Introduzione all'audit dei progetti informatici

Seminario ATED – Manno, 12 gennaio 2007

Eugenio G. Corti
Controllo cantonale delle finanze del Cantone Ticino
Capo settore della revisione informatica

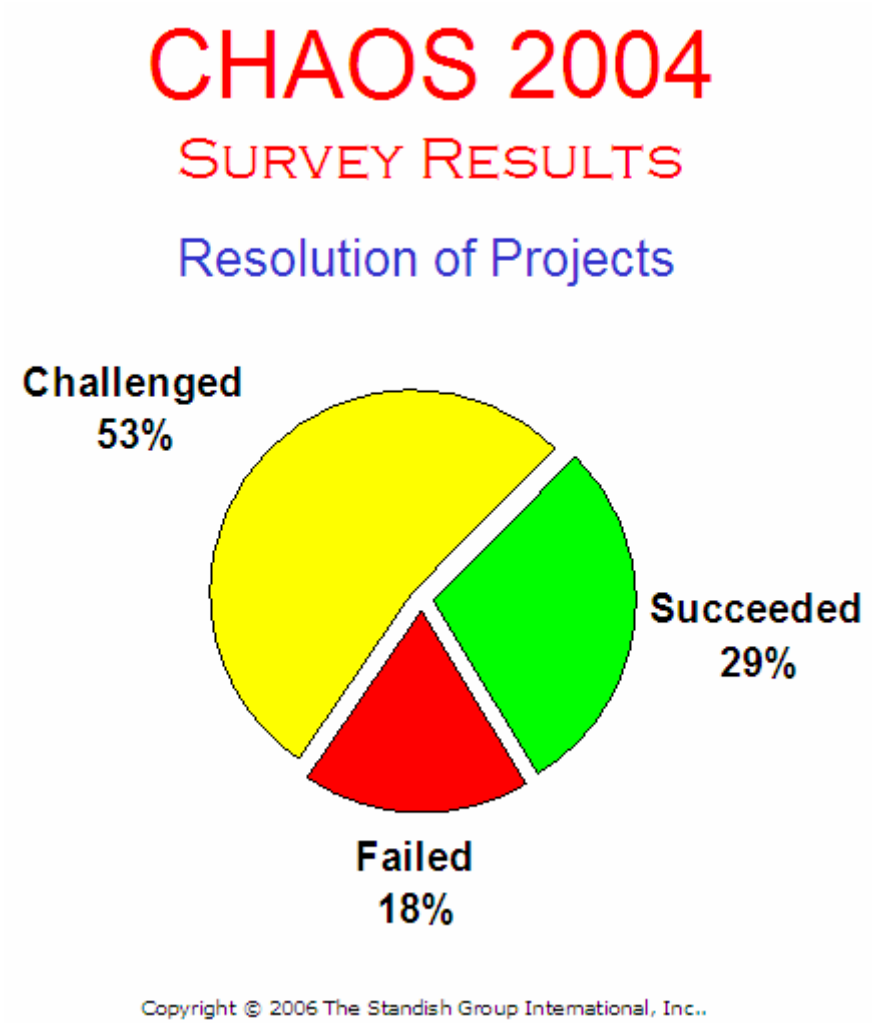
eugenio.corti@ti.ch

Repubblica e Cantone Ticino
Controllo cantonale delle finanze
Piazza Governo
6501 Bellinzona
Svizzera

Agenda

- Problematiche relative ai sistemi informativi:
  - in fase di sviluppo (i progetti)
  - in fase di esercizio (le applicazioni in produzione)
- I possibili rischi
- Scopo e obiettivi dell'audit di progetto
- Ruolo dei diversi protagonisti
- Norme, metodi e strumenti
- Conclusioni

Un po' di dati sui progetti a livello mondiale …



Spiegazione delle categorie

Progetti completati con successo (Succeeded)

Progetti che sono stati completati entro la scadenza e il budget previsti e con tutte le funzioni inizialmente specificate.

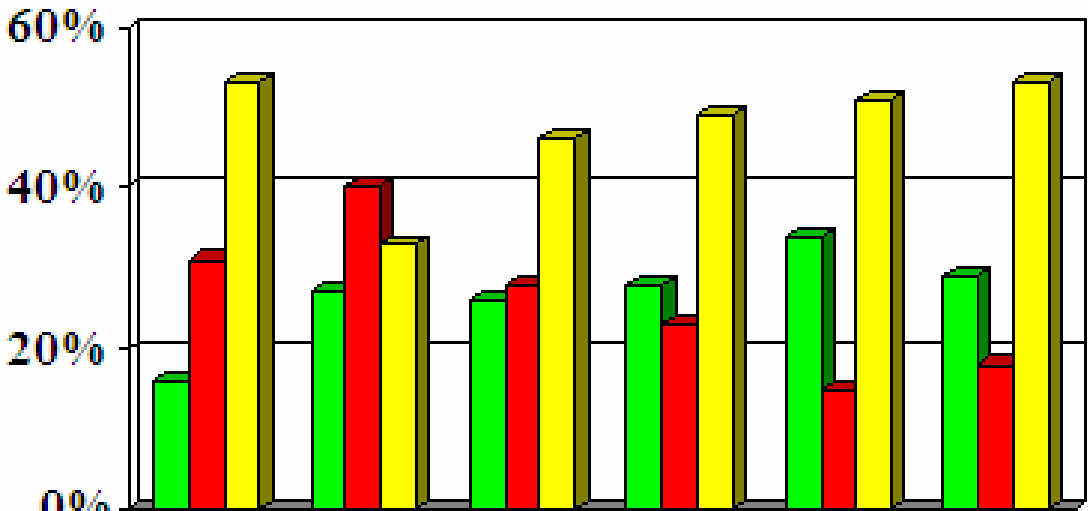
Progetti che hanno avuto difficoltà nel raggiungere gli obiettivi (Challenged)

Progetti completati e operativi, ma che sono stati consegnati in ritardo, hanno superato il preventivo e offrono meno funzioni di quelle specificate inizialmente.

