ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI PALERMO

aicq Sicilia
TALQ

rAisk
DOMINIO DEL RISCHIO LEGALE

Palermo 26.01.2026 – Seminario
I sistemi di gestione aziendali integrati e il loro rapporto con il D.Lgs. 231/2001. Interventi e utilizzo dell'Intelligenza Artificiale

Seminario

"Opportunità dei sistemi gestionali integrati, caso di studio Italtel
Cenni ai vincoli sull'utilizzo dell'AI per i professionisti "

Relatore:

Ing. Bruno Lo Torto

NASCONO LE NORME ISO

Norme internazionali: la nascita dell'ISO

- ✓ Nel **1947** fu fondato l'ISO (International Organization for Standardization), che cominciò a sviluppare standard tecnici e industriali in vari settori.
- ✓ Negli **anni '70 e '80**, con la globalizzazione crescente e il commercio internazionale in forte espansione, si sentì il bisogno di norme internazionali per garantire la qualità dei prodotti in modo uniforme in tutto il mondo.
- ✓ Uno degli standard più rilevanti per la qualità è la serie di norme della famiglia **ISO 9000**, pubblicata per la prima volta nel **1987**, sulla scorta della norma britannica **BS 5750:1979**, sviluppata dal British Standards Institution (BSI): «Specification for Design, Development, Production, Installation and Servicing» con l'obiettivo di fornire requisiti per i sistemi di gestione della qualità applicabili a diversi settori, con lo scopo di garantire prodotti e servizi conformi agli standard specificati.

Cenni ai sistemi gestionali ISO

NON PIU' SOLO QUALITA' – EVOLUZIONE DELLE NORME ISO

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 20000:2005, *Information technology – Service management*

ISO 9001:2000, *Quality management systems – Requirements*

ISO 14001:2004, *Environmental management systems – Requirements with guidance for use*

ISO 22000:2005, *Food safety management systems – Requirements for any organization in the food chain*

OHSAS 18001:1999, *Occupational health and safety management systems – Specifications*

2013: ISO/IEC *Directives, Part1 Consolidated ISO Supplement,* ***Annex SL (normative)*** *High level structure, identical core text and common terms and core definitions for use in Management System Standard,* ***Appendix 2***

High level structure: sommario (indice) di alto livello
Harmonized strutture: identici punti norma, titoli, testo e termini comuni e definizioni principali

Approccio basato sul rischio: ogni scelta e ogni decisione deve essere presa a seguito di approccio basato sull'analisi del rischio

Rischio: effetto dell'incertezza (rispetto ad un risultato atteso) effetto: scostamento da quanto atteso, **positivo o negativo**

Incertezza: stato anche parziale di carenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della sua probabilità di accadimento.

Cenni ai sistemi gestionali ISO

EVOLUZIONE DELLE NORME ISO

		1997-1994	2000-2008 VISION 2000	2015-2026
Quality Control	**Quality Assessment**	**Quality Assurance**	**Quality Improvement**	**Quality Risk Approach**
Fuori dal processo produttivo	Fuori dal processo produttivo	Dentro il processo produttivo	Clienti e fornitori dentro il processo produttivo	Risk based thinking Approccio basato sul rischio
Dopo che il processo produttivo si era compiuto	Dopo che il processo produttivo si era compiuto	Prima che le diverse parti dei cicli operativi siano compiuti	Prima e durante il compimento dei cicli operativi	Prevenire le minacce prima del compimento dei cicli operativi
Contro coloro che svolgono il lavoro	Con coloro che svolgono il lavoro	Con coloro che svolgono il Lavoro	Con coloro che svolgono il Lavoro	Con coloro che svolgono il Lavoro
		Documentazione	Solo Documentazione necessaria per efficacia SG	Informazioni documentate

Vision 2000:

- ✓ Revisione chiave per rendere i sistemi di gestione meno orientati alla conformità burocratica e più incentrata sul valore aggiunto per l'organizzazione.
- ✓ Miglioramento continuo => PDCA (ciclo di Deming).
- ✓ Coinvolgimento della Leadership ed orientamento al cliente.
- ✓ Focus sui Processi Primari e di Supporto.
- ✓ L'attenzione si sposta dalla semplice conformità alla creazione di valore.

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

rAisk DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

EVOLUZIONE DELLE NORME ISO
ARRIVA LA STRUTTURA DI ALTO LIVELLO- STRUTTURA ARMONIZZATA

1	*Scopo e campo di applicazione*
2	*Riferimenti normativi*
3	*Termini e definizioni*

4	*Contesto dell'organizzazione*
5	*Leadership*
6	*Pianificazione*
7	*Supporto*
8	*Attività operative*
9	*Valutazione delle prestazioni*
10	*Miglioramento*

Cenni ai sistemi gestionali ISO

STRUTTURA DI ALTO LIVELLO- STRUTTURA ARMONIZZATA
VALIDA PER TUTTI I SISTEMI GESTIONALI
CONVENIENZA DI UN SISTEMA INTEGRATO 27001-20000-1-22301

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

5.2 **POLITICA** ⟷ **CONTESTO DELL'ORGANIZZAZIONE**

6.2 **OBIETTIVI S.M.A.R.T.** ⟷ Fattori esterni
Fattori interni
Parti interessate e loro aspettative
4.1 + 4.2

VALUTAZIONE DEI RISCHI E OPPORTUNITA'

Azioni per raggiungere gli Obiettivi e loro pianificazione

6.1

Azioni per fronteggiare Rischi e Opportunità e loro pianificazione

4.4 **SISTEMA DI GESTIONE per i punti da 7 a 10**

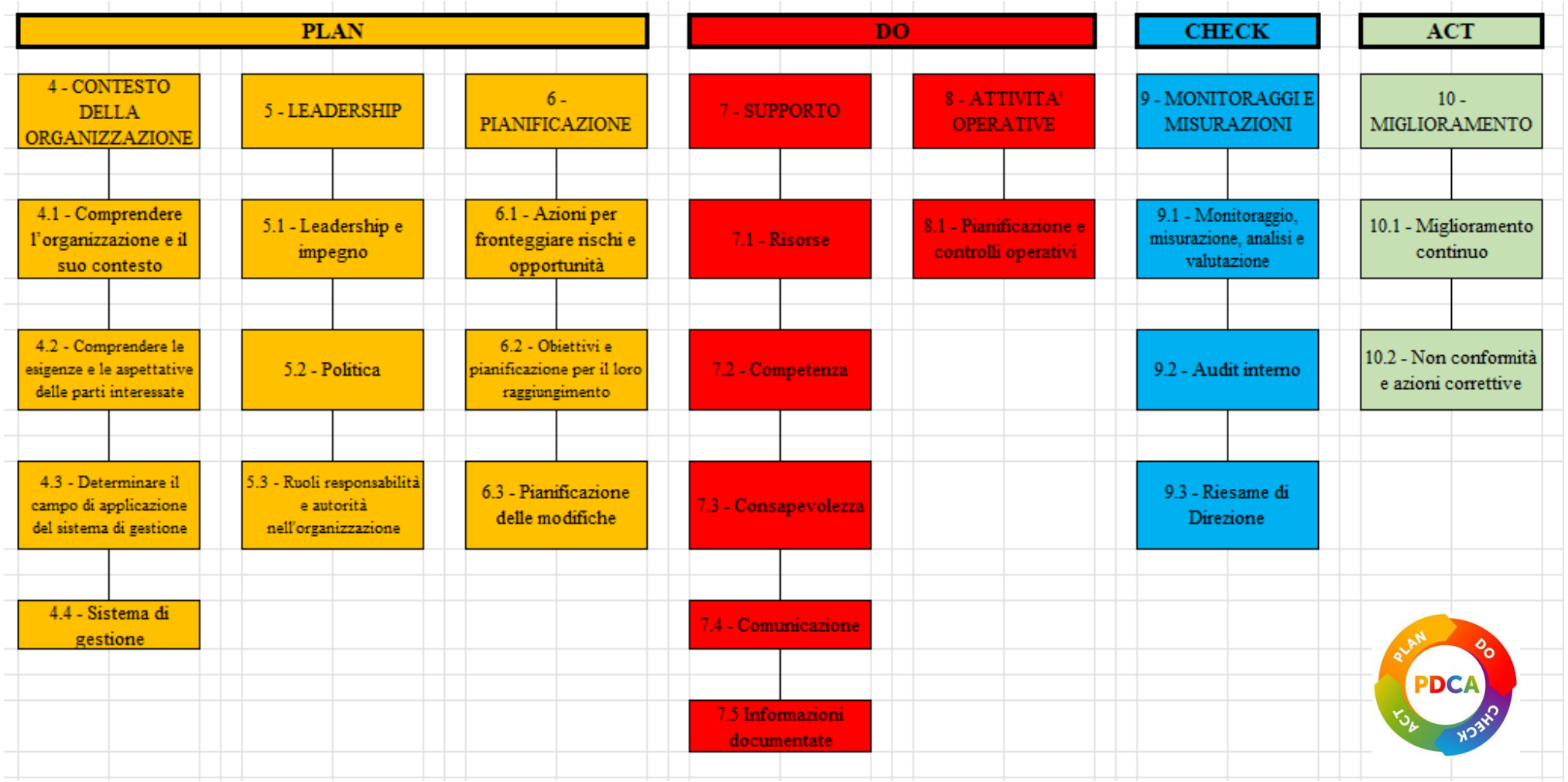
1. **Requisiti legali e cogenze applicabili**
2. **Norma del sistema di gestione (27001 + 20000-1 + 22301)**
3. **Sistema documentale (Manuale, Procedure, Istruzioni operative, Registrazioni, ecc.)**
4. **Aspettative delle parti interessate (clienti, mercato, territorio, ecc.)**
5. **Azioni decise per fronteggiare rischi e opportunità**
6. **Azioni decise per il raggiungimento degli obiettivi aziendali.**

rAisk DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

STRUTTURA DI ALTO LIVELLO- STRUTTURA ARMONIZZATA VALIDA PER TUTTI GLI SCHEMI DI CERTIFICAZIONE ISO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO



aicq TALQ

rAisk DOMINIO DEL RISCHIO LEGALE

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

CAMBIAMENTO CLIMATICO

L'impatto dei cambiamenti climatici sui sistemi di gestione riguarda la necessità di integrare la valutazione e il management dei rischi climatici in tutti i sistemi di gestione, come ISO 9001, ISO 27001 ISO 14001, ISO 45001 etc. … . Questo significa considerare come il cambiamento climatico può influenzare l'attività caratteristica, la catena del valore, le opportunità di mercato, l'impatto reputazionale e i procedimenti legali. I sistemi di gestione devono ora includere l'analisi del contesto organizzativo, valutando i rischi e le opportunità legate al cambiamento climatico e implementando azioni per la sua mitigazione e adattamento.

