Anforderungen der Revision an Informatik-Systeme

1 Zielsetzungen

Die vorliegenden Anforderungen beinhalten Massnahmen und Vorkehrungen zur Gewährleistung der Betriebssicherheit, Qualität, Ordnungsmässigkeit sowie zur Verstärkung des Internen Kontrollsystems (IKS) von IT-Systemen. Sie legen die nach heutigem Wissensstand für die Praxis bedeutsamen Anforderungskriterien fest, die jedoch – wie alle generellen Empfehlungen – dem System und der technologischen Informatik-Situation im Einzelfall anzupassen sind. Soweit immer möglich sind sie bei Projektrealisierungen und beim Betrieb von Informatik-Systemen einzuhalten.

Die Anforderungen richten sich an:
- Projektleiter und Benutzervertreter von Informatikprojekten,
- Verantwortliche für die Planung, Realisierung und den Betrieb von Informatik-Infrastrukturen.

Die Anforderungen zeigen auf, wie die spezifischen Anforderungen an Qualität, Sicherheit, Zuverlässigkeit und Compliance gestützt auf Risikoanalysen ermittelt werden können. Sie gliedern sich nach der Grundstruktur einer IT-Lösung (Dateneingabe, Datenverarbeitung, Datenausgabe, Datenübermittlung und Datenspeicherung). Im Anhang 2 sind praktische Beispiele aufgeführt.

2 Grundlagen

Die vorliegenden Anforderungen stützen sich auf folgende Grundlagen:
- Finanzhaushaltgesetzgebung (FLG, FLV und FLW),
- Datenschutzgesetzgebung,
- RRB's und Weisungen der Finanzdirektion betreffend Informatik,
- Wegleitung für die Abwicklung von Informatikprojekten im Kanton Bern,
- Schweizer Handbuch der Wirtschaftsprüfung,
- COBIT - Governance, Control and Audit for Information and Related Technology.

3 Anforderungskriterien

IT-Systeme und Informationsverarbeitungsprozesse haben bestimmten Anforderungen zu genügen, die wie folgt definiert sind:

a) Die **Qualität** (Wirksamkeit und Wirtschaftlichkeit) wird in den Kriterien *Effizienz* und *Effektivität* abgebildet.
   - ***Effektivität*** (Wirksamkeit) bedeutet, dass die Informationen und Daten für die Geschäfts- bzw. Verwaltungsprozesse wichtig sind, zu ihnen in einem engen Zusammenhang stehen und rechtzeitig in einer fehlerfreien, konsistenten und verwendbaren Form abgerufen werden können.
   - ***Effizienz*** (Wirtschaftlichkeit) bedeutet die Bereitstellung und Weiterverarbeitung von Informationen und Daten unter optimaler Ressourcenverwendung.

b) Die **Sicherheitsanforderungen** haben die Kriterien *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* zu erfüllen.
   - ***Vertraulichkeit*** betrifft den Schutz von sensitiven Informationen und Daten vor unberechtigtem Zugriff (Einsichtnahme und Verwendung).
   - ***Integrität*** steht im Zusammenhang mit der Richtigkeit und Vollständigkeit von Informationen und Daten sowie ihrer Übereinstimmung mit den betriebswirtschaftlichen Fakten.

- ***Verfügbarkeit*** bedeutet, dass Informationen und Daten dann abrufbar sind, wenn sie im Rahmen des Verarbeitungsprozesses benötigt werden. Verfügbarkeit hat auch den Schutz von Ressourcen (Personen, Applikationen, Technologie, Einrichtungen) zum Gegenstand.

c) Die **Zuverlässigkeit** garantiert die Bereitstellung und Verwendung gesicherter Informationen und Daten.

d) Für die **Compliance**, d.h. die Einhaltung der rechtlichen Rahmenbedingungen (Rechtserlasse) sowie der internen und externen Regulative gilt das Kriterium *Einhaltung rechtlicher Vorschriften.*

- ***Einhaltung rechtlicher Vorschriften*** bedeutet, dass die für den Geschäfts- bzw. Verwaltungsprozess gültigen Rechtserlasse (Gesetze, Verordnungen, etc.), verwaltungsinternen Reglemente und Weisungen (Regulative) sowie die vertraglich begründeten Rechte und Pflichten eingehalten werden.

