

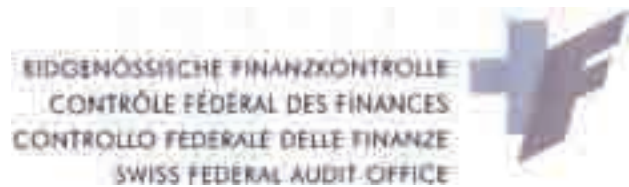
# Recommendations on IT projects

## Working group IT Government Audit

The group brings together IT auditors of the Swiss public administration.

Contact: [info@efk.admin.ch](mailto:info@efk.admin.ch)

An initiative of:



# Why is this brochure necessary?

A variety of restrictions are often placed on project leaders, so that the circumstances under which they must try to achieve their objectives are sometimes very difficult.

Involving an auditor is an added challenge, and is often felt to be an unnecessary intrusion. Audit offices, however, consider open and consequential communication with project leaders to be of great importance. The **following brochure aims to answer questions which auditors are often asked**, and to provide interesting information for decision-makers, for IT coordinators and for those working in quality assurance.

In particular, this brochure provides a list of the most important documents required for auditing purposes, and aims to define the questions which such documents should answer. It concentrates on a project phase which is of importance in the application process.

Various development methods exist in Switzerland (some are also offered by suppliers), and as a result use of terminology may differ from one method to the next. This brochure concentrates on document content and makes only brief reference to the various methods.

Any further questions will be gladly answered by the federal audit office ([info@efk.admin.ch](mailto:info@efk.admin.ch)).

## Objectives

Despite the medley of local, cantonal and federal regulations, all IT projects should have the same objectives. These objectives are based on:

- the higher principle of economic use of resources (effectiveness and efficiency);
- the principle of legality (conformity to legal requirements) and
- accounting standards in accordance with regulations (integrity, availability and reliability).

These principles cover the classic security and quality notions of information processing.

Auditors often like to make use of the governance framework CobiT ([www.isaca.org](http://www.isaca.org)), especially when general IT controls are required. CobiT works with seven criteria which correspond to the aforementioned objectives.

# Overview:

## What are the objectives?

<b>Effectiveness</b> <b>Efficiency</b>	Achieving initial objectives Using resources to maximum effect
<b>Compliance</b>	Conformity with laws, regulations and contracts
<b>Integrity</b> <b>Confidentiality</b> <b>Availability</b>	Accuracy, validity and completeness of information Protection from unauthorized publication Availability of systems, resources and data
<b>Reliability</b>	Provision of reliable information

## Key Documents

The «Hermes» method ([www.hermes.admin.ch](http://www.hermes.admin.ch)) defines about a hundred documents which are necessary during the life of an IT project.

Ten of these are essential for the auditor, regardless of the development methods employed (including new so-called «agile» ones).