La rilevanza intrinseca dei cambiamenti climatici sarà in gran parte diversa per i vari standard a causa dei loro diversi ambiti di applicazione e finalità. La rilevanza dipenderà anche da fattori quali l'ubicazione e la natura dell'organizzazione, ad esempio il settore di attività, il tipo di processi, prodotti e servizi, ecc. L'Italtel ne dà contezza nelle attività del comitato ESG e nel Bilancio di sostenibilità disponibile al seguente link: Sustainability – Italtel

Quali sono i **requisiti** ISO ?

La modifica è inclusa nel Capitolo 4 della "Harmonized Structure" (Appendice 2 dell'Allegato SL delle Direttive ISO/IEC Parte 1 "Consolidated ISO Supplement"):

4.1 Comprendere l'organizzazione e il suo contesto, dove è aggiunta la seguente frase: "*The organization **shall** determine whether **climate change** is a relevant issue*".

4.2 Comprendere le esigenze e le aspettative delle parti interessate, dove viene aggiunta la seguente frase: "*NOTE: Relevant interested parties **can** have requirements related to **climate change***".

ISO 9001:2015

1 SCOPO E CAMPO DI APPLICAZIONE

La presente norma internazionale specifica i requisiti di un sistema di gestione per la qualità quando un'organizzazione:

a) ha l'esigenza di dimostrare la propria capacità di fornire con regolarità prodotti o servizi che soddisfano i requisiti del cliente e i requisiti cogenti applicabili; e

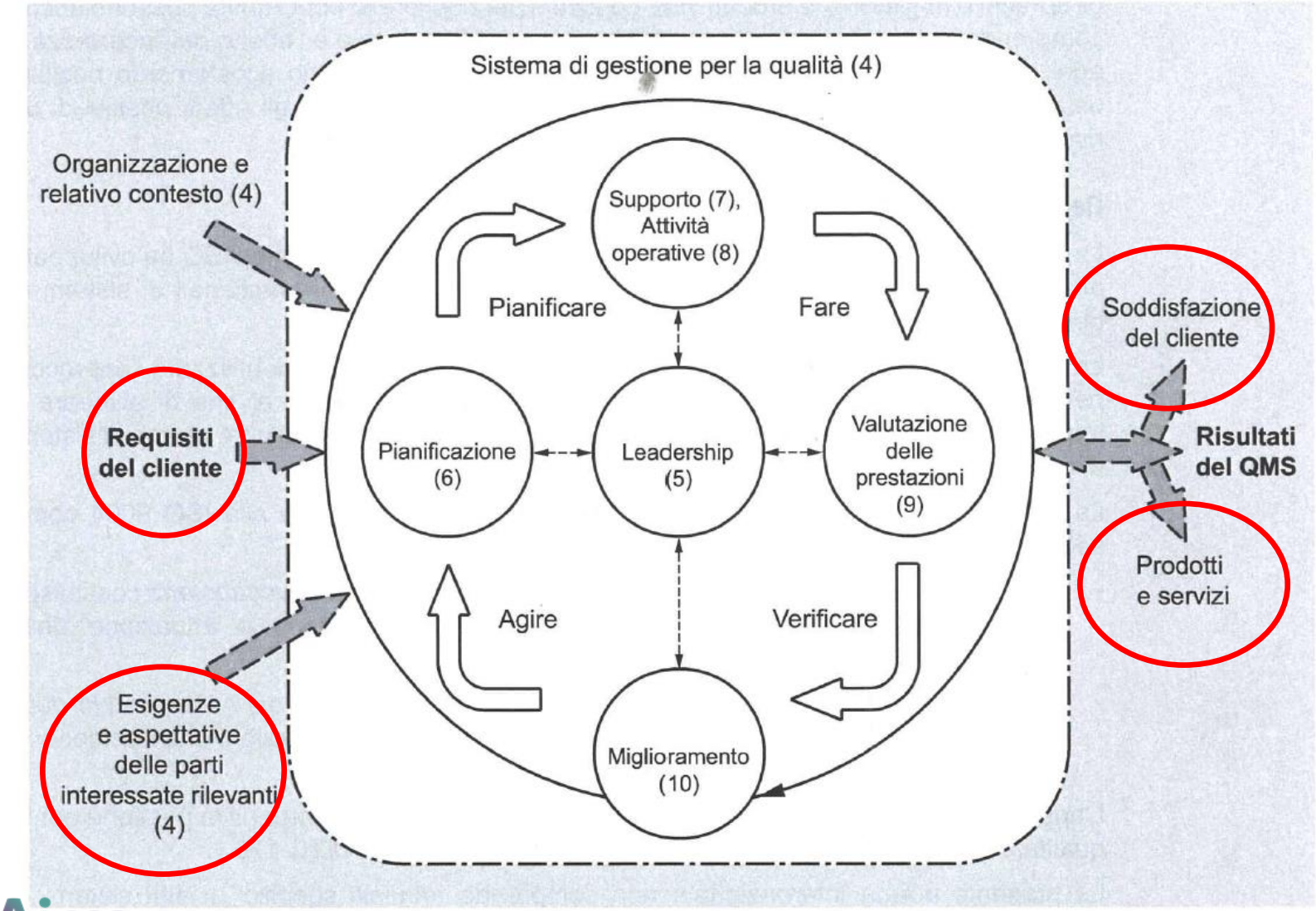
b) mira ad accrescere la soddisfazione del cliente tramite l'applicazione efficace del sistema, compresi i processi per migliorare il sistema stesso e assicurare la conformità ai requisiti del cliente e ai requisiti cogenti applicabili.

Tutti i requisiti della presente norma internazionale sono di carattere generale e previsti per essere applicabili a tutte le organizzazioni, indipendentemente da tipo o dimensione, o dai prodotti forniti e servizi erogati.

Nota 1 Nella presente norma internazionale i termini "prodotto" o "servizio" si applicano unicamente ai prodotti e servizi destinati ad un cliente o da esso richiesti.

Nota 2 È possibile che i requisiti cogenti siano espressi come requisiti legali.

