IT Governance: scelte e soluzioni

Cesare Gallotti, Indipendent Consultant
Roma, 18 novembre 2010

Agenda

1. Presentazione
2. IT Governance
3. I “quadri di riferimento”
4. Le attività di controllo
5. Privacy e log management

Presentazione

Cesare Gallotti

Free-lance consultant:

- ✓ Consultancy in ISMS, QMS, Risk Assessment and Data Protection requirements
- ✓ Third party audits (for DNV) and assessments on Information Security, Quality Management Systems, IT Service Management, MMD
- ✓ Training for LA ISO/IEC 27001, ITIL Foundation and Quality Assurance courses
- ✓ Activities in Europe, Africa and Asia for different kind of customers

University degree in Mathematics, Lead Auditor ISO/IEC 27001 (CEPAS), ISO 9001:2000 (IRCA), ISO/IEC 20000-1 (itSMF); ITIL Expert (Exin); CISA; Computer Forensics (Post Univ.)

IT Governance

Enterprise governance

La "Governance" è un insieme di responsabilità e prassi seguite dalla Direzione di un'impresa con la finalità di:

- ✓ dare direzione strategica
- ✓ stabilire gli obiettivi e perseguirne il raggiungimento
- ✓ garantire che i rischi siano appropriatamente gestiti
- ✓ verificare che le risorse aziendali siano utilizzate responsabilmente

IT Governance (da Cobit 4.1)

L'IT Governance è parte della Enterprise Governance dedicata a

- ✓ garantire che l'IT sostenga e le strategie e gli obiettivi aziendali
- ✓ portare il contributo dell'IT alla loro definizione (estendendoli)

L'IT Governance è responsabilità della Direzione aziendale.

L'IT Governance, quindi, comporta un insieme di attività (organizzate secondo un quadro di riferimento) affinché l'IT supporti gli obiettivi di business.

I “quadri di riferimento”

I “quadri di riferimento”

Attualmente, l’orientamento è basato sul rischio:

- ✓ rischio di business (perdite economiche o di opportunità)
- ✓ rischio operativo (con conseguenti perdite economiche)

Tali rischi sono collegabili a:

- ✓ mancato rispetto della normativa in vigore
- ✓ mancanza di processi orientati alla qualità
- ✓ attacchi (deliberati o involontari) agli asset aziendali

Alcuni esempi orientati all'IT

Rispetto della normativa:

- ✓ "Modello organizzativo" ex Dlgs 231 del 2001
- ✓ "Gestione privacy" ex Dlgs 196 del 2003

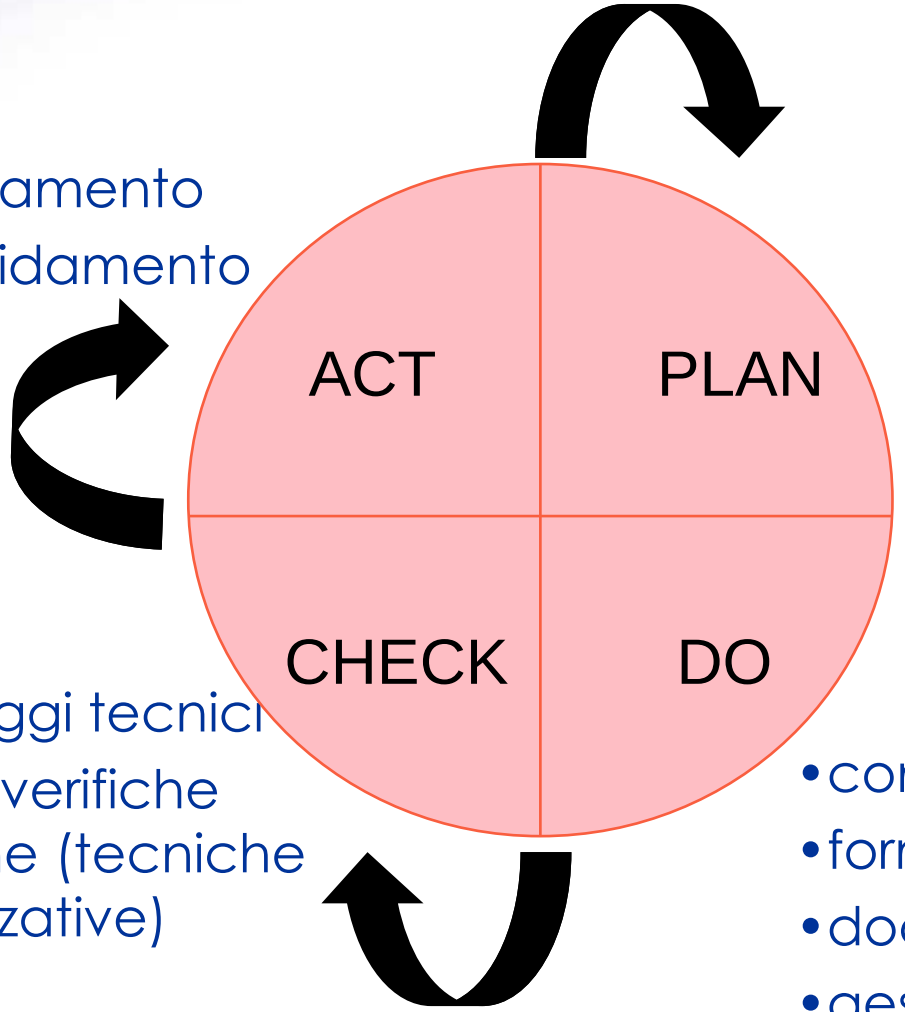
Processi di qualità:

- ✓ ISO 9001 (edizione 2008)
- ✓ ISO/IEC 20000 (edizione 2005)
- ✓ Cobit (edizione 4.1)

Sicurezza delle informazioni

- ✓ ISO/IEC 27001 (edizione 2005)

Schema generale



- miglioramento
- consolidamento

- analisi preliminare
- pianificazione
- obiettivi

- monitoraggi tecnici
- riesami e verifiche periodiche (tecniche e organizzative)
- audit
- assessment tecnici e organizzativi

- comunicazione
- formazione
- documentazione
- gestione dei fornitori
- gestione delle emergenze

Il Decreto Legislativo 231 del 2001

“Disciplina della responsabilità amministrativa delle persone giuridiche”. Richiede di

- ✓ “adottare modelli di organizzazione e di gestione idonei a prevenire reati” (Plan)
- ✓ vigilare sul funzionamento e l'osservanza dei modelli (Check)

La vigilanza riguarda anche il corretto funzionamento dei sistemi IT.

Privacy – Il Dlgs 196 del 2003

“Codice in materia di protezione dei dati personali”

Richiede (anche attraverso la normativa collegata) di:

- ✓ adottare opportune misure di sicurezza
- ✓ redigere e aggiornare un “Documento Programmatico”, che specifichi le misure adottate sulla basa di un’analisi dei rischi
- ✓ condurre verifiche periodiche sull’operato degli Amministratori di Sistema

Qualità (ISO 9001)

Con "Qualità", si intende il livello di soddisfacimento dei requisiti (stabiliti esplicitamente o implicitamente o generalmente attesi) previsti per un prodotto o un servizio.

I sistemi di gestione per la qualità si basano sul ciclo di Deming affinché i prodotti o i servizi (IT) soddisfino i clienti:

- ✓ Plan
- ✓ Do
- ✓ Check
- ✓ Act

Gestione dei servizi IT (ISO/IEC 20000)

La gestione dei servizi IT di qualità parte dai principi espressi dalle norme generali in materia di qualità.

Anch'essa si basa sul ciclo di Deming:

- ✓ Plan
- ✓ Do
- ✓ Check
- ✓ Act

Controlli dell'IT (Cobit)

Per erogare servizi IT coerenti con i requisiti di business, è necessario mettere in atto delle misure affinché:

- ✓ ci sia un collegamento tra IT e requisiti di business
- ✓ le attività dell'IT siano organizzate secondo un modello riconosciuto
- ✓ le risorse IT siano identificate

Le attività sono categorizzate in:

- ✓ pianificazione
- ✓ acquisizione e sviluppo
- ✓ rilascio, erogazione e supporto
- ✓ monitoraggio

Sicurezza (ISO/IEC 27001)

La sicurezza delle informazioni si fonda sulle seguenti proprietà dei dati:

- ✓ Riservatezza
- ✓ Integrità
- ✓ Disponibilità

I processi della sicurezza delle informazioni sono organizzati secondo il ciclo di Deming:

- ✓ Plan (sulla base di un risk assessment)
- ✓ Do
- ✓ Check (audit organizzativi e assessment tecnici)
- ✓ Act

Le attività di controllo

Tipologie di controlli

- **Controlli tecnologici:**
  - ✓ monitoraggi e allarmi
  - ✓ verifiche periodiche
  - ✓ assessment (reti, sistemi, sicurezza e vulnerabilità)
- **Controlli organizzativi**
  - ✓ riesami dell'efficacia ed efficienza dei processi
  - ✓ verifiche periodiche
  - ✓ audit
  - ✓ assessment (analisi dei processi)

I processi di controllo

Il processi di controllo devono basarsi sui seguenti:

- **programmare cosa controllare e con che frequenza**
  - ✓ controllare troppo è inefficiente e inefficace
  - ✓ controllare troppo poco è inutile
- **definire chi deve condurre i controlli**
  - ✓ imparzialità
  - ✓ competenza
- **condividere le modalità di condivisione del piano**
  - ✓ "a sorpresa" o "previsto"
- **condividere le modalità di reporting (a chi?)**
- **stabilire le azioni seguenti**

Questo anche per rispetto della normativa vigente e per garantire l'efficacia del processo

Privacy e log management

Log Management: Garante Privacy

Dal Provvedimento del 27 novembre 2008:

- ✓ Devono essere adottati sistemi idonei alla registrazione degli accessi logici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica.
- ✓ L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica

Si osservi che tale requisito non è stato emendato.

Caso del log management

Il log management soddisfa le necessità di controllo (check), fondamentali per qualsiasi sistema di governance, oltre che richiesto dalla normativa vigente.

E' importante, anche per evitare di sprecare risorse, comprendere:

- ✓ cosa controllare attraverso i log
- ✓ come verificare efficacemente i risultati

Inoltre, come per tutti gli strumenti informatici, è necessario che sia:

- ✓ usabile
- ✓ sicuro

GRAZIE!

Cesare Gallotti
Web: http://www.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it