Progetti abbandonati (Failed)

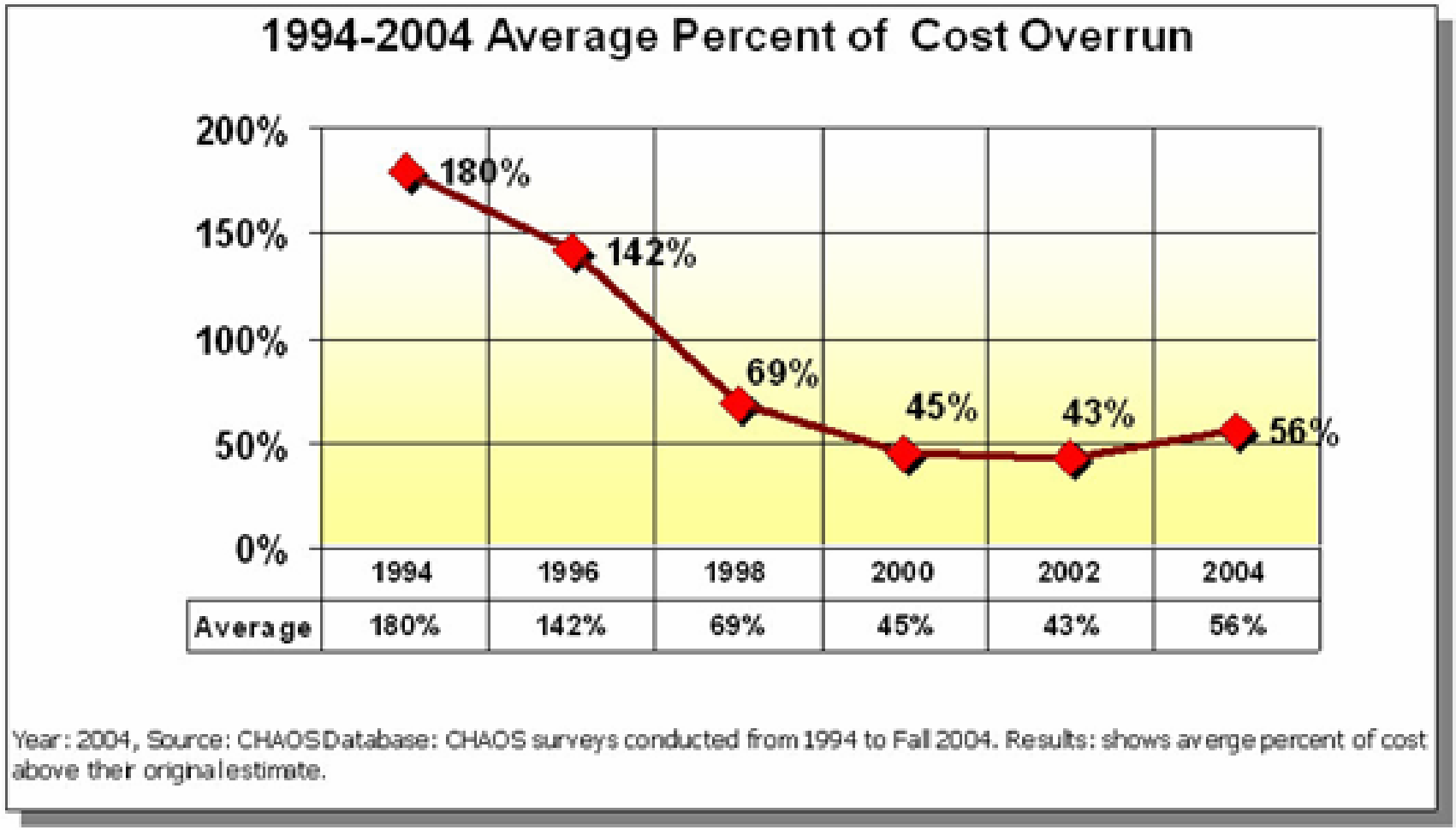
Progetti compromessi, che sono stati bloccati in un determinato momento del loro sviluppo oppure progetti che sono stati terminati, ma non sono utilizzati.

