COMPLIANCE E ORGANIZZAZIONE
(con norme ISO di riferimento)

Cesare Gallotti

Pescara, 19 giugno 2009

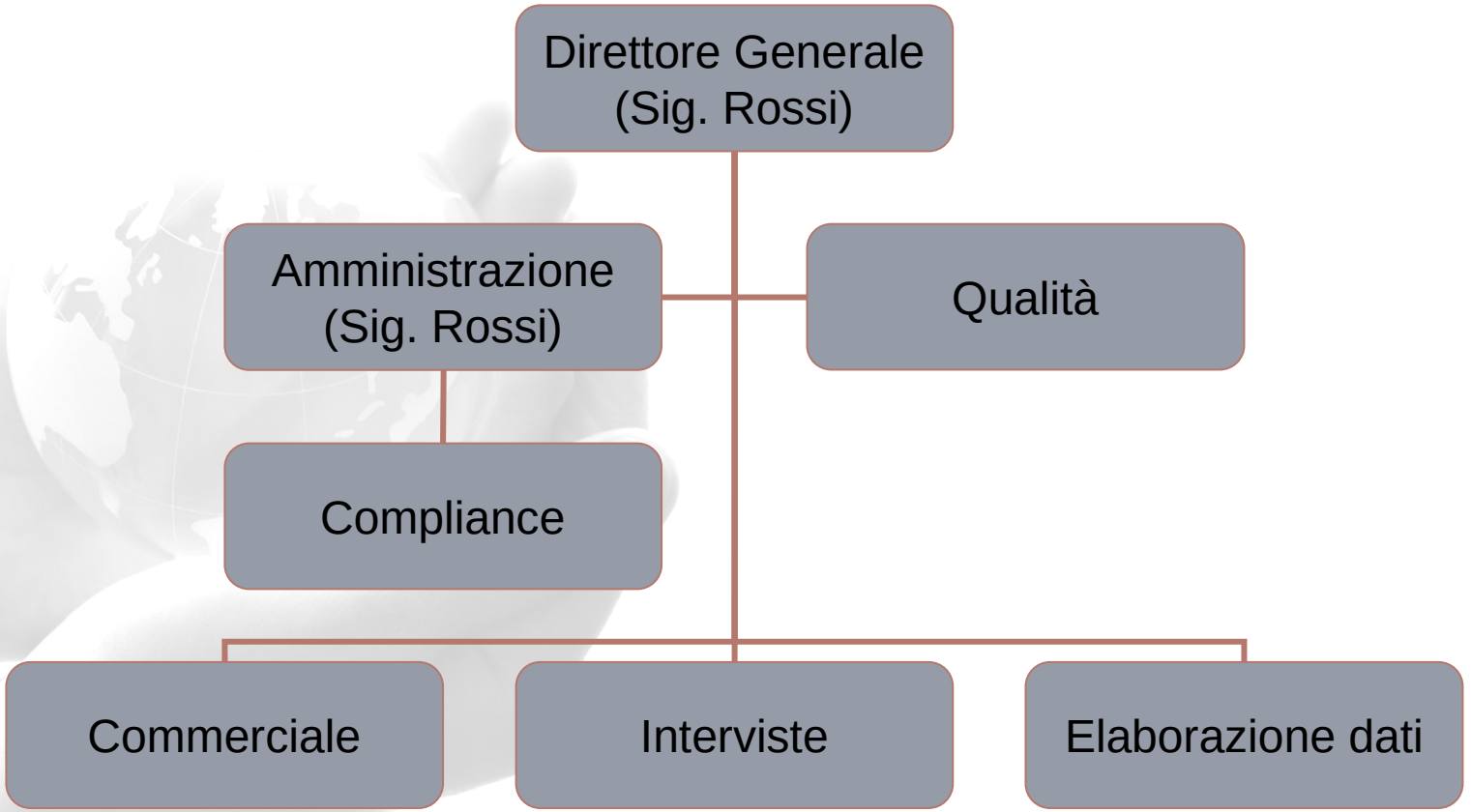
I principi di riferimento delle norme ISO (9001 e 27001)

a) Orientamento al cliente
b) Leadership
c) Coinvolgimento del personale
d) Approccio per processi
e) Approccio sistemico alla gestione
f) Miglioramento continuo
g) Decisioni basate su dati di fatto
h) Rapporti di reciproco beneficio con i fornitori

- I requisiti normativi devono essere recepiti e applicati dai processi aziendali in modo che siano gestiti efficacemente ed efficientemente

Esempio 1: dove è il problema?

