

PERCORSO FORMATIVO — AMMINISTRAZIONE, CONTROLLO E AUDITING

Dispensa 8

Audit di Sistemi di Gestione Qualità (ISO 9001/45001/27001)

L'approccio PDCA e la conduzione degli audit di certificazione secondo gli standard internazionali di gestione.

A cura di Marco Consiglio

Formatore e Course Director — Contenuti aggiornati al 2026

Indice

1. Introduzione e obiettivi didattici	3
2. I sistemi di gestione: le basi e la struttura comune (HLS).....	4
3. ISO 9001: il sistema di gestione della qualità.....	6
4. ISO 45001: il sistema di gestione della sicurezza sul lavoro.....	8
5. ISO 27001: il sistema di gestione della sicurezza delle informazioni	10
6. Il percorso di certificazione	12
7. L'audit di certificazione: tipologie e fasi.....	14
8. Come si conduce un audit di sistema	16
9. Non conformità, osservazioni e opportunità di miglioramento	18
10. L'integrazione tra sistemi di gestione.....	19
11. Caso pratico guidato.....	20
12. Glossario dei termini chiave	22
13. Checklist finale e autoverifica	23
14. Riferimenti e risorse aggiornate al 2026.....	24

1. Introduzione e obiettivi didattici

Questa dispensa prosegue il modulo settoriale del percorso, dedicandosi a un ambito che riprende e sviluppa concetti già introdotti nella Dispensa 1 a proposito del modello COSO e degli standard di audit: i sistemi di gestione certificabili secondo le norme internazionali della famiglia ISO, con particolare attenzione a tre standard di grandissima diffusione: ISO 9001 (qualità), ISO 45001 (sicurezza sul lavoro) e ISO 27001 (sicurezza delle informazioni).

Comprendere la logica di questi sistemi di gestione, e le modalità con cui vengono verificati attraverso gli audit di certificazione, è una competenza trasversale preziosa per chiunque operi in ruoli di controllo, qualità o auditing, applicabile a organizzazioni di qualunque settore e dimensione.

A chi si rivolge questa dispensa

Si rivolge a chi desidera comprendere, partendo da zero, la logica dei sistemi di gestione certificati e le modalità con cui vengono condotti gli audit di certificazione, sia per orientarsi all'interno di un'organizzazione che li adotta, sia per avvicinarsi a un ruolo di auditor, interno o presso un organismo di certificazione.

Obiettivi di apprendimento

1. Comprendere la struttura comune (High Level Structure) condivisa dalle principali norme ISO sui sistemi di gestione;
2. Conoscere i principi fondamentali di ISO 9001, ISO 45001 e ISO 27001;
3. Comprendere le fasi del percorso di certificazione e le tipologie di audit associate;
4. Applicare le tecniche di conduzione di un audit di sistema di gestione;
5. Distinguere correttamente non conformità, osservazioni e opportunità di miglioramento;
6. Comprendere la logica dell'integrazione tra più sistemi di gestione.

2. I sistemi di gestione: le basi e la struttura comune (HLS)

Un sistema di gestione è l'insieme organizzato di politiche, processi, procedure e risorse che un'organizzazione adotta per perseguire in modo strutturato e continuativo determinati obiettivi — di qualità, di sicurezza, di protezione delle informazioni, o di altra natura, secondo lo standard di riferimento adottato.

La logica del miglioramento continuo: il ciclo PDCA

Come già accennato nella Dispensa 1 a proposito del processo di audit, tutti i principali sistemi di gestione certificabili si fondano sul ciclo PDCA (Plan-Do-Check-Act, ovvero Pianifica-Fai-Verifica-Agisci), un modello di miglioramento continuo applicabile a qualunque processo organizzativo:

- Plan (Pianifica): si definiscono obiettivi, processi e risorse necessarie;
- Do (Fai): si attuano i processi pianificati;
- Check (Verifica): si monitorano e misurano i risultati rispetto agli obiettivi, anche attraverso audit interni;
- Act (Agisci): si intraprendono azioni per il miglioramento continuo delle performance, sulla base di quanto rilevato in fase di verifica.