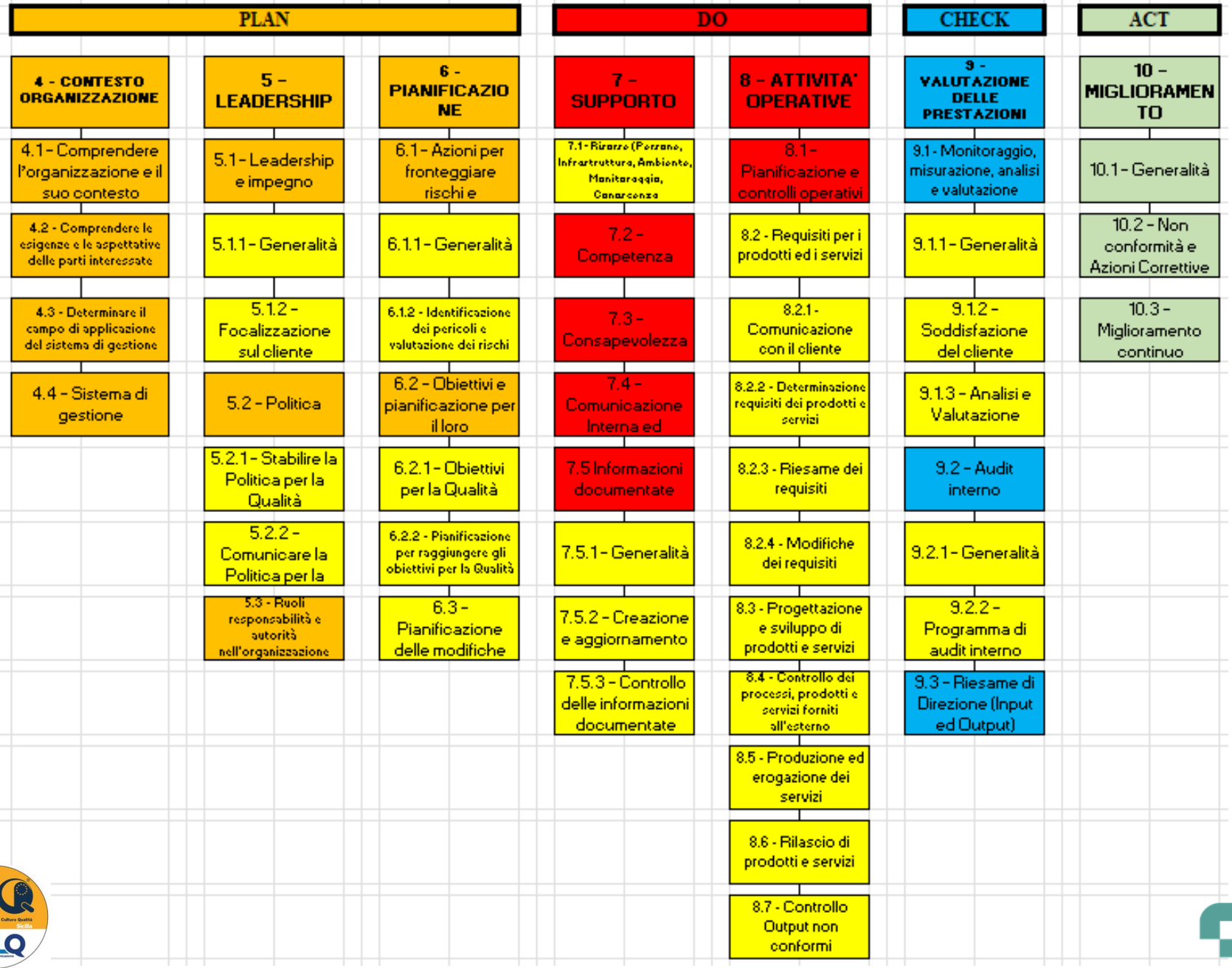
ISO 9001:2015



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO
rAiSK DOMINIO DEL RISCHIO LEGALE
PDCA PLAN DO CHECK ACT

Cenni ai sistemi gestionali ISO

STRUTTURA ISO 9001:2015



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

PDCA

aicq TALQ

rAiSK DOMINIO DEL RISCHIO LEGALE

ISO 14001:2015

1 SCOPO E CAMPO DI APPLICAZIONE

La presente norma internazionale specifica i requisiti di un sistema di gestione ambientale che un'organizzazione può utilizzare per migliorare le proprie prestazioni ambientali. La presente norma internazionale è destinata all'utilizzo da parte di un'organizzazione che cerca di gestire le proprie responsabilità ambientali in un modo sistematico, che contribuisca al pilastro ambientale della sostenibilità.

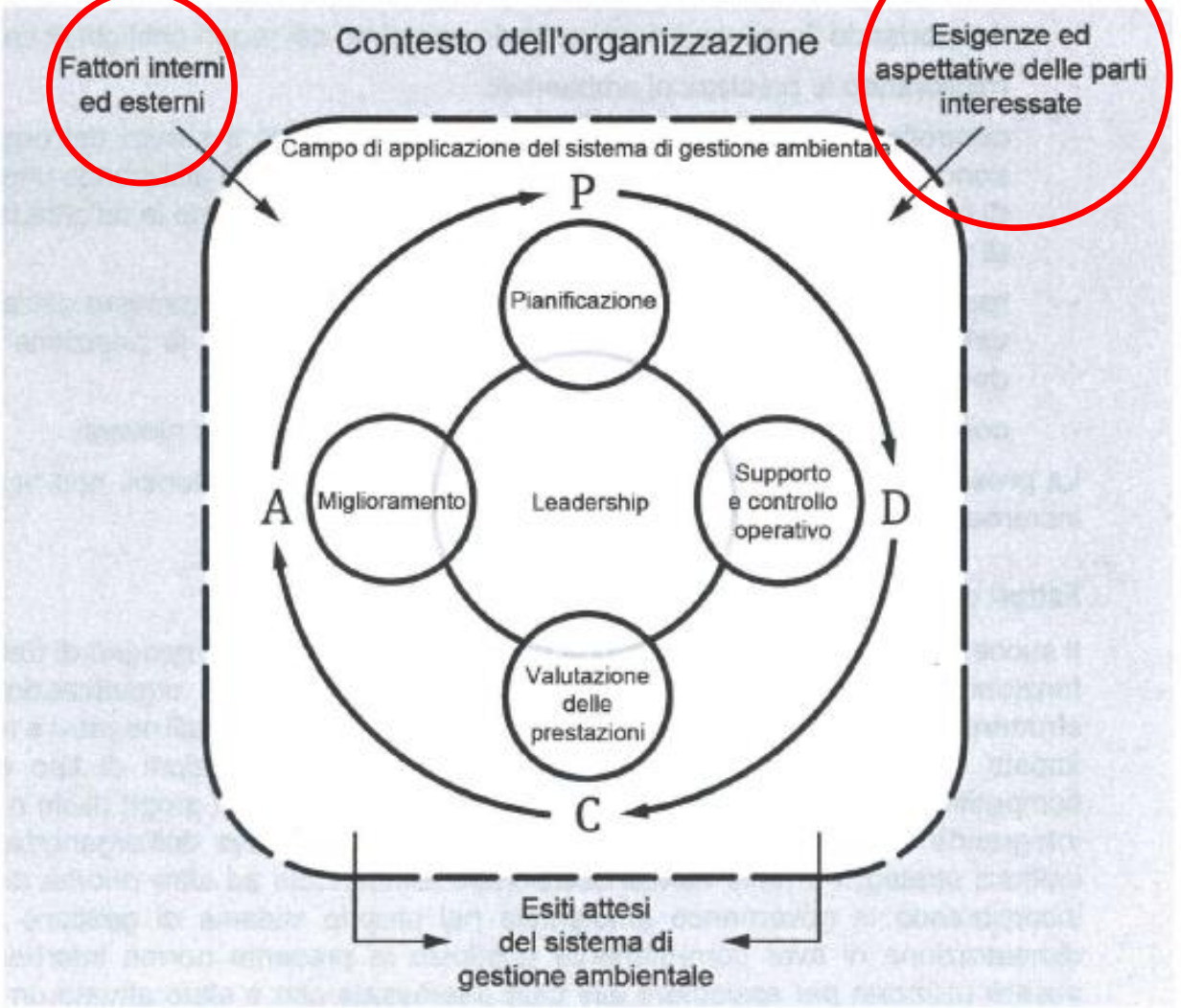
La presente norma internazionale aiuta un'organizzazione a raggiungere gli esiti attesi del proprio sistema di gestione ambientale, che forniscano valore per l'ambiente, per l'organizzazione stessa e per le parti interessate. Coerentemente con la politica ambientale dell'organizzazione, gli esiti attesi di un sistema di gestione ambientale comprendono:

- miglioramento delle prestazioni ambientali;
- soddisfacimento degli obblighi di conformità;
- raggiungimento degli obiettivi ambientali;

Cenni ai sistemi gestionali ISO

ISO 14001:2015

figura 1 **Relazione tra PDCA e il quadro di riferimento nella presente norma internazionale**



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

STRUTTURA ISO 14001:2015

PLAN			DO		CHECK	ACT
4 - CONTESTO ORGANIZZAZIONE	5 – LEADERSHIP	6 – PIANIFICAZIONE	7 – SUPPORTO	8 – ATTIVITA' OPERATIVE	9 - MONITORAGGI E MISURAZIONI	10 – MIGLIORAMENTO
4.1 – Comprendere l'organizzazione e il suo contesto	5.1 – Leadership e impegno	6.1 – Azioni per fronteggiare rischi e	7.1 – Risorse	8.1 – Pianificazione e controlli operativi	9.1 – Monitoraggio, misurazione, analisi e valutazione	10.1 – Generalità
4.2 – Comprendere le esigenze e le aspettative delle parti interessate	5.2 – Politica	6.1.1 – Generalità	7.2 – Competenza	8.2 – Preparazione e risposta alle	9.1.1 – Generalità	10.2 – Non conformità e Azioni Correttive
4.3 – Determinare il campo di applicazione del sistema di gestione ambientale	5.3 – Ruoli responsabilità e autorità nell'organizzazione	6.1.2 – Aspetti ambientali	7.3 – Consapevolezza		9.1.2 – Valutazione della conformità	10.3 – Miglioramento continuo
4.4 – Sistema di gestione Ambientale		6.1.3 – Obblghi di conformità	7.4 – Comunicazione		9.2 – Audit interno	
		6.1.4 – Attività di pianificazione	7.4.1 – Generalità		9.2.1 – Generalità	
		6.2 – Obiettivi e pianificazione per il loro raggiungimento	7.4.2 – Comunicazione interna		9.2.2 – Programma di audit interno	
		6.2.1 – Obiettivi ambientali	7.4.3 – Comunicazione esterna		9.3 – Riesame di Direzione	
		6.2.2 – Attività di pianificazione per raggiungere gli obiettivi ambientali	7.5 Informazioni documentate			
			7.5.1 – Generalità			
			7.5.2 – Creazione e aggiornamento			
			7.5.3 – Controllo delle informazioni documentate			

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

PDCA

rAisk DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

ISO 45001:2018

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento specifica i requisiti per un sistema di gestione per la salute e sicurezza sul lavoro (SSL) e fornisce una guida per il suo utilizzo, al fine di consentire alle organizzazioni di predisporre luoghi di lavoro sicuri e salubri, prevenendo lesioni e malattie correlate al lavoro, nonché migliorando proattivamente le proprie prestazioni in termini di SSL.

Il presente documento è applicabile a qualsiasi organizzazione che desideri istituire, attuare e mantenere un sistema di gestione per la SSL per migliorare la salute e la sicurezza sul lavoro, eliminare i pericoli e minimizzare i rischi per la SSL (incluse carenze del sistema), cogliere le opportunità per la SSL e prendere in carico le non conformità del sistema di gestione per la SSL associate alle proprie attività.