Il confronto su più anni

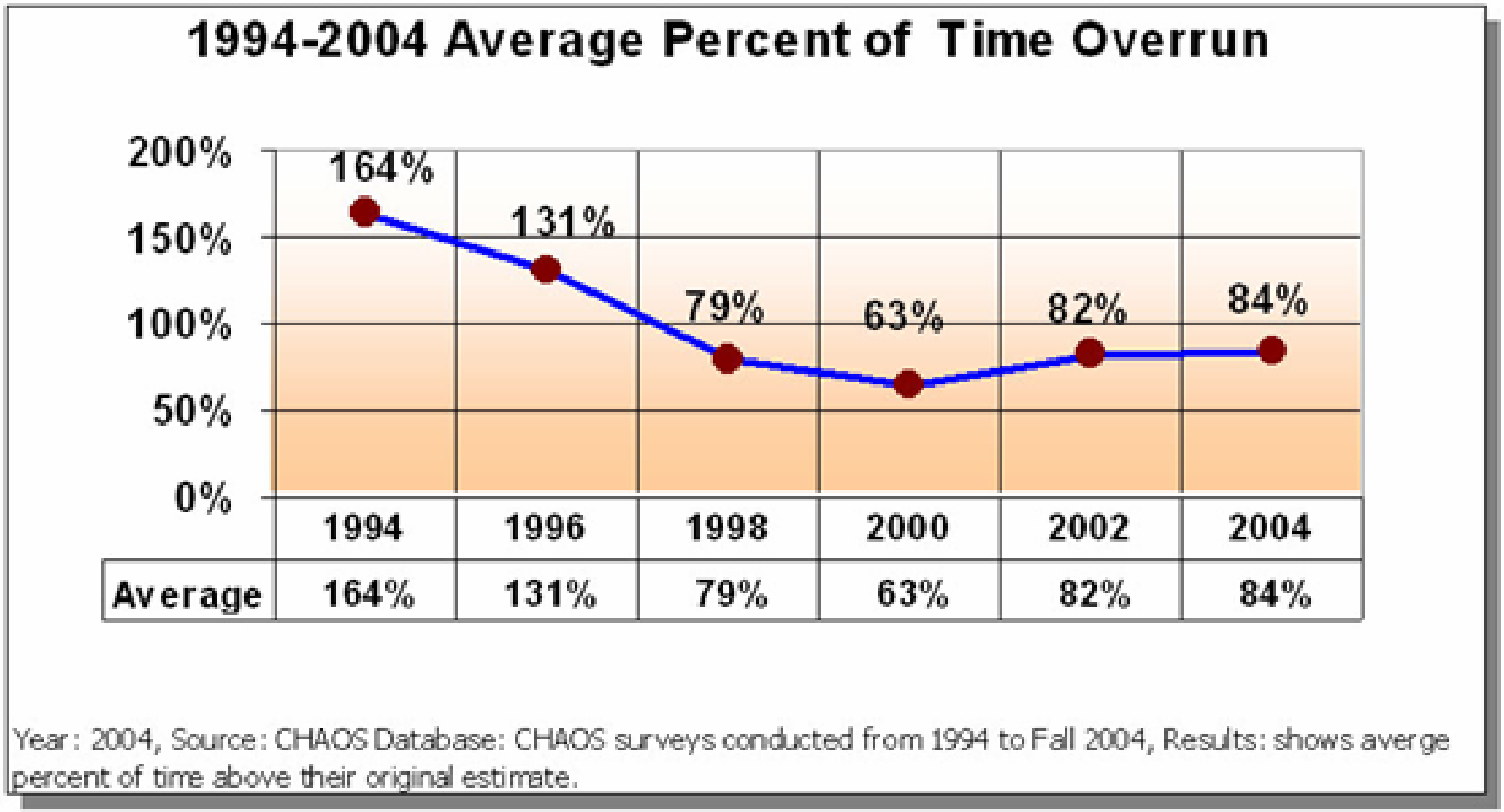


	1994	1996	1998	2000	2002	2004
Succeeded	16%	27%	26%	28%	34%	29%
Failed	31%	40%	28%	23%	15%	18%
Challenged	53%	33%	46%	49%	51%	53%

