

Empfehlungen der Schweizerischen Finanzkontrollen für Informatikprojekte

Arbeitsgruppe IT Government Audit

Die Gruppe vereint die Informatik-Auditoren der öffentlichen Verwaltungen der Schweiz.

Kontakt: info@efk.admin.ch



Warum diese Broschüre?

Den Projektverantwortlichen werden oft vielfältige Beschränkungen auferlegt, so dass sie manchmal versuchen müssen, ihre Vorhaben unter widrigen Umständen zum Erfolg zu führen.

Der Einbezug eines Revisors ist eine zusätzliche Herausforderung, die von den Projektverantwortlichen häufig als überflüssige Schikane empfunden wird. Die Finanzkontrollen messen jedoch einer offenen und konsequenten Kommunikation mit den Projektverantwortlichen grosse Bedeutung bei. Die vorliegende Broschüre soll Fragen beantworten, die den Revisoren oft gestellt werden. Sie liefert zudem interessante Informationen für Entscheidungsträger, Informatikverantwortliche oder Qualitätsbeauftragte.

Die Broschüre bezweckt insbesondere die Erstellung einer Liste der wichtigsten Dokumente aus der Sicht der Revision. Sie will ferner die Fragen definieren, **die diese Dokumente beantworten müssen**. Die Broschüre beschränkt sich auf die im Lebenszyklus einer Anwendung wichtige Projektphase.

In der Schweiz existieren verschiedene Entwicklungsmethoden (auch Lieferanten bieten solche an). Die Terminologie unterscheidet sich deshalb möglicherweise von einer Methode zur andern. Die Broschüre beschränkt sich auf inhaltliche Aspekte und liefert lediglich einen Hinweis auf die verschiedenen Methoden, indem sie die entsprechenden Referenzen angibt.

Wenn Sie weitere Fragen haben, wird ihre (kommunale, kantonale oder eidgenössische) Finanzkontrolle sie gerne beantworten.

Ziele

Informatikprojekte sollten überall dieselben Ziele verfolgen, auch wenn die einschlägigen kommunalen, kantonalen und eidgenössischen Gesetzesbestimmungen sehr vielfältig sind.

Diese Ziele leiten sich her aus:

- dem übergeordneten Grundsatz des sparsamen Mitteleinsatzes (Effektivität und Effizienz);
- dem Legalitätsprinzip (Einhaltung rechtlicher Erfordernisse) sowie
- den Grundsätzen der ordnungsmässigen Rechnungslegung (Integrität, Verfügbarkeit und Zuverlässigkeit).

In diesen Grundsätzen sind die klassischen Vorstellungen von Sicherheit und Qualität der Informationsverarbeitung enthalten.

Die Revisoren bedienen sich gerne des Referenzmodells CobiT (www.isaca.org), insbesondere, wenn es um allgemeine Kontrollen im Informatikbereich geht. CobiT arbeitet mit 7 Kriterien, die den oben erwähnten Zielen entsprechen.

Überblick:

Welche Ziele sollen erreicht werden?

| | |
|---|--|
| Effektivität Effizienz | Erreichen der anfänglich festgelegte Zielen Optimale Verwendung der Ressourcen |
| Einhaltung | Einhaltung von Gesetzen, Reglementationen und Verträge |
| Integrität Vertraulichkeit Verfügbarkeit | Richtigkeit, Gültigkeit und Vollständigkeit der Informationen Schutz vor unberechtigter Veröffentlichung Verfügbarkeit der Systeme, Ressourcen und Daten |
| Zuverlässigkeit | Bereitstellung zuverlässiger Informationen |

Die Schlüsseldokumente

Die Methode «Hermes» (www.hermes.admin.ch) definiert für den Lebenszyklus eines Informatikprojekts etwa Hundert Dokumente.

Zehn davon sind für den Revisor unerlässlich, und zwar unabhängig von der Entwicklungsmethode, die angewandt wird (einschliesslich der neuen so genannten «agilen» Methoden).

