

Università di Venezia

Corso di Laurea in Informatica

“Laboratorio di Informatica Applicata – Introduzione all’IT Governance”

Lezione 4



Marco Fusaro – KPMG S.p.A.

CobiT

Obiettivi del CobiT (Control Objectives for Information and related Technologies)

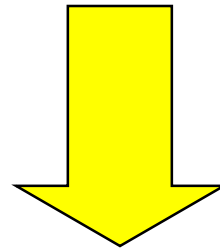
- strumento per la comprensione di una organizzazione IT
- linee guida per il management (“best practice”)
- ...

Ricordiamo che è uno strumento in evoluzione.

Assunzioni del modello

Il modello del CobiT. Assunzioni:

- l'azienda necessita delle informazioni per i propri processi di business
- le informazioni sono gestite da risorse informatiche
- le risorse informatiche sono gestite tramite processi



Il CobiT ragiona per “processi”

Processi

CobiT ragiona per processi:

➤ dice “cosa si deve fare”

Può anche non essere personale del reparto IT

➤ non dice “chi lo deve fare” (... in realtà qualche responsabile viene citato ...)



CobiT

Concetti utilizzati nel modello del CobiT:

➤ Risorse

Dati	Oggetti informativi (anche non strutturati)
Applicazioni	Sistemi comprensivi di procedure manuali e automatiche
Tecnologia	Hardware, sistemi operativi, DBMS, dispositivi per il networking, ...
Infrastrutture	Risorse destinate ad ospitare e garantire il funzionamento dei sistemi informatici (gli edifici, ...)
Risorse Umane	Risorse umane coinvolte a qualunque livello nei processi IT

CobiT

Concetti utilizzati nel modello del CobiT:

➤ Criteri delle informazione

Ad ogni processo devono essere associati controlli specifici finalizzati a garantire che l'informazione mantenga, nel corso del trattamento, specifici attributi.

Rispetto alle caratteristiche CIA relative alla sicurezza il CobiT considera anche caratteristiche dell'informazione relative alla qualità del dato.

Esiste un grado di sovrapposizione tra gli attributi dell'informazione definiti nel CobiT.

CobiT

Efficacia	Rilevanza e pertinenza delle informazioni, disponibilità tempestiva e senza errori, fruibilità
Efficienza	Uso ottimale delle risorse
Riservatezza	Protezione da accessi non autorizzati
Integrità	Accuratezza e completezza
Disponibilità	Disponibilità quando necessario
Conformità	Elaborazione effettuata rispettando leggi, regolamenti e accordi contrattuali
Affidabilità	Affidabilità per alimentare processi decisionali aziendali e per far fronte a responsabilità finanziarie e ad obblighi di bilancio e statutari dell'azienda

Processi

Struttura del modello CobiT:

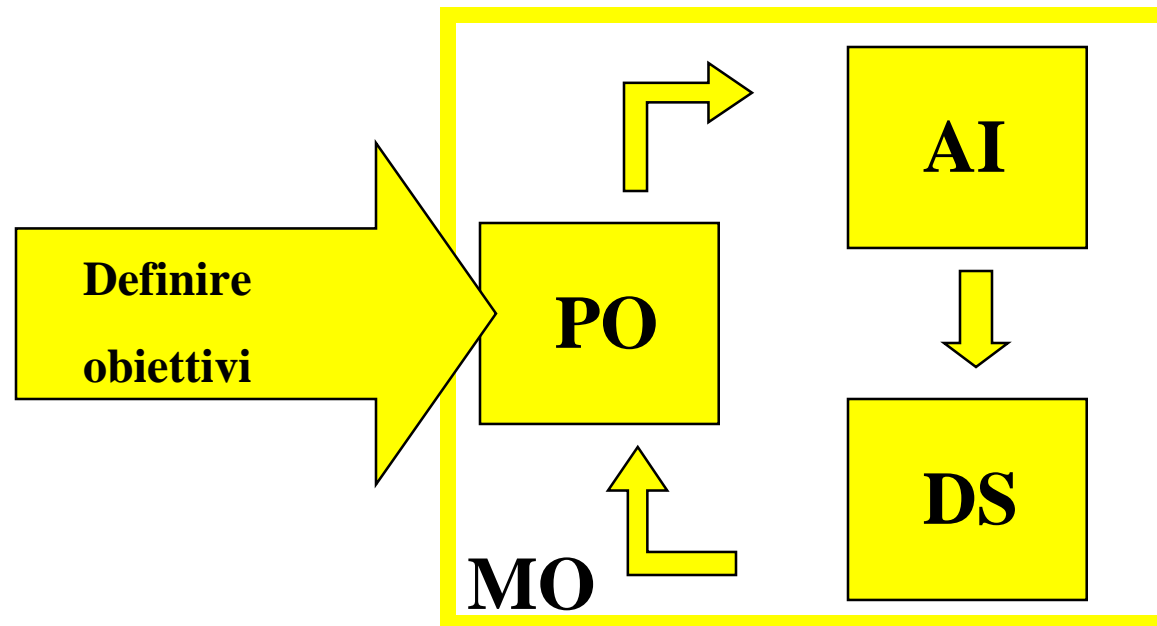
- Domini (4)
- Processi (34)
- Obiettivi di controllo (318)

- Risorse
- Criteri dell'informazione

Domini

I processi sono organizzati in Domini:

- Planning & Organization PO
- Acquisition & Implementation AI
- Delivery & Support DS
- Monitoring MO

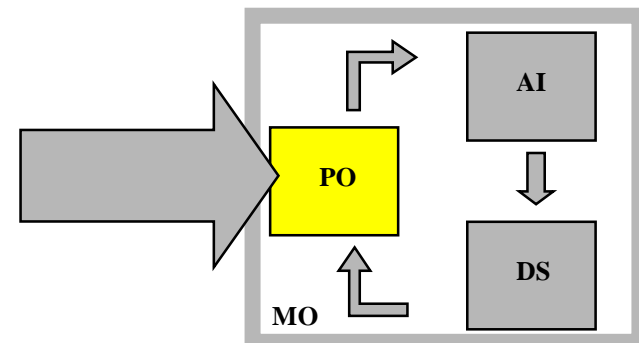


Processi

Processi del dominio PO (Planning & Organization)

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Definizione degli indirizzi strategici dell'IT
- Definizione dell'assetto organizzativo dell'IT
- Comunicazione della strategia alla struttura IT
- ...



Processi

Processi del dominio PO (Planning & Organization):

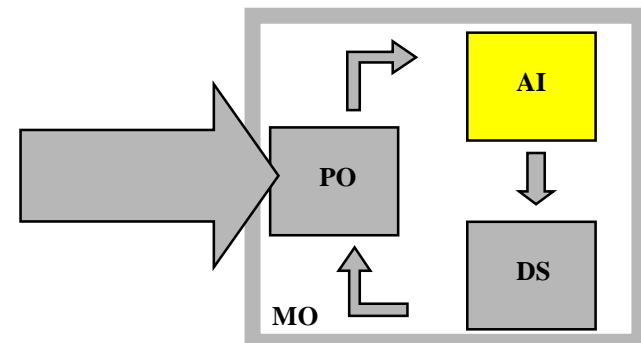
- **PO1 - Definizione del piano strategico per l'IT**
- **PO2 - Definizione dell'architettura informativa**
- **PO3 - Definizione dell'indirizzo tecnologico**
- **PO4 - Definizione dell'organizzazione IT e delle sue relazioni**
- **PO5 - Gestione degli investimenti IT**
- **PO6 - Comunicazione degli indirizzi e degli obiettivi del management**
- **PO7 - Gestione delle risorse umane**
- **PO8 - Conformità a leggi e norme**
- **PO9 - Valutazione dei rischi**
- **PO10 - Gestione dei progetti**
- **PO11 - Gestione della qualità**

Processi

Processi del dominio AI (Acquisition & Implementation)

