Il valore del vero audit interno

La nuova norma ISO 9001:2015 ripropone al punto 9.2, praticamente senza modifiche significative rispetto alla precedente edizione della norma, il requisito relativo all'Audit interno. La ISO 9001:2015 probabilmente pone maggiore enfasi sulla necessità di intraprendere tempestivamente le azioni finalizzate al trattamento dei rilievi (correzioni, azioni correttive o quant'altro) e certamente recepisce l'approccio basato sui rischi (*Risk Based Thinking*), per il quale la pianificazione e la conduzione degli audit interni dovrà riflettere la necessità di monitorare più frequentemente e più approfonditamente i processi maggiormente a rischio per il perseguimento degli obiettivi aziendali. Però in questo articolo l'aspetto che vorrei sottolineare è un altro: qual è il valore aggiunto di un "vero" audit interno?

La domanda, forse un po' provocatoria, vuole evidenziare il fatto che gli audit interni "finti" servono a poco, se non a coprire il punto della norma in occasione degli audit dell'ente di certificazione e nulla più.

Ormai lo hanno capito anche gli auditor degli Organismi di Certificazione: numerose aziende – che vivono male il loro sistema qualità – poco prima della visita di sorveglianza o rinnovo della certificazione si ritrovano ad adempiere a questo requisito di norma e per varie ragioni (risparmiare tempo e costi, incompetenza, indisponibilità del personale da auditare, urgenza di sbrigare la pratica…) preferiscono registrare audit interni fasulli – ovvero non svolti realmente – piuttosto che effettuare una vera verifica sulla corretta attuazione dei processi aziendali.

Tale pratica, molto diffusa anche da parte di consulenti compiacenti, spesso non sfugge ad un attento auditor dell'Organismo di Certificazione, che però non può o non vuole infierire sull'azienda, spesso anche per mancanza di evidenze oggettive che possano comprovare la falsità dei rapporti di audit.

In realtà predisporre un rapporto di audit interno fittizio, magari con tanto di check-list compilate, è tempo perso, anche se molti responsabili qualità credono di aver risparmiato tempo (e rogne) rispetto a condurre un vero audit.

Il vero audit, infatti, permette di capire cosa effettivamente viene svolto secondo le regole (procedure, specifiche del cliente, norme, ecc.) e cosa no, se i processi sono condotti in modo efficace e, soprattutto, efficiente, se il personale opera secondo i compiti assegnati e così via.

Certamente non svolgere gli audit e far risultare che tutto va bene talvolta

permette al responsabile qualità o altro auditor incaricato, di evitare conflitti interni con i responsabili dei vari reparti(che così potranno continuare a fare quello che pare a loro) o con soggetti troppo permalosi se qualcuno osa sindacare il loro operato. Ma tutto ciò giova realmente all'azienda?

La Direzione, o meglio l'alta Direzione della norma ISO 9001, preferisce vedere dei rapporti di audit fasulli che sono dei "percorsi netti" pur di liberarsi di torno questo adempimento oppure preferisce sapere quali sono i reali problemi dell'azienda?

Un audit ben fatto, condotto da personale competente e imparziale (ovvero non solo indipendente dai responsabili dei processi verificati, ma anche in grado di giudicare in modo imparziale quello che rileva, senza farsi condizionare da chi ha di fronte) porta del grande valore aggiunto all'azienda, perché permette di capire quali sono i problemi attuali dell'organizzazione e quali potrebbero essere quelli futuri; ad esempio rilevare, durante un audit, che non viene controllato il prodotto acquistato, non registrandone nemmeno le informazioni che ne garantiscono la rintracciabilità, potrebbe portare guai all'azienda in caso di richiesta di risarcimento danni da parte del cliente per prodotto difettoso provocato dal prodotto/servizio acquistato presso il fornitore, impedendo anche di potersi rivalere sul fornitore che ha causato la non conformità. Il vero audit, dunque, tutela l'azienda e permette di fronteggiare possibili rischi di vario genere e natura.

Un audit reale può fornire anche molti spunti di miglioramento, se non altro per il fatto di esaminare i processi insieme al personale operativo che avrebbe l'opportunità di evidenziare possibili migliorie.