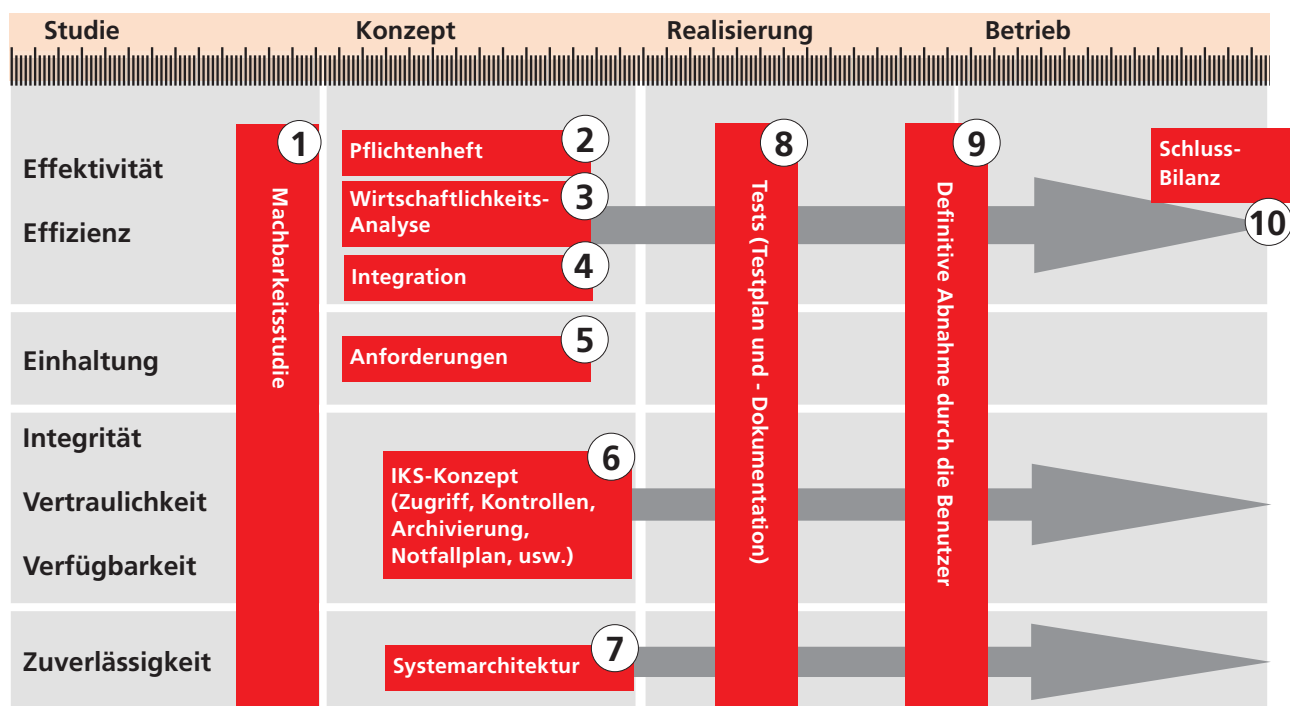
Diese Schlüsseldokumente haben jedoch strengen formalen Anforderungen zu genügen:

- Sie müssen validiert und unterzeichnet sein.
- Sie müssen zu einem bestimmten Zeitpunkt des Projekts vorliegen (eine Machbarkeitsstudie, die erst nach der Konzeptphase zur Verfügung steht, ist nutzlos).
- Manche Dokumente müssen nicht nur während der gesamten Projektdauer, sondern auch nach der Implementierung und bis zur definitiven Beendigung einer Anwendung (beispielsweise einer Systemarchitektur oder eines internen Kontrollsystem-Konzeptes fortlaufend aktualisiert werden.

Die Empfehlungen beschränken sich auf die im Rahmen des Projekts produzierten Dokumente



Die 10 Schlüsseldokumente eines Projektzyklus



Zustellung der zehn Schlüsseldokumente

Braucht die Finanzkontrolle eine Kopie jedes Dokuments? Im Prinzip nicht, denn bei Bedarf kann sie die Dokumente bei der Revision eines Projekts oder einer zukünftigen Anwendung einsehen. Hingegen ist es unerlässlich, dass die Finanzkontrolle von der Existenz aller bedeutenden* Informatikprojekte Kenntnis hat, weswegen:

- ihr alle «Projektaufträge» systematisch und unaufgefordert zugestellt werden müssen;
- ihr ein kontinuierlich aktualisiertes Inventar der laufenden Projekte zur Verfügung stehen muss.

