IoT, IoBT, OoT - Nuovi scenari per il teatro operativo

Un unico modello organizzativo di sicurezza IT per attività multidisciplinari e distribuite geograficamente

Francesca Balducci
Serco Europe – Safety, Risk & Compliance Director
Serco Europe – Information Security Director
Serco Europe – Head of Strategic Initiative Defence

InfoSec

- Cos'è l'Information Security

L'Information Security si occupa principalmente di proteggere **dati** e **risorse aziendali** da incidenti non intenzionali e dagli **attacchi hacker**.

InfoSec copre tutte le misure che un'azienda può adottare per proteggere le **proprie informazioni sensibili** seguendo un approccio basato sulla **valutazione del rischio**.

- Principi dell'Information Security

Proprietà di un'informazione di essere accessibile unicamente a individui, entità o processi autorizzati.

Riservatezza

Proprietà di un'informazione di mantenersi completa e accurata, senza possibilità di alterazione da parte di eventi esterni.

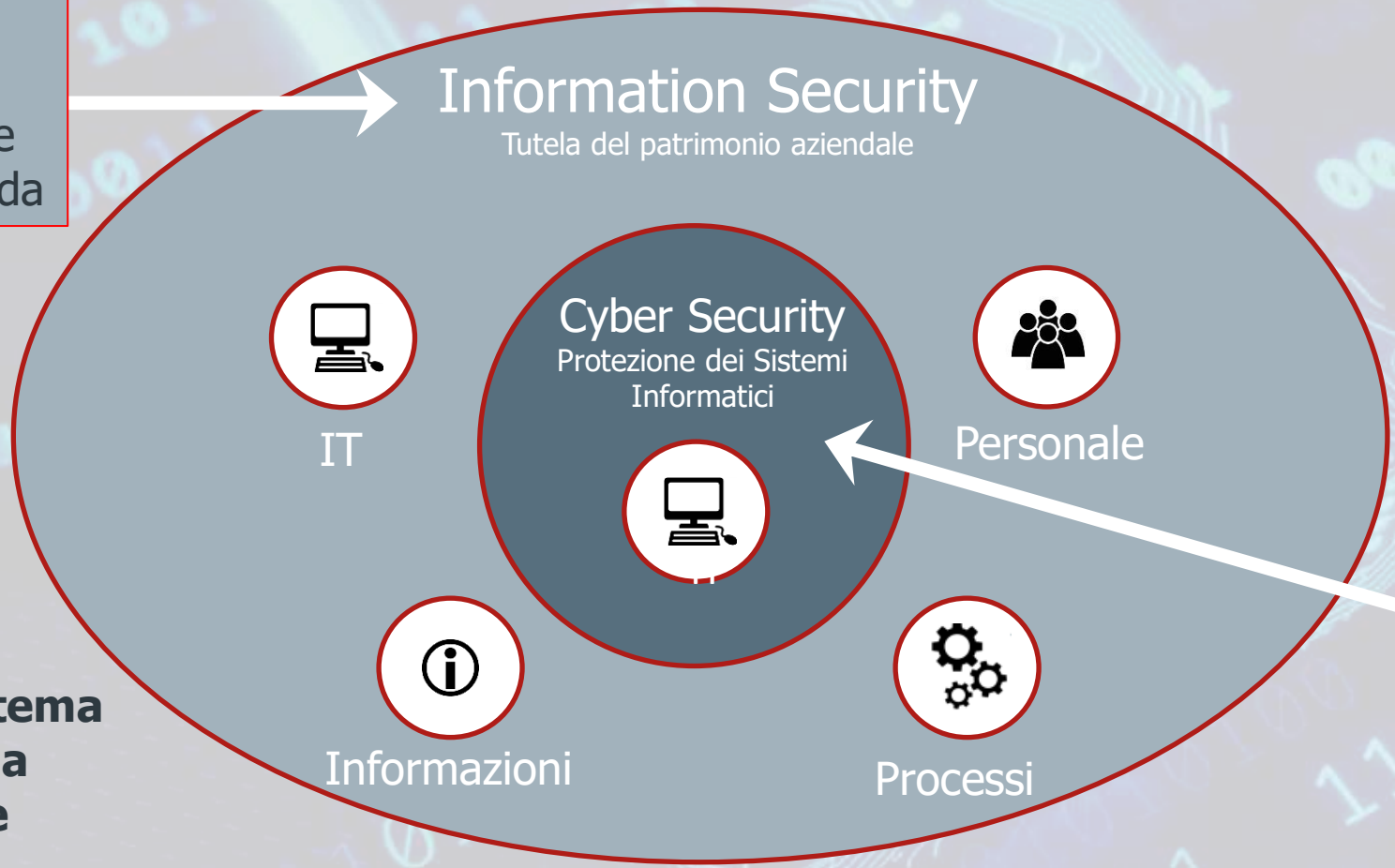
Integrità

proprietà di un'informazione di essere accessibile e utilizzabile (entro i tempi previsti) su richiesta di un individuo, entità o processo autorizzato.