Un vero audit permette di rilevare delle anomalie, dei problemi, che poi dovranno essere risolti, affrontandoli in tempi ragionevoli. L'audit finto non rileva i problemi, ma questo non vuol dire che non ci sono!

Un vero audit ha bisogno di molto più tempo da parte dell'auditor e del personale intervistato, ma fornisce valore aggiunto, il finto audit non serve all'azienda, ma solo ad evitare rilievi in fase di verifica di certificazione/sorveglianza o rinnovo.

Spesso il finto audit è figlio di procedure finte: che cosa faccio a fare gli audit se dovrei verificare la conformità a procedure che non segue nessuno perché non rappresentano la realtà aziendale? A volte questo è un altro problema: il sistema di gestione per la qualità non è aderente alla realtà aziendale, dunque così com'è non serve a nulla.

Il vero audit va anche ad investigare sull'efficienza dei processi e sui relativi indicatori. Questi ultimi spesso sono deficitari (carenti o addirittura fasulli) per monitorare i processi e dovrebbero essere messi in discussione dal bravo auditor. Ma

anche quello degli indicatori poco pertinenti, imprecisi e non sistematicamente misurati è un altro problema di molti sistemi qualità.

Tutto questo, però, deve essere capito dalla Direzione, da chi governa l'azienda, dalla proprietà e forse alcuni non lo capiranno mai, ma se tutti coloro che lavorano in questo ambito operassero con l'obiettivo di far risaltare i vantaggi di possedere un vero sistema qualità, forse alcune aziende si farebbero un esame di coscienza e ripenserebbero al loro sistema qualità sotto un'ottica differente. Anche questo sarebbe un valore aggiunto di un vero audit interno.

Le regole applicative della UNI EN ISO 9001:2015

L'adeguamento delle aziende alla norma UNI EN ISO 9001:2015 prosegue a rilento con il solito approccio italiano "qual è la scadenza? Settembre 2018? Bene, cominciamo a pensarci a Giugno 2018 perché poi ci sono le ferie!"

Forse senza sapere che ben difficilmente si riuscirà a migrare in tempo utile, senza perdere la certificazione almeno per qualche mese; se non altro perché gli Organismi di Certificazione non avranno modo di gestire un'elevata mole di adeguamenti negli ultimi mesi del periodo di transizione. Oltre al fatto che se l'adeguamento non viene effettuato in occasione di un rinnovo o di una sorveglianza si spenderà di più.

Ma quali sono i **requisiti aggiuntivi per le aziende italiane** che vogliono recepire questa normativa? Sia in fase di transizione dalla vecchia norma ISO 9001:2008, sia come nuova certificazione di qualità?

Quali sono i contenuti dell'**Appendice C della UNI EN ISO 9001:2015 (versione italiana)** che dovrebbero aiutare le imprese del nostro Paese a recepire nel modo corretto questa norma?

Visto il tenore della nuova norma, infatti, noi italiani abbiamo bisogno di **regole più chiare**, espresse in termini di **obblighi e doveri** ("l'organizzazione DEVE"), senza troppe frasi del tipo "se ritenuto necessario", "quando necessario", "conservare informazioni documentate affinché si possa avere fiducia del fatto che…", "le informazioni documentate che l'organizzazione determina necessarie per…" e così via.

Vediamo sinteticamente quali sono queste regole applicative che dovrebbero agevolare anche il compito dell'auditor dell'Organismo di Certificazione, evitando inutili discussioni su cosa richiede la norma e cosa dovrebbe effettivamente essere presente per dimostrare la conformità del sistema di gestione per la qualità.