La High Level Structure (HLS): un linguaggio comune tra standard diversi

A partire dal decennio 2010, l'organizzazione internazionale di normazione ha adottato una struttura di alto livello comune (High Level Structure, HLS) per tutte le principali norme sui sistemi di gestione, con l'obiettivo di facilitarne l'integrazione all'interno delle organizzazioni che adottano più standard contemporaneamente. Questa struttura comune si articola in dieci capitoli, di cui i più operativamente rilevanti sono:

7. Contesto dell'organizzazione: comprensione dei fattori interni ed esterni rilevanti e delle esigenze delle parti interessate;
8. Leadership: impegno della direzione, definizione della politica e dei ruoli organizzativi;
9. Pianificazione: individuazione di rischi e opportunità, definizione degli obiettivi;
10. Supporto: gestione delle risorse, delle competenze, della documentazione;
11. Attività operative: pianificazione e controllo operativo dei processi;
12. Valutazione delle prestazioni: monitoraggio, misurazione, audit interno, riesame di direzione;
13. Miglioramento: gestione delle non conformità e azioni correttive, miglioramento continuo.

Comprendere la logica della struttura comune è particolarmente utile per chi si occupa di audit: una volta acquisita familiarità con questo schema generale, diventa molto più agevole orientarsi in qualunque standard specifico della famiglia ISO, anche non trattato

direttamente in questa dispensa, poiché l'impalcatura concettuale di fondo rimane sostanzialmente la stessa.

3. ISO 9001: il sistema di gestione della qualità

La norma ISO 9001 è lo standard internazionale più diffuso al mondo per i sistemi di gestione della qualità, applicabile a organizzazioni di qualunque settore e dimensione, con l'obiettivo di garantire la capacità di fornire con continuità prodotti e servizi conformi ai requisiti dei clienti e alle prescrizioni normative applicabili.

I principi di gestione della qualità

ISO 9001 si fonda su alcuni principi di gestione, che è utile conoscere per comprendere lo spirito, oltre che la lettera, dello standard:

- Focalizzazione sul cliente: comprendere e soddisfare le esigenze presenti e future dei clienti;
- Leadership: creare le condizioni affinché le persone siano coinvolte nel conseguimento degli obiettivi;
- Coinvolgimento del personale: valorizzare le competenze delle persone a tutti i livelli dell'organizzazione;
- Approccio per processi: gestire le attività come processi correlati e comprensibili nel loro insieme;
- Miglioramento: mantenere un focus continuativo sul miglioramento delle prestazioni, secondo la logica del ciclo PDCA;
- Processo decisionale basato su evidenze: fondare le decisioni sull'analisi di dati e informazioni oggettive;
- Gestione delle relazioni: gestire in modo efficace i rapporti con fornitori e altre parti interessate.

Il pensiero basato sul rischio (risk-based thinking)

Un elemento importante introdotto nelle versioni più recenti dello standard è il pensiero basato sul rischio: l'organizzazione è chiamata a identificare rischi e opportunità rilevanti per la conformità dei propri prodotti e servizi, pianificando azioni adeguate per affrontarli, secondo una logica coerente con quanto già illustrato nella Dispensa 3 a proposito del risk management.

Gli elementi documentali tipici di un sistema ISO 9001

1. Politica per la qualità: dichiarazione degli intenti e degli indirizzi generali dell'organizzazione in materia di qualità;
2. Obiettivi per la qualità: traguardi misurabili, coerenti con la politica, definiti per le funzioni e i livelli pertinenti;
3. Procedure documentate: descrizione delle modalità operative per i processi ritenuti critici;

4. Registrazioni: evidenze oggettive dell'avvenuto svolgimento delle attività previste (analoghe, per funzione, alle carte di lavoro già illustrate nella Dispensa 1);
5. Riesame di direzione: momento periodico in cui la direzione valuta l'adeguatezza e l'efficacia complessiva del sistema di gestione.

Un errore da evitare

Un fraintendimento comune, specie in organizzazioni che si avvicinano per la prima volta a questi temi, è considerare la certificazione ISO 9001 come una mera certificazione della qualità dei prodotti o servizi offerti. In realtà, lo standard certifica la solidità e l'adeguatezza del sistema di gestione con cui l'organizzazione persegue la qualità, non il livello qualitativo assoluto del prodotto o servizio in sé: un'organizzazione può essere certificata ISO 9001 pur offrendo un prodotto posizionato su una fascia di mercato economica, purché il proprio sistema di gestione sia solido e coerente con gli obiettivi dichiarati.

