 - Abhängigkeitskontrolle
 - Mussfelder

- Prüzfziffern
- Abgleich mit gespeicherten Daten
- Eingabemasken
- Bildschirmkontrollen
- Eingabe vorbereiteter Daten
- automatische Erfassung zB mit Magnetkarten
- Fehlerbehandlung

2 Verarbeitung

Risiken: (S. 65 Bitterli)

- unvollständiges oder falsches Nachführen der Hauptdateien
- fehlerhafte Programmfunktionen, falsche Berechnungen, Analysen, Zuordnungen
- Verlust von Daten
- Verarbeitung zum falschen Zeitpunkt
- Manipulieren und Einschleusen von falschen od fiktiven Daten
- ungenügende Vertraulichkeit

Kontrollziele: (S. 66 Bitterli)

- Alle in das System eingegebenen und akzeptierten Daten werden richtig und vollständig in den (Haupt-) Dateien aktualisiert
- Die programmierten Verfahren (Berechnungen, Totalisierungen, Analysen und Zuordnungen) sind richtig.
- Verarbeitungsfehler werden so früh wie möglich erkannt, protokolliert und zeitgerecht korrigiert
- Erkannte Fehler werden ohne Beeinträchtigung der restlichen Verarbeitung bereinigt.

Kontrolltechniken: (S 66 –67)

- Kontrolltechniken der Dateneingabe (siehe oben zB Einzelpostenvergleich, Stapelkontrollsummen, Reihenfolgekontrolle und Datenabgleich)
- Anschlussrechnung (Abstimmung von Kontrollsummen)
- Staffettenvergleich
- Kontrolle durch externe Bestätigungen
- Datenabgleich
- Fehlerbehandlung, Ueberwachung mittels Spezialauswertungen

3 Datentransport/Uebermittlung

Risiken: (S. 68 Bitterli)

- Abhören resp Anzapfen (Verlust der Vertraulichkeit)
- Daten manipulieren / einschleusen
- Versand, Empfang oder Meldungsinhalt werden abgestritten
- fehlerhafte Uebermittlung
- falsche Kostenverrechnung

Kontrollziele: (S. 68 Bitterli)

- Alle Daten werden vollständig und richtig übermittelt
- Die Vertraulichkeit der transportierten Daten ist gewährleistet
- Absender und Empfänger können Versand / Empfang und Inhalt nicht abstreiten
- Uebermittlungsfehler werden vor Weiterverarbeitung erkannt

Kontrolltechniken: (S. 68 Bitterli)

- Sequenznummern (innerhalb 1 Batch; über mehrere)
- Doppelübermittlung mit Prüfung durch den Empfänger
- Rückübermittlung mit Prüfung durch Absender
- Kontrolltotale (Summen / Hash-Totale)
- Authentisierung (für Integrität, Absenderidentität)
- Verschlüsselung / Chiffrierung (für Vertraulichkeit, Unversehrtheit, Originalität Absender)

4 Datenspeicherung

Risiken: (S. 69 Bitterli)

- Verarbeitung erfolgt mit der falschen Dateigeneration
- Verarbeitung erfolgt mit falschen oder mit `veralteten' (nicht aktuellen) Daten
- Lange Antwort-, Verarbeitungs- und Datensicherstellungszeiten infolge mangelnder Datenpflege (Reorganisationen)
- Daten werden unautorisiert (absichtlich od unabsichtlich) verändert

Kontrollziele: (S. 69 Bitterli)

- Daten bleiben im Zeitablauf integer
- Gespeicherte (Stamm-) Daten sind aktuell und richtig
- Redundant gespeicherte Daten werden periodisch miteinander abgeglichen

- Daten werden nach einer Störung vollständig und richtig wiederhergestellt
- Nicht mehr benötigte Daten werden durch einen autorisierten Vorgang gelöscht
- Vertraulichkeit gespeicherter Daten ist gewährleistet

Kontrolltechniken (S70 Bitterli)

- Kontrolle periodischer Ausdrücke
- Abstimmung von Kontrollsummen
- Anschlussrechnung, period. Nachvollzug, Datenabgleich (vgl. Verarbeitung von Daten)
- Ausdruck und Analyse von Ausnahmefällen

5 Datenausgabe

Risiken (S71 Bitterli)