Il presente documento facilita l'organizzazione nel raggiungimento dei risultati attesi del suo sistema di gestione per la SSL. In coerenza con la politica per la SSL dell'organizzazione, i risultati attesi di un sistema di gestione per la SSL includono:

a) miglioramento continuo delle prestazioni in termini di SSL;

b) soddisfacimento dei requisiti legali e di altri requisiti;

c) raggiungimento degli obiettivi per la SSL.

Il presente documento è applicabile a qualsiasi organizzazione indipendentemente dalle sue dimensioni, tipo e attività. È applicabile ai rischi per la SSL sotto il controllo dell'organizzazione, tenendo conto di fattori come il contesto in cui opera l'organizzazione e le esigenze e le aspettative dei suoi lavoratori e di altre parti interessate.

Il presente documento non stabilisce criteri specifici per le prestazioni in termini di SSL, né è prescrittivo in merito alla progettazione di un sistema di gestione per la SSL.

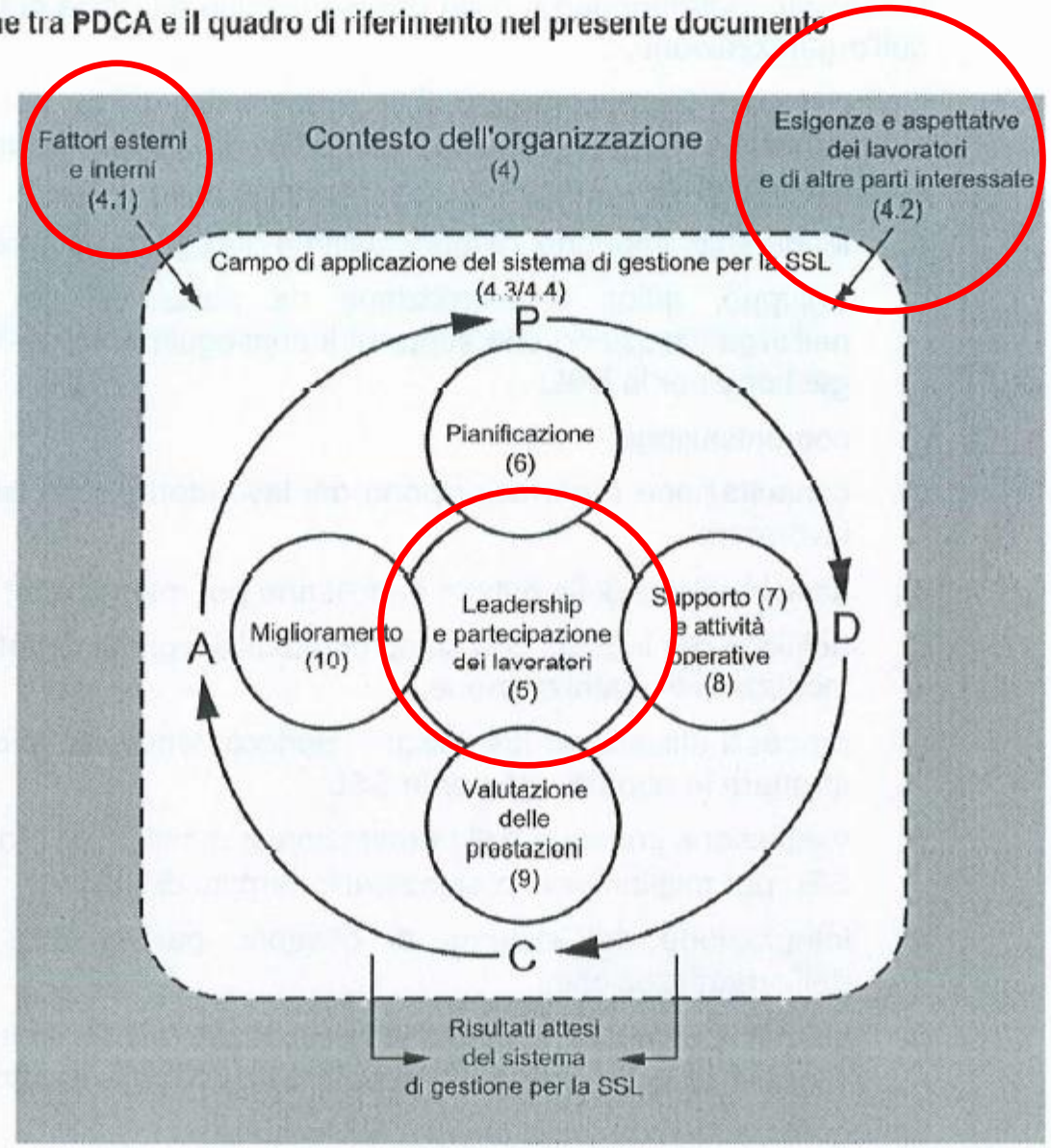
Il presente documento consente ad un'organizzazione, attraverso il suo sistema di gestione per la SSL, di integrare altri aspetti della salute e della sicurezza, come il benessere e la qualità della vita dei lavoratori.

Il presente documento non riguarda tematiche come la sicurezza dei prodotti, danni alla proprietà o impatti ambientali, a meno che non comportino rischi per i lavoratori e altre parti interessate pertinenti.

Il presente documento può essere utilizzato, in tutto o in parte, per migliorare in modo sistematico la gestione della salute e della sicurezza. Tuttavia, le dichiarazioni di conformità al presente documento non sono accettabili a meno che tutti i requisiti della norma non siano incorporati in un sistema di gestione per la SSL di una organizzazione e soddisfatti senza esclusioni.

ISO 45001:2018

figura 1 **Relazione tra PDCA e il quadro di riferimento nel presente documento**



Nota I numeri indicati tra parentesi si riferiscono ai numeri dei punti del presente documento.

Cenni ai sistemi gestionali ISO

STRUTTURA ISO 45001:2018

PLAN			DO		CHECK	ACT
4 - CONTESTO ORGANIZZAZIONE	5 - LEADERSHIP	6 - PIANIFICAZIONE	7 - SUPPORTO	8 - ATTIVITA' OPERATIVE	9 - VALUTAZIONE DELLE PRESTAZIONI	10 - MIGLIORAMENTO
4.1 - Comprendere l'organizzazione e il suo contesto	5.1 - Leadership e impegno	6.1 - Azioni per fronteggiare rischi e	7.1 - Risorse	8.1 - Pianificazione e controlli	9.1 - Monitoraggio, misurazione, analisi e valutazione	10.1 - Generalità
4.2 - Comprendere le esigenze e le aspettative delle parti interessate	5.2 - Politica	6.1.1 - Generalità	7.2 - Competenza	8.1.1 - Generalità	9.1.1 - Generalità	10.2 - Incidenti, Non conformità e Azioni
4.3 - Determinare il campo di applicazione del sistema di gestione	5.3 - Ruoli responsabilità e autorità	6.1.2 - Identificazione dei pericoli e valutazione dei rischi	7.3 - Consapevolezza	8.1.2 - Eliminazione dei pericoli e riduzione dei rischi	9.1.2 - Valutazione della conformità	10.3 - Miglioramento continuo
4.4 - Sistema di gestione	5.4 - Consultazione e partecipazione dei lavoratori	6.1.3 - Determinazione dei requisiti legali e altri requisiti	7.4 - Comunicazione	8.1.3 - Gestione del cambiamento	9.2 - Audit interno	
		6.1.4 - Attività di pianificazione	7.4.1 - Generalità	8.1.4 - Procurement	9.2.1 - Generalità	
		6.2 - Obiettivi e pianificazione per il loro raggiungimento	7.4.2 - Comunicazione interna	8.2 - Preparazione e risposta alle emergenze	9.2.2 - Programma di audit interno	
		6.2.1 - Obiettivi per la SSL	7.4.3 - Comunicazione esterna		9.3 - Riesame di Direzione	
		6.2.2 - Pianificazione per raggiungere gli obiettivi per la SSL	7.5 Informazioni documentate			
			7.5.1 - Generalità			
			7.5.2 - Creazione e aggiornamento			
			7.5.3 - Controllo delle informazioni			

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

PDCA

rAiSK DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

SISTEMA INTEGRATO ITALTEL QHSE

- In Italtel il primo sistema integrato è stato realizzato con riferimento agli schemi ISO 9001:2015, ISO 14001:2015 ed ISO 45001:2018.
- Si è partiti da una nuova politica integrata per i tre schemi che è pubblicata sul sito aziendale al seguente link: Politica-Integrata-QHSE_ITA_signed.pdf .
- Anche l'analisi del contesto dell'organizzazione è stata unificata per i tre schemi individuando le parti interessate a volte comuni ed a volte tipiche di ciascuno schema
- Ciò ha consentito di analizzare i processi primari e di supporto coinvolti nei tre schemi da più punti di vista al fine di perseguire lo scopo di ciascuno schema.
- E' stata anche ottimizzata la redazione delle check list sugli obblighi legislativi cogenti soprattutto per i due schemi 14001 e 45001
- I certificati sono stati emessi dall'ente di parte terza separatamente per ciascuno schema, sono disponibili sul sito di Accredia ed anche sul sito aziendale dell'Italtel al seguente link: Certificazioni & Policies - Italtel

INTERNATIONAL STANDARD ISO/IEC 27001:2022(E)

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

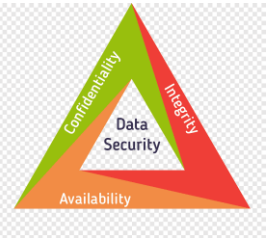
Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

PILLOLE SULLA NORMA ISO/IEC 27001:2022
CLASSIFICAZIONE DELLE INFORMAZIONI

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

ISO 27001:2022 è una norma internazionale che definisce i requisiti per costruire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni (ISMS-SGSI). **Lo scopo** principale della norma è proteggere la **riservatezza, l'integrità e la disponibilità (RID) delle informazioni all'interno dell'intera organizzazione o di un ambito specifico della stessa**.