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Identificazione delle soluzioni IT da sviluppare o acquistare per il soddisfacimento delle necessità aziendali
- Gestione del cambiamento dei sistemi



Processi

Processi del dominio AI (Acquisition & Implementation):

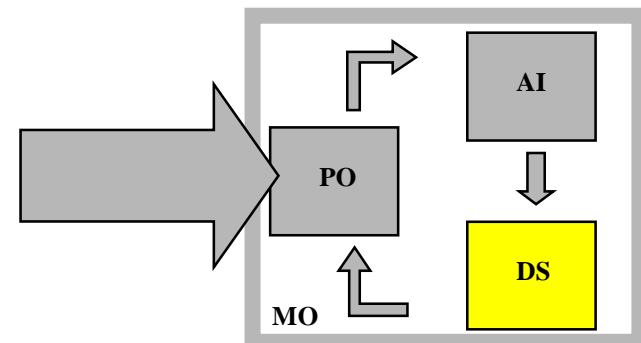
- **AI1 - Identificazione delle soluzioni**
- **AI2 - Acquisizione e manutenzione del software applicativo**
- **AI3 - Acquisizione e manutenzione dell'architettura tecnologica**
- **AI4 - Sviluppo e manutenzione delle procedure IT**
- **AI5 - Installazione e validazione dei sistemi**
- **AI6 - Gestione del cambiamento**

Processi

Processi del dominio DS (Delivery & Support):

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Gestione degli aspetti operativi dell'erogazione dei servizi
- Gestione degli aspetti relativi alla sicurezza dei sistemi



Processi

Processi del dominio DS (Delivery & Support):

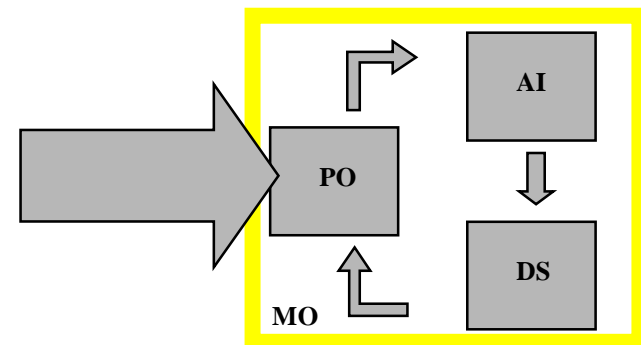
- **DS1 - Definizione dei livelli di servizio**
- **DS2 - Gestione dei servizi di terze parti**
- **DS3 - Gestione delle prestazioni e del dimensionamento**
- **DS4 - Gestione della continuità del servizio**
- **DS5 - Gestione della sicurezza dei sistemi**
- **DS6 - Identificazione e attribuzione dei costi**
- **DS7 - Formazione ed addestramento degli utenti**
- **DS8 - Assistenza e consulenza agli utenti**
- **DS9 - Gestione della configurazione**
- **DS10 - Gestione di anomalie ed incidenti**
- **DS11 - Gestione dei dati**
- **DS12 - Gestione delle infrastrutture**
- **DS13 - Attività operative e di sala macchine**

Processi

Processi del dominio MO (Monitoring)

Sono processi i cui obiettivi sono sintetizzabili nei seguenti punti:

- Valutazione periodica dei processi IT finalizzata alla verifica di conformità con gli obiettivi di controllo che l'azienda si è data



Processi

Processi del dominio MO (Monitoring):

- **M1 - Monitoraggio dei processi**
- **M2 - Valutazione dell'adeguatezza dei controlli interni**
- **M3 - Certificazione da terze parti**
- **M4 - Revisione indipendente dei controlli interni**

Processi

Ad ogni processo il modello associa:

- i requisiti aziendali cui il processo deve soddisfare
- istruzioni di alto livello per il controllo
- pratiche di controllo

Inoltre, sono associate:

- le risorse aziendali gestite dal processo (e non quelle che prendono semplicemente parte al processo stesso)
- i criteri per le informazioni cui gli obiettivi di controllo devono fare specifico riferimento