4. ISO 45001: il sistema di gestione della sicurezza sul lavoro

La norma ISO 45001 è lo standard internazionale di riferimento per i sistemi di gestione della salute e sicurezza sul lavoro (OH&S Management System), che ha sostituito il precedente standard britannico OHSAS 18001, adottando la medesima struttura di alto livello (HLS) già illustrata nel capitolo 2, per facilitarne l'integrazione con ISO 9001 e altri sistemi di gestione.

Gli elementi distintivi di ISO 45001

- Coinvolgimento attivo dei lavoratori nella progettazione e nel miglioramento del sistema di gestione, elemento particolarmente valorizzato rispetto al precedente standard OHSAS;
- Identificazione dei pericoli e valutazione dei rischi per la salute e sicurezza, con un approccio sistematico e documentato;
- Gestione degli obblighi di conformità normativa, in stretto raccordo, nel contesto italiano, con gli adempimenti previsti dalla normativa nazionale in materia di sicurezza sul lavoro;
- Pianificazione e gestione delle emergenze;
- Investigazione degli incidenti, dei near miss (quasi-infortuni) e delle non conformità, con l'obiettivo di prevenire il ripetersi di eventi simili.

Il collegamento con la normativa nazionale italiana

È importante chiarire che la certificazione ISO 45001, pur essendo uno standard internazionale volontario, non sostituisce gli obblighi di legge previsti dalla normativa nazionale in materia di sicurezza sul lavoro, ma li integra all'interno di un sistema di gestione strutturato secondo la logica del miglioramento continuo. Un'organizzazione italiana che intenda certificarsi ISO 45001 deve comunque assolvere a tutti gli obblighi specifici previsti dalla normativa nazionale (documento di valutazione dei rischi, nomina delle figure della sicurezza, sorveglianza sanitaria, formazione dei lavoratori), che costituiscono anzi la base documentale imprescindibile su cui costruire il sistema di gestione certificabile.

I benefici tipici di un sistema ISO 45001 ben implementato

- Riduzione della frequenza e della gravità degli infortuni sul lavoro, attraverso un approccio preventivo strutturato;
- Maggiore consapevolezza e coinvolgimento dei lavoratori sui temi della sicurezza;
- Migliore gestione della conformità normativa, riducendo il rischio di sanzioni;
- In alcuni contesti, accesso a specifiche premialità (ad esempio riduzioni del tasso applicato ai premi assicurativi obbligatori, ove previste dalla normativa vigente).

Per un auditor che si occupa di audit su sistemi ISO 45001, è essenziale possedere anche una solida conoscenza della normativa nazionale sottostante in materia di sicurezza sul lavoro: lo standard internazionale definisce la cornice del sistema di gestione, ma il suo

contenuto sostanziale, in un contesto italiano, si intreccia inevitabilmente con gli obblighi normativi specifici del D.Lgs. 81/2008 e delle relative disposizioni attuative.

5. ISO 27001: il sistema di gestione della sicurezza delle informazioni

La norma ISO 27001 è lo standard internazionale di riferimento per i sistemi di gestione della sicurezza delle informazioni (Information Security Management System, ISMS), particolarmente rilevante in un contesto, come quello attuale, caratterizzato da una crescente esposizione delle organizzazioni a rischi informatici e da obblighi normativi sempre più stringenti in materia di protezione dei dati.

I tre pilastri della sicurezza delle informazioni

ISO 27001 si fonda sulla tutela di tre proprietà fondamentali delle informazioni, spesso indicate con l'acronimo CIA (dall'inglese, da non confondere con altri significati dello stesso acronimo):

- **Confidenzialità (Confidentiality):** garantire che le informazioni siano accessibili solo ai soggetti autorizzati;
- **Integrità (Integrity):** garantire l'accuratezza e la completezza delle informazioni, proteggendole da modifiche non autorizzate;
- **Disponibilità (Availability):** garantire che le informazioni siano accessibili e utilizzabili dai soggetti autorizzati quando necessario.