Die spezifischen Anforderungen an **Qualität, Zuverlässigkeit** und **Compliance** werden in der Regel von den Benutzervertretern eingebracht und im laufenden Betrieb sichergestellt. Hingegen wird den **Sicherheitsanforderungen,** durch die Benutzervertreter wie auch Entwickler, oft zu wenig Gewicht beigemessen. Daher beschränken sich die Ausführungen in den Kapiteln 4 und 5 im Wesentlichen auf die Darstellung der **Sicherheitsanforderungen**.

4 Sicherheitsanforderungen

An die einzelnen Phasen der "Datenverarbeitung" (Dateneingabe, Datenverarbeitung, Datenausgabe, Datenübermittlung und Datenspeicherung) sind folgende Sicherheitsanforderungen zu stellen:

4.1 Dateneingabe

- jeder nachweispflichtige Geschäftsvorfall wird erfasst (Integrität),
- alle materiell wichtigen Datenfelder werden ausreichend plausibilisiert (Integrität),
- die Eingabe, Mutation und Löschung von Daten ist nachzuweisen (Integrität, Zuverlässigkeit),
- die Eingabe von Daten kann nur von berechtigten Mitarbeitern erfolgen (Integrität).

4.2 Datenverarbeitung

- alle Daten werden vollständig und richtig in den Dateien aktualisiert (Integrität, Zuverlässigkeit, Effektivität),
- die Programm-Algorithmen werden richtig ausgeführt (Integrität, Zuverlässigkeit, Effektivität),
- die Verarbeitung der Daten kann nachvollzogen und nachgeprüft werden (Integrität, Zuverlässigkeit, Einhaltung rechtlicher Vorschriften).

4.3 Datenübermittlung

- alle Daten werden vollständig und richtig übermittelt (Integrität),
- die Daten sind vor unberechtigtem Zugriff (während der Datenübermittlung) geschützt (Integrität und Vertraulichkeit),
- die Datenübermittlung kann nachvollzogen und nachgeprüft werden (Integrität, Zuverlässigkeit, Einhaltung rechtlicher Vorschriften).

Sinngemäss gelten diese Anforderungen auch für die Datenmigration sowie für die Schnittstellen zu anderen Systemen.

4.4 Datenspeicherung

- betriebsnotwendige Datenbestände bleiben unversehrt und unverändert erhalten (Integrität),
- die Daten sind vor unberechtigtem Zugriff geschützt (Vertraulichkeit).

4.5 Datenausgabe

- die Datenausgabe erfolgt vollständig, richtig und zeitgerecht (Integrität, Zuverlässigkeit, Effektivität),
- Informationen werden nur berechtigten Empfängern zur Verfügung gestellt (Vertraulichkeit).

5 Vorgehen zur Ermittlung der erforderlichen Massnahmen

Der Ausbaugrad der zu implementierenden und zu unterhaltenden Qualitäts-, Zuverlässigkeits- und Sicherheitsmassnahmen und -standards kann nicht generell festgelegt werden. Er hängt insbesondere von der Zweckbestimmung der Applikation und deren Betriebsumgebung ab. Ein bewährtes Instrument zur Ermittlung des Ausbaugrades ist die Risikoanalyse.

In der nachstehenden Beschreibung wird von einem zu entwickelnden System ausgegangen. Sinngemäss kann diese Vorgehensweise auch für die Beurteilung eines bereits implementierten Systems angewandt werden. Der Unterschied besteht darin, dass bei einem zu entwickelnden System anhand der Risikoanalyse die zu realisierenden Sicherheitsanforderungen bestimmt werden; bei einem bereits eingeführten System hingegen die implementierten Sicherheitsmassnahmen beurteilt werden. Anhang 1 zeigt einen möglichen Aufbau einer Kontrollmatrix.

5.1 Risikoanalyse zur Bestimmung der Sicherheitsmassnahmen

5.1.1 Ermitteln der Anforderungen (Kontrollanforderung)

Für jedes Sicherheitskriterium (Vertraulichkeit, Integrität, Verfügbarkeit) werden für die in Ziff. 4.1 - 4.5 beschriebenen Phasen die Anforderungen ermittelt (beispielsweise durch die Fragestellung: "Wie wird sichergestellt, dass jeder nachweispflichtige Geschäftsvorfall erfasst wird?").