Il sorpasso del preventivo …

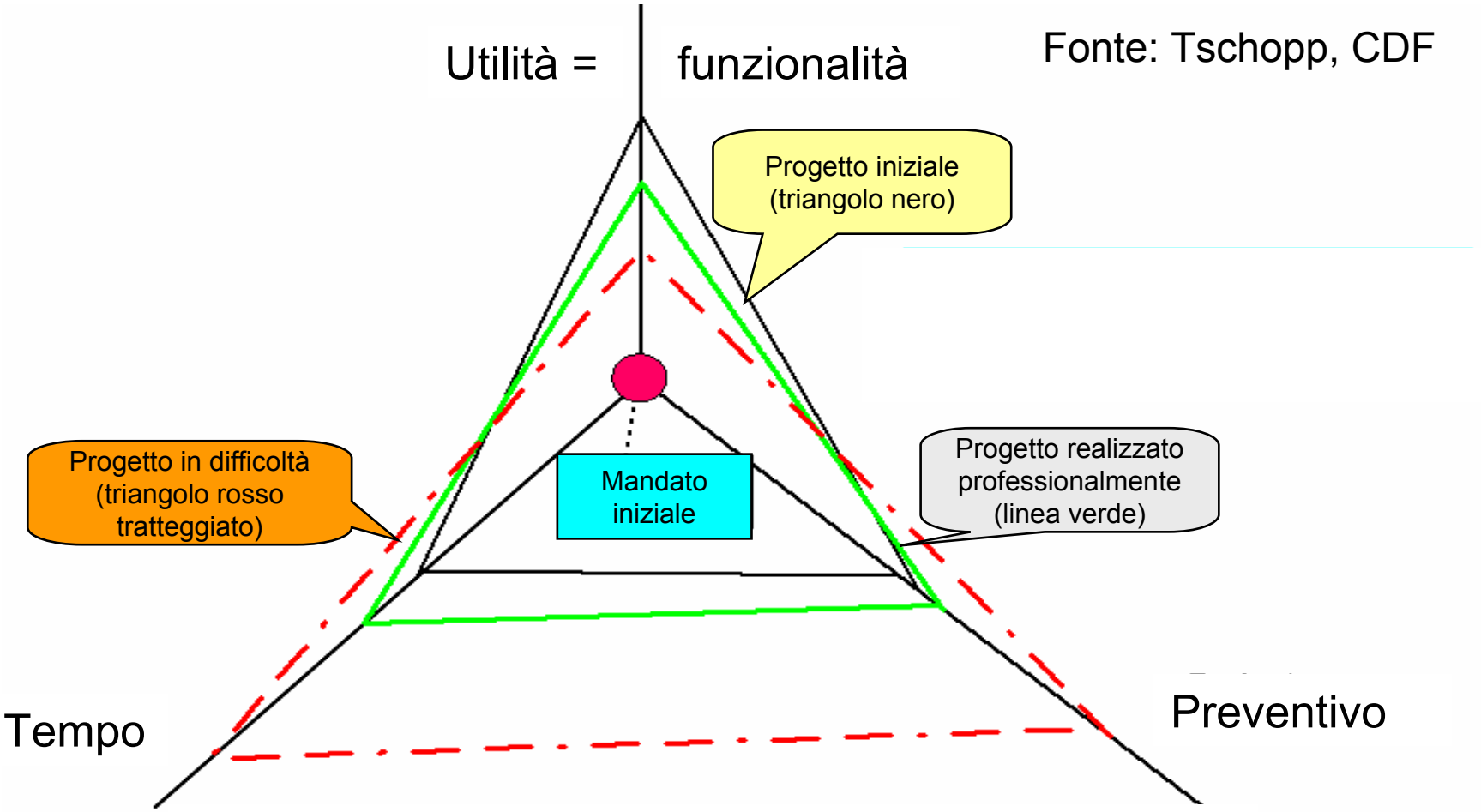


Il ritardo rispetto alla scadenza prevista …



Riassunto delle problematiche dei progetti

Se terminano …



Un altro possibile problema …

Bruxelles

Dubbi sulla contabilità dell'UE

… l'ex capo contabile dell'UE Martha Andreasen …..ha criticato pubblicamente l'efficacia e la sicurezza del sistema informatico contabile dell'UE che gestisce 98 miliardi di euro ogni anno.

(Notizia riportata dal Corriere del Ticino del 26 settembre 2002)

Un altro possibile problema …

Londra

Pensioni col « buco »
A causa di un errore informatico, fino a 10 milioni di lavoratori britannici si sono trovati a far fronte a un « buco » nelle loro pensioni statali minime.

Notizia del 15.5.2003 pubblicata dal Daily Telegraph ....
(Notizia riportata da LaRegione del 16 maggio 2003)

Un altro possibile problema …

Locarno

Impiegata della Pretura sotto inchiesta

Un'impiegata della Pretura di Locarno-Campagna è accusata di aver trattenuto dei soldi in modo fraudolento. La dipendente si è autodenunciata, ammettendo di avere manomesso i sistemi informatici.

(Notizia riportata dal Giornale del Popolo del 4 settembre 2003)

Un altro possibile problema …

Zurigo

Conti Swiss Life errati

Gli impressionanti scostamenti nei risultati finanziari forniti dalla Swiss Life (ex Rentenanstalt) per i conti 2001 erano dovuti a un errore nel nuovo programma di valutazione dei titoli.

La procura distrettuale zurighese competente per i reati economici ha archiviato il caso poiché non si trattava di errori intenzionali.

(Corriere del Ticino, 19.02.2004)

Un altro possibile problema …

USA

Aerei bloccati da computer

Centinaia di aerei della American Airlines e della US Airways, domenica sono rimasti bloccati a terra per alcune ore per il malfunzionamento di un computer provocato probabilmente da un errore umano.

(Corriere del Ticino, 3 agosto 2004)

Un altro possibile problema …

Savona

Errori del computer dell'ente nazionale degli infortuni (Inail)

Un ristoratore ligure ha ricevuto una richiesta di conguaglio dall'Inail di € 86 mio. Il caso è solo l'ultimo di una serie di cartelle pazze inviate a 37'000 artigiani liguri da parte dell'Inail a causa di un computer difettoso. (LaRegione, 10.9.2004)