L'analisi del rischio informativo

Il cuore metodologico di ISO 27001 è un processo strutturato di identificazione, analisi e trattamento dei rischi relativi alla sicurezza delle informazioni, applicando alla materia specifica i principi generali di risk management già illustrati nella Dispensa 3: identificazione degli asset informativi rilevanti, individuazione delle minacce e delle vulnerabilità, valutazione del rischio residuo, definizione dei controlli di sicurezza da implementare.

L'Allegato A e i controlli di sicurezza

Lo standard è accompagnato da un elenco di controlli di sicurezza di riferimento (riportati in un apposito allegato normativo, periodicamente aggiornato), organizzati per macroaree tematiche: controlli organizzativi, controlli relativi alle persone, controlli fisici e controlli tecnologici. L'organizzazione seleziona, in base alla propria analisi del rischio, i controlli effettivamente pertinenti, motivando le eventuali esclusioni attraverso un apposito documento (dichiarazione di applicabilità).

Il collegamento con la normativa sulla protezione dei dati personali

Analogamente a quanto illustrato per ISO 45001 rispetto alla normativa sulla sicurezza sul lavoro, anche ISO 27001 non sostituisce gli obblighi di legge in materia di protezione dei dati personali già accennati nella Dispensa 3, ma può costituire un solido framework organizzativo entro cui strutturare la relativa compliance, offrendo un sistema di gestione riconosciuto

internazionalmente per dimostrare l'adeguatezza delle misure di sicurezza tecniche e organizzative adottate.

Un ambito in forte crescita

La certificazione ISO 27001 ha conosciuto una crescita significativa negli ultimi anni, in ragione della crescente digitalizzazione dei processi organizzativi e della sempre maggiore attenzione — anche da parte di clienti e partner commerciali, che spesso la richiedono come requisito contrattuale — alla sicurezza delle informazioni trattate. Rappresenta quindi un ambito professionale di crescente interesse per chi si specializza in audit di sistemi di gestione.

6. Il percorso di certificazione

Indipendentemente dallo standard specifico considerato, il percorso che conduce un'organizzazione a ottenere e mantenere una certificazione ISO segue tipicamente fasi comuni, che è utile conoscere sia per chi implementa il sistema di gestione, sia per chi ne verifica successivamente la conformità.

Fase 1 — Analisi del contesto e gap analysis

L'organizzazione analizza la propria situazione attuale rispetto ai requisiti dello standard prescelto, individuando le aree da sviluppare o rafforzare, secondo una logica di autovalutazione già incontrata a proposito dell'accreditamento nella Dispensa 5.

Fase 2 — Progettazione e implementazione del sistema di gestione

Vengono sviluppati i documenti di sistema richiesti (politica, procedure, registrazioni), e vengono attuati concretamente i processi previsti, con un periodo di applicazione sul campo sufficiente a generare evidenze oggettive di funzionamento.

Fase 3 — Audit interno e riesame di direzione

Prima di richiedere la certificazione, l'organizzazione deve condurre almeno un ciclo di audit interno sul proprio sistema di gestione, secondo i principi già illustrati nella Dispensa 1, e un riesame di direzione che ne valuti complessivamente l'adeguatezza.

Fase 4 — Selezione dell'organismo di certificazione

L'organizzazione sceglie un organismo di certificazione accreditato, cioè autorizzato da un ente nazionale di accreditamento a rilasciare certificazioni riconosciute secondo lo standard prescelto, verificando la sua competenza specifica nel settore di attività dell'organizzazione.

Fase 5 — Audit di certificazione (Stage 1 e Stage 2)

L'audit di certificazione si articola tipicamente in due momenti distinti, approfonditi nel prossimo capitolo: una verifica documentale preliminare (Stage 1) e una verifica operativa approfondita (Stage 2).

Fase 6 — Rilascio del certificato e sorveglianza periodica

A esito positivo dell'audit, l'organismo di certificazione rilascia il certificato, tipicamente con validità triennale, soggetto a verifiche di sorveglianza periodiche (solitamente annuali) per confermarne il mantenimento, fino a un audit di rinnovo completo alla scadenza del ciclo triennale.