* was unter einem «Informatikprojekt von Bedeutung» zu verstehen ist, kann man in den kommunalen, kantonalen und eidgenössischen Weisungen nachlesen.

Links zu den wichtigsten erwähnten Quellen

Hermes SE/DS (Ausgabe 2003), Hermes SA/AS (Ausgabe 2005), <http://www.hermes.admin.ch>

Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV, SR 221.431)

http://www.bk.admin.ch/ch/f/rs/221_431/index.html

CobiT Version 4.0 (Download), <http://www.isaca.ch>

Schweizer Handbuch der Wirtschaftsprüfung (HWP) und Prüfungsstandards der Treuhand-Kammer

<http://www.treuhand-kammer.ch>

PRINCE 2, www.ogc.gov.uk/prince

1. Machbarkeitsstudie



Welche Ziele verfolgt das System?
Welche Lösungen sind vorstellbar?

- Systemanforderungen ermitteln und analysieren
- Lösungsvorschläge (Varianten) erarbeiten
- Kosten, Risiken und Vorteile dieser Varianten vergleichen

Welche Anforderungen werden an das Projekt und die Organisation gestellt?
Ist das Projekt realisierbar?
Kann das Projekt in die Konzeptphase treten (Projektauftrag) ?

Verantwortlich:
Benutzerdienst (mit Unterstützung des Informatikdienstes was technische Fragen anbelangt)

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : Kap. 3.3 (SE und SA)
POSAT ZH : Ablaufschritt 2
CobIT 4.0 : AI 1.3
PRINCE 2 : Prozess SU

2. Pflichtenheft



Welches sind die Zielsetzungen?
Welches sind die Erwartungen der Benutzer?

- Welche Funktionalitäten (Nutzungsmöglichkeiten) bestehen?
- Wie gross ist das zu verarbeitende Volumen?

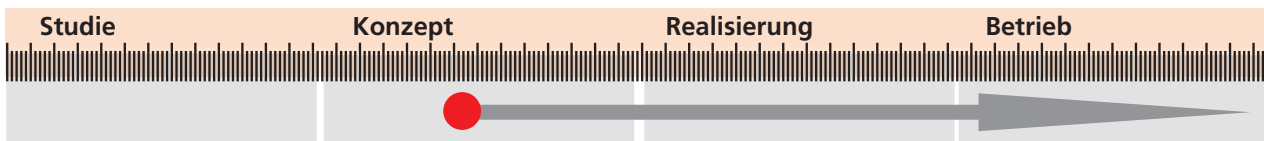
Welche Vorgaben und Einschränkungen sind zu berücksichtigen?
Mit welchen technischen Hilfsmitteln können diese Ziele erreicht werden?

Verantwortlich:
Benutzerdienst (mit Unterstützung des Informatikdienstes, was technische Fragen anbelangt)

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 5.3.47, SA Kap. 3.4.1, 5.3.50
POSAT ZH : Ablaufschritt 3
CobIT 4.0 : PO 10.5, AI 1.1
PRINCE 2 : Prozess IP

3. Wirtschaftlichkeitsanalyse



Wie hoch sind die Gesamtkosten des Projekts (einschliesslich der Ausführungskosten, z.B.: Kosten von Datenmigration, Kapazitätserhöhung der Einrichtungen, Benutzerschulung, usw...)?
Wie kann der geplante Nutzen quantitativ und qualitativ bewertet werden?
Wie wirtschaftlich ist das Projekt?
Welche Szenarien sind vorstellbar, um die Wirtschaftlichkeit des Projekts zu verbessern?