Un altro possibile problema …

Zurigo

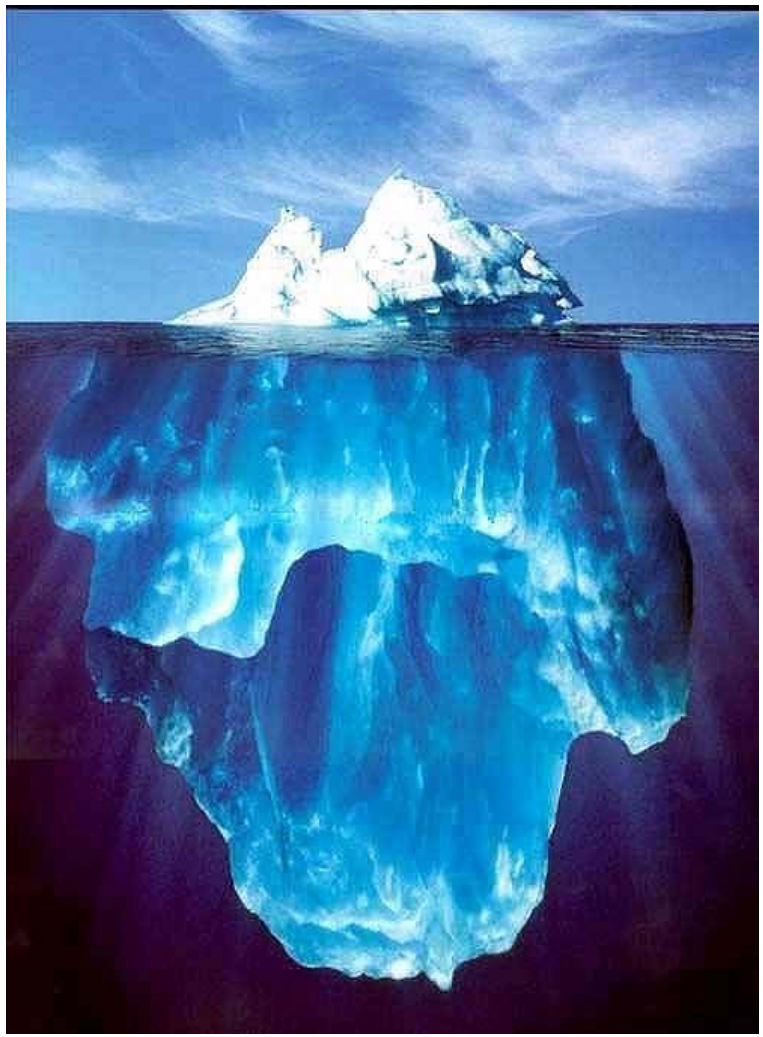
Nel caos la rete ferroviaria
La panne è iniziata alle 8:40 e si è appurato che dei lavori effettuati sulla rete dei dati FFS hanno messo fuori uso gli ordinatori. L'inondazione di segnalazioni d'errore è stata troppo forte anche per il sistema informatico di supporto, il cosiddetto « back up », che non si è attivato al momento della panne.
(Corriere del Ticino, 8 febbraio 2005)

Un altro possibile problema …

Roma

Violata l'Anagrafe di Roma
Da due postazioni di Laziomatica sono stati violati gli archivi informatici dell'Anagrafe di Roma e spiate le liste. Sono state effettuate numerose verifiche non autorizzate mediante appropriazione illecita dei codici di accesso oppure con codici scaduti che sono stati riabilitati. (Corriere della Sera, 18 marzo 2005)