Il percorso di certificazione ricalca, ancora una volta, la stessa logica generale già incontrata più volte in questo percorso formativo: pianificazione, implementazione, verifica

indipendente, e monitoraggio continuativo nel tempo — un filo conduttore che lega tutte le dispense di questo percorso, applicato di volta in volta a contesti specifici diversi.

7. L'audit di certificazione: tipologie e fasi

Approfondiamo ora, in ottica più operativa, la conduzione dell'audit di certificazione, distinguendo le diverse tipologie di audit che un'organizzazione certificata può trovarsi ad affrontare nel corso del tempo.

Le tre tipologie di audit, secondo la classificazione già introdotta nella Dispensa 1

- Audit di prima parte (audit interno): condotto da personale della stessa organizzazione (o da consulenti da essa incaricati), per verificare la conformità del proprio sistema di gestione, in preparazione dell'audit di certificazione o come attività di controllo periodico;
- Audit di seconda parte: condotto da un'organizzazione nei confronti di un proprio fornitore, per verificarne l'adeguatezza rispetto a requisiti contrattuali o di qualificazione;
- Audit di terza parte: condotto dall'organismo di certificazione indipendente, ed è quello che conduce al rilascio o al mantenimento della certificazione.

Lo Stage 1: verifica documentale preliminare

Il primo momento dell'audit di certificazione di terza parte è tipicamente una verifica documentale, finalizzata a valutare se il sistema di gestione documentato dall'organizzazione sia sufficientemente maturo e completo per procedere alla successiva verifica operativa, e a pianificare in dettaglio quest'ultima sulla base delle caratteristiche specifiche dell'organizzazione.

Lo Stage 2: verifica operativa

È la fase centrale dell'audit di certificazione, condotta presso le sedi operative dell'organizzazione, con l'obiettivo di verificare l'effettiva e efficace attuazione del sistema di gestione documentato, attraverso l'osservazione diretta dei processi, interviste al personale a tutti i livelli, ed esame di evidenze oggettive di funzionamento.

Gli audit di sorveglianza e di rinnovo

Dopo il rilascio della certificazione, l'organizzazione è soggetta a verifiche periodiche di sorveglianza (tipicamente annuali), che esaminano un sottoinsieme rappresentativo dei requisiti dello standard, secondo un piano di audit pluriennale che assicuri, nell'arco del ciclo di certificazione, la copertura di tutti gli aspetti rilevanti. Al termine del ciclo triennale, viene condotto un audit di rinnovo, di ampiezza analoga all'audit di certificazione iniziale.

Un principio di indipendenza già incontrato

Coerentemente con i principi di indipendenza già illustrati nella Dispensa 1, gli auditor degli organismi di certificazione devono operare con piena autonomia di giudizio rispetto all'organizzazione certificata, ed è buona prassi che l'organizzazione stessa non affidi la conduzione dei propri audit interni preparatori allo stesso soggetto che effettuerà, o ha effettuato in passato, l'audit di certificazione, per evitare situazioni di autoriesame già segnalate come minaccia all'indipendenza.

8. Come si conduce un audit di sistema

Approfondiamo ora, in chiave operativa, le tecniche concrete con cui un auditor conduce la verifica di un sistema di gestione, integrando quanto già illustrato nella Dispensa 1 con alcuni strumenti specifici degli audit di sistema.

Il piano di audit

Prima della visita, l'auditor (o il team di audit, per organizzazioni più complesse) predispone un piano di audit, che definisce le aree e i processi da esaminare, i tempi dedicati a ciascuna area, e le persone da intervistare, in modo da assicurare una copertura adeguata dell'intero sistema di gestione nel tempo a disposizione.

La tecnica del tracciamento (process approach auditing)

Una tecnica particolarmente efficace, coerente con l'approccio per processi già illustrato a proposito di ISO 9001, consiste nel tracciare un processo dall'inizio alla fine (ad esempio, dall'ordine di un cliente fino alla consegna del prodotto o servizio), verificando in sequenza tutte le fasi intermedie e i relativi controlli, anziché esaminare in modo isolato singoli documenti o singole procedure scollegate tra loro.

