

Raccomandazioni dei Controlli delle finanze concernenti i progetti informatici

Gruppo di lavoro IT Government Audit

Questo gruppo è composto da revisori informatici delle amministrazioni pubbliche svizzere.

Contatto: info@efk.admin.ch



Perché di questo opuscolo ?

I capi progetto sono tenuti a rispettare numerosi vincoli e devono condurre i loro progetti al successo in condizioni spesso difficili.

L'intervento di un revisore informatico costituisce una sfida supplementare spesso percepita come un' inutile complicazione dai responsabili. I controlli delle finanze reputano importante comunicare in modo trasparente con i responsabili di progetto e scopo di questa presentazione è di **rispondere alle domande che sono spesso formulate ai revisori**. Il presente documento contiene pure informazioni suscettibili di interesse per le istanze decisionali, i responsabili dell'informatica oppure per le persone incaricate del controllo qualità.

L'obiettivo è in particolare quello di determinare la liste dei documenti più importanti per un revisore e di definire i quesiti ai quali tali documenti devono rispondere. Questa presentazione si focalizza sulla fase di sviluppo del progetto che costituisce un passaggio importante nel ciclo di vita di un'applicazione.

Esistono in Svizzera differenti metodi di sviluppo (compreso quelli proposti da alcuni fornitori) e la terminologia può variare da uno all'altro. Questa presentazione si concentra sul contenuto dei documenti e vi fornisce le referenze ad alcuni di questi metodi.

Il vostro controllo delle finanze (federale, cantonale o comunale) è a disposizione se avete delle ulteriori domande.

Gli obiettivi da raggiungere

Malgrado la diversità delle legislazioni comunali, cantonali e federali, gli obiettivi da raggiungere per i progetti informatici sono gli stessi dappertutto.

Questi obiettivi derivano dal:

- principio superiore della buona gestione dei crediti accordati (principi d'efficacia e d'efficienza),
- principio della legalità (conformità) e
- principio della tenuta regolare della contabilità (principi d'integrità, della disponibilità e dell'affidabilità).

Questi principi coprono completamente le nozioni classiche della sicurezza e della qualità del trattamento dell'informazione.

Il modello di riferimento CobiT (www.isaca.org) è spesso utilizzato dai revisori, in particolare quando si tratta di esaminare i controlli generali nell'ambito informatico. CobiT propone 7 criteri corrispondenti a questi obiettivi.

Riassunto:

Quali sono gli obiettivi da raggiungere?

efficacia efficienza	Raggiungimento degli obiettivi fissati inizialmente Utilizzo ottimale delle risorse
conformità	Rispetto delle leggi, regolamenti e clausole contrattuali
integrità confidenzialità disponibilità	Esattezza, validità e completezza delle informazioni Protezione contro qualsiasi divulgazione non autorizzata Disponibilità dei sistemi, delle risorse e dei dati
affidabilità	Messa a disposizione di informazioni affidabili

I documenti chiave

La metodologia « Hermes » (www.hermes.admin.ch) definisce un centinaio di documenti che dovrebbero essere elaborati durante la vita di un progetto informatico.

Per un revisore, una decina sono indispensabili, indipendentemente dalla metodologia di sviluppo adottata (compreso i nuovi metodi di sviluppo « rapido »!).