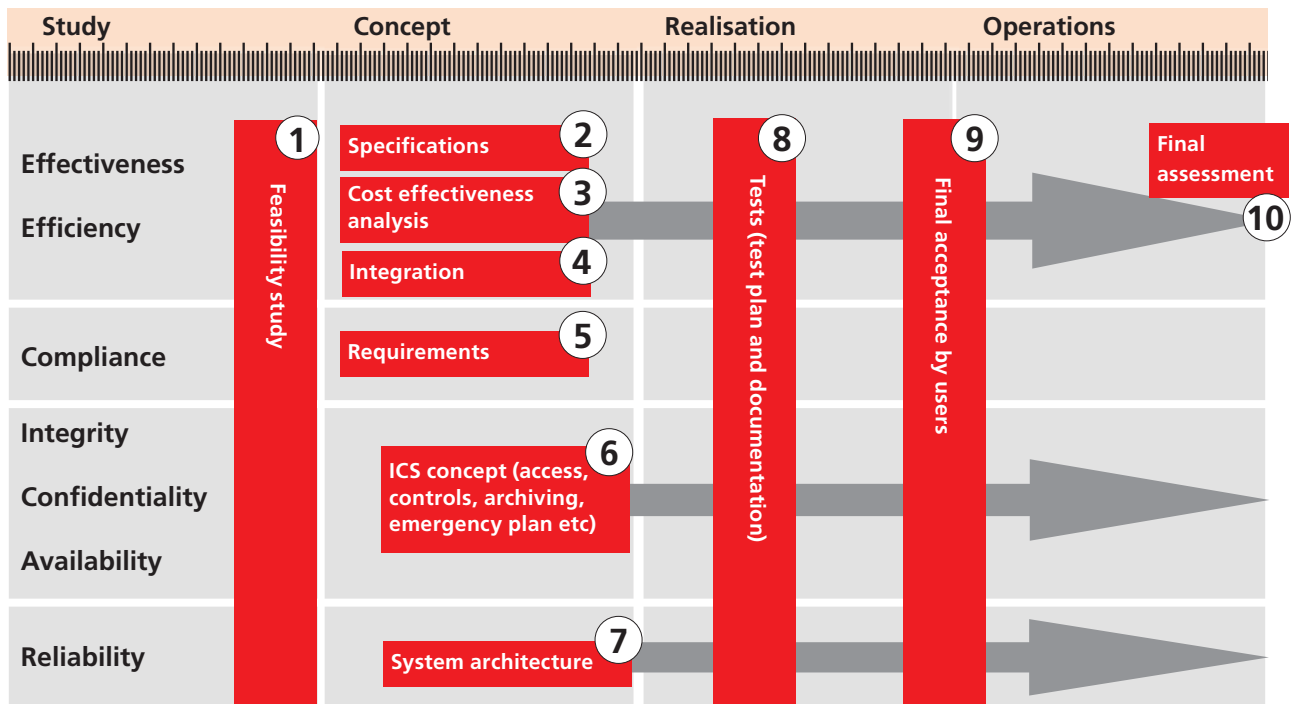
These key documents must however meet certain strict formal requirements:

- They must be validated and signed.
- They must be available at any given time during the project (a feasibility study which appears after the concept phase is of no use at all).
- Some documents require updating regularly during the whole project process; they may also need to be updated following implementation of an application right up to its completion (for instance of a system architecture or an internal control system (ICS) concept).

**The recommendations are limited to documents produced within the project framework.**



# The 10 Key Documents in a project life cycle



## Providing the 10 key documents

Does the audit office require a copy of each document? The answer is no in theory, as documents can be looked at as required during the auditing of a project or other future application. It is however essential that the auditors know of the existence of all significant\* IT projects, as:

- there must be systematic and unsolicited provision of all «project tasks»;
- a regularly updated inventory of the current project must always be available.

\* Local, cantonal and federal directives define the term «significant IT project».

## Links to the most important sources

Hermes SE/DS (2003 Edition), Hermes SA/AS (2005 Edition), <http://www.hermes.admin.ch>  
 Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Accounts Ordinance) (GeBüV, SR 221.431) [http://www.bk.admin.ch/ch/f/rs/221\\_431/index.html](http://www.bk.admin.ch/ch/f/rs/221_431/index.html)  
 CobiT Version 4.0, <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](http://www.ogc.gov.uk/prince)

# 1. Feasibility study



What objectives does the system want to pursue?  
What are the possible solutions?

- Determine and analyse system demands.
- Elaborate possible solutions (variants).
- Compare costs, risks and advantages of these variants.

What demands will be put on the project and the organisation?  
Is the project feasible?  
Can the concept phase of the project begin (commissioning of project)?

Department responsible:  
User Department (supported in technical questions by IT Services)

## Useful references (not an exhaustive list!)

Hermes : Chap. 3.3 (SE and SA)  
POSAT ZH : Ablaufschritt 2  
CobiT 4.0 : AI 1.3  
PRINCE 2 : Process SU

# 2. Specifications



What are the objectives?  
What are the users' expectations?

- What functionalities are available?
- How big is the project?