Le domande aperte come strumento di indagine

Coerentemente con le tecniche di intervista già accennate nella Dispensa 1, un buon auditor privilegia domande aperte ("Come procedete quando...?", "Che cosa fareste se...?") rispetto a domande chiuse che invitano a una risposta puramente affermativa o negativa, poiché le prime permettono di raccogliere evidenze molto più ricche sull'effettivo funzionamento dei processi, riducendo il rischio di risposte meramente formali.

La verifica dell'evidenza oggettiva

Un principio cardine, già incontrato più volte in questo percorso, è che ogni affermazione raccolta durante l'audit debba essere, per quanto possibile, corroborata da un'evidenza oggettiva verificabile: non è sufficiente che un intervistato dichiari di seguire una determinata procedura, l'auditor dovrebbe sempre cercare di verificarne concretamente l'applicazione, ad esempio attraverso l'esame di registrazioni recenti o l'osservazione diretta dell'attività in corso.

La sintesi giornaliera e la riunione di chiusura

Al termine di ciascuna giornata di audit (per verifiche pluri-giornaliere), è buona prassi condividere con i referenti dell'organizzazione un breve riepilogo delle osservazioni raccolte, per evitare sorprese nella riunione di chiusura finale, in cui l'auditor presenta formalmente l'esito complessivo della verifica, comprensivo delle eventuali non conformità riscontrate, secondo i principi di reporting equilibrato e costruttivo già illustrati nella Dispensa 1.

9. Non conformità, osservazioni e opportunità di miglioramento

Un elemento tecnico particolarmente rilevante negli audit di sistemi di gestione è la corretta classificazione degli esiti riscontrati, secondo categorie standard riconosciute a livello internazionale, la cui comprensione è essenziale per chi si avvicina a questo ambito professionale.

Non conformità maggiore

Si tratta di una carenza significativa, che compromette la capacità del sistema di gestione di raggiungere i risultati previsti, o che riguarda un requisito cogente dello standard totalmente disatteso, oppure un insieme di non conformità minori concentrate sullo stesso processo che, nel loro complesso, ne indicano un malfunzionamento sistemico. Una non conformità maggiore, se non risolta nei tempi previsti, può precludere il rilascio o il mantenimento della certificazione.

Non conformità minore

Si tratta di una carenza puntuale e circoscritta rispetto a un requisito dello standard, che non compromette nel complesso l'efficacia del sistema di gestione, ma richiede comunque un'azione correttiva formale da parte dell'organizzazione, con verifica della relativa efficacia in occasione della successiva visita di audit.

Osservazione

Segnala un'area di potenziale futura criticità, non ancora configurabile come una violazione di un requisito specifico dello standard, ma meritevole di attenzione da parte dell'organizzazione per prevenire l'insorgere di una futura non conformità.

Opportunità di miglioramento

Suggerimento propositivo dell'auditor, non collegato a una carenza rispetto ai requisiti dello standard, ma finalizzato a stimolare un ulteriore miglioramento delle prestazioni del sistema di gestione, secondo la logica di miglioramento continuo che permea l'intero impianto delle norme ISO.

Categoria	Gravità	Conseguenza tipica
Non conformità maggiore	Elevata: compromette l'efficacia del sistema	Blocca il rilascio/mantenimento del certificato fino a risoluzione
Non conformità minore	Media: carenza puntuale e circoscritta	Richiede azione correttiva con verifica successiva
Osservazione	Bassa: area di potenziale criticità futura	Da monitorare, senza obbligo formale immediato

Categoria	Gravità	Conseguenza tipica
Opportunità di miglioramento	Nessuna: suggerimento propositivo	Valutazione facoltativa da parte dell'organizzazione

Saper distinguere correttamente tra queste categorie è una competenza tecnica fondamentale per un auditor di sistemi di gestione: una classificazione troppo severa genera inutile allarme e sfiducia nell'organizzazione verificata, mentre una classificazione troppo indulgente rischia di non innescare le necessarie azioni correttive su criticità realmente significative.

10. L'integrazione tra sistemi di gestione

Come già accennato nel capitolo 2, la struttura di alto livello comune (HLS) condivisa dalle principali norme ISO facilita l'adozione, da parte di una stessa organizzazione, di più sistemi di gestione integrati tra loro (ad esempio qualità, sicurezza sul lavoro e sicurezza delle informazioni), evitando duplicazioni di documentazione e di attività di verifica.