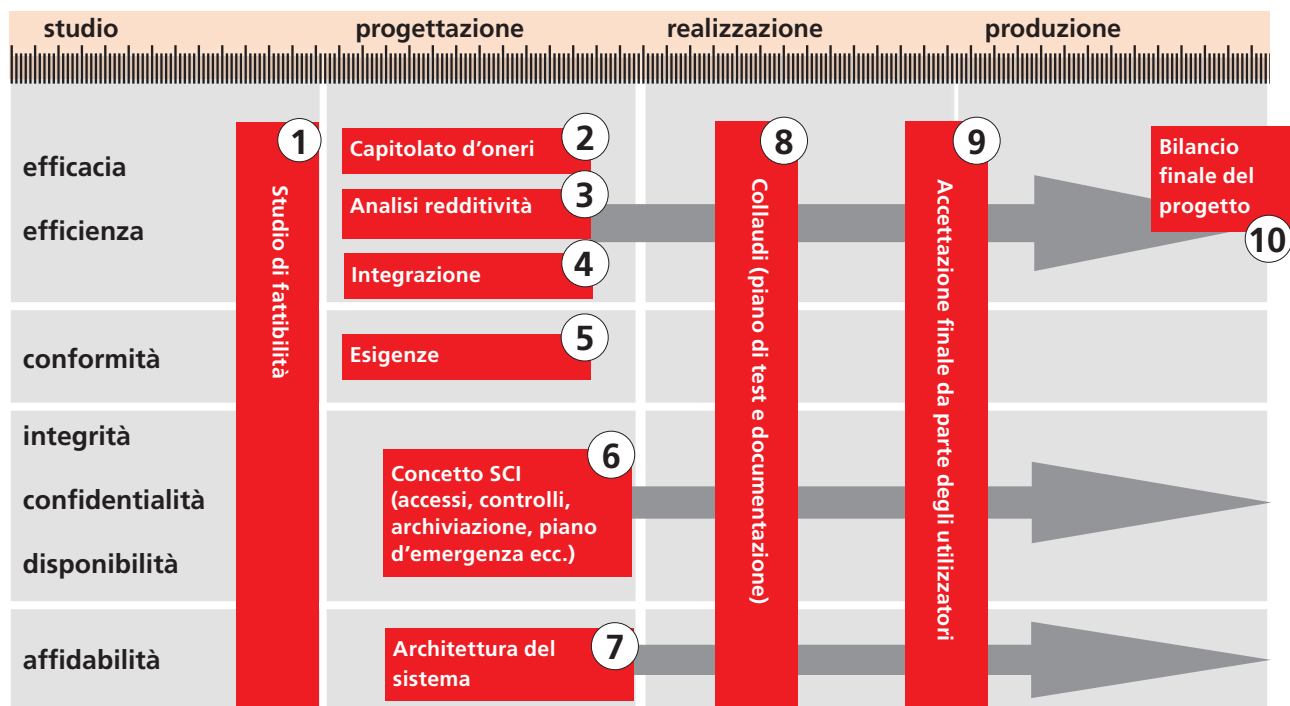
Le esigenze formali che li riguardano sono però elevate:

- devono essere validati e firmati
- devono essere a disposizione ad un momento preciso del progetto (uno studio di fattibilità finalizzato dopo la fase di progettazione non è più utile)
- alcuni di essi devono essere aggiornati regolarmente non soltanto durante il progetto, ma anche dopo il passaggio in produzione fino allo smantellamento finale dell'applicazione (l'architettura del sistema o il concetto del sistema di controllo interno per esempio)

Le raccomandazioni si concentrano sui documenti prodotti dal progetto



I 10 documenti chiave della vita di un progetto



Trasmissione dei 10 documenti chiave

Il Controllo delle finanze desidera ricevere una copia di ciascuno di questi documenti per ogni progetto in corso? In linea di principio no, ma li consulterà secondo il caso in occasione di un audit del progetto o della futura applicazione.

Per contro è essenziale che la revisione interna sia a conoscenza dell'esistenza di tutti i progetti informatici importanti*, ragion per cui:

- tutti i « mandati di progetto » devono essere trasmessi sistematicamente e spontaneamente alla revisione interna,
- un inventario sempre aggiornato dei progetti in corso deve essere tenuto a disposizione.

*per esempio le direttive comunali, cantonali e federali definiscono che cosa si intende per « progetto informatico importante »

Collegamenti alle principali referenze citate

Hermes SE/DS (edizione 2003), Hermes SAVAS (edizione 2005), <http://www.hermes.admin.ch>
 Ordinanza concernente la tenuta e la conservazione dei libri di commercio (Olico, RS 221.431)
http://www.bk.admin.ch/ch/f/rs/221_431/index.html

COBIT Versione 4.0, <http://www.isaca.ch>

Manuale svizzero di audit (PS/NAS) e norme della Camera Fiduciaria Svizzera <http://www.treuhand-kammer.ch>

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

1. Studio di fattibilità



Quali sono gli obiettivi del sistema?
Quali sono le soluzioni possibili?

- Censire e analizzare le esigenze del sistema
- Elaborare delle proposte di soluzione (varianti)
- Paragonare i costi, i rischi e i vantaggi di queste varianti

Quali sono le esigenze nei confronti del progetto e dell'organizzazione?
Il progetto è realizzabile?
Il progetto può passare alla fase di progettazione (mandato di progetto)?

Responsabile
Servizio utente (con il sostegno del Servizio informatico per le questioni tecniche)

Referenze utili (lista non esauriente!)