Processi

ESEMPIO: DS4 – Assicurare la continuità del servizio

Il controllo sul processo IT di

Assicurare la continuità del servizio

Requisito aziendale

Che soddisfi il requisito aziendale

Di far sì che i servizi IT siano disponibili come richiesto e assicurino un minimo impatto aziendale in caso di grave evento distruttivo

È reso possibile

Dal possesso di un piano di continuità operativo e testato dall'IT che sia in linea con il piano globale di continuità aziendale e con i suoi requisiti aziendali correlati

Istruzioni di alto livello

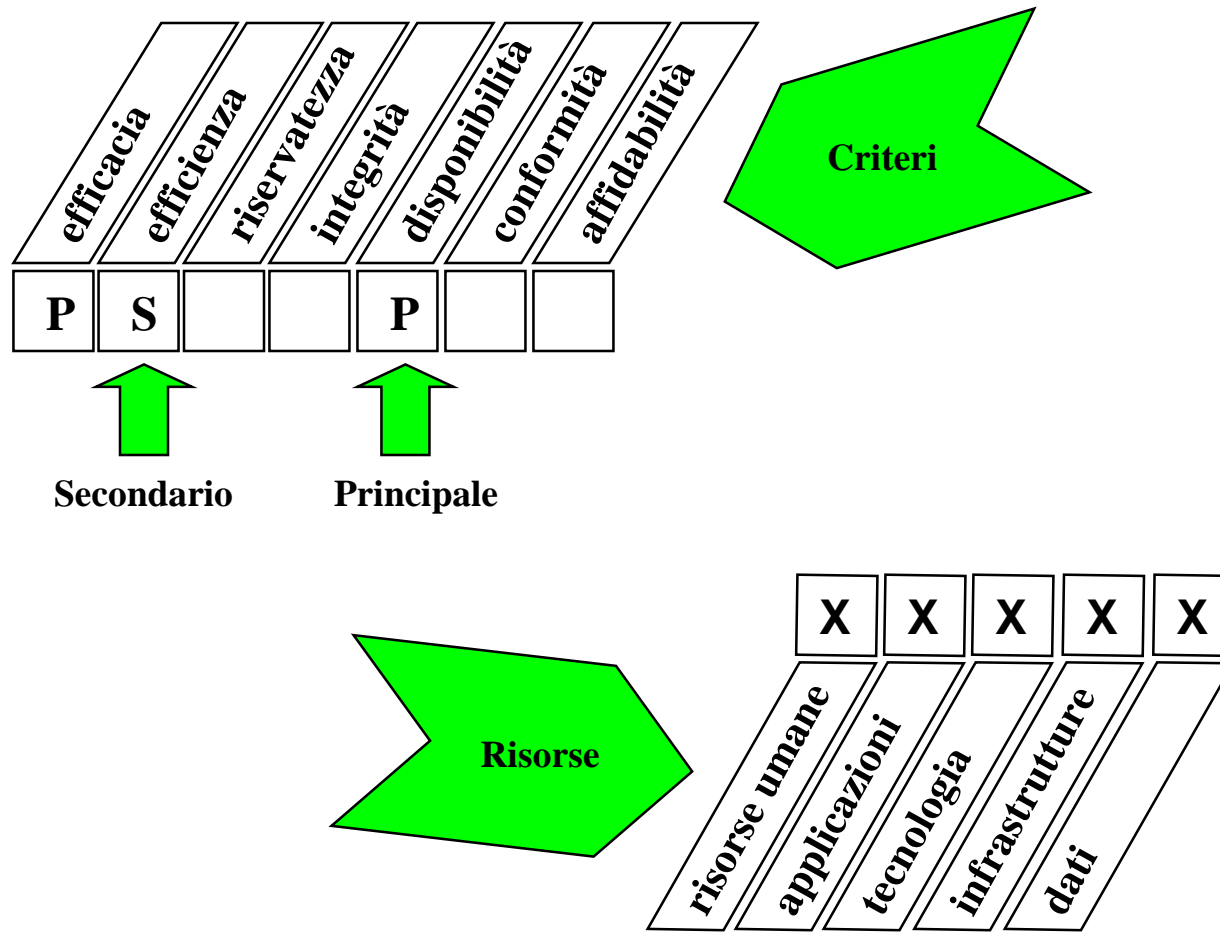
E considera

- classificazione delle criticità
- procedure alternative
- salvataggio e ripristino
- attività di test e addestramento sistematiche e regolari
- processi di monitoraggio ed escalation
- responsabilità organizzative interne ed esterne
- ...