Disponibilità

- Information Security Vs Cyber Security

Impegno della direzione che coinvolge tutte le divisioni dell'azienda



Attività del dipartimento IT

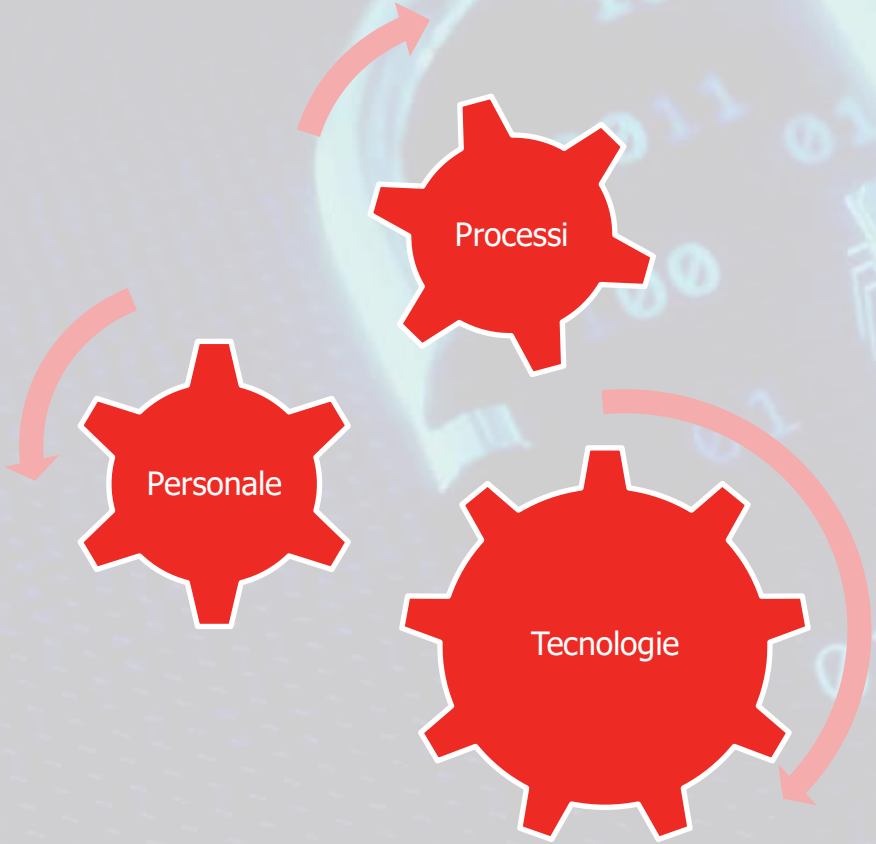
Istituzione del Sistema di gestione della sicurezza delle informazioni (ISMS)

- Information Security Vs Cyber Security

Ogni misura di sicurezza informatica contribuisce alla sicurezza delle informazioni, ma non è vero il contrario.

Non tutti i problemi relativi alla sicurezza delle informazioni riguardano anche la Cyber sicurezza

- ISMS



Un Information Security Management System (ISMS) è un modello organizzativo basato su **processi, tecnologie e personale** che aiuta a:

- ✓ **monitorare**, **verificare** e **migliorare** le pratiche di sicurezza delle informazioni della nostra organizzazione.
- ✓ **gestire** tutti i processi di sicurezza in un unico posto, in modo coerente ed economico.
- ✓ **promuovere la cultura e la consapevolezza della sicurezza delle informazioni** in tutta l'azienda.
- ✓ **proteggere tutte le nostre informazioni aziendali e la proprietà intellettuale**, nonché i dati personali.

- ISO 27001

ISO 27001 è uno standard di gestione di Information Security che fornisce una

guida dettagliata per l'adozione delle misure di sicurezza appropriate,

sotto forma di ISMS, per proteggere l'attività aziendale da una violazione dei dati.