Hermes : Cap. 3.3 (SE e SA)
POSAT ZH : Ablaufschritt 2
CobIT 4.0 : AI 1.3
PRINCE 2 : Processo SU

2. Capitolato d'oneri (Cahier des charges)



Quali sono gli obiettivi da raggiungere?
Quali sono le aspettative degli utilizzatori?

- Quali sono le funzionalità richieste?
- Quali sono i volumi da trattare?

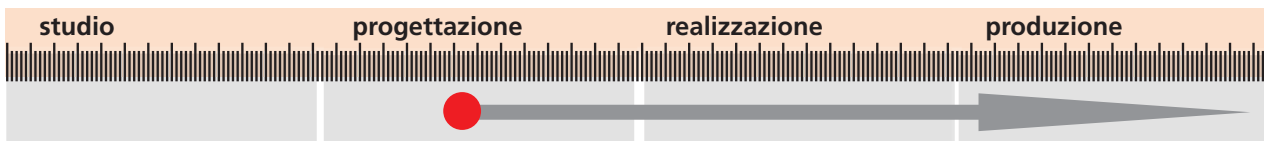
Quali sono i vincoli da rispettare?
Quali sono i mezzi tecnici necessari per il raggiungimento di questo obiettivi?

Responsabile:
Servizio utente (con il sostegno del Servizio informatico per le questioni tecniche)

Referenze utili (lista non esauriente!)

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

3. Analisi della redditività



Quali sono i costi completi del progetto (compreso le spese correlate, per esempio: costo della migrazione dei dati, aumento della capacità delle infrastrutture, formazione degli utenti...)?

Come apprezzare quantitativamente e qualitativamente l'utilità preventivata?

Qual'è la redditività del progetto?

Quali sono gli scenari atti a modificare la redditività del progetto?

Responsabile:
Servizio utente

Referenze utili (lista non esauriente!)

Hermes : SE Cap. 5.3.92, SA Cap. 5.3.98
POSAT ZH : Ablaufschritt 5
CobiT 4.0 : AI 1.1, AI 1.2, AI 1.3
PRINCE 2 : Processi DP e CS

4. Integrazione nell'ambiente informatico



Il progetto si integra armoniosamente nella strategia e nell'architettura informatica dell'azienda?

Il progetto non è (parzialmente) un doppiante di un altro progetto o di una applicazione esistente?

Esistono delle sinergie con altri progetti?

Il progetto rispetta gli standard adottati dall'azienda?

Quali interfacce automatiche o manuali sono previste?

Responsabile:
Servizio informatico

Referenze utili (lista non esauriente!)

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

5. Esigenze da rispettare



Quali sono le esigenze interne (prassi, procedure, norme di qualità)?

Quali sono le esigenze esterne (leggi, regolamenti, direttive, contratti) eventualmente applicabili in modo specifico a determinati settori (protezione dei dati, pubblicazione dei dati, procedure d'acquisto, banche, « best practices », ecc.)?

Quali sono le conseguenze di queste esigenze in termini di procedure o di equipaggiamento (architettura, sicurezza ecc.)?

Responsabile:

Servizio utente (con il sostegno del Servizio informatico per le questioni tecniche)

Referenze utili (lista non esauriente!)

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

POSAT ZH : Ablaufschritt 1

CobIT 4.0 : PO 2, ME 3

Esempi delle esigenze da rispettare (lista non esauriente)

Esigenze relative al Settore del personale

- fiscalità (certificato di salario, imposte alla fonte ecc.)
- assicurazioni sociali (AVS, AD, IPG ecc.)
- protezione dei dati (dichiarazione di confidenzialità, diritti di accesso, ecc.)

Esigenze relative al Settore finanziario

- Ordinanza concernente la tenuta e la conservazione dei libri di commercio (Olico)
- Legge contro il riciclaggio

Esigenze relative al Settore sanitario

- contabilità analitica negli ospedali
- tracciabilità dei prodotti e dei medicinali
- protezione dei dati

Ecc.

6. Concetto del sistema di controllo interno (SCI)



Quali controlli automatici sono necessari (validazione inserimento dati, riconciliazioni automatiche, liste d'errori ecc.) ?
Quali separazioni di funzioni sono necessarie e come si ripercuotono nella gestione dei diritti d'accesso ?
Quali sono i provvedimenti da prendere per assicurare la tracciabilità delle operazioni, compreso la parametrizzazione dell'applicazione?
Quali sono i provvedimenti da prendere per assicurare la continuità dell'esercizio (piano di soccorso) e la conservazione dei dati (piano di archiviazione)?