I vantaggi di un sistema di gestione integrato

- Riduzione della duplicazione documentale: politiche, procedure e registrazioni comuni a più standard possono essere unificate in un unico impianto documentale coerente;
- Ottimizzazione degli audit: gli audit interni ed esterni possono essere pianificati e condotti in modo congiunto su più standard, riducendo l'impatto organizzativo delle verifiche;
- Visione unificata dei rischi: un unico processo di risk management può affrontare in modo coordinato rischi di natura diversa (qualità, sicurezza, informazioni), evitando un approccio frammentato per singoli standard;
- Maggiore coerenza culturale: un sistema di gestione integrato comunica con maggiore chiarezza, a tutta l'organizzazione, un approccio unitario al miglioramento continuo, anziché una pluralità di iniziative percepite come scollegate tra loro.

Le cautele nell'integrazione

Pur con i vantaggi illustrati, l'integrazione tra sistemi di gestione richiede attenzione a non appiattire eccessivamente le specificità di ciascuno standard: i requisiti tecnici specifici di ISO 45001 in materia di sicurezza sul lavoro, ad esempio, restano sostanzialmente diversi da quelli di ISO 27001 in materia di sicurezza informatica, e un audit integrato ben condotto deve comunque garantire una copertura adeguata e competente di ciascun ambito specifico, evitando superficialità dovute a un eccesso di generalizzazione.

Per un auditor, operare su sistemi di gestione integrati richiede competenze multidisciplinari, o quantomeno la capacità di riconoscere i propri limiti di competenza tecnica specifica e di avvalersi, quando necessario, di specialisti per gli aspetti più tecnici di ciascuno standard, secondo il principio di competenza professionale già richiamato nella Dispensa 1 a proposito dell'etica dell'auditor.

11. Caso pratico guidato

Concludiamo la parte teorica con un caso pratico semplificato, che applica gli strumenti presentati in questa dispensa a una situazione concreta.

Il contesto

Un'azienda manifatturiera di medie dimensioni, già certificata ISO 9001 da diversi anni, decide di estendere il proprio sistema di gestione integrato anche a ISO 45001, a seguito di un piano di investimento in nuovi macchinari che ha reso necessaria una revisione complessiva delle procedure di sicurezza.

Passo 1 — Gap analysis

Un consulente esterno conduce una gap analysis rispetto ai requisiti di ISO 45001, evidenziando che gran parte della documentazione di sicurezza già esistente per obbligo di legge (documento di valutazione dei rischi, procedure di emergenza) può essere valorizzata all'interno del nuovo sistema di gestione, con integrazioni relative soprattutto al coinvolgimento strutturato dei lavoratori e alla gestione sistematica dei near miss.

Passo 2 — Implementazione e primo ciclo di audit interno

Dopo un periodo di implementazione di circa sei mesi, viene condotto un primo ciclo di audit interno integrato (qualità e sicurezza), che utilizza un'unica checklist strutturata secondo la logica della High Level Structure comune, riducendo significativamente il tempo complessivo dedicato alle verifiche rispetto a due audit separati.

Passo 3 — Audit di certificazione Stage 1 e Stage 2

L'organismo di certificazione conduce lo Stage 1, verificando la maturità documentale del nuovo sistema ISO 45001, seguito a distanza di alcune settimane dallo Stage 2, condotto con la tecnica del tracciamento dei processi già illustrata nel capitolo 8, seguendo ad esempio l'intero percorso di gestione di un intervento di manutenzione su uno dei nuovi macchinari, dalla valutazione del rischio specifico fino alla chiusura dell'intervento.

Passo 4 — Gestione delle non conformità riscontrate

L'audit evidenzia una non conformità minore, relativa alla mancata formalizzazione di un piano di coinvolgimento periodico dei lavoratori nella revisione delle procedure di sicurezza, e un'osservazione relativa alla necessità di rafforzare la formazione specifica sui nuovi macchinari per il personale di recente assunzione. L'azienda predispone un piano di azioni correttive, con responsabili e scadenze definite, secondo lo schema già illustrato nella Dispensa 1.