5.1.2 Festlegen der Sicherheitsmassnahmen (Kontrolle)

Zu jeder Sicherheitsanforderung wird eine geeignete Kontrolle festgelegt. (Bsp.: Automatische Prüfung der Lückenlosigkeit der Belegnummern im Falle einer externen Belegnummernvergabe).

5.1.3 Beschreibung der Sicherheitsmassnahmen (Durchführung / Kontrollziel / Wirkung)

Festgelegt werden: Die Art der Kontrolle[1], die damit abgedeckten Kontrollziele und die Wirkung der Kontrolle.

Die Kennzeichnung der betroffenen Kontrollziele (Vertraulichkeit, Integrität, Verfügbarkeit) erlaubt die Beurteilung des Erfüllungsgrades der Sicherheitsmassnahmen.

Ein wirksames und wirtschaftliches Kontrollsystem zeichnet sich aus durch optimal aufeinander abgestimmte präventive (vorbeugende) und detektive (aufdeckende) Kontrollen.

5.1.4 Beurteilung der Wirksamkeit der Sicherheitsmassnahmen (Beurteilung)

Es wird beurteilt, ob die festgelegten Kontrollen die ermittelten Anforderungen erfüllen.

Die Beurteilung der Wirksamkeit bildet die Grundlage für die Festlegung von Korrekturmassnahmen und die Prüfungsplanung (Revision des Informatik-Systems). In einem Portfolio lässt sich die zusammenfassende Beurteilung anschaulich darstellen, um anhand von Kosten- / Nutzenüberlegungen die Prioritäten festzulegen.

5.2 Integration der Risikobeurteilung in das Projektphasenkonzept

Die Risikobeurteilung erzielt den grössten Nutzen, wenn sie während jeder Projektphase (Vorstudie, Grobkonzept usw.) durchgeführt und mit laufendem Projektfortschritt vertieft wird (zunehmender Detaillierungsgrad). Input für die jeweilige Projektphase liefern die Anforderungen. Die Kontrollpunkte werden in der Projektphase erarbeitet; die Beurteilung der Wirksamkeit ist Bestandteil der Abnahme

[1] Unter 'Art der Kontrolle' wird definiert bzw. beschrieben, ob es sich um eine manuelle oder automatisierte (programmierte Kontrolle) handelt. Daraus lassen sich die Anforderungen an die Funktionentrennung ableiten.

der Projektphasenergebnisse. Sie bildet auch Grundlage für sämtliche Tests. Als Ergebnis entsteht eine übersichtliche Dokumentation der Sicherheitsmassnahmen (Kontrollen).

5.3 Berücksichtigung besonderer Betriebszustände

Bei der Festlegung der Sicherheitsmassnahmen ist zu beachten, dass der sichere Systembetrieb *jederzeit* gewährleistet sein muss. Das gilt insbesondere bei ausserordentlichen Betriebszuständen. Darunter fallen:

- Ausfall einzelner Ressourcen (Personal, Daten, Anwendungen, Technologien, Anlagen),
- Software-Fehler,
- Bedienungsfehler,
- mutwillige Störungen (Sabotage).

6 Erfüllung der Anforderungskriterien

Wichtig ist, dass die Anforderungskriterien nicht durch eine Anhäufung vieler einzelner Kontrollen zu erreichen versucht wird, sondern Kontrollen entsprechend ihrer Wirkung und Art gezielt implementiert werden. Aufgrund der unterschiedlichen Bedeutung und Wirkungsintensität ergeben sich Massnahmen- prioritäten. Verhältnismässigkeit und Wirtschaftlichkeit einzelner Massnahmen sind mitzuberücksichtigen. Qualitativ gute Kontrollen:

- sind in den Arbeitsablauf integriert und werden nicht als störende, zusätzliche Mehrarbeit empfunden,
- wirken auf alle Transaktionen und Daten,
- bilden ein eigenes, gut dokumentiertes Subsystem.

Auf die generellen Anforderungen an Entwicklung, Betrieb und Wartung des IT-Systems, welche bereits Teil der Systementwicklungsmethodik sind (z.B. Dokumentationskonzept, Testkonzept) wird im Rahmen der vorliegenden Anforderungen nicht näher eingetreten.