- Conformità ISMS alla ISO 27001

Un ISMS conforme alla norma ISO 27001 prevede di:

- ✓ **identificare e gestire regolarmente i rischi per la sicurezza dei dati** tenendosi al passo con la costante evoluzione delle minacce alla sicurezza.
- ✓ **implementare le misure appropriate per mitigare tali rischi,** con misure tecniche raccomandate in linea con i requisiti del GDPR.
- ✓ **soddisfare i requisiti di sicurezza dei dati per conformarsi al GDPR.**

• Come la ISO 27001 aiuta a rispettare il GDPR

1. GARANZIA

L'uso dello schema di certificazione ISO 27001 dimostra che i rischi per la sicurezza delle informazioni, come raccomandato dal GDPR, vengano gestiti efficacemente

2. NON SOLO DATI PERSONALI

La ISO 27001 aiuta a mettere in atto processi che proteggano tutte le risorse informative

3. CONTROLLI E QUADRO DI SICUREZZA

La certificazione ISO 27001 dimostra che l'azienda pone in essere controlli per mitigare i rischi identificati, come raccomandato dal GDPR

4. PERSONE, PROCESSI E TECNOLOGIA

I rischi non sono solo basati sulla tecnologia, ma anche minacce comuni, come personale poco informato o procedure inefficaci.

5. RESPONSABILITÀ

La ISO 27001 richiede che il regime di sicurezza sia supportato dai massimi dirigenti e incorporato nella cultura e nella strategia dell'organizzazione. Richiede anche la nomina di una figura responsabile per l'ISMS.

6. VALUTAZIONI DEI RISCHI

La conformità alla ISO 27001 significa condurre valutazioni dei rischi regolari per identificare minacce e vulnerabilità e adottare misure per proteggere tali dati, come richiesto dal GDPR

7. MIGLIORAMENTO CONTINUO

La ISO 27001 richiede che l'ISMS sia costantemente monitorato, aggiornato e rivisto, utilizzando un processo di miglioramento continuo che si adatti ai cambiamenti.

8. TEST E AUDIT

Essere conformi a GDPR e alla ISO 27001 significa che l'organizzazione deve effettuare test e audit regolari per dimostrare che il suo regime di sicurezza funziona in modo efficace.

9. CERTIFICAZIONE

Il conseguimento della certificazione ISO 27001 fornisce una valutazione indipendente ed esperta del fatto che siano state implementate misure adeguate per proteggere i dati (come richiesto dal GDPR)

I sistemi di gestione aziendale e il dipartimento Safert Risk and Compliance

I Sistemi di Gestione Aziendale sono modelli organizzativi adottati su base volontaria, attuati attraverso l'applicazione sistematica di regole e procedure.

I sistemi di gestione sono costituiti da un insieme di politiche, processi e documenti utilizzati dall'organizzazione e adottati a tutti i livelli per garantire che essa possa svolgere i compiti richiesti per raggiungere i suoi obiettivi.

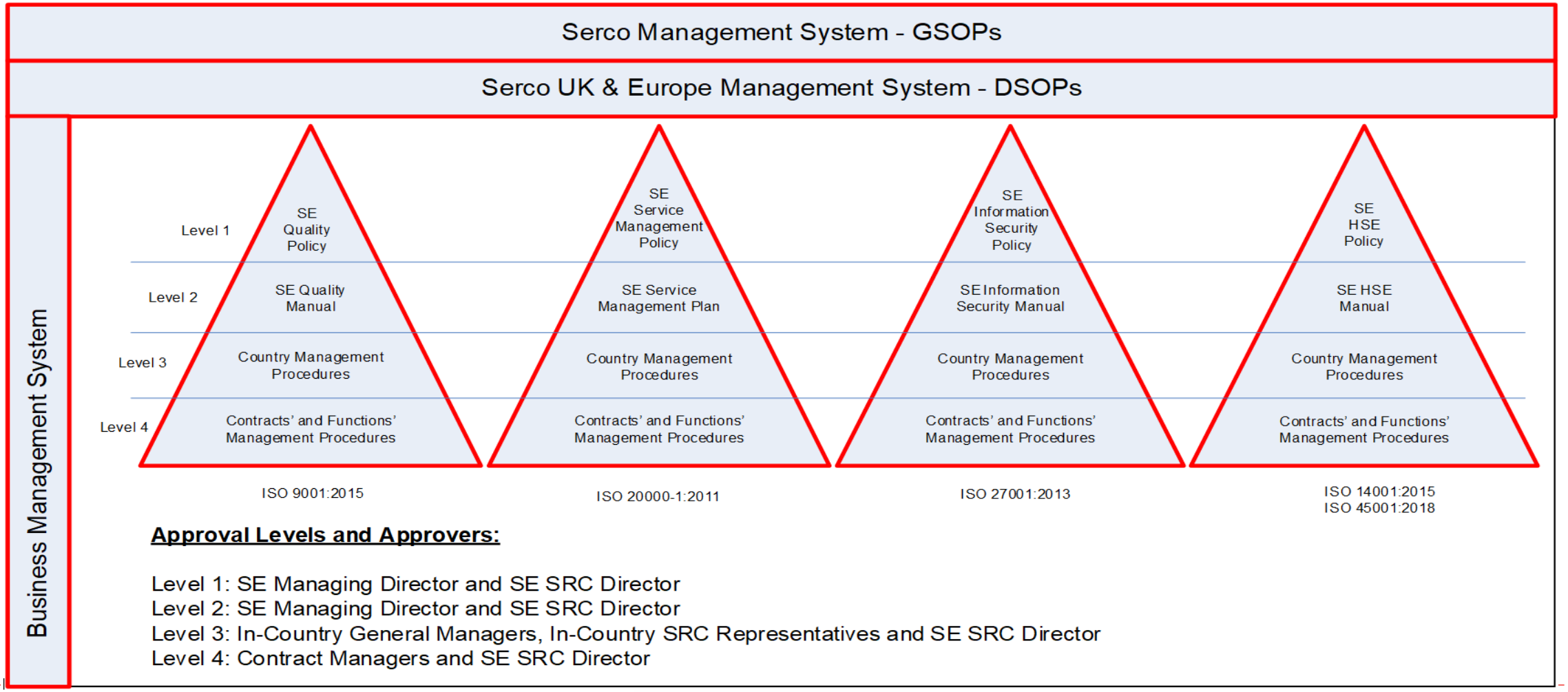
Questi obiettivi coprono molti aspetti delle operazioni dell'organizzazione (inclusi il successo finanziario, il funzionamento sicuro, la qualità dell'erogazione dei servizi, le relazioni con i clienti, la conformità legislativa e normativa, la gestione dei lavoratori).