Passo 5 — Rilascio della certificazione e pianificazione della sorveglianza

A seguito della verifica di efficacia delle azioni correttive, l'organismo di certificazione rilascia il certificato ISO 45001, integrato con la certificazione ISO 9001 già esistente, pianificando le successive visite di sorveglianza in forma congiunta su entrambi gli standard.

Che cosa insegna questo caso

Il caso mostra come l'integrazione tra sistemi di gestione, se ben pianificata, permetta di valorizzare investimenti già effettuati (in questo caso la documentazione di sicurezza già esistente per obbligo di legge) all'interno di un sistema più ampio e strutturato, ottenendo al contempo efficienze organizzative significative nella gestione degli audit, sia interni sia di certificazione.

12. Glossario dei termini chiave

Come per le dispense precedenti del percorso, riportiamo un glossario di sintesi dei principali termini tecnici introdotti.

Sistema di gestione	Insieme organizzato di politiche, processi e procedure che un'organizzazione adotta per perseguire determinati obiettivi in modo strutturato.
Ciclo PDCA	Modello di miglioramento continuo articolato in quattro fasi: Plan, Do, Check, Act.
High Level Structure (HLS)	Struttura di alto livello comune adottata dalle principali norme ISO sui sistemi di gestione, per facilitarne l'integrazione.
Audit di prima/seconda/terza parte	Classificazione degli audit in base al soggetto che li conduce: l'organizzazione stessa, un cliente verso un fornitore, o un organismo indipendente.
Stage 1 / Stage 2	Le due fasi dell'audit di certificazione: verifica documentale preliminare e verifica operativa approfondita.
Non conformità maggiore/minore	Carenza rispetto a un requisito dello standard, classificata secondo la sua gravità e il suo impatto sull'efficacia del sistema di gestione.
Dichiarazione di applicabilità	Documento previsto da ISO 27001 che motiva la selezione o l'esclusione dei controlli di sicurezza rispetto all'analisi del rischio condotta.
Sistema di gestione integrato	Sistema che unifica, all'interno di un'unica struttura organizzativa, più standard di gestione (ad esempio qualità, sicurezza, informazioni).

13. Checklist finale e autoverifica

Come nelle dispense precedenti, dedichiamo un momento all'autoverifica personale prima di proseguire il percorso.

Domande di autoverifica

6. Sapresti spiegare la logica del ciclo PDCA?
7. Ricordi che cos'è la High Level Structure e a cosa serve?
8. Sapresti indicare i tre pilastri (CIA) della sicurezza delle informazioni secondo ISO 27001?
9. Ricordi la differenza tra Stage 1 e Stage 2 nell'audit di certificazione?
10. Sapresti distinguere una non conformità maggiore da una minore e da un'osservazione?
11. Ricordi almeno tre vantaggi di un sistema di gestione integrato?

Come procedere

Se le risposte sono arrivate con sicurezza, si può proseguire con la Dispensa 9, dedicata all'Audit e Controllo per RSPP/RLS in materia di Sicurezza sul Lavoro, che approfondisce ulteriormente i temi già introdotti a proposito di ISO 45001. In caso di incertezza, si consiglia di rileggere i capitoli corrispondenti.

14. Riferimenti e risorse aggiornate al 2026

Per approfondimenti autonomi, si segnalano le principali fonti di riferimento citate in questa dispensa:

- Norma ISO 9001 — Sistemi di gestione per la qualità, requisiti;
- Norma ISO 45001 — Sistemi di gestione per la salute e sicurezza sul lavoro, requisiti;
- Norma ISO 27001 — Sistemi di gestione della sicurezza delle informazioni, requisiti;
- Organizzazione internazionale di normazione (ISO) — documentazione tecnica e Annex SL relativo alla High Level Structure;
- Enti nazionali di accreditamento, per l'elenco degli organismi di certificazione accreditati;
- Normativa nazionale in materia di sicurezza sul lavoro (D.Lgs. 81/2008) e protezione dei dati personali, per il necessario collegamento con i rispettivi standard ISO.

Chiusura della Dispensa 8

Con questa dispensa prosegue il modulo settoriale del percorso, approfondendo la logica dei sistemi di gestione certificabili secondo gli standard internazionali ISO. Le dispense successive proseguiranno l'esplorazione di altri contesti settoriali specifici del percorso.

Marco Consiglio

Formatore e Course Director — 2026