Pratiche di controllo

Processi

ESEMPIO: DS4 – Assicurare la continuità del servizio



Documentazione CobiT

- Executive Summary
 - ✓ descrizione dei principi del modello
- Framework
 - ✓ domini e processi
 - ✓ requisiti di dettaglio, istruzioni di alto livello e pratiche di controllo
- Control Objectives
 - ✓ obiettivi di controllo per i processi
- Management Guidelines
 - ✓ CSF, KGI, KPI e maturity model
- Audit Guidelines
 - ✓ linee guida per l'attività di audit
- Implementation Tool Set
 - ✓ tool di supporto all'applicazione del CobiT in azienda

Ne stiamo parlando

Ne stiamo parlando

Adesso !

Prossima volta

Non lo tratteremo

Non lo tratteremo

Control Objectives

Nel documento “Control Objectives” per ogni processo sono dettagliati obiettivi di controllo minimi per il processo stesso.

Per ogni processo sono definiti da 3 a 30 obiettivi di controllo.

Ogni obiettivo di controllo rappresenta requisiti che dovrebbero essere soddisfatti dai controlli in atto.

Non sono mai fatti riferimenti a piattaforme tecnologiche.

Quindi, il CobiT:

- non dice quali siano i controlli da prevedere in un processo
- dice gli obiettivi cui i controlli devono soddisfare

Control Objectives

**Delivery &
Support**

Esempio:

Processo 2

DS2 – Gestire i servizi di terze parti

Obiettivo di controllo 4 – Requisiti delle terze parti

La Direzione dovrebbe assicurare che, prima della selezione, le potenziali terze parti siano qualificate in modo appropriato attraverso una valutazione delle loro capacità di erogare i servizi richiesti.

Nel processo di gestione dei fornitori devono essere previste attività che abbiano come obiettivo quello di arrivare ad una appropriata valutazione della capacità di erogazione dei servizi

Control Objectives

Esempio:

DS2 – Gestire i servizi di terze parti

Obiettivo di controllo 4 – Requisiti delle terze parti

La Direzione dovrebbe assicurare che, prima della selezione, le potenziali terze parti siano qualificate in modo appropriato attraverso una valutazione delle loro capacità di erogare i servizi richiesti.

Non è specificata la forma assunta
dal controllo

Control Objectives

Osservazioni:

- Nei “Control Objectives” i rischi non sono definiti in modo esplicito
 - ✓ è possibile desumerli !

DS2 – Gestire i servizi di terze parti

Obiettivo di controllo 4 – Requisiti delle terze parti

La Direzione dovrebbe assicurare che, prima della selezione, le potenziali terze parti siano qualificate in modo appropriato attraverso una valutazione delle loro capacità di erogare i servizi richiesti.

La selezione di un fornitore non affidabile comporta il rischio che il servizio sia erogato con qualità scadente o non sia erogato, con possibili perdite economiche dirette o indirette per l'azienda

Control Objectives

Proviamo ad usare il CobiT!