Responsabile:

Servizio utente (con il sostegno del Servizio informatico per le questioni tecniche)

Referenze utili (liste non esauriente!)

Hermes : SE Cap. 5.3.31, SA Cap. 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 : processo SU
Camera
fiduciaria : PS/NAS 400, MSA cifre 3.24233, 3.3222 e seg.

7. Architettura del sistema



Come è strutturato il sistema informatico?
Quale è l'architettura delle informazioni (modello dei dati)?
Quali sono le funzionalità del sistema?
Come si integra il sistema nell'architettura dei sistemi esistenti?
Come interagiscono le informazioni tra di loro?
Quali sono le interfacce?

Responsabile:

Servizio informatico

Références utiles (lista non esauriente!)

Hermes : SE Cap. 5.3.81, 5.3.82, SA Cap. 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. Collaudi (piano dei test e documentazione)



Quali sono gli obiettivi dei collaudi?
Quali sono i test previsti (metodi, programmi di utilità, criteri, casi)?
Quali sono le risorse e i termini per l'esecuzione dei test?
Le correzioni dell'ultimo momento saranno ancora collaudate?
Come saranno documentati lo svolgimento e i risultati esatti dei test?

Responsabile:
Servizio informatico (e Servizio utente)

Referenze utili (lista non esauriente!)

Hermes : SE Cap. 5.3.85 fino a 5.3.90, SA Cap. 5.3.91 fino a 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. Accettazione da parte degli utenti



Qual'è la portata dell'accettazione?
Chi sono i proprietari dei dati e i responsabili dell'applicazione?
Chi è responsabile dell'accettazione?
Su quali test si basa l'accettazione?
Quali sono le eventuali riserve all'accettazione?

Responsabile :
Servizio utente

Referenze utili (lista non esauriente!)

Hermes : SE Cap. 3.3.6, 3.4.7, 3.5.8, 3.6.7, SA Cap. 3.3.7, 3.4.9, 3.5.11, 3.6.7
POSAT ZH : Ablaufschritt 14, 15
CobiT 4.0 : AI 3.1 fino a 3.3, AI 7.6, AI 7.7, PO 10.6

10. Bilancio finale



- Gli obiettivi e le esigenze poste al progetto sono stati raggiunti?
- Quali sono i costi definitivi e le spiegazioni circa gli eventuali scostamenti dai preventivi?
- Qual'è il calcolo definitivo della redditività del progetto?
- Quali sono i rischi esistenti dopo l'implementazione?
- Quali sono gli errori intervenuti dopo il passaggio in produzione?
- Quali sono le raccomandazioni e i provvedimenti proposti?
- Quali sono gli insegnamenti che si possono trarre dal progetto?

Responsabile:
Servizio utente

Referenze utili (lista non esauriente!)

- Hermes : Cap. 5.3.13 (SE e SA)
- POSAT ZH : Ablaufschritt 16
- CobIT 4.0 : PO 10.6, PO 10.13, PO 10.14, AI 7.12