Verantwortlich:
Benutzerdienst

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 5.3.92, SA Kap. 5.3.98
POSAT ZH : Ablaufschritt 5
CobiT 4.0 : AI 1.1, AI 1.2, AI 1.3
PRINCE 2 : Prozesse DP und CS

4. Integration ins Informatikumfeld



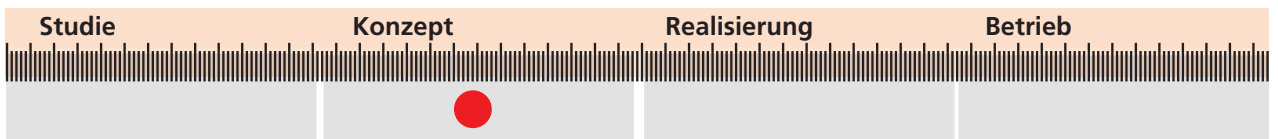
Fügt sich das Projekt harmonisch in die Unternehmensstrategie und in die IT-Architektur ein?
Führt das Projekt zu Doppelspurigkeiten mit allfälligen anderen Projekten oder Anwendungen?
Gibt es Synergien mit anderen Projekten?
Hält sich das Projekt an die vom Unternehmen verabschiedeten Standards?
Welche automatischen oder manuellen Schnittstellen sind vorgesehen?

Verantwortlich:
Informatikdienst

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 5.3.83, SA Kap. 5.3.31, 5.3.89
POSAT ZH : Ablaufschritt 8
CobiT 4.0 : PO 2, AI 1.3
PRINCE 2 : Prozess SB

5. Anforderungen



Welches sind die internen Anforderungen (Abmachungen, Verfahren, Qualitätsnormen)?
Welches sind die externen Anforderungen (Gesetze, Verordnungen, Weisungen, Verträge), die möglicherweise branchenspezifisch sind (Datenschutz, Publikation, Beschaffungsverfahren, Banken, Best practices, Good xxx Practice, usw.)?
Wie wirken sich diese Anforderungen auf die Verfahren oder die Infrastruktur (Architektur, Sicherheit, usw.) aus?

Verantwortlich:
Benutzerdienst (mit Unterstützung des Informatikdienstes, was technische Fragen anbelangt)

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 3.4.4, 5.3.31, 5.3.80, SA Kap. 5.3.32, 5.3.87
POSAT ZH : Ablaufschritt 1
CobIT 4.0 : PO 2, ME 3

Anforderungsbeispiele (keine abschliessende Aufzählung)

Personalbereich

- Steuern (Lohnausweis, Quellensteuern, usw.)
- Sozialversicherungen (AHV, ALV, EO, usw.)
- Datenschutz (Berechtigungskonzept, Vertraulichkeitsklärung, usw.)

Finanzbereich

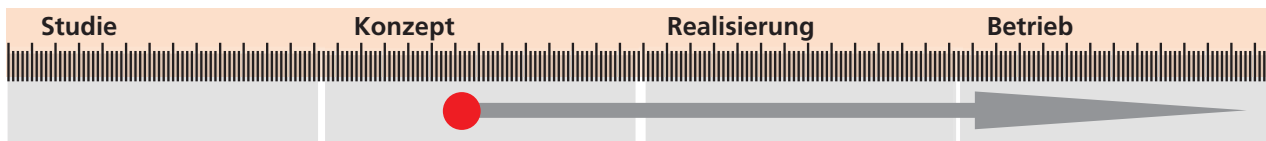
- Führung und Aufbewahrung der Geschäftsbücher (GeBüV)
- Geldwäscherei

Gesundheitsbereich

- Kostenrechnung in den Spitälern
- Rückverfolgbarkeit von Produkten und Medikamenten
- Datenschutz

usw.

6. Konzept für ein internes Kontrollsystem (IKS)



Welche automatischen Kontrollen (Eingabegültigkeitsprüfung, automatische Abgleiche, Fehlerlisten, usw.) sind erforderlich?

Welche Funktionstrennungen braucht es und wie wirken sie sich auf die Zugriffsberechtigungen aus?

Welche Massnahmen braucht es zur Gewährleistung der Nachprüfbarkeit der einzelnen Schritte, einschliesslich der Parametrierung der Anwendung?

Welche Massnahmen braucht es zur Sicherstellung der betrieblichen Kontinuität (Notfallplan) sowie der Datenaufbewahrung (Archivierungsplan)?