1. Se l'organizzazione migra dalla versione 2008 della ISO 9001 avrà un **Manuale Qualità** ed anche se esso non è espressamente richiesto dalla ISO 9001:2015 farà meglio a tenerselo. Naturalmente revisionandolo e rendendolo più snello, evitando inutili ridondanze con le procedure. Perché comunque il Manuale rappresenta il vertice della c.d. "piramide della documentazione", il documento di maggior sintesi che richiama documenti più di dettaglio (è un po' come il "*main program*" che richiama le varie "*subroutine*" dei programmi software). Del resto eliminando il Manuale, comunque dovremo documentare la Politica, i Processi ed altro…. dove li mettiamo se non nel manuale? Le aziende che pensano in futuro di certificarsi secondo la normativa del settore automotive IATF 16949:2016 considerino che tale standard richiede il manuale qualità.
2. Le **procedure** chi ce le ha se le tenga e chi è di nuova certificazione ci pensi bene a non predisporle. L'evoluzione dell'organizzazione aziendale negli ultimi 20-30 anni è andata sempre verso la definizione in forma documentata delle modalità di svolgimento delle attività, per definire regole precise che devono essere seguite da tutti, per evitare il caos ove ciascuno fa quello che gli pare. Se non ci sono procedure e istruzioni documentate nelle aziende italiane non solo si tende ad interpretare i processi in modo "personalizzato", secondo quello che il singolo ritiene meglio, ma i nuovi nell'incarico non hanno modo di imparare a ricoprire il ruolo perché l'addestramento è sempre scarso e non trovano regole scritte precise su cosa fare e cosa non fare. Ovviamente ci sono casi e casi: in determinate situazioni l'operatività è guidata dai sistemi informativi e, pertanto, non è facile portare a termine attività in modo diverso, per cui dettagliare troppo non serve.
3. L'**analisi del contesto dell'organizzazione** e la **valutazione dei rischi** sono da documentare. Infatti se suddette attività devono essere riesaminate periodicamente (ad esempio in occasione del riesame di direzione) come facciamo a ricordarci quello che abbiamo detto sull'argomento un anno o sei mesi fa se non scriviamo nulla? Quale imprenditore o Direttore Generale riesce ad analizzare il contesto interno ed esterno della propria organizzazione, identificare e valutare i rischi oralmente nello stesso modo a distanza di tempo, senza nemmeno tenersi una traccia scritta? Dal momento che poi le azioni pianificate per affrontare rischi ed opportunità devono essere documentate con tanto di responsabilità, tempi e valutazione dell'efficacia che senso ha

documentare le azioni, ma non i rischi che le hanno scaturite?

4. La norma ISO 9001:2015 non richiede più il **Rappresentante della Direzione**, che in molte realtà coincideva con la figura del Responsabile Qualità (ce se diverso dal rappresentante della Direzione non era richiesto neanche prima): non ha nessun senso eliminare il Responsabile Qualità. Alcuni imprenditori che non hanno ben compreso la questione hanno cominciato a dire: "ma allora possiamo eliminare il responsabile qualità, con quello che costa!". In un mondo perfetto nel quale la Qualità è patrimonio di tutti e tutti applicano la norma in modo adeguato il Responsabile Qualità potrebbe effettivamente non servire, ma nelle nostre aziende italiane chi fa e fa fare le cose che servono per mantenere la certificazione senza il Responsabile Qualità? Oggi in molte realtà il Responsabile Qualità non solo svolge più attività di quelle di sua stretta pertinenza, ma costringe gli altri (responsabili di funzione, Direzione ed altri) a fare il loro dovere. Bisognerebbe alzargli lo stipendio, altro che eliminare la figura!
5. La norma prevede che sia l'organizzazione a determinare "cosa è necessario monitorare e misurare", come e quando farlo per ottenere risultati validi. Ora più di prima è necessario identificare **indicatori** pertinenti con gli obiettivi ed in grado di misurare l'efficacia – se non anche l'efficienza – dei processi. Le aziende non pensino che questa libertà possa permettere loro di decidere gli indicatori a loro convenienza: l'aumento di fatturato per il processo commerciale e il numero assoluto delle non conformità per la produzione non sono indicatori sufficienti a misurare suddetti processi e gli obiettivi di nessuna azienda.
6. La norma non prevede più le **azioni preventive**, ma le azioni finalizzate a migliorare l'efficacia e l'efficienza del Sistema e dei suoi processi sono state rinforzate. Le azioni preventive, ovvero quelle azioni finalizzate ad evitare il verificarsi di non conformità potenziali, sono solo un "di cui" delle azioni di miglioramento: chiamiamole così, non solo AP.