- Approfondiamo un processo
- Vediamo come effettuare una valutazione in relazione ad un obiettivo di controllo

Control Objectives

DS10 – Gestire i problemi e gli incidenti:

Il controllo sul processo IT di

Gestire i problemi e gli incidenti

*Incidenti per la sicurezza,
malfunzionamenti del
software, cadute di
sistemi, ...*

Che soddisfi il requisito aziendale

Di assicurare che i problemi e gli incidenti siano risolti e le loro cause esaminate per prevenire qualsiasi ripetizione

È reso possibile

Da un sistema di gestione del problema che registra e segue tutti gli incidenti

E considera

- tracce di audit (audit trail) dei problemi e delle soluzioni
- tempestiva risoluzione dei problemi documentati
- procedure di escalation dei problemi (trasferimento ad un livello di responsabilità superiore per la soluzione)
- report relativi agli incidenti
- disponibilità di informazioni relative alla configurazione
- responsabilità dei fornitori
- coordinamento con il change management

Control Objectives

DS10 – Gestire i problemi e gli incidenti

<i>efficacia</i>	<i>efficienza</i>	<i>riservatezza</i>	<i>integrità</i>	<i>disponibilità</i>	<i>conformità</i>	<i>affidabilità</i>
P	P			S		

X	X	X	X	X
<i>risorse umane</i>	<i>applicazioni</i>	<i>tecnologia</i>	<i>infrastrutture</i>	<i>dati</i>

Control Objectives

DS10 - Obiettivo di controllo 1 – Sistema per la gestione dei problemi

La direzione IT dovrebbe definire e realizzare un sistema di gestione dei problemi per assicurare che tutti gli eventi operativi che esulano dalla normale attività (incidenti, problemi ed errori) siano registrati, analizzati e tempestivamente risolti.

Le procedure di modifica dei programmi di emergenza dovrebbero essere prontamente collaudate, approvate, documentate e associate a report.

In occasione di problemi significativi dovrebbe essere prevista la redazione di report sugli incidenti.

Quindi:

- deve essere stato sviluppato un sistema per la registrazione dei problemi
- deve essere sviluppata una procedura per l'intervento in emergenza sui programmi
- in caso di problemi significativi devono essere previsti report specifici

Rischi sottesi dagli obiettivi di controllo:

- I problemi non sono risolti in modo tempestivo
- Il management non ha consapevolezza della frequenza dei problemi

Control Objectives

Come conduco un audit rispetto ad un obiettivo di controllo?

- Individuazione dei controlli relativi a questo obiettivo di controllo
 - ✓ effettuazione di interviste
 - ✓ esame di documentazione aziendale relativa a policy e procedure
- Valutazione dell'efficacia e dell'efficienza del singolo controllo
 - ✓ analisi del controllo per valutarne l'efficacia a livello logico
- Raccolta di evidenze che dimostrino che il controllo è applicato
 - ✓ interviste incrociate
 - ✓ raccolta di documentazione relativa al controllo
 - ✓ individuazione di eccezioni rispetto alle procedure formalmente approvate

Control Objectives

Come conduco un audit rispetto a questo obiettivo di controllo?

➤ Individuazione dei controlli relativi a questo obiettivo di controllo → acquisizione di informazioni sulle procedure in atto per la registrazione dei problemi

- ✓ intervista a responsabili IT per comprendere la procedura
- ✓ esame del sistema con cui sono tracciati gli incidenti (c'è il supporto di un sistema automatico? L'attività è svolta manualmente? ...)
- ✓ raccolta di statistiche relative a tipologie di problemi, frequenza di problemi e tempi di risoluzione
- ✓ raccolta di esempi di report sugli incidenti
- ✓ ...

Control Objectives

➤ Analisi del controllo

- ✓ le procedure e gli strumenti in atto permettono di individuare e risolvere in modo tempestivo i problemi?
- ✓ è svolta una attività di analisi dei problemi al fine di individuare e risolvere problemi ricorrenti? (→ inutile registrare gli eventi se poi tali informazioni non sono utilizzate)
- ✓ ...

➤ Raccolta di evidenze che dimostrino che il controllo è applicato

- ✓ selezione di alcuni problemi registrati
- ✓ verifica che le registrazioni permettano di risalire alle cause
- ✓ verifica delle attività seguite alla rilevazione di specifici problemi

Control Objectives

Completata l'analisi posso dire:

- se sono attivi controlli relativi all'obiettivo di controllo
- se tali controlli sono efficaci
- se tali controlli sono efficienti

Posso quindi:

- emettere un giudizio
- fornire dei suggerimenti per il miglioramento dei controlli

Control Objectives

DS10 - Obiettivo di controllo 2 – Riportare a livello superiore il problema

La direzione IT dovrebbe definire e realizzare procedure per una risposta modulata ai problemi in modo da assicurare che i problemi individuati siano risolti nel modo più efficiente e tempestivo.