Il Triangolo della sicurezza delle informazioni



TASSONOMIA DI CLASSIFICAZIONE

Il sistema di classificazione delle informazioni, tipicamente si basa su quattro livelli di riservatezza: **Public, Internal, Confidential StrictlyConfidential**. Questa struttura ha lo scopo di proteggere i dati aziendali e garantire che ogni informazione sia trattata con il livello di sicurezza adeguato, limitando l'accesso solo a chi realmente necessita di conoscerla. Ogni livello ha precauzioni specifiche e i potenziali rischi aumentano con il crescere della sensibilità delle informazioni.

rAisk DOMINIO DEL RISCHIO LEGALE

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

ESEMPI DI ETICHETTATURA DEI DOCUMENTI IN FORMATO ELETTRONICO –

RICHIEDE LA PERSONALIZZAZIONE DEI SOFTWARE SECONDO LE ESIGENZE DELL'ORGANIZZAZIONE.

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

- ✓ **Public** è l'etichetta di un file non crittografato che può essere letto e/o modificato liberamente da chiunque.
- ✓ **Internal** è l'etichetta dei documenti riservati all'uso interno, i documenti devono essere crittografati e non accessibili all'esterno dell'organizzazione.
- ✓ **Confidential/Riservato** qui si possono avere due etichette:
  - ✓ Any User - no encryption si tratta di dati di uso interno ma che in virtù del principio del " need to know " possono essere resi leggibili anche all'estero (clienti, fornitori, auditor …); questi documenti non devono essere condivisi su canali pubblici.
  - ✓ Any User - encryption riservati a team specifici o funzioni aziendali selezionate, devono essere crittografati; questi documenti non devono essere condivisi su canali pubblici.
- ✓ **StrictlyConfidential/Strettamente Riservato** La condivisione è limitata a pochi individui strettamente autorizzati, devono essere crittografati e può essere richiesta la firma di un NDA per accedere a queste informazioni; questi documenti non devono essere condivisi su canali pubblici.

rAisk DOMINIO DEL RISCHIO LEGALE

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

MODALITA' DI DEFINIZIONE DEI DOCUMENTI ITALTEL

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

Italtel

PUBLIC DOCUMENT / INTERNAL DOCUMENT / CONFIDENTIAL DOCUMENT / STRICTLY CONFIDENTIAL DOCUMENT *[keep the appropriate level of confidentiality only]*

Lorem Ipsum Docet Magna Semper Summa Title Document

Sottotitolo

Codice	
Data di emissione	
Edizione	
Classe di Riservatezza	
Scopo del documento	
Distribuzione	
Canale di comunicazione	
Riferimenti	
Proprietario dei contenuti	
Verificatore	
Approvatore	
Registro dei cambiamenti	

rAisk DOMINIO DEL RISCHIO LEGALE

Confidentiality Integrity Data Security Availability

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

MODALITA' DI DEFINIZIONE DEI DOCUMENTI ITALTEL

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

Italtel

Struttura del Sistema Documentale e Responsabilità di Italtel S.p.A.

Codice	PR-I-00120
Data di emissione	26.11.2025
Edizione	3
Classe di Riservatezza	Documento Interno
Scopo del documento	Descrivere la struttura documentale di Italtel S.p.A, specificando per ciascuna tipologia di documento responsabilità delle funzioni aziendali coinvolte, canali di pubblicazione e comunicazione, conservazione e revisione periodica.
Distribuzione	Tutto il personale di Italtel S.p.A.
Canale di comunicazione	ed intranet aziendale.
Riferimenti	Disposizioni organizzative in vigore PR-I-00109: "Classificazione di riservatezza delle informazioni" PR-I-00102 "Gestione delle Informazioni Documentate", UNI EN ISO 9000:2015 "Sistemi di gestione per la qualità – Fondamenti e vocabolario"
Proprietario dei contenuti	Human Resources & Organization – Organization Development, Internal Audit & Compliance – ISO Certifications
Verificatore	Giuliana Lerro, *Organization Development*
Approvatore	Michele Saracino, *Human Resources & Organization* Lorenzo Priolo, *Internal Audit & Compliance*
Registro dei cambiamenti	Inserito riferimento al gestionale dei documenti Hyperdoc che ha sostituito Docsweb, ed al significato delle date utilizzate al suo interno.

rAisk DOMINIO DEL RISCHIO LEGALE

Confidentiality Integrity Data Security Availability

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

PILLOLE SULLA NORMA ISO/IEC 27001:2022 **SOA E BIA**

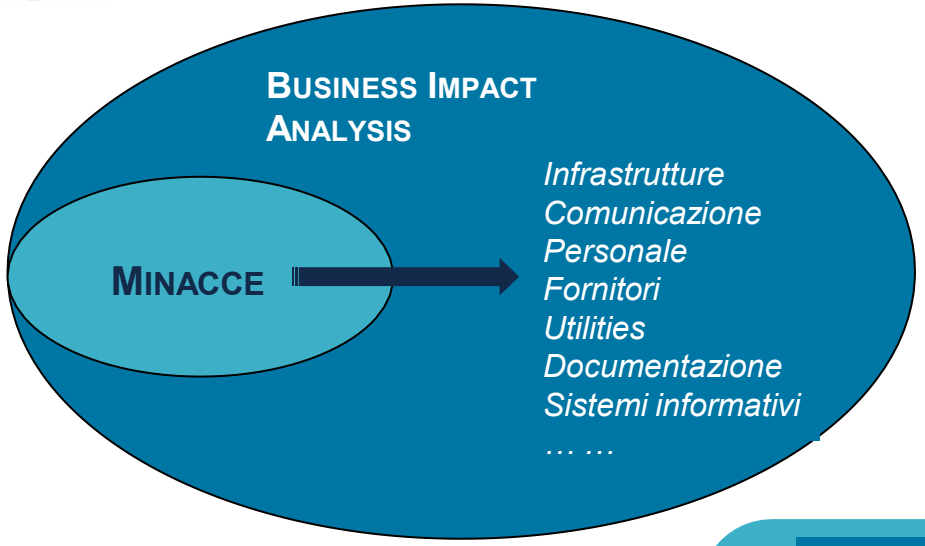
Il punto 6.1.3 individua come requisito mandatorio " shall " la redazione della **SOA** (Statement of Applicability) dei **controlli indicati nell'Appendice A**. La SOA viene redatta sulla base della valutazione dei rischi e dei requisiti di sicurezza dell'organizzazione ed **elenca tutti i controlli (93) di sicurezza delle informazioni previsti**. Nella SOA va evidenziata la motivazione secondo la quale taluni controlli sono applicabili e quali non lo sono; inoltre va anche inserita una descrizione di come i controlli applicabili sono stati implementati o sono pianificati per essere implementati. **L'edizione e la data della SOA viene indicata nel certificato**.

L'organizzazione deve pianificare come mantenere la sicurezza delle informazioni a un livello adeguato durante le interruzioni e/o crisi della sicurezza delle informazioni. Si deve redigere una **BIA** (Business Impact Analysis). La BIA consiste nell'identificare le funzioni aziendali critiche per la continuità operativa dell'organizzazione; queste funzioni devono essere documentate e valutate in termini di importanza strategica e operativa. Si deve valutare l'**impatto** potenziale delle interruzioni (**incidenti sulla sicurezza delle informazioni**) in termini dei costi, delle perdite di produttività, delle implicazioni legali e della reputazione dell'organizzazione. Si devono stabilire le **risorse** umane, tecnologiche e finanziarie prioritariamente necessarie per il ripristino delle condizioni normali di operatività. Quindi si devono definire **i tempi di ripristino** accettabili per ciascuna funzione critica. Questo garantisce che l'organizzazione possa riprendere le operazioni il più rapidamente possibile in caso di interruzione => E' utile un **BCP** (Business Continuity Plan). Nuova figura aziendale importante è il **CISO** (Chief Information Security Officer) che si interfaccia, ad esempio nei casi di Data Breach, con il **DPO** (Data Protection Officer)

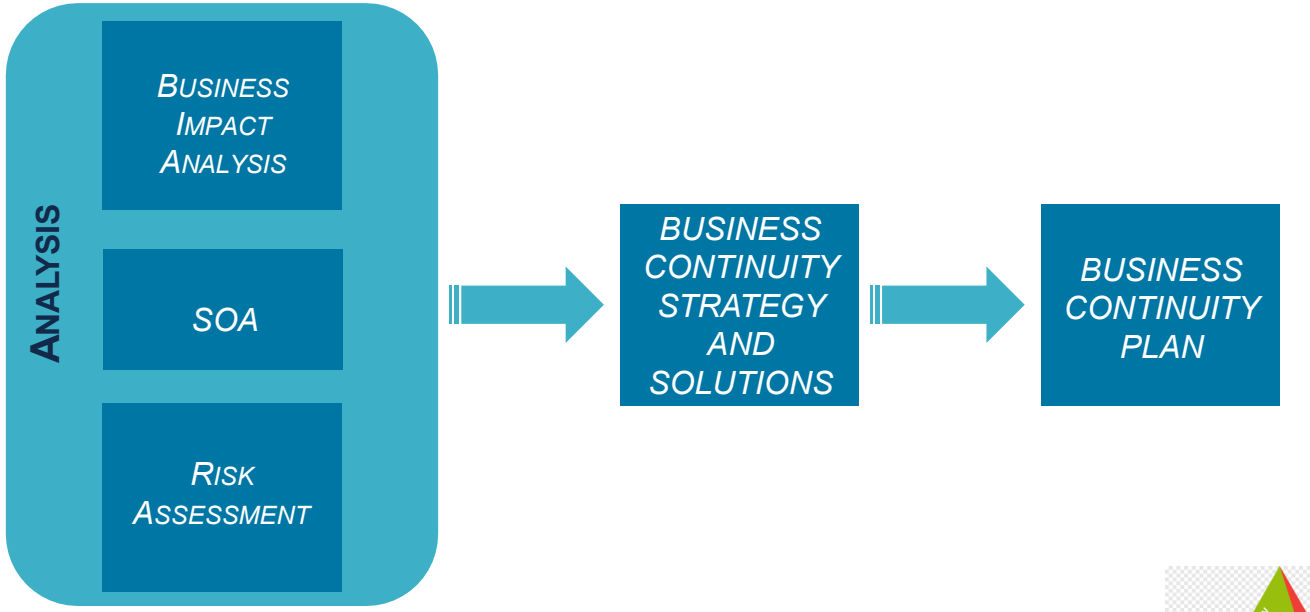
Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