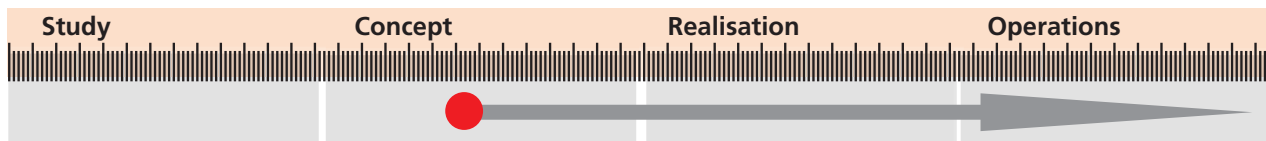
Under what constraints does one have to operate?  
What technical aids are available to achieve the objectives?

Department responsible:  
User Department (supported in technical questions by IT Services)

## Useful references (not an exhaustive list!)

Hermes : SE Chap. 5.3.47, SA Chap. 3.4.1, 5.3.50  
POSAT ZH : Ablaufschritt 3  
CobiT 4.0 : PO 10.5, AI 1.1  
PRINCE 2 : Process IP

### 3. Cost effectiveness analysis



How high are the total costs of the project (including operational costs, eg costs of data migration, increasing capacity of installations, user training etc...)?

How can the intended use be assessed for quantity and quality?

How cost-effective is the project?

What scenarios can be envisaged to improve the cost effectiveness of the project?

Department responsible:  
User Department

#### Useful references (not an exhaustive list!)

- Hermes : SE Chap. 5.3.92, SA Chap. 5.3.98
- POSAT ZH : Ablaufschritt 5
- CobiT 4.0 : AI 1.1, AI 1.2, AI 1.3
- PRINCE 2 : Processes DP and CS

### 4. Integration into the IT environment



Can the project be easily integrated into corporate strategy and into IT structures?

Does the project overlap with other projects or applications?

Are there synergies with other projects?

Does the project conform to the enterprise's agreed standards?

What automatic or manual interfaces will there be?

Department responsible:  
IT Services.

#### Useful references (not an exhaustive list!)

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

# 5. Requirements



What internal requirements are there (agreements, procedures, quality norms)?

What external requirements are there (laws, regulations, directives, contracts) which may be specific to a particular area (data protection, publication, procurement procedures, banks, best practices, good xxx practice etc.)?

What is the effect of these requirements on processes or infrastructure (architecture, security etc)?

Department responsible:

User Department (supported in technical questions by IT Services)

## Useful references (not an exhaustive list!)

Hermes : SE Chap. 3.4.4, 5.3.31, 5.3.80, SA Chap. 5.3.32, 5.3.87

POSAT ZH : Ablaufschritt 1

CobiT 4.0 : PO 2, ME 3

## Example Requirements (not an exhaustive list)

### Personnel

- Taxes (end of year salary statement, tax at source etc)
- Social insurance (AHV, unemployment insurance, income compensation regulations etc.)
- Data protection (authorisation concept, confidentiality declaration, etc.)

### Finances

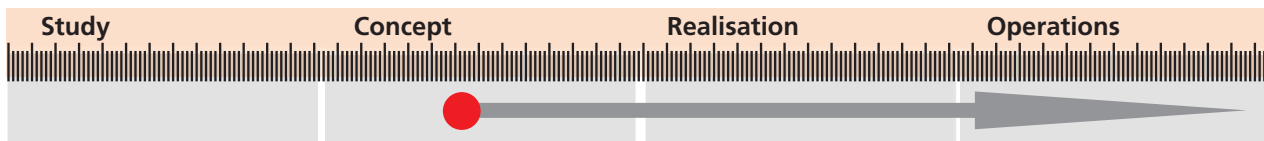
- Keeping and retention of accounts
- Money laundering

### Health

- Calculation of costs in hospitals
- Traceability of products and medicines
- Data protection

etc.