Queste procedure dovrebbero garantire che le priorità di intervento siano fissate in modo appropriato.

Le procedure dovrebbero anche documentare il processo di escalation che porta all'attivazione del piano di continuità dell'IT.

Quindi:

- in caso di difficoltà di soluzione di un problema deve essere previsto il trasferimento della responsabilità della soluzione ad un livello di competenze/responsabilità superiore
- le procedure devono permettere di stabilire una scala di priorità tra i problemi
- in caso di problemi particolarmente gravi le procedure devono prevedere la possibilità di invocazione di piani di business continuity

Rischi sottesi dagli obiettivi di controllo:

- Un problema non risolto in tempi ragionevoli potrebbe rimanere “incagliato”
- Una scorretta definizione delle priorità potrebbe portare a ritardi nella soluzione di problemi più importanti
- In caso di problemi di gravità molto elevata, procedure non ottimali potrebbero rallentare il trasferimento delle responsabilità ad alti livelli gerarchici

Control Objectives

DS10 - Obiettivo di controllo 3 – Tracciamento dei problemi e audit trail

Il sistema di gestione dei problemi dovrebbe fornire strumenti per ottenere adeguate tracce di audit che permettano di seguire il flusso dall'incidente alla cause (ad esempio: nuova versione applicativa o realizzazione di variazioni urgenti) e viceversa.

Esso dovrebbe interagire strettamente con la gestione delle modifiche, la gestione delle disponibilità e la gestione della configurazione.

Quindi:

- I log prodotti dai sistemi o le registrazioni manuali dei problemi devono permettere un tracciamento che parte dall'evento e arriva alle cause
- La definizione di ciò che deve essere registrato deve essere fatta collaborando con chi sviluppa il software e con chi gestisce i problemi a livello operativo

Rischi sottesi dagli obiettivi di controllo:

- Il tracciamento potrebbe essere insufficiente per analizzare i problemi

Control Objectives

DS10 - Obiettivo di controllo 4 – Autorizzazioni di accesso di emergenza e temporanee

Le autorizzazioni per gli accessi in emergenza e temporanee dovrebbero essere documentate su moduli standard e mantenute in un archivio, approvate da appositi responsabili, comunicate in modo sicuro alla funzione sicurezza e terminate automaticamente dopo un periodo predefinito.

Quindi:

- E' necessario tenere traccia di chi accede ai sistemi in situazioni di emergenza, con profili che solitamente hanno elevati diritti
- Gli accessi in emergenza devono essere approvati da responsabili
- I profili di emergenza devono avere un tempo di vita limitato

Rischi sottesi dagli obiettivi di controllo:

- Si potrebbe operare in condizioni di emergenza anche se la situazione non lo giustifica (mettendo a repentaglio la sicurezza del sistema)
- I profili ad alta autorità potrebbero rimanere attivi ed essere utilizzati anche quando non sono necessari

Control Objectives

DS10 - Obiettivo di controllo 5 – Priorità delle elaborazioni di emergenza

Le priorità delle elaborazioni di emergenza dovrebbero essere stabilite, documentate e approvate dall'appropriata direzione della programmazione e dell'area IT.

Quindi:

➤ Attività di emergenza sui sistemi (che possono consistere in lanci di procedure particolari, spegnimenti a scopo diagnostico o per riparazione, eccetera) devono essere approvate da responsabili di funzione

Rischi sottesi dagli obiettivi di controllo:

➤ Personale non avente un adeguato livello di responsabilità / esperienza / competenze potrebbe trovarsi nella condizione di ritenere di dover prendere decisioni di particolare importanza

Materiale per consultazione

- I manuali del CobiT

<http://www.isaca.org>