Im Anhang 2 (Massnahmenkatalog) sind mögliche Massnahmen zur Sicherstellung der Anforderungen an Qualität, Sicherheit, Zuverlässigkeit und Compliance aufgeführt, die sich in der Praxis bewähren.

Nebst den im Anhang 2 erwähnten applikationsspezifischen Massnahmen sind jeweils auch zu berücksichtigen:

- Physische Sicherheitsmassnahmen (z.B. Elementarschäden, Sabotage, Zutrittskontrolle, Notfallkonzept),
- Informatik- und Betriebsorganisation, Benutzeradministration (z.B. Informatik-Standards, [Datensicherung, Releaseverfahren usw.], Problemmanagement, IT-Verträge und Versicherungen),
- Zugriffskontrolle und Funktionentrennung,
- Kontrollfunktionen der Fachabteilungen (z.B. Abstimmkontrollen mit Visum),
- Weisungen zur Aufbewahrung (s. Handbuch Haushaltführung der Finanzverwaltung, Kap. 8. Archivierung).

Für den Datenschutz wird auf die einschlägigen Vorschriften verwiesen.

7 Weitere Informationen

Für zusätzliche Informationen, die Beantwortung von Fragen und die fachliche Unterstützung zur Erfüllung der Anforderungskriterien steht Ihnen die Finanzkontrolle zur Verfügung.

Bern, im Juni 2004 **Finanzkontrolle des Kantons Bern**

Kontrollmatrix

Kontrollanforderung	Kontrolle	Durchführung	Kontrollziel			Wirkung		Beurteilung
„Wie wird sichergestellt, dass ...?“	Beschreibung der Sicherheitsmassnahme	„Wer (Person / Stelle / Programm) führt die Kontrolle aus?“	Vertraulichkeit	Integrität	Verfügbarkeit	präventiv	detektiv	
Beispiel für Dateneingabe:								
alle Fakturen in die Finanzbuchhaltung übernommen werden?	Vollständigkeitskontrolle in der Schnittstelle Fakturierungssystem / Finanzbuchhaltung.	„Schnittstellenprogramm“		x		x		Teilweise wirksam: die Fehler werden nur ins Fehlerprotokoll geschrieben und können dort vergessen gehen. Vorschlag: Fehlerdatei einrichten.
	Monatliche Abstimmung der Fakturierten Umsätze gemäss Fakturierungssystem mit Finanzbuchhaltung anhand der Liste „Abstimmreport“.	Sachbearbeiter „Abstimmung“		x			x	wirksam