## 6. Concept for an internal control system (ICS)



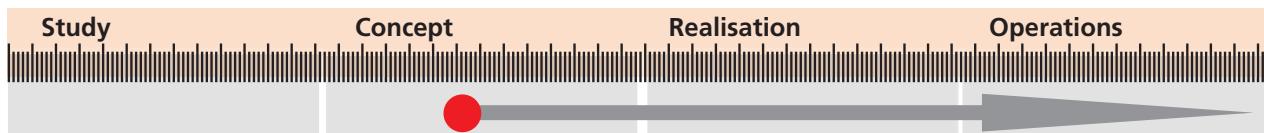
Which automatic controls (data input validity check, automatic comparisons, error lists etc.) are necessary?  
How should functions be separated, and what are the repercussions on access permission?  
Which measures are necessary to maintain controls over individual steps in a process, including customizing?  
Which measures are necessary to ensure continuity in operations (emergency plan) and preservation of data (archive plan)?

Department responsible:  
User Department (supported in technical questions by IT Services)

### Useful references (not an exhaustive list!)

Hermes : SE Chap. 5.3.31, SA Chap. 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 : Process SU  
Treuhand-  
Kammer : NAS 400, HWP Ziff. 3.24233, 3.3222 ff.

## 7. System architecture



How is the IT system structured?  
What form does the information architecture take (data model)?  
Which functionalities does the system offer?  
How does the system conform to the existing system architecture?  
Are there systems in place for the exchange of information?  
What are the interfaces?

Department responsible:  
IT Services

### Useful references (not an exhaustive list!)

Hermes : SE Chap. 5.3.81, 5.3.82, SA Chap. 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 (test plan and documentation)



- What is the purpose of the tests?
- What tests are planned (methods, tools, criteria, case studies)?
- What resources are available and what time constraints are there?
- Will last minute corrections be tested?
- How exactly are the tests carried out and how are the test results documented?

Department responsible:  
IT Services (and User Department)

### Useful references (not an exhaustive list!)

- Hermes : SE Chap. 5.3.85 to 5.3.90, SA Chap. 5.3.91 to 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. Acceptance by the user



- What exactly does acceptance involve?
- Who does the data belong to and who is responsible for its application?
- Who is responsible for the acceptance process?
- Upon which tests is acceptance based?
- Are there any possible reservations concerning acceptance?

Department responsible:  
User Department

### Useful references (not an exhaustive list!)

- Hermes : SE Chap. 3.3.6, 3.4.7, 3.5.8, 3.6.7, SA Chap. 3.3.7, 3.4.9, 3.5.11, 3.6.7
- POSAT ZH : Ablaufschritt 14, 15
- CobIT 4.0 : AI 3.1 to 3.3, AI 7.6, AI 7.7, PO 10.6

# 10. Final assessment



- Have the project objectives been achieved and the requirements fulfilled?
- What are the final costs and how can possible discrepancies with initial cost estimates be explained?
- What is the final calculation of cost effectiveness?
- What risks are there after implementation of the project?
- What mistakes arose after implementation?
- What recommendations can be made and what future measures suggested?
- What lessons can be learnt from the project?