Riassunto dei problemi in esercizio …

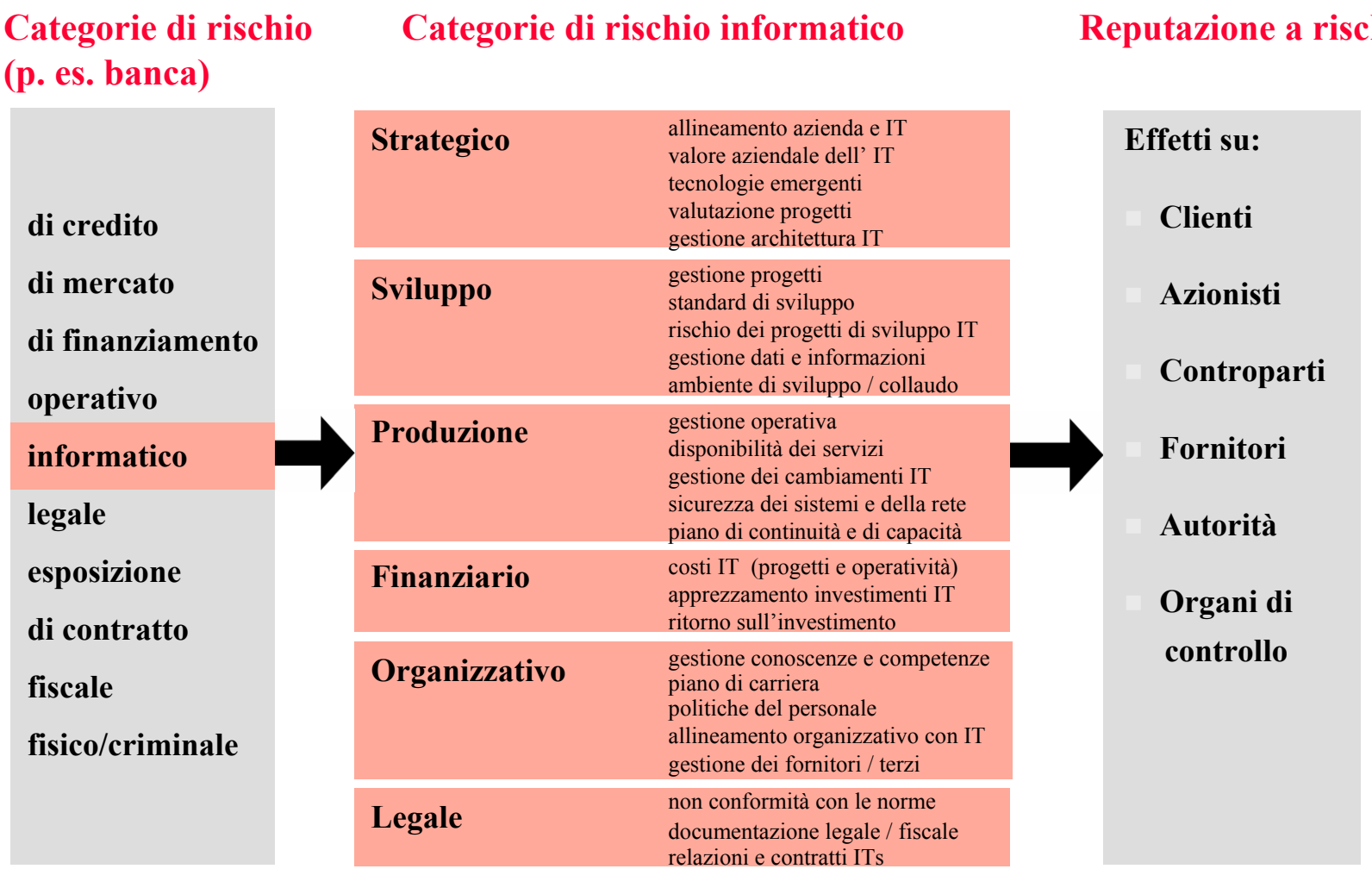


Riassunto dei problemi in esercizio …

- interruzione del servizio informatico
- errori applicativi (test insufficienti ?)
- errori umani
- mancanza di dati (p. es. non ripresi dal sistema precedente)
- degrado dei dati (p. es. cancellazione)
- inaffidabilità dei risultati
- violazione della sicurezza

➢ **debolezza del sistema informativo**

I rischi aziendali e i rischi informatici



IT-Risikomanagement und IT-Audit: Der schweizer Treuhänder, 12/1999, p. 1191

Riassunto dei possibili rischi …

- perdite, sprechi e mancate entrate
- violazione della sicurezza e delle norme legali
- rischio d'immagine
- inaffidabilità delle informazioni
- impossibilità di ricostruzione e di analisi

Le possibili cause …

- errori dovuti alla complessità, alla negligenza, alla mancanza di conoscenze ecc.
  - errori di manipolazione
  - errori di trattamento (p. es. errori di analisi e di programmazione)
  - errori casuali
  - ➢ **Assenza di strumenti per padroneggiare la situazione ?**

- i problemi informatici non sono stati identificati ?
- i problemi sono stati identificati al momento opportuno, ma non sono stati indirizzati o portati a conoscenza degli stakeholder ?
  - ➢ **Controllo interno carente ?**
  - ➢ **Assenza di revisione (informatica) ?**

Una possibile contromisura ?

La revisione (informatica) e l'audit di progetto

Premessa

Nota bene:

La revisione non è una condizione sufficiente per fare funzionare le cose !

Progetti in difficoltà e Gestione progetto carente sono cose diverse !

Revisione informatica: dove è l'accento ?

Applicazioni informatiche
in fase di esercizio (PRODUZIONE)

Come sono utilizzate ?

Applicazioni informatiche
in fase di sviluppo (PROGETTI)

Come sono costruite ?

Interventi della revisione informatica

Scopo e obiettivi dell'audit di progetto

- Gli obiettivi da raggiungere per i progetti sono gli stessi per tutti e derivano dal:
  - ✓ principio superiore della corretta gestione del *budget* accordato,
  - ✓ principio della legalità e
  - ✓ principio della tenuta regolare della contabilità
- Modello di riferimento COBIT:

efficacia	Raggiungimento degli obiettivi fissati inizialmente	= qualità
efficienza	Utilizzo ottimale delle risorse	
integrità	Esattezza, validità e completezza delle informazioni	
riservatezza	Protezione contro qualsiasi divulgazione non autorizzata	= sicurezza
disponibilità	Disponibilità dei sistemi, delle risorse e dei dati	
conformità	Rispetto delle leggi, delle direttive e dei contratti	= regolarità
affidabilità	Messa a disposizione d'informazioni affidabili	

- Scopo della revisione informatica è la verifica del raggiungimento di questi obiettivi

Fonte: GL IT Audit Amm. pubbl.

Ruolo e obiettivi di alcune istanze aziendali

- Qualità /
- Organizzazione

⇨

- Soddisfazione del cliente
- Efficienza
- Certificazione (ISO ecc.)