Verantwortlich:

Benutzerdienst (mit Unterstützung des Informatikdienstes, was technische Fragen anbelangt)

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 5.3.31, SA Kap. 5.3.32

POSAT ZH : Ablaufschritt 10, 11

CobiT 4.0 : PO 8, AI 1.1, AI 1.2, AI 2.2, AI 2.3, AI 2.4, DS 4, DS 5, DS 11, ME 2

PRINCE 2 : Prozess SU

Treuhand-

Kammer : NAS 400, HWP Ziff. 3.24233, 3.3222 ff.

7. Systemarchitektur



Wie ist das Informatiksystem aufgebaut?

Wie sieht die Informationsarchitektur aus (Datenmodell)?

Welche Funktionalitäten bietet das System?

Wie fügt sich das System in die bestehende Systemarchitektur ein?

Welche Wechselwirkungen bestehen zwischen den Informationen?

Welche Schnittstellen gibt es?

Verantwortlich:

Informatikdienst

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 5.3.81, 5.3.82, SA Kap. 5.3.88, 5.3.89

POSAT ZH : Ablaufschritt 14

CobiT 4.0 : PO 2, AI 1.3, AI 2.1, AI 2.2, AI 2.5, AI 2.6

8. Tests (Testplan und - Dokumentation)



Was bezwecken die Tests?

Welche Tests sind geplant (Methoden, Tools, Kriterien, Fälle)?

Welche Ressourcen sind vorhanden und wie sehen die Ausführungsfristen aus?

Werden Korrekturen, die in letzter Minute erfolgen, noch getestet?

Wie ist der genaue Testverlauf und wie sind die Testergebnisse dokumentiert?

Verantwortlich:

Informatikdienst (und Benutzerdienst)

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 5.3.85 bis 5.3.90, SA Kap. 5.3.91 bis 5.3.96

POSAT ZH : Ablaufschritt 14

CobIT 4.0 : PO 8, AI 2.8, AI 3.4, AI 5.6, AI 7.2, AI 7.4, AI 7.6, AI 7.7

9. Abnahme durch die Benutzer



Was umfasst die Abnahme, worauf bezieht sie sich?

Wem gehören die Daten und wer ist für die Anwendung verantwortlich?

Wer ist für die Abnahme zuständig?

Auf welchen Tests beruht die Abnahme?

Welche Vorbehalte sind bei der Abnahme gemacht worden?

Verantwortlich:

Benutzerdienst

Nützliche Hinweise (keine abschliessende Aufzählung!)

Hermes : SE Kap. 3.3.6, 3.4.7, 3.5.8, 3.6.7, SA Kap. 3.3.7, 3.4.9, 3.5.11, 3.6.7

POSAT ZH : Ablaufschritt 14, 15

CobIT 4.0 : AI 3.1 bis 3.3, AI 7.6, AI 7.7, PO 10.6

10. Schlussbilanz



- Wurden die Ziele des Projekts erreicht und die Anforderungen erfüllt?
- Wie hoch sind die definitiven Kosten und wie lassen sich allfällige Abweichungen gegenüber den anfänglichen Prognosen erklären?
- Wie sieht die definitive Wirtschaftlichkeitsrechnung aus?
- Welche Risiken bestehen nach der Implementierung?
- Welche Fehler traten nach der Implementierung auf?
- Welche Empfehlungen und Massnahmen werden vorgeschlagen?
- Welche Lehren können aus dem Projekt gezogen werden?

Verantwortlich:
Benutzerdienst

Nützliche Hinweise (keine abschliessende Aufzählung!)

- Hermes : Kap. 5.3.13 (SE und SA)
- POSAT ZH : Ablaufschritt 16
- CobiT 4.0 : PO 10.6, PO 10.13, PO 10.14, AI 7.12