Il Dipartimento Safery Risk and Compliance definisce tali strategie in accordo con la direzione aziendale coordinando, gestendo e assicurando l'esecuzione delle attività di Governance, Management e Compliance.

Sistemi di gestione certificati Serco

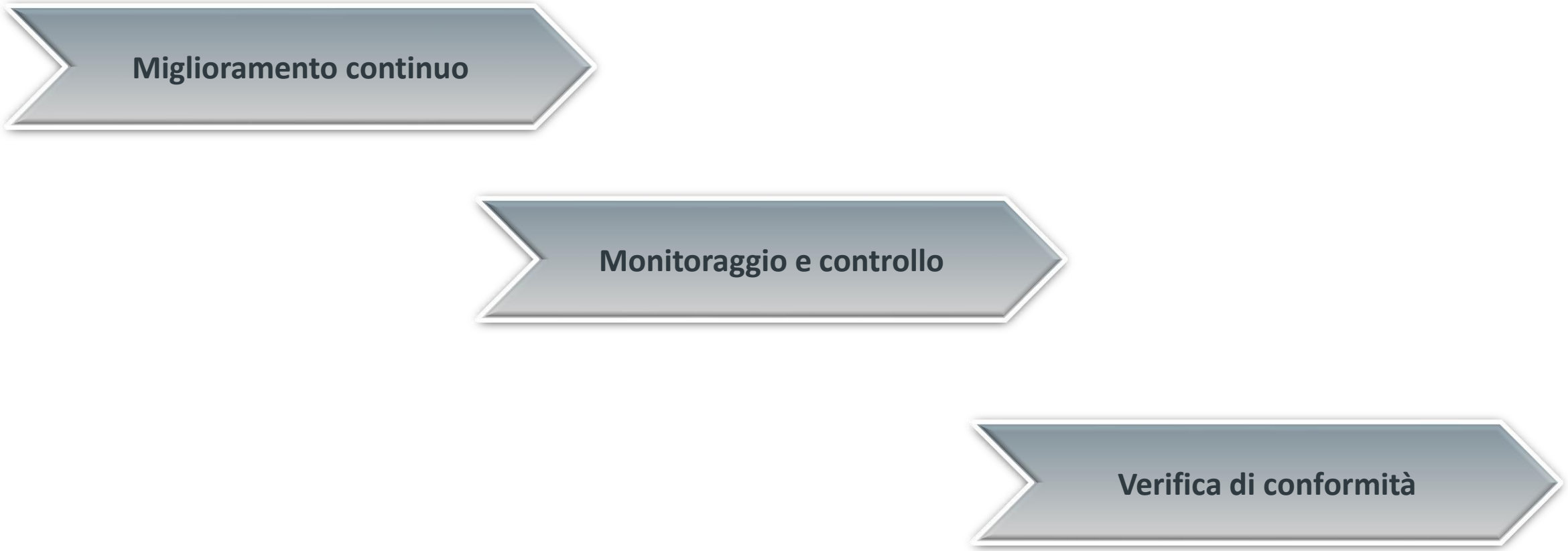
Gerarchia della documentazione e interazione del sistema – autorizzazioni