- Sicurezza

⇨

- Protezione dei beni aziendali
- Rispetto della normativa

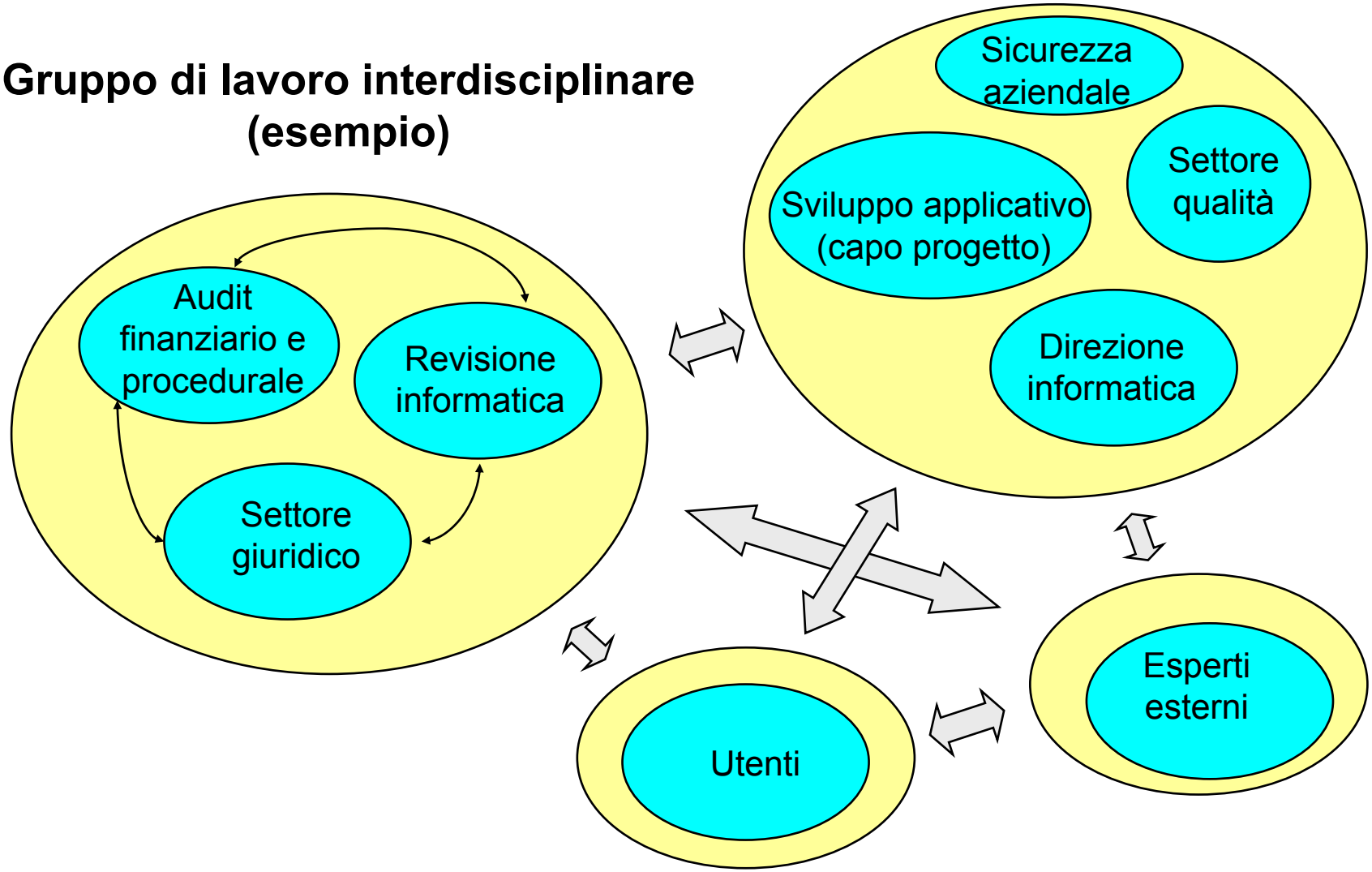
- Revisione interna

⇨

- Efficacia ed efficienza del sistema di controllo interno
- Accertamento della sicurezza (assurance)

Partecipanti in un audit …

Gruppo di lavoro interdisciplinare (esempio)



Ruoli: il controllo qualità

Il controllo della qualità (quality control) e la garanzia della qualità (quality assurance) sono delle funzioni spesso presenti nel gruppo di sviluppo.

I compiti del controllo qualità comprendono generalmente:

- rivedere i risultati di ogni fase del progetto
- valutare se i risultati sono in sintonia con gli obiettivi, con i requisiti e con le norme in vigore (p. es. funzionalità richieste, livello della documentazione, conformità con la metodologia)
- formulare delle raccomandazioni (interne all'area di sviluppo).

Ruoli: la revisione informatica

L'accompagnamento di un progetto informatico può comprendere:

- fornire consulenza sui seguenti aspetti: esposizione al rischio, identificazione e selezione dei controlli appropriati, tracce di revisione (*audit trail*) minime

- monitorare l'iter di sviluppo (p. es. rispetto del procedimento per fasi, esame documentazione di progetto, sviluppo dei controlli come concordato, supervisione dei collaudi, stato di avanzamento del progetto)

Opportunità per la revisione informatica

Collaborare nello sviluppo del sistema di controllo interno
da incorporare nelle nuove applicazioni.

➔ efficacia ed efficienza del controllo interno

Essere di supporto per esigenze di verifica indipendente (perizie, test, accertamenti ecc.) dei sistemi informativi sviluppati internamente o da terzi

➔ consulenza, supporto decisionale

Contribuire a promuovere un uso corretto e parsimonioso dell'informatica

➔ efficacia, efficienza ed economicità

➔ osservanza della politica informatica e delle direttive di sicurezza

Contribuire alla sensibilizzazione dell'utenza sull'utilizzo dei sistemi informativi