PILLOLE SULLA NORMA ISO/IEC 27001:2022
SICUREZZA DELLE INFORMAZIONI

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO



La norma ISO 31000:2018 è una linea guida per il "Risk Management" che può essere utilizzata da qualsiasi organizzazione



rAisk
DOMINIO DEL RISCHIO LEGALE

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

STRUTTURA NORMA ISO 27001:2022
SISTEMA SICUREZZA DELLE INFORMAZIONI (SGSI)

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

PLAN			DO		CHECK	ACT
4 - CONTESTO DELLA ORGANIZZAZION	5 - LEADERSHIP	6 - PIANIFICAZIONE	7 - SUPPORTO	8 - ATTIVITA' OPERATIVE	9 - MONITORAGGI E MISURAZIONI	10 - MIGLIORAMENTO
4.1 - Comprendere l'organizzazione e il suo contesto	5.1 - Leadership e impegno	6.1 - Azioni per fronteggiare rischi e opportunità **(v. controlli Annex A e SOA** :Statement of Applicability)	7.1 - Risorse	8.1 - Pianificazione e controlli operativi	9.1 - Monitoraggio, misurazione, analisi e valutazione	10.1 - Miglioramento continuo
4.2 - Comprendere le esigenze e le aspettative delle parti interessate	5.2 - Politica	6.2 - Information security objectives and plans to achieve them	7.2 - Competenza	8.2 - Information security risk assessment	9.2 - Audit interno	10.2 - Non conformità e azioni correttive
4.3 - Scope of the Information management System	5.3 - Ruoli responsabilità e autorità nell'organizzazione	6.3 - Pianificazione delle modifiche	7.3 - Consapevolezza	8.3 - Information security risk treatment	9.3 - Riesame di Direzione	
4.4 - Information Management System			7.4 - Comunicazione			
			7.5 Informazioni documentate			

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento specifica i requisiti per attuare, mantenere e migliorare un sistema di gestione per proteggere l'organizzazione da interruzioni, ridurre la probabilità che si verifichino, prepararsi, rispondere e riprendersi dalle stesse quando accadono.

I requisiti specificati nel presente documento sono generici e sono destinati ad essere applicabili a tutte le organizzazioni, o a parti di esse, indipendentemente dal tipo, dalle dimensioni e dalla natura dell'organizzazione. La portata dell'applicazione di questi requisiti dipende dall'ambiente operativo e dalla complessità dell'organizzazione.

Il presente documento è applicabile a tutti i tipi e dimensioni di organizzazioni che:

a) attuano, mantengono e migliorano un BCMS;

b) cercano di garantire la conformità con la politica per la continuità operativa dichiarata;

c) hanno la necessità di essere in grado di continuare a fornire prodotti e servizi ad una capacità predefinita accettabile durante un'interruzione;

d) cercano di migliorare la loro resilienza attraverso l'effettiva applicazione del BCMS.

Il presente documento può essere utilizzato per valutare la capacità di un'organizzazione di soddisfare le proprie esigenze e obblighi per la continuità operativa.

PILLOLE SULLA NORMA ISO/IEC 22301:2019
LINEE GUIDA

ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI PALERMO

- ✓ **Oltre ai parametri tipici della BIA utili a definire i tempi di ripristino accettabili dal punto di vista della 27001, nella 22301 si aggiunge un altro parametro:**

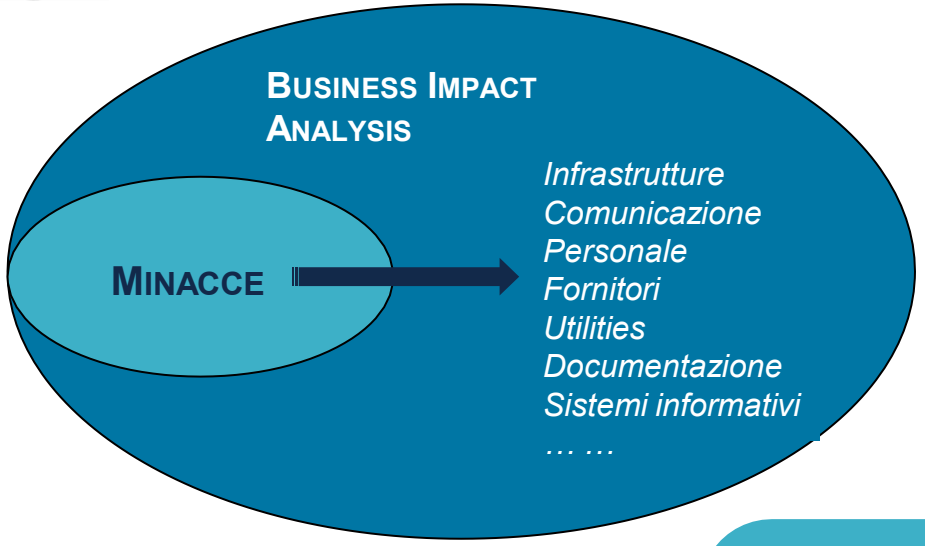
- ✓ **Minimum Business Continuity Objective** (MBCO), che indica il livello minimo di servizio che deve essere mantenuto a fronte di una interruzione o una degradazione delle prestazioni del servizio stesso. Questo è un fattore esterno quasi sempre di natura contrattuale, o conseguenza di richieste specifiche del cliente o potrebbe anche essere prescritto da una legge specifica.

- ✓ **ISO/IEC 22313** fornisce indicazioni e raccomandazioni per l'applicazione dei requisiti del sistema di gestione della continuità operativa (BCMS) previsti dalla norma ISO 22301

- ✓ Nella BIA vanno inserite le valutazioni sull'interruzione delle operazioni e sul ripristino dei servizi rispettando l'MBCO.

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

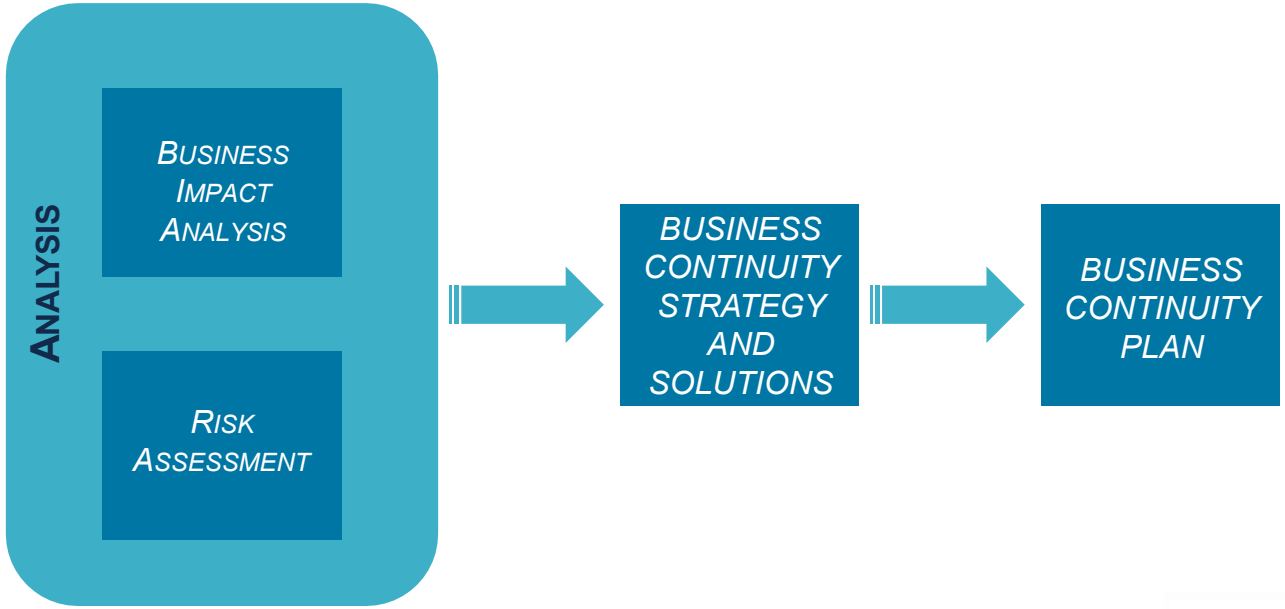
PILLOLE SULLA NORMA ISO/IEC 22301:2019
CONTINUITA' OPERATIVA