In conclusione la norma ISO 9001:2015 deve essere vista con lo spirito giusto dalle aziende italiane, dimenticandosi di quello che è stato fatto in passato, per evitare di buttare via tempo e denaro per un adeguamento forzoso che non porterebbe alcun vantaggio nel tempo all'impresa. Sarà compito anche degli auditor degli Organismi di Certificazione cercare di far capire alle aziende il reale significato di questa norma, ma bisognerà vedere se avranno tempo e voglia per farlo, soprattutto se osteggiati da rappresentanti dell'azienda e consulenti che affermeranno che la norma non richiede un manuale, non richiede delle procedure e non è prescrittiva per tante altre attività. Il rischio, in tal caso, è che l'auditor alzi bandiera bianca e dica "fate un po' quello che volete… se non avete capito voi a cosa servono certe cose…".

A proposito l'Appendice C della UNI ISO 9001:2015 italiana non esiste, ma è meglio far finta che le regola sopra esposte esistano veramente.

Come e quando migrare alla ISO 9001:2015?

Ad oggi sono molte le organizzazioni certificate ISO 9001:2008 che non hanno ancora adeguato il loro sistema di gestione per la qualità alla nuova ISO 9001:2015. Anche se il termine per effettuare il passaggio alla nuova norma è abbastanza lontano (15/09/2018) i tempi per effettuare una migrazione efficace ed efficiente non sono abbondanti per molte imprese, infatti sarebbe opportuno effettuare la migrazione in occasione di un **rinnovo della certificazione** oppure di una **visita di sorveglianza/mantenimento** al fine di contenere i costi di certificazione.

Questo perché in occasione degli audit di rinnovo l'Organismo di Certificazione già deve verificare tutti i processi dell'organizzazione e la documentazione di sistema, dunque i costi aggiuntivi sono minimi, se non addirittura nulli.

Negli audit di sorveglianza richiedere l'adeguamento alla ISO 9001:2015 potrebbe essere un po' più oneroso, ma per quelle organizzazioni che hanno la scadenza del certificato oltre la data limite per l'adeguamento (14 settembre 2018) questa è l'occasione migliore per passare alla nuova norma.

Visto che ormai il 2016 è passato, resta di fatto poco più di un anno e mezzo, ovvero solo una o due visite dell'Organismo di Certificazione – a seconda dei casi – per effettuare il passaggio, che comunque dovrà avvenire durante un audit svolto con congruo anticipo rispetto alla data limite sopra indicata, per consentire all'Ente di sbrigare tutte le pratiche necessarie per il rinnovo del certificato in ISO 9001:2015.

Le organizzazioni che avranno la visita dell'Organismo di Certificazione nella seconda parte dell'anno avranno solo una occasione per rinnovare il loro certificato secondo queste modalità.

Rimandare eccessivamente può portare a costi aggiuntivi, infatti sarebbe necessario richiedere una visita straordinaria nell'estate 2018 (probabilmente prima della chiusura per ferie di agosto) per rinnovare in tempo il certificato, consci del fatto che lasciare scadere il certificato vorrà dire perdere di fatto la certificazione ISO 9001 e, quindi, dover intraprendere l'iter dal principio per

riottenere la certificazione di qualità. In questi casi sicuramente ci sarebbero costi aggiuntivi.

Ma quale sono le ragioni dell'evidente attendismo di molte imprese nell'effettuare il passaggio? Le principali motivazioni possono probabilmente riassumersi nelle seguenti:

- Posticipare i costi di adeguamento (organismo di certificazione, consulenza, impegno interno,…);
- Incertezza sul mantenimento della certificazione oltre la scadenza del certificato;
- Incertezza sul futuro dell'organizzazione;
- Timore sull'impatto dell'adeguamento nell'organizzazione interna.