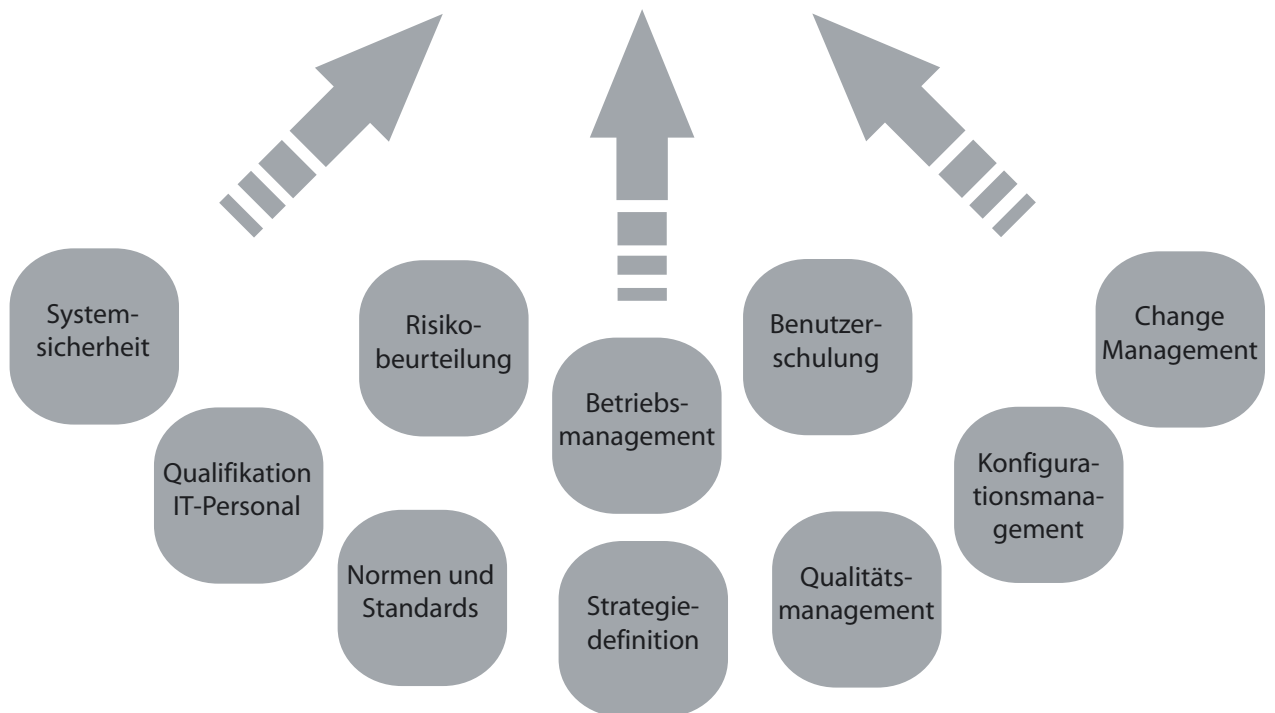
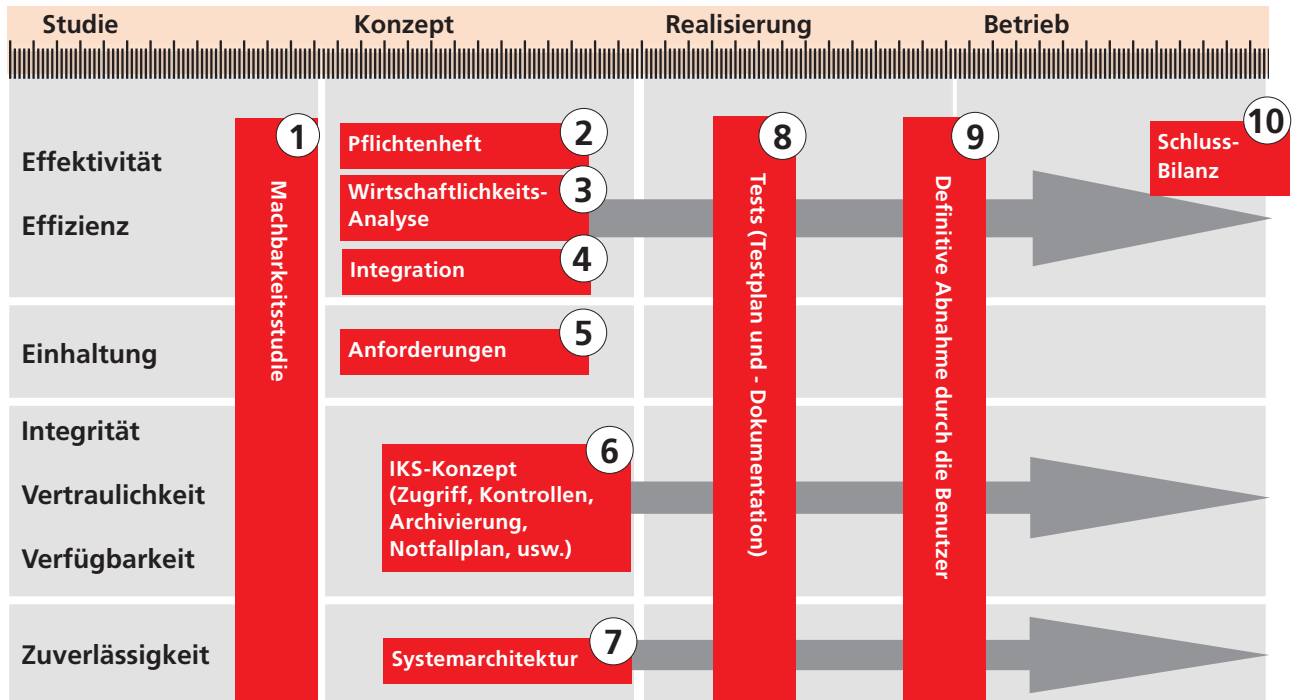
Projektumfeld nicht vernachlässigen!