La norma ISO 31000:2018 è una linea guida per il "Risk Management" che può essere utilizzata da qualsiasi organizzazione

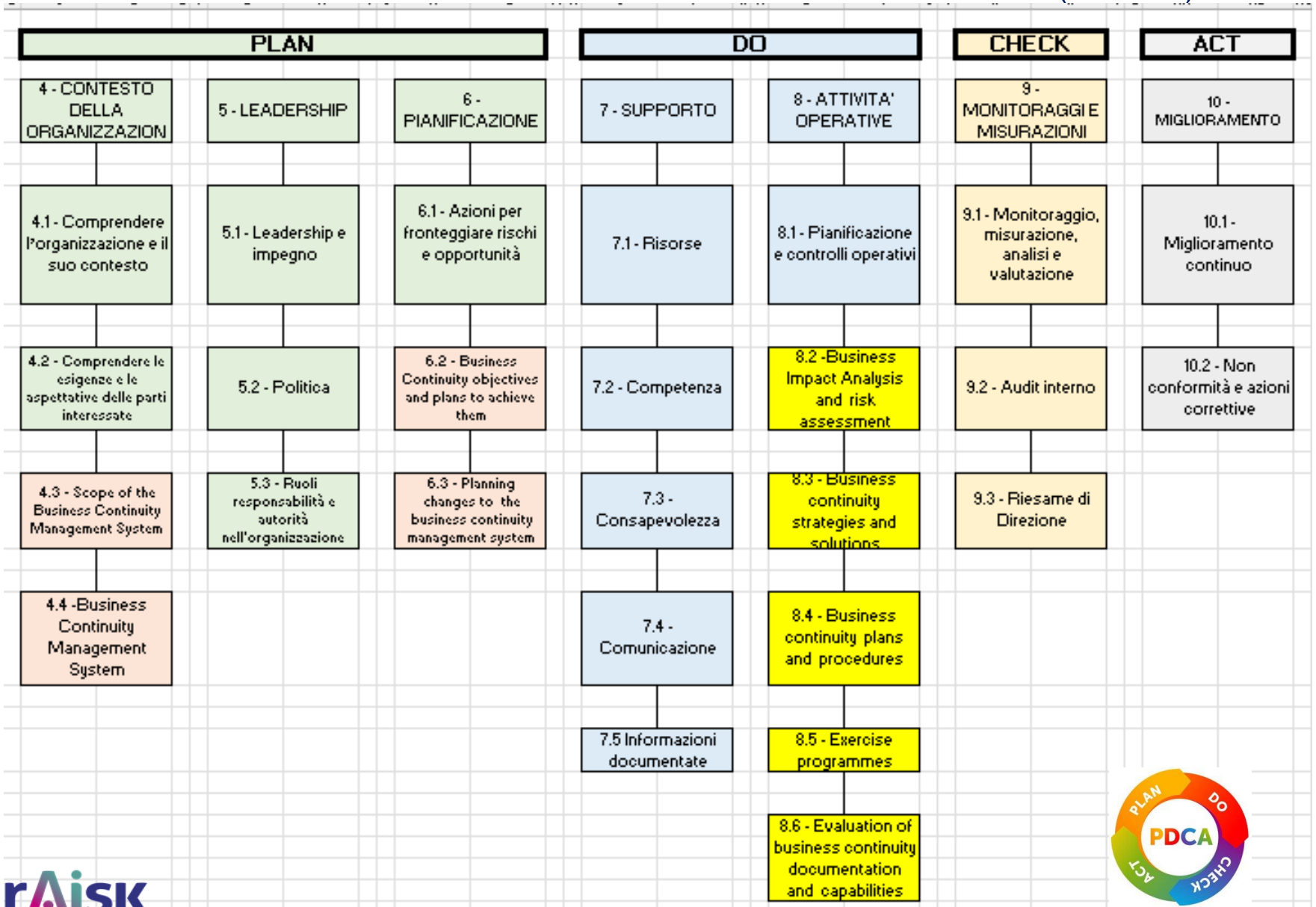
Rispetto alla ISO 27001 manca la SOA

Il focus è sulle minacce che possono provocare interruzione e/o crisi nella disponibilità dei servizi e non più sulla sicurezza delle informazioni



Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

STRUTTURA NORMA ISO 22301:2019
BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

rAisk DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

ISO 20000-1:2018

Information technology — Service management —

Part 1:
Service management system requirements

1 Scope

1.1 General

This document specifies requirements for an organization to establish, implement, maintain and continually improve a service management system (SMS). The requirements specified in this document include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value. This document can be used by:

a) a customer seeking services and requiring assurance regarding the quality of those services;

b) a customer requiring a consistent approach to the service lifecycle by all its service providers, including those in a supply chain;

c) an organization to demonstrate its capability for the planning, design, transition, delivery and improvement of services;

d) an organization to monitor, measure and review its SMS and the services;

e) an organization to improve the planning, design, transition, delivery and improvement of services through effective implementation and operation of an SMS;

f) an organization or other party performing conformity assessments against the requirements specified in this document;

g) a provider of training or advice in service management.

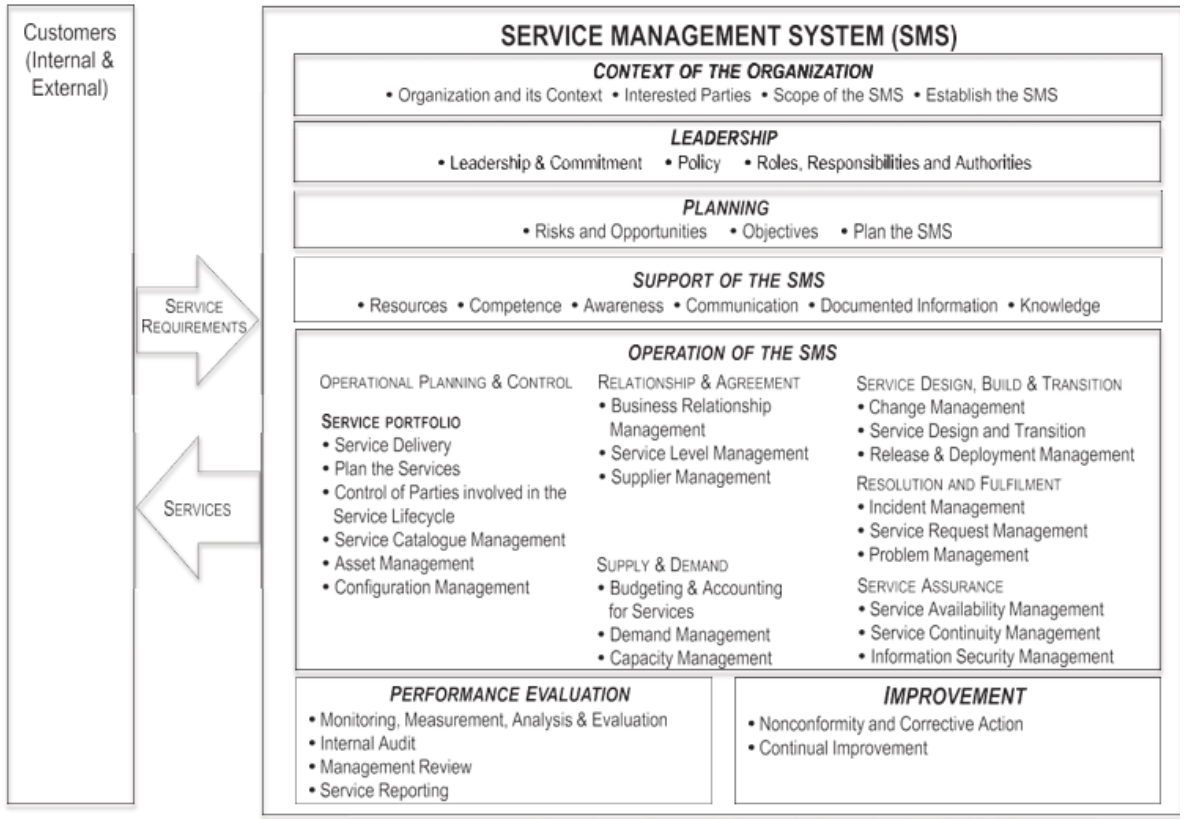
The term "service" as used in this document refers to the service or services in the scope of the SMS. The term "organization" as used in this document refers to the organization in the scope of the SMS that manages and delivers services to customers. The organization in the scope of the SMS can be part of a larger organization, for example, a department of a large corporation. An organization or part of an organization that manages and delivers a service or services to internal or external customers can also be known as a service provider. Any use of the terms "service" or "organization" with a different intent is distinguished clearly in this document.