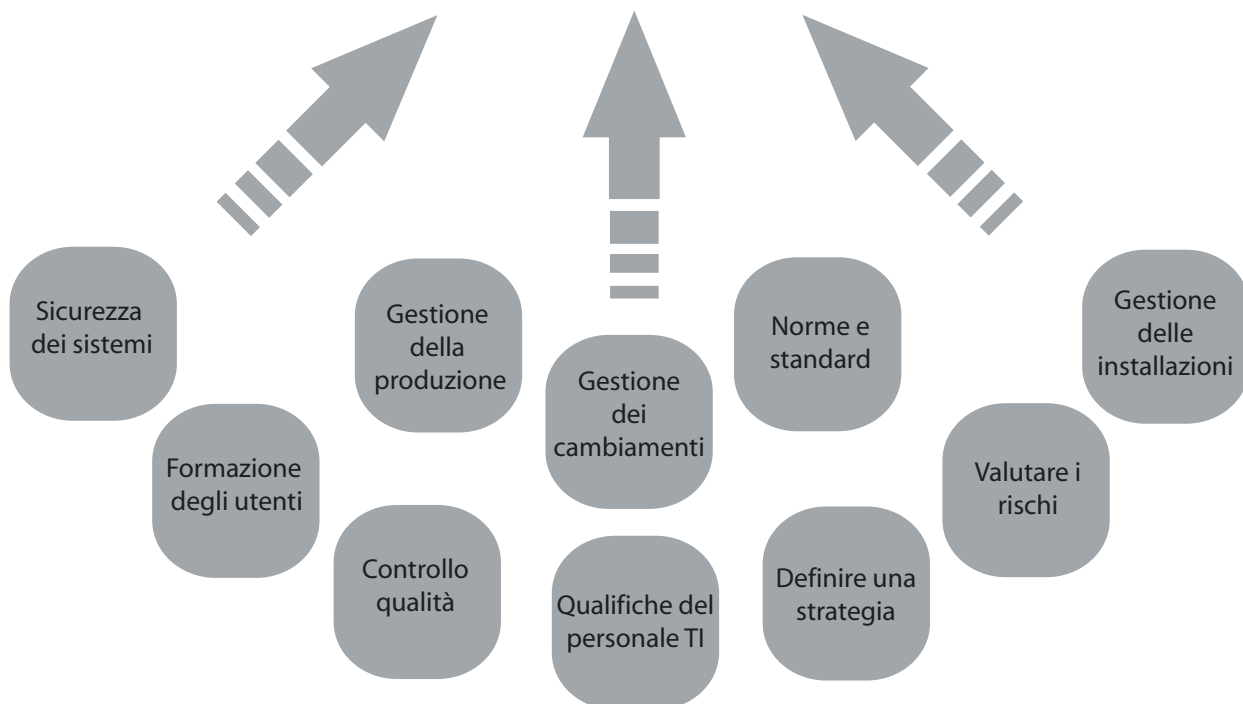
Non sottovalutare il contesto del progetto ...

Un progetto non si sviluppa in una campana di vetro. Il suo successo è direttamente influenzato dal contesto nel quale è condotto. I fattori importanti per una buona riuscita di un progetto sono: il forte impegno degli utenti nel progetto, le qualifiche delle persone intervenute nel progetto, il grado di standardizzazione dell'azienda, i sistemi di controllo qualità e le procedure a garanzia di una gestione corretta delle differenti versioni del sistema.

Cobit identifica, per 34 processi informatici standard, gli obiettivi di controllo da rispettare per padroneggiare l'informatica.

Il processo Cobit (Distribution & Support 8) « Gestire il Service desk e gli incidenti » tratta per esempio le regole applicabili al sistema di gestione dei problemi, la loro segnalazione al livello superiore, il controllo dell'iter di risoluzione e alle tracce di audit, le autorizzazioni d'accesso provvisorie o d'emergenza, come pure le priorità degli interventi urgenti.

Tenere conto dei vari fattori ...



...e dei principi della buona gestione di progetto

Alcuni insegnamenti tratti dagli audit congiunti dei Controlli delle finanze:

- La realizzazione di un progetto di grande dimensione è possibile unicamente con del personale che lavora a tempo pieno per tale progetto
- Un progetto importante deve beneficiare di un sostegno « politico » corrispondente
- È essenziale riorganizzare e armonizzare prima di informatizzare
- Accorciare la durata del progetto oppure suddividerlo in più sottoprogetti autonomi
- Evitare le tecnologie emergenti
- L'equilibrio tra informatici e specialisti del « mestiere » deve essere adeguato
- Non troppi organi di controlling, ma un vero controlling
- Identificare e valutare il più presto possibile i problemi, in particolare mediante degli studi e dei test di fattibilità che coinvolgono gli utenti
- Identificare correttamente i fornitori e regolare contrattualmente le loro relazioni con il progetto
- Ripercuotere nei contratti gli eventuali adattamenti nell'organizzazione di progetto
- Non sottovalutare i problemi posti dallo sviluppo in due o tre lingue

E come conclusione

La decisione d'intervenire in un progetto informatico appartiene in ultima analisi al Controllo delle finanze. Numerose considerazioni guideranno la scelta, per esempio l'apprezzamento dei rischi che presenta il progetto in paragone ad altri progetti.

Il nostro intervento può prendere la forma di un esame del progetto (in particolare al termine di una fase del progetto) o di una presa di posizione su delle questioni particolari (per esempio la valutazione del concetto di SCI prima della messa in esercizio del nuovo sistema informativo).

Non esitate a sottoporci i vostri eventuali problemi !