- La responsabile "Compliance" non riesce a capire quanto tempo debbano essere conservati i dati (personali) relativi alle interviste effettuate.



Esempio 2: cosa manca?

- Un'azienda informatica con molti sistemi ha deciso di installare un CRM per la gestione degli utenti.
- Ha quindi:
  - stabilito il bisogno
  - sentito i possibili fornitori
  - ha valutato le offerte
  - redatto una richiesta per acquistare il prodotto denominato IAM+ (nome inventato)
  - l'ha inviata all'ufficio acquisti,
  - che l'ha portata avanti
- Si è poi "accorta" che il CRM non permetteva agli utenti di cambiare la propria password

Esempio 3: di chi è la responsabilità?

- Un ISP fornisce ai clienti un servizio di posta elettronica
- Se un utente dimentica la password, chiede al contact center (Numero Verde) di azzerarla
- Il responsabile del contact center ha deciso che per autenticare i clienti è necessario chiedere loro: nome, cognome, data di nascita, codice fiscale (o partita IVA)
- Il responsabile sicurezza (facente parte della Direzione) quando scopre il meccanismo, si lamenta che è troppo debole

Risposta

- Esempio 1:
  - Compliance e Organizzazione sono troppo lontane tra loro:
  - I requisiti normativi (Compliance) devono essere inseriti nei processi aziendali (Organizzazione)
  - Più processi aziendali coinvolti: almeno il Commerciale e la Gestione commesse
  - Principi di "approccio per processi" e "approccio sistemico"
- Esempio 2:
  - L'azienda non ha stabilito i propri requisiti (processo di progettazione o processo di pianificazione)
- Esempio 3:
  - Era compito del Responsabile Sicurezza stabilire le politiche di autenticazione (Plan o Policy) che il contact center avrebbe dovuto seguire (Do o Enforcement)
  - Era compito della Direzione stabilire degli audit (Check o Control) per verificare l'efficacia del meccanismo e via via migliorarlo (Act)
  - Principi di "Leadership" e di "Miglioramento Continuo"

Norme di riferimento

- ISO 9001:2008 per modellizzare i principali processi di business (Commerciale, Gestione delle commesse, Acquisti, ...)
- ISO/IEC 20000-1 per modellizzare i principali processi di gestione dei servizi informatici
  - > ISO/IEC 20000-2 per approfondimenti
- ISO/IEC 27001:2005 per la pianificazione e gestione delle misure di sicurezza (Risk Assessment, Gestione del rischio) e dell'organizzazione con riferimento alla sicurezza
  - > ISO/IEC 27002:2005 per approfondire le possibili misure di sicurezza
- ISO/IEC 9126-1:2007 per i criteri di qualità del software (non solo requisiti funzionali)

- Non sono norme burocratiche.

Conclusioni (per la Carta di Pescara)

- Attuare il ciclo di miglioramento anche a livello istituzionale: a seguito dei controlli e delle domande effettuate all'Ufficio del Garante, mettere a disposizione le interpretazioni
  - > chiare ed esaurienti (vedere FAQ 14 del Provvedimento Amministratori di Sistema)
  - > facilmente accessibili (non attraverso la ricerca di vecchi numeri di giornale)
  - > opportunamente pubblicizzate (via newsletter)
- Rivedere alcune incongruenze (p.e. la richiesta di pianificare la formazione a livello di DPS, ma non di effettuarla) e riesaminare l'allegato B alla luce della norma ISO/IEC 27002:2005 (già ISO/IEC 17799:2005 e BS 7799-1)
- Sottolineare l'importanza di misure sostanziali (p.e. il non uso di password generiche o attestazione da parte dei fornitori) oggi raramente applicate, al posto di misure formali come il DPS (oggi oggetto di troppe discussioni) : il PDCA non deve essere sviluppato nella parte Plan!
- Promuovere la pubblicazione di modelli anche per le aziende (es. DPS) per ridurre le spese necessarie alla "sicurezza formale".