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

PILLOLE SULLA NORMA ISO/IEC 20000-1:2018
LINEE GUIDA DI RIFERIMENTO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

- ✓ **ISO/IEC 20000-2** fornisce indicazioni sull'applicazione di un sistema di gestione dei servizi (SMS) basato su ISO/IEC 20000-1.
- ✓ Va definito un **catalogo dei servizi oggetto di certificazione ed anche un Portfolio**. **Data ed edizione del catalogo sono citate nel certificato**



Figure·1·—·Service·management·system¶

Sistemi gestionali legati alla sicurezza informatica ed alla continuità operativa

STRUTTURA NORMA ISO 20000-1:2018
SERVICE MANAGEMENT SYSTEM (SMS)

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

PLAN			DO		CHECK	ACT
4 - CONTESTO DELLA ORGANIZZAZION	5 - LEADERSHIP	6 - PIANIFICAZIONE	7 - SUPPORTO	8 - ATTIVITA' OPERATIVE	9 - MONITORAGGI E MISURAZIONI	10 - MIGLIORAMENTO
4.1 - Comprendere l'organizzazione e il suo contesto	5.1 - Leadership e impegno	6.1 - Azioni per fronteggiare rischi e opportunità	7.1 - Risorse	8.1 - Pianificazione e controlli operativi	9.1 - Monitoraggio, misurazione, analisi e valutazione	10.1 - Miglioramento continuo
4.2 - Comprendere le esigenze e le aspettative delle parti interessate	5.2 - Politica	6.2 - Service management objectives and plans to achieve them	7.2 - Competenza	8.2 - Service Portfolio	9.2 - Audit interno	10.2 - Non conformità e azioni correttive
4.3 - Scope of the Service Management System	5.3 - Ruoli responsabilità e autorità nell'organizzazione	6.3 - Plan the service management system	7.3 - Consapevolezza	8.3 - Relationship and agreement	9.3 - Riesame di Direzione	
4.4 - Service Management System			7.4 - Comunicazione	8.4 - Supply and demand	9.4 - Service reporting	
			7.5 Informazioni documentate	8.5 - Service design, build and		
			7.6 Knowledge	8.6 - Resolution and fulfillment		
				8.7 - Service assurance		

rAisk
DOMINIO DEL RISCHIO LEGALE

Cenni ai sistemi gestionali ISO

SECONDO SISTEMA INTEGRATO ITALTEL

- In Italtel è stato realizzato un secondo sistema integrato con riferimento agli schemi ISO 20000-1:2018, 22301:2019 e 27001:2022.
- Si è partiti da una nuova politica integrata per i tre schemi che è pubblicata sul sito aziendale al seguente link Politica_Integrata_20000-1_22301_27001_signed.pdf .
- Anche l'analisi del contesto dell'organizzazione è stata unificata per i tre schemi individuando le parti interessate a volte comuni ed a volte peculiari di ciascuno schema
- Ciò ha consentito di analizzare i processi primari e di supporto coinvolti nei tre schemi da più punti di vista al fine di perseguire lo scopo di ciascuno schema.
- Nel sistema integrato eseguita l'analisi dei rischi per SGSI (27001) e per BCMS (22301) questa va anche bene per l'SMS (20000-1).
- La BIA è stata condivisa.
- I certificati sono stati emessi dall'ente di parte terza separatamente per ciascuno schema, sono disponibili sul sito di Accredia ed anche sul sito aziendale dell'Italtel al seguente link: Certificazioni & Policies - Italtel

VANTAGGI DEI SISTEMI INTEGRATI

Si possono condividere ad esempio:

1. Una sola Politica Integrata valida per gli schemi coinvolti
2. L'esame unico del Contesto dell'Organizzazione
3. L'analisi dei processi primari e di supporto dell'Organizzazione
4. L'individuazione della Leadeship dell'Organizzazione
5. Il sistema documentale può essere unico individuando le procedure che sono comuni come ad esempio: "Qualificazione e Monitoraggio dei fornitori", "Modalità di gestione dei programmi e piani di Audit interni e di parte terza", " Gestione delle opportunità di miglioramento e delle non conformità individuando le correzioni e le azioni correttive", etc. …
6. Unico Riesame della Direzione
7. Lo scopo di certificazione potrebbe anche essere unificato ma questo dipende dagli schemi.
8. Alcuni rischi sono in comune (ad esempio il rischio incendio per 14001 e 45001) ed i relativi monitoraggi dei KPI
9. Le check list legislative connesse ad esempio con le tematiche ambientali e di salute e sicurezza nei luoghi di lavoro
10. E così via

VANTAGGI DEI SISTEMI INTEGRATI

Dal punto di vista delle risorse dell'organizzazione impegnate nella gestione dei sistemi gestionali l'utilizzo di un sistema integrato presenta i seguenti vantaggi:

1. Riduzione del numero di Audit interni e di Audit di certificazione e sorveglianza
2. Sinergia nel coinvolgimento delle parti interessate interne nell'analisi dei rischi e delle opportunità e nella valutazione dei KPI connessi con gli obiettivi degli schemi di certificazione ISO.
3. Migliore comunicazione interna delle opportunità/rischi connessi con le attività tipiche delle risorse umane
4. Maggiore consapevolezza all'interno dell'organizzazione del funzionamento dei processi primari e di supporto coinvolti negli schemi ISO
5. Supporto nella qualificazione dell'organizzazione presso clienti e/o nella gestione di contratti offerte e gare ad evidenza pubblica.
6. Etc. …

COSA RIMANE DISTINTO PER SCHEMA DI CERTIFICAZIONE IN UN SISTEMA INTEGRATO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

1. L'ANALISI DEI RISCHI E DELLE OPPORTUNITA' NON PUO' ESSERE COMPLETAMENTE CONDIVISA TRA I VARI SCHEMI. VERRANNO REDATTE MATRICI DI RISCHIO DISTINTE PER SCHEMA.
2. IL CERTIFICATO RILASCIATO DAGLI ENTI DI CERTIFICAZIONE RIMANE SEPARATO PER CIASCUNO SCHEMA.
3. LE PARTI INTERESSATE INTERNE ED ESTERNE SARANNO IN PARTE IN COMUNE MA ALCUNE RIMARRANNO TIPICHE DI OGNI SCHEMA.
4. I REQUISITI MANDATORI PER LEGGE SARANNO IN PARTE IN COMUNE MA ALCUNE RIMARRANNO TIPICHE DI OGNI SCHEMA.

Refluenze dei sistemi gestionali sul Protocollo 231

1. Italtel ha emesso una politica per la prevenzione della corruzione, in conformità alla norma ISO 37001, ed ha realizzato un sistema di gestione per la prevenzione della corruzione certificato ai sensi di quest'ultimo schema.
2. L'Iitaltel agisce quindi nel rispetto della richiamata politica, unitamente al Codice etico della Società, al Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001 e alle vigenti leggi.
3. L'Italtel incoraggia i dipendenti, i collaboratori e tutti coloro che, a qualunque titolo, operano in nome e per conto della stessa a segnalare ogni manifestazione di corruzione, anche presunta in buona fede, utilizzando la piattaforma aziendale whistleblowing (https://www.italtel.com/it/about/whistleblowing).
4. E' stato quindi redatto un «Modello di Organizzazione, Gestione e Controllo» ex Decreto Legislativo 8 giugno 2001 n. 231, l'Organismo di Vigilanza verifica il funzionamento, l'efficacia, l'osservanza e l'aggiornamento del Modello.
5. Esaminando i reati inclusi nel protocollo 231 dell'Italtel sene individuano alcuni che sono correlati con i sistemi gestionali.

Cenni ai sistemi gestionali ISO

Esempi di reati previsti nel Protocollo 231 che hanno una relazione con i sistemi gestionali

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

1. REATI COMMESSI IN VIOLAZIONE DELLE NORME RELATIVE ALLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO => ISO 45001:2018
2. DELITTI INFORMATICI => ISO 27001:2022
3. REATI AMBIENTALI => ISO 14001:2015

NON SOLO QUINDI IL SISTEMA GESTIONALE CONFORME ALLA ISO 37001:2016 MA ANCHE GLI ALTRI SISTEMI GESTIONALI INDUCONO UNA SINERGIA POSITIVA NEL RISPETTO DEL PROTOCOLLO 231 ED UNA MAGGIORE CONSAPEVOLEZZA DA PARTE DI TUTTI I LAVORATORI E DELLE PARTI COINVOLTE.

L'APPLICAZIONE DEI SISTEMI GESTIONALI E DEL MODELLO DEL PROTOCOLLO 231 CHE EFFICACIA ESIMENTE ASSICURA ALL'ORGANIZZAZIONE ?

aicq TALQ

rAisk DOMINIO DEL RISCHIO LEGALE

Vincoli per i professionisti per l'utilizzo dell'Intelligenza Artificiale

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PALERMO

- La legge 23 settembre 2025 n.123 " *Disposizioni in materia di intelligenza Artificiale* "e ed in particolare l'art. 13 prevede l'obbligo di informativa al cliente.
- La circolare del CNI n. 343/XX Sess./2025 ha individuato un modello di dichiarazione a beneficio degli iscritti, per adempiere all'obbligo di legge.
- Detta dichiarazione può essere semplice o sotto forma di dichiarazione sostitutiva dell'atto di notorietà a firma del professionista ed in entrambi i casi prevede che :
  - il professionista dichiara di avvalersi dei sistemi di Intelligenza Artificiale (AI) elencati per lo svolgimento di attività meramente strumentali e di supporto;
  - il lavoro intellettuale del professionista costituisce l'elemento prevalente e fondante della prestazione d'opera resa;
  - il professionista si assume la piena ed esclusiva paternità intellettuale e responsabilità professionale, civile, penale e disciplinare per ogni elaborato, calcolo, relazione, disegno e conclusione forniti al committente nell'ambito del suddetto incarico, indipendentemente dagli strumenti utilizzati per la loro elaborazione.
  - il professionista informa e garantisce al Committente il pieno rispetto della normativa vigente sul trattamento dei dati personali (Reg. UE 2016/679 e d.lgs. n.193/2006), come da specifica informativa.

ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI PALERMO

Bruno Lo Torto

Bruno.Lotorto@gmail.com

https://www.linkedin.com/in/bruno-lo-torto-399b8593/

George Bernard Shaw ha scritto :

«Se tu hai una mela e io ho una mela e ce le scambiamo, abbiamo sempre una mela per uno, ma se tu hai un'idea e io ho un'idea e ce le scambiamo, allora abbiamo entrambi due idee».

Grazie per l'attenzione.

Confidential