Lo schema seguente sintetizza l'interazione tra i Sistemi certificati ISO e il Sistema di gestione aziendale Serco, la gerarchia della documentazione e le autorità competenti per l'approvazione della documentazione



Sistemi di gestione certificati Serco

Elementi cardine delle attività cicliche per raggiungere la conformità aziendale



Sistemi di gestione certificati Serco

ISO 9001:2015 - Quality Management System

Un insieme di politiche, processi aziendali e procedure necessarie per la pianificazione e l'esecuzione del servizio nell'area di attività principale incentrate sulla soddisfazione coerente dei requisiti dei clienti.

ISO/IEC 20000-1:2011 - Service Management System

È un "sistema" complesso di processi manuali e automatizzati utilizzati per gestire un Servizio IT; in particolare, la sua pianificazione, sviluppo, attuazione, funzionamento e miglioramento.

ISO-IEC 27001:2013 – Information Security Management System

Sistema volto alla difesa dei dati finanziari, della proprietà intellettuale e delle informazioni sensibili sui clienti, proteggendo la riservatezza, la disponibilità e l'integrità delle risorse da minacce e vulnerabilità.

ISO 14001:2015 - Environmental Management System

Un insieme di politiche, processi e procedure aziendali che aiutano a migliorare continuamente le prestazioni ambientali attraverso un uso più efficiente delle risorse e la riduzione degli sprechi.

ISO 45001:2018 - Safety & Risk Management System

Combinazione di persone, processi, procedure, strutture e risorse necessarie per identificare i pericoli e comprendere e gestire i rischi per la sicurezza.

Verifica di conformità

A cosa serve l'audit di conformità

Gli Audit (interni ed esterni) sono effettuati per garantire la continua conformità con gli standards ISO, il sistema di gestione di Serco UK, le Politiche e le Procedure Operative del Gruppo.

I Revisori esaminano le questioni relative alle pratiche e ai rischi aziendali, cercando evidenze oggettive che il sistema di gestione sia mantenuto nella sua interezza (in termini di politiche, obiettivi, KPI), migliorato e corretto secondo necessità.

Evidenze oggettive: sono prove tangibili che rendono dimostrabili i fatti. E' possibile provare i fatti mediante misurazione, analisi e osservazione.

Verifica di conformità

1ª Linea (attività di audit interno in Europa)

- Svolti da revisori interni qualificati (dipendenti Serco/personale SRC);
- Almeno uno all'anno;
- Garantire il rispetto di:
  - ✓ SMS – Sistema di gestione Serco
  - ✓ ISO 9001:2015 - Sistema di gestione della qualità
  - ✓ ISO 14001:2015 - Sistema di gestione ambientale
  - ✓ ISO 45001:2018 – Sistema di gestione della salute e sicurezza
  - ✓ ISO/IEC 20000-1:2011 - Sistema di gestione dei servizi IT
  - ✓ ISO/IEC 27001:2013 - Sistema di gestione della sicurezza delle informazioni

Verifica di conformità

2ª Linea (Attività di Revisione Esterna di Divisione)

- Risk Based Audit, svolto da revisori esterni qualificati (dipendenti Serco)
- Condurre almeno uno all'anno
- Garantire il rispetto di:
  - ✓ Etica e condotta aziendale
  - ✓ Business continuity
  - ✓ Finanza
  - ✓ Informazioni di sicurezza
  - ✓ Ambiente
  - ✓ Conformità contrattuale e accuratezza KPI

Sistemi di gestione certificati Serco

Verifica di conformità

3ª Linea (attività di audit esterno del Gruppo/LRQA)

- Svolti da revisori esterni qualificati (dipendenti Serco/LRQA)
- Condotto uno all'anno
- Garantire il rispetto di:
  - ✓ SMS – Sistema di gestione Serco
  - ✓ ISO 9001:2015 - Sistema di gestione della qualità
  - ✓ ISO 14001:2015 - Sistema di gestione ambientale
  - ✓ ISO 45001:2018 – Sistema di gestione della salute e sicurezza
  - ✓ ISO/IEC 20000-1:2011 - Sistema di gestione dei servizi IT
  - ✓ ISO/IEC 27001:2013 - Sistema di gestione della sicurezza delle informazioni