Kein Projekt findet im luftleeren Raum statt. Der Erfolg eines Projekts hängt unmittelbar vom Kontext ab, in welchem es durchgeführt wird. Zu den einflussreichsten Faktoren gehören: Starker Einbezug der Benutzer, Qualifikation der Projektteilnehmenden, Ausmass der Unternehmensstandardisierung, Qualitätssicherungssysteme und Verfahren, die eine optimale Verwaltung der verschiedenen Programmversionen erlauben.

CobiT listet für 34 standardisierte Informatikprozesse Kontrollziele auf, die es ermöglichen, den ganzen Informatikbereich unter Kontrolle zu haben.

Beim Prozess (Verteilung und Support 8) «Umgang mit Problemen und Zwischenfällen» geht es beispielsweise um die Vorschriften für das Problemmeldewesen, die Eskalation der Probleme, die Problemverfolgung und die Prüfspuren, die vorübergehenden und notfallmässigen Zugriffsberechtigungen sowie die Prioritäten der Notfallbearbeitung.

Einflussfaktoren berücksichtigen



Die Grundsätze des guten Projektmanagements nicht vergessen!

Einige Lehren aus den gemeinsamen Revisionen der Finanzkontrollen:

- Die Realisierung eines Grossprojekts ist nur mit vollzeitlich zugeteilten Personen möglich.
- Jedes Projekt von Bedeutung braucht die entsprechende politische Unterstützung.
- Vor der Computerisierung braucht es eine Reorganisation und Harmonisierung.
- Es empfiehlt sich, die Projektdauer zu verkürzen oder das Vorhaben in unabhängige Teilprojekte aufzuteilen.
- Noch nicht ganz ausgereifte Technologien vermeiden.
- Zwischen Informatikern und Fachleuten muss ein ausgewogenes Verhältnis bestehen.
- Nicht zu viele Controllingorgane, dafür ein echtes Controlling.
- Probleme möglichst rasch erkennen und einschätzen, insbesondere mit Hilfe von Machbarkeitstests.
- Lieferanten gut auswählen und ihre Beziehung zum Projekt vertraglich regeln.
- Allfällige Anpassungen in der Projektorganisation auch in den vertraglichen Abmachungen nachvollziehen.
- Das Problempotenzial einer zwei- oder sogar dreisprachigen Entwicklung nicht unterschätzen.

Schlusswort

Der Entscheid, ein bestimmtes Informatikprojekt zu prüfen, liegt bei der Finanzkontrolle. Sie lässt sich dabei von mehreren Kriterien leiten, insbesondere von der Beurteilung der Risiken im Vergleich zu ähnlichen Projekten.

Der Einbezug der Finanzkontrolle kann in Form einer Projektprüfung erfolgen (insbesondere am Ende einer Projektphase) oder in Form einer Stellungnahme zu besonderen Fragen (zum Beispiel als Evaluation des IKS-Konzepts vor dessen praktischer Umsetzung).

Zögern Sie nicht, uns Ihr Problem zu unterbreiten!