- unvollständige und/oder fehlerhafte Datenausgabe
- die Datenausgabe folgt zu spät
- die Verteilung der Auswertungen ist falsch oder erfolgt zu spät
- die Vernichtung falscher Ausdrücke oder heikler Daten ist unkontrolliert
- Auswertungen werden unerlaubt mehrfach dargestellt oder unterdrückt
- Vertraulichkeitsstufen werden nicht beachtet, unberechtigte Personen erhalten Informationen

Kontrollziele (S. 71 Bitterli)

- Datenausgabe erfolgt zeitgerecht
- Der Output ist richtig, vollständig und wird in der vorbestimmten Menge am richtigen Ort ausgedruckt
- Der Output wird regelmässig mit den entsprechenden Kontrolltotalen der Verarbeitung abgestimmt
- Informationen werden nur an berechtigte Personen abgegeben
- Ausgedruckte Informationen werden entsprechend den gesetzlichen Bestimmungen aufbewahrt
- Aufbewahrung, Behandlung und Vernichtung ausgegebener Daten sind so geregelt, dass die Vertraulichkeit sensibler Informationen sichergestellt ist.

Kontrolltechniken: (S. 72 Bitterli)

- Versand- / Empfangskontrolle resp. Verteillisten
- Reihenfolge- / Vollständigkeitskontrolle (Vornummerieren zB Checks)
- Benutzerberechtigungen
- Periodische Auswertungen (Stichproben)

6 Gültigkeit der Geschäftsvorfälle (validity)

Risiken: (S. 73 Bitterli)

- unerlaubte Veränderungen an den Daten
- Hinzufügen fiktiver oder unautorisierter Daten
- Ausschliessen autorisierter Daten von der weiteren Verarbeitung

Kontrollziele: (S. 73 Bitterli)

- Nur gültige Daten werden verarbeitet
- Alle verarbeiteten Daten basieren auf echten und autorisierten Geschäftsvorfällen
- Die Identität des Benutzers ist bekannt (dh User-ID wird nicht geteilt)

Kontrolltechniken (S.73 Bitterli)

- Kontrolltechniken der Identifikation
 - Einsatz von logischen Merkmalen (zB Passwörter)
 - Einsatz von physischen Token (zB Magnetkarten)
 - biometrische Techniken (zB Unterschriften)
- Kontrolltechniken für Berechtigung
 - manuelle Genehmigung durch Kontrollvermerk
 - autom. Selektion für manuelle Genehmigung
 - Benutzerberechtigungen (Zugriffsschutzsystem)
 - Systemmässige und manuelle Genehmigung kombiniert

HZ 131-20 **Einrichtung und Verwaltung von Systemberechtigungen organisieren, Zugriffsschutzsysteme, Sicherheitsanforderungen an Zugriffsschutzsysteme**

Uebergeordnete Anforderungen an Zugriffsschutzsysteme: (S. 77 u. 78 Bitterli)

- Sicherheitsverantwortlicher bestimmen
- einmalige, eindeutige Anmeldung (Single-Sign-On) einrichten
- Zentrale, zeitgerechte Einrichtung und Verwaltung von Accounts
- formales Genehmigungsverfahren für Benutzerkonten einrichten
- Need-to-know Prinzip: Berechtigung nach nachgewiesenen Bedürfnissen vergeben
- Ueberprüfung Benutzeraccounts einrichten (Rollenbasierte Standardprofile)
- Single-point-of-maintenance: anwendungsübergreifende Berechtigungsdatenbank einrichten (Kostenreduktion)
- Selbstkontrolle durch Benutzer ermöglichen
- Rapportierung von Verstößen / Sicherheitsaktivitäten

IT Sicherheitskriterien: (www.bsi.de)

Kategorien:

der Bedrohungen, Schutzziele, technischen und organisatorischen Massnahmen

nach ITSEC (IT Security Evaluation Criteria)

1. Identifikation und Authentisierung
2. Rechteverwaltung und -prüfung
3. Nachvollziehbarkeit
4. Revidierbarkeit
5. Wiederaufbereitung
6. Genauigkeit / Fehlerüberbrückung
7. Gewährleistung der Funktionalität
8. Uebertragungssicherung

1 Identifikation und Authentisierung

Erfassen und Löschen von Benutzern
Aendern der Authentisierungsinformationen

Kriterien Benutzeridentifikation

- eindeutig (innerhalb des gesamten Systems)
- sprechend (Inhaber leicht erkennbar)
- dauerhaft (über gesamte Lebensdauer des Systems)
- technisch einfach realisierbar (nicht so wichtig)

Anforderungen: (zu definieren und zu gewichten)

Subjekte:

- welche Subjekte müssen identifiziert werden?
- Personen
- Prozesse
- Systeme / Maschinen

Objekte:

- welche Objekte müssen identifiziert werden?
- Dateien: Daten, Programme
- Ressourcen: CPU, RAM, Anzahl Prozesse
- Geräte: Disk, Tape Drucker, Fax

Aktionen:

- Lesen
- Kopieren
- Schreiben
- Löschen

Ausführen

Umstände:

- unter welchen Umständen muss eine Identifikation und Authentisierung erfolgen?

Aktionen:

- welche Aktionen müssen bei nicht erfolgreicher Identifikation und Authentisierung durchgeführt werden?

2 Rechteverwaltung und Prüfung: Administration von Autorisierungsprivilegien (Berechtigungen)
Ueberprüfen von Autorisierungsprivilegien (Default-Schutz, default to denial)

Anforderungen: (S. 82 Bitterli)

Rechteverwaltung:

- Subjekt- rsp. Objekt(klassen) der Rechteverwaltung?

- Arten von Rechten zwischen Subjekten und Objekten?
- Verantwortlicher bei Vergabe / Aenderung von Rechten?
- Regeln bei Vergabe / Aenderung von Rechten?
- Voraussetzungen vor Vergabe / Aenderung von Rechten?
- Rollen die durch Rechteverwaltung definiert werden?
- Rechte gebunden an spezielle Rollen?
- Rollen miteinander unvereinbar?

Rechteprüfung:

- Rechteprüfung bei welchen Aktionen?
- Massnahmen bei Aktionsausführung, Rechtausübung
- Ausnahmen bei Rechteprüfung und unter welchen Umständen?

Kriterien / Aspekte:

- Vollständigkeit Rechteverwaltung
- Widerspruchsfreiheit, Ueberschaubarkeit Rechtestruktur
- Schutz vor verdeckten Rechteänderungen,
- Schutz vor nicht änderbarer Rechtebeziehungen

3+4 Beweissicherung (3 Nachvollziehbarkeit 4 Revidierbarkeit) (Protokollierung Benutzer / Aktion (accountability))

Anforderungen:

- Ereignisse, die protokolliert werden sollen?
- Informationen, die aufgezeichnet werden sollen?
- Aufzeichnungen wo?
- Zugriff auf Aufzeichnungen: wer, wann, wo?
- Aufzeichnungen: Nach welchen Kriterien auszuwerten?
- Aufzeichnungen: Wie lange und wo aufbewahrt?

Kriterien / Aspekte:

- Untäuschbarkeit der Beweissicherung
- Vollständigkeit der Beweissicherung

5 Wiederaufbereitung (object reuse)

(Daten in (Zwischen-)speichern)

Anforderungen:

- Betriebsmittel: welche werden wiederaufbereitet?
- Wiederaufbereitung: wie durchzuführen?
- Wiederaufbereitung: nach / vor welchen Aktionen?

Kriterien / Aspekte:

- Art der Wiederaufbereitung
- Zeitpunkt der Wiederaufbereitung

6 Genauigkeit / Fehlererkennung / Fehlerüberbrückung

(Richtigkeit Konsistenz Verfügbarkeit)

Anforderungen:

- Eingaben: welche müssen validiert werden?
- Operationen: welche müssen validiert werden?
- Validierung: wie durchzuführen?
- Entdeckung von Fehlern: welche Aktionen sind durchzuführen?

Kriterien / Aspekte:

- Vollständigkeit der Fehlererkennung (alle, die erkannt werden sollen werden erkannt)
- Korrektheit der Fehleranalyse (korrekte Informationsextraktion bei erkannten Fehlern)

7 Gewährleistung der Funktionalität

(Verfügbarkeit reliability of service)

Anforderungen:

- Funktionalität – Priorität der Funktionalitäten bezüglich Verfügbarkeit?
- Funktionalität: aufrechtzuerhalten unter welchen Randbedingungen?
- Funktionalität: Verzicht unter welchen Umständen?

Kriterien / Aspekte:

- Erkennung von fehlerkritischen Situationen adäquat (Systembelastung)
- Massnahmen zur Fehlervermeidung (Beeinträchtigung anderer Funktionen)

8 Uebertragungssicherung

(Data exchange)

Anforderungen:

- Authentisierung auf Partnerebene Authentisierung Sender Empf.
- Zugriffskontrolle
- Vertraulichkeit von Daten
- Integrität von Daten
- Anerkennung übermittelten Daten (berechtigte Sender / Empfänger)