Sicuramente la prospettiva nel breve termine di molte piccole imprese è sui processi primari essenziali (produzione, commerciale) e viene evitato tutto ciò che porta impegno e costi su altri processi, soprattutto in realtà sottodimensionate in termini di risorse. Evidentemente non è stata adeguatamente compresa la portata di questa norma e del **sistema di gestione per la qualità come reale strumento di gestione**, **di controllo e di miglioramento di tutta l'azienda**. Un po' di paura nell'affrontare un cambiamento normativo non indifferente come quello del 2008 completa il quadro di parecchie organizzazioni.

Le interpretazioni sbagliate sulla nuova norma ISO 9001:2015 non mancano, da quelle eccessivamente "terroristiche" (requisiti molto più difficili da soddisfare) a quelle eccessivamente semplicistiche (si può buttare via il manuale e tutte le procedure ed anche rottamare il responsabile qualità).

Le linee guida UNI-Conforma, la linea guida ISO/TS 9002:2016 da poco pubblicata ed altri documento potrebbero aiutare nella corretta interpretazione dei requisiti.

L'approccio corretto – a mio parere – dovrebbe essere quello di pianificare l'adeguamento per tempo, allocando le risorse necessarie al progetto. Purtroppo molte organizzazioni chiedono e continueranno a chiedere "*quanto costa passare alla nuova norma*?", "*quanto tempo ci si mette?*". A queste domande non c'è una risposta univoca corretta e rivolgersi al tal consulente piuttosto che ad altri solo perché promette costi e tempi inferiori è un grave errore che molti imprenditori commetteranno.

Costi e **tempi** per l'adeguamento dipendono da svariati fattori:

- Il sistema qualità è stato mantenuto aggiornato alla realtà aziendale oppure è obsoleto, modificato solo a fronte di rilievi dell'organismo di certificazione?
- I processi sono adeguatamente descritti oppure sono delineati in modo minimale e generico?
- Vengono sistematicamente calcolati e monitorati indicatori idonei a misurare le

prestazioni dei processi oppure sono gestiti solo pochi indici standard poco aderenti alla realtà aziendale?
- La Direzione vuole semplicemente mantenere il certificato con il minimo sforzo oppure vuole sfruttare questo strumento per tenere sotto controllo l'organizzazione e cercare di migliorare?

Dalle risposte a queste domande si può capire meglio il lavoro che sarà da fare.

Situazioni con organizzazioni vicine alle prime parti delle domande sopra riportate sarebbero difficilmente certificabili secondo la nuova norma ISO 9001:2015, ma probabilmente lo saranno ugualmente ingannando se stesse. Il risparmio di tempi e costi nell'adeguamento potrà essere pagato in futuro mantenendo prassi obsolete e non efficienti, contrarie al vero spirito della norma.

Il tanto vituperato appesantimento della norma sulla certificazione di qualità, soprattutto dal punto di vista documentale, in realtà non esiste, a maggior ragione ora che bisogna "mantenere le informazioni documentate che servono". Il problema che molti detrattori della ISO 9001 non si rendono conto che molte evidenze (informazioni documentate) servono anche a cautelarsi quando qualcosa va storto (gestione dei rischi).

Di fatto molte piccole e medie imprese italiane sono lontane dai principi ispiratori della nuova norma sui sistemi di gestione per la qualità, ma non è detto che per ottenere la certificazione serva essere completamente in linea con essi, il percorso di miglioramento potrebbe essere più lungo, la verifica di passaggio alla ISO 9001:2015 potrebbe evidenziare molti rilievi, ma pian piano le carenze potranno essere eliminate e l'azienda potrà essere condotta su principi di gestione migliori di quelli attuali, secondo standard internazionali riconosciuti.