Department responsible:  
User Department

## Useful references (not an exhaustive list!)

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

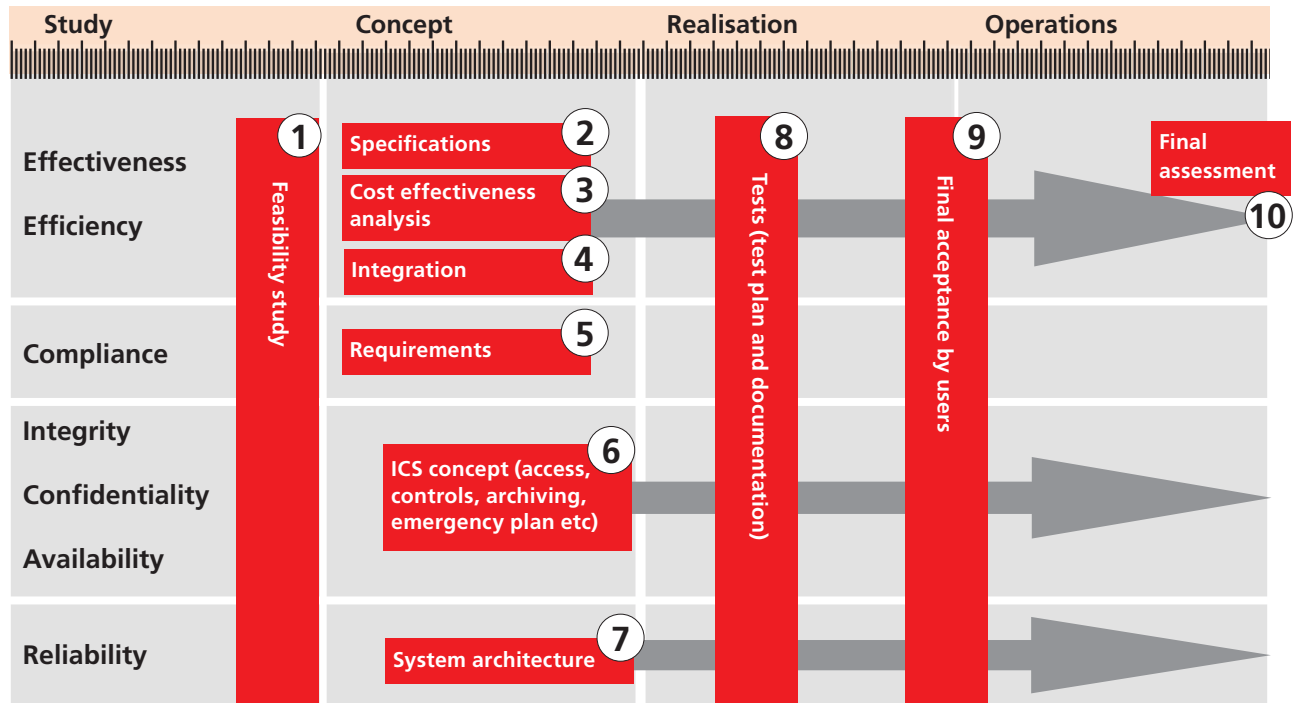
## Do not neglect the project context!

No project takes place in isolation. A project's success depends directly on the context in which it is carried out. Some of the most influential factors are: Extensive user involvement, performance appraisal of project participants, extent of standardisation within the enterprise, quality assurance systems and procedures leading to optimum management of different programme versions.

CobiT lists control objectives for 34 standardised IT processes which enable comprehensive IT control.

For instance, process (deliver and support 8) «Manage Service desk and Incidents» deals with regulations concerning the recording of problems, escalation procedures, tracking of problems and audit trail, temporary and emergency access authorisations and emergency processing priorities.

# Take account of external influences



# Not forgetting the principles of good project management

## Some lessons learnt in joint audits by swiss audit offices:

- It is only possible to carry out a large-scale project with staff who can work full time on it.
- All significant projects require the corresponding political backing.
- Reorganisation and harmonisation is required before the project is computerised.
- It is worth reducing the length of the project or creating independent sub-projects.
- Avoid technologies which have not been tried and tested.
- There should be a balanced relationship between IT employees and business specialist staff.
- Avoid using too many cost control systems, but make sure effective cost control takes place.
- Identify and evaluate problems as soon as possible, in particular by means of feasibility tests.
- Choose your suppliers well and draw up a contract regarding their involvement in the project.
- Any changes to project organisation should also be written into the contracts.
- Do not underestimate the potential problems when working in two or even three languages.

## Final comments

The decision to audit any given IT project lies with the audit office. This decision is determined by several criteria, in particular by an assessment of the project risks compared with other projects.

Audit office involvement may take the form of a project audit (in particular at the end of a project phase). Alternatively, the audit office may just comment on specific issues (e.g. giving an opinion on the ICS concept before its implementation).

Please do not hesitate to tell us your problems!