➔ sicurezza, diligenza

Panoramica delle modalità d'intervento

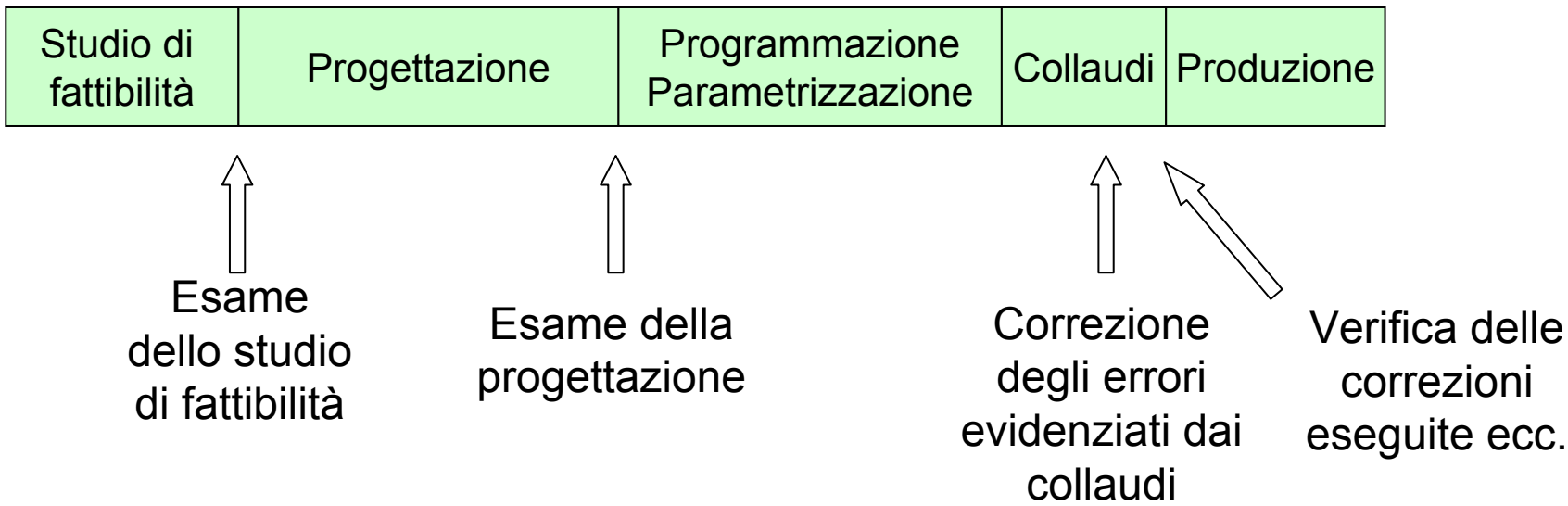
	Valutazione dell'applicazione	**Valutazione dello ambiente di sviluppo**
Durante lo sviluppo	Accompagnamento del progetto di sviluppo	Verifica dei metodi e degli standard per l'implementazione dei SI
Accettazione in produzione	Verifica delle funzionalità e dei controlli dell'applicazione	Verifica dei collaudi e delle procedure di accettazione da parte dell' utente
Durante l'esercizio	Controlli dipendenti dall'applicazione	Verifica dei metodi e degli standard per la manutenzione dei SI
	Controlli applicativi	**Controlli generali**

Audit di progetto

Fonte: Huissoud, CDF

Identificare i rischi nella pianificazione di un progetto di sviluppo

I progetti sono generalmente suddivisi in fasi:



Tipologia d'interventi (esempi) Fonte: Huissoud, CDF

Quando la revisione informatica può intervenire e secondo quali criteri ?

Esame della parsimonia	Il progetto è necessario ? (tutti i progetti) si integra nella strategia/architettura generale ?				
Esame dell' economicità	Il progetto è governato e gestito correttamente ? (tutti i progetti)				
Esame della conformità (compliance)	Le disposizioni legali generali (protezione dei dati, proprietà intellettuale, norme penali ecc.) e specifiche sono rispettate ? (tutti i progetti)				
Esame della regolarità (contabile e informatica)	Le norme contabili sono rispettate ? Le soluzioni scelte assicurano l'integrità dei dati, un sistema di controllo interno e una traccia di revisione ? (progetti finanziari) L'integrità e l'esattezza dei dati ripresi è garantita ?				
	Studio di fattibilità	Concetto	Analisi	Programmazione Parametrizzazione	Collaudi

Norme, metodi e strumenti (esempi)

Norme: Codice delle obbligazioni, MSA, Direttive interne …

Modelli: COBIT

Metodologie: Hermes, Prince2 …

Strumenti per il controllo del progetto:
- contabilità di progetto / controlling
- controllo qualità

Strumenti per il controllo dell'applicazione
- sistema di controllo interno (automatizzato)
- esecuzione regolare delle batterie di test
- strutture dati per il controllo esterno (p. es. revisione informatica)

Contenuto del sistema di controllo interno

Fortunatamente non siamo completamente disarmati e possiamo proteggerci da numerosi errori, ma occorre chinarsi in anticipo su questo aspetto.

In pratica, si tratta di attuare dei controlli adeguati ai rischi (p. es. controlli di coerenza dei dati, analisi di possibili anomalie) mediante dei dispositivi specifici espressamente concepiti e adibiti a tale scopo.

Per lo sviluppo di tali dispositivi, si tratta di ingegnarsi a immaginare le possibili tipologie di errore e dedurre le contromisure più indicate nei seguenti ambiti:

- dati
- elaborazioni
- risultati.

La premessa è la disponibilità di strumenti (strutture, dati ecc.) per assicurare la controllabilità del sistema.

Contenuto del sistema di controllo interno

Il sistema di controllo interno non si limita alla questione della separazione delle funzioni, ma copre pure tutti i controlli automatizzati e no, incluso le procedure di utilizzo e la documentazione, per esempio:

- abilitazioni e controllo accessi
- controlli di plausibilità al momento della ripresa dei dati
- riconciliazioni automatiche, totali di controllo
- liste di errori e/o di possibili anomalie
- giornali (tracce di revisione o *audit trail*), registri delle operazioni (*log*), storico delle modifiche
- monitoraggio e controllo continuo delle applicazioni e dei sistemi, segnalazione e analisi delle possibili anomalie
- strumenti per ricerche nei dati storici (movimenti, ricostruzione di transazioni ecc.).

Conclusione

Conclusione

- Problematiche relative ai sistemi informativi
- I possibili rischi
- I progetti e le applicazioni informatiche che ne derivano

  devono rispettare il:
  - ✓ principio superiore della corretta gestione del *budget* accordato,
  - ✓ principio della legalità e
  - ✓ principio della tenuta regolare della contabilità
- Pensare alla sicurezza (applicativa) dall'inizio del progetto
- Revisione informatica soprattutto quale misura preventiva.

Introduzione all'audit dei progetti: fine