Operativamente la maggior parte dei sistemi qualità ISO 9001:2008 necessiterà delle seguenti attività:

- **Formazione del personale** sulla norma ISO 9001:2015;
- Identificazione e descrizione del **contesto dell'organizzazione**;
- **Valutazione dei rischi** di business (generali e specifici dei vari processi aziendali), attività che passa attraverso l'identificazione dei rischi, la loro ponderazione e la definizione delle misure da porre in essere per il loro trattamento;
- Revisione della **mappatura dei processi** (il livello di approfondimento dipende dallo stato del sistema qualità esistente);
- Rivalutare l'insieme di indicatori da monitorare (anche in questo caso dipende

da cosa esiste attualmente);
- Revisione della **documentazione del sistema qualità** esistente: sicuramente il manuale qualità andrà per lo meno snellito, procedure e istruzioni saranno da aggiornare per riferimenti obsoleti, per recepire le azioni di trattamento dei rischi, per aggiornarle alla realtà aziendale e migliorarle in ottica di efficacia ed efficienza;
- Sottoporre ad **audit interno** il sistema di gestione per la qualità secondo le prassi abituali;
- Effettuare un **riesame della direzione** sul sistema di gestione per la qualità che recepisca i nuovi elementi.

L'eliminazione di documenti di tipo procedurale e il non tener evidenza documentale di talune attività (analisi del contesto, valutazione dei rischi, …) sono false semplificazioni, adatte solo a chi sa recitare senza leggere il copione, ovvero ad organizzazioni che hanno ben chiaro il proprio contesto organizzativo, i propri rischi, le azioni attuate per mitigarli, le procedure aziendali e tutte le prassi da adottare a tutti i livelli dell'organizzazione.

Le attività da completare potrebbero essere non eccessivamente impegnative e non tutte devono necessariamente essere completate prima della visita di certificazione.

Se in qualche caso l'impegno appare eccessivamente gravoso è perché probabilmente non è stato fatto nulla o quasi negli anni scorsi per mantenersi aggiornati. L'inadeguatezza della gestione attuale rispetto ai requisiti della norma ISO 9001:2015 e l'elevato gap da colmare per raggiungere la conformità con la nuova norma dovrebbe far riflettere la Direzione sul fatto che la gestione aziendale non è andata al passo coi tempi.

Esempi di questa situazione si possono trovare quando:

- risulta difficoltoso correlare strategie, politiche ed obiettivi aziendali;
- risulta estremamente impegnativo individuare e soprattutto calcolare indicatori idonei a misurare gli obiettivi e le prestazioni dei processi in termini di efficacia ed efficienza;
- emergono rischi importanti non adeguatamente gestiti;
- emergono carenze di risorse umane e delle relative competenze necessarie;
- emerge che la conoscenza organizzativa ed il know-how aziendale non è curato e tutelato adeguatamente;
- risultano carenze dal punto di vista tecnologico: hardware e software obsoleti, strumenti inadeguati, ecc.

In tutti questi casi la nuova norma ISO 9001:2015 può rappresentare un **valido strumento e stimolo per migliorare l'efficacia e l'efficienza interna**, molto più che costituire un obbligo certificativo.

Effetti della Brexit sulla PMI

Ormai la Brexit, ovvero l'uscita della Gran Bretagna dalla UE, è ormai fatto certo, anche se i tempi non saranno immediati. Analizziamo, dunque, quali potranno essere gli effetti di questo avvenimento, oserei dire storico, sull'industria italiana che intrattiene rapporti commerciali diretti o indiretti con l'industria britannica.

In particolare, numerose imprese italiane hanno acquisito, soprattutto negli ultimi anni, alcuni clienti del Regno Unito, magari grazie ai **prezzi particolarmente competitivi**, grazie al cambio favorevole per la Sterlina nei confronti dell'Euro.

Ora, però, la Gran Bretagna sta per uscire dall'Unione Europea e si paventano nuovi ostacoli al commercio fra Europa dell'Unione e Regno Unito. Al momento non ci è dato sapere quali e quanti nuovi problemi sorgeranno negli scambi commerciali con la Gran Bretagna, in quanto le regole sono da riscrivere e ciò porterà via un po' di tempo.

Di certo c'è il consistente **calo della quotazione della Sterlina Britannica nei confronti dell'Euro** e ciò se da un lato favorisce il turismo e in generale i viaggi ed i soggiorni di lavoro verso la Gran Bretagna, dall'altro rende meno competitivi i prodotti italiani nei confronti dell'industria britannica. L'effetto si potrà avere non solo per clienti diretti inglesi, ma anche per la fornitura di prodotti a clienti che, a loro volta, forniscono imprese britanniche.