Kontrollmassnahmen		Hauptwirkung							Durch-führung		Art				
		Qualität		Sicherheits-anforderungen			Zuver-lässigkeit	Compliance							
Nr.	Beschreibung	Effektivität	Effizienz	Vertraulichkeit	Integrität	Verfügbarkeit	Zuverlässigkeit	Einhaltung rechtlicher Vorschriften	manuell	programmiert	präventiv	detektiv	Priorität	Praktische Beispiele	Hinweise
1. Dateneingabe															
1.1	Projektentwicklungsmethodik	●	●	○	○	○	○	●	●		●	●	1		
1.2	Plausibilitätsprüfungen				●	○				●	●		1	Grenzwerte, Abhängigkeiten, Format, Prüfziffern, Mussdatenfelder, Limiten	Verhindert, dass Fehler ins System gelangen
1.3	Protokollierung						●			●	●		1	Protokollierung der wertrelevanten Datenveränderungen (Stamm- und Steuerungsdaten)	Prüfspur
1.4	Stapelkontrollsummen				●		○		●	●	●		1	Hash-/Batchtotale als Kontrollsummen	Wirkungsvolle Kontrolle der vollständigen und richtigen Datenerfassung
1.5	Zugriffsschutz			●	●		○	●		●	●		1	Steuerung der Zugriffsrechte (Daten anlegen, lesen, mutieren, löschen)	Funktionentrennung
1.6	Benutzerführung		●		●		○			●	●		2	Help-Funktionen, ergonomische Arbeitsabläufe	Vermindert Bedienungsfehler
1.7	Bildschirmgestaltung			●	●					●	●		2	Standardisierung der Bildschirmeingabe, ergonomische Arbeitsabläufe	Vermindert Bedienungsfehler
1.8	Datenabgleich / -abstimmung				●				●	●	●		2	Ausgleich offene Posten, Quervergleich	Vermindert Erfassungsfehler
1.9	Elektronisches Visum				●				●	●	●		2	Kontrolle und Freigabe der erfassten Daten durch eine unabhängige Person	Sinnvolle Kontrolle zur Entdeckung von Erfassungsfehlern
1.10	Kritische Durchsicht				●		○		●		●		2	Visuelle Kontrolle der erfassten Daten	Als ergänzende Kontrolle wirksam, setzt gute Kenntnisse voraus
1.11	Reihenfolge-Kontrolle				●				●	●	●		2	Lückenlose Belegnummernfolge	Sinnvoll zur Kontrolle der vollständigen Erfassung
1.12	Einzelpostenvergleich				●				●		●		3	Jede Eingabe wird einzeln nachkontrolliert	Aufwändig, in einzelnen Fällen sinnvoll
2. Datenverarbeitung															
2.1	Projektentwicklungsmethodik	●	●	○	○	○	○	●	●		●	●	1		
2.2	Ausdruck / Anzeige Ausnahmefälle		○		●				●	●		●	1	Selektion und Kontrolle von Grenzwerten	Unterstützung bei der Kontrolle von Transaktionen mit höherem Fehlerrisiko
2.3	Journalisierung					●		●		●		●	1	Chronologische Aufzeichnung der Buchungen	Prüfspur
2.4	Protokollierung				●	○		●		●		●	1	Protokollierung der wertrelevanten Datenveränderungen im Regelwerk (Stamm- und Steuerungsdaten)	Prüfspur

Kontrollmassnahmen		Hauptwirkung							Durch-führung		Art				
		Qualität		Sicherheits-anforderungen			Zuver-lässigkeit	Compliance							
Nr.	Beschreibung	Effektivität	Effizienz	Vertraulichkeit	Integrität	Verfügbarkeit	Zuverlässigkeit	Einhaltung rechtlicher Vorschriften	manuell	programmiert	präventiv	detektiv	Priorität	Praktische Beispiele	Hinweise
2.5	Zugriffsschutz			●	●		○	●		●	●		1	Steuerung der Zugriffsrechte (Daten anlegen, lesen, mutieren, löschen)	Funktionentrennung
2.6	Externe Bestätigungen		○		●				●			●	2	Bestätigungen von Posten / Salden durch Dritte	Wichtige „externe Kontrolle“
2.7	Anschlussrechnung				●				●	●		●	2	Vergleich Stand alt / neu zu Bewegung	Wichtige Pauschalabstimmung
2.8	Datenabgleich / -abstimmung				●				●	●		●	2	Vergleich von redundanten Datenbeständen	Sinnvoll bei redundanten Daten
2.9	Stafetten-Kontrollen				●					●		●	3	Abstimmung bei Batch-Job-Ketten	Kontrolle des Datenflusses
3. Datenübermittlung															
3.1	Projektentwicklungsmethodik	●	●	○	○	○	○	●	●		●	●	1		
3.2	Authentifizierung			●	●	○				●	●		1	Authentifikator als Schlüssel-Prüffeld	Primär für sensitive Daten
3.3	Chiffrierung			●	●	○		○		●	●		1	Chiffrierung der übermittelten Daten	Primär für sensitive Daten
3.4	Nutzung Funktionen LAN			●	●	●				●	●		1	Netzbetriebssoftware bietet Standard-Sicherheitsfunktionen	Optimierte Sicherheit
3.5	Nutzung Funktionen WAN			●	●	●				●	●		1	Auto-Call-Back, Closed-User-Group	Reduktion der externen Risiken
3.6	Zugriffsschutz			●	●		○	●		●	●		1	Steuerung der Zugriffsrechte (Daten anlegen, lesen, mutieren, löschen)	Funktionentrennung
3.7	Kontrolltotale		○		●					●	●		2	Mitsenden von Hash- / Batchtotalen	Einfache, aber nützliche Kontrolle
3.8	Doppelübermittlung				●					●	●		3	Doppelte Übermittlung mit automatisiertem Abgleich	In Einzelfällen sinnvoll
3.9	Rückübermittlung				●					●	●		3	Die empfangenen Daten werden zum Abgleich rückübermittelt	In Einzelfällen sinnvoll
3.10	Sequenznummer				●					●	●		3	Nummerierung der Datenpakete	In Einzelfällen sinnvoll
4. Datenspeicherung															
4.1	Projektentwicklungsmethodik	●	●	○	○	○	○	●	●		●	●	1		
4.2	Ausdruck / Anzeige Ausnahmefälle				●				●	●		●	1	Selektion und Kontrolle von Grenzwerten	Unterstützung bei der Kontrolle von Transaktionen mit höherem Fehlerrisiko
4.3	Zugriffsschutz			●	●		○	●		●	●		1	Steuerung der Zugriffsrechte (Daten anlegen, lesen, mutieren, löschen)	Funktionentrennung
4.4	Anschlussrechnung				●				●	●		●	2	Vergleich Stand alt / neu zu Bewegung	Wichtige Pauschalabstimmung

Kontrollmassnahmen		Hauptwirkung							Durch-führung		Art				
		Qualität		Sicherheits-anforderungen			Zuver-lässigkeit	Compliance							
Nr.	Beschreibung	Effektivität	Effizienz	Vertraulichkeit	Integrität	Verfügbarkeit	Zuverlässigkeit	Einhaltung rechtlicher Vorschriften	manuell	programmiert	präventiv	detektiv	Priorität	Praktische Beispiele	Hinweise
4.5	Abstimmen Kontrollsummen				●				●	●		●	3	Nachführen von Kontrollsummen und Abstimmung mit Summe der Einzelposten	Einfache, pauschale Kontrolle
4.6	Datenabgleich				●					●		●	3	Vergleich von redundanten Datenbeständen	Sinnvoll bei redundanten Daten
4.7	Kontrolle periodischer Ausdrucke				●				●			●	3	Periodischer (selektiver) Ausdruck und Abstimmung	Ergänzende Kontrollfunktion
5. Datenausgabe															
5.1	Projektentwicklungsmethodik	●	●	○	○	○	○	●	●		●	●	1		
5.2	Kritische Durchsicht				●				●			●	1	Visuelle Kontrolle der Ausgabedaten	Als ergänzende Kontrolle wirksam, setzt gute Kenntnisse voraus
5.3	Lagerung- / Entsorgung			●	●	●			●	●	●	●	1	Aufbewahrung von Belegen, Journalen, Protokollen, Auswertungen, Dateien	Gemäss Aufbewahrungsvorschriften
5.4	Verteiler-Organisation			●					●	●	●		1	Empfänger-Liste oder Aufdruck der Empfänger	Abgestimmt auf Aufbau- / Ablauforganisation
5.5	Zugriffsschutz			●	●		○	●		●	●		1	Steuerung der Zugriffsrechte (Daten anlegen, lesen, mutieren, löschen)	Funktionentrennung
5.6	Outputgestaltung			●	●					●	●		2	Standardisierung der Datenausgabe, Ausdruck von Selektionsparametern	Normierung Listenlayout
5.7	Reihenfolgekontrolle				●				●	●		●	2	Kontrolle von Nummernsequenzen	Checks, Wertpapiere, Seitennummern

Legende

Wirkung:
● = primäre Wirkung
○ = sekundäre Wirkung

Durchführung:
- manuell durchzuführende Kontrolle, z.B. Kontrolle des Zahlungsvorschlages anhand der Originalrechnungen
- programmierte, automatisierte Kontrolle, z.B. Plausibilitätsprüfungen, Zugriffsschutz, Kontenfindung

Art:
- präventiv (vorbeugend); Fehler sollen verhindert werden. Es handelt sich häufig um programmierte Kontrollen.
- detektiv (aufdeckend); Fehler sollen aufgedeckt werden. Es handelt sich häufig um manuelle Kontrollen, die auch systemgestützt erfolgen können.
➢ in einem wirksamen und wirtschaftlichen IKS ergänzen sich vorbeugende und aufdeckende Kontrollen.

Priorität:
1 = Muss (wenn immer möglich vorzusehen)
2 = Soll (oft sinnvoll, sollen verwendet werden)
3 = Kann (in spezifischen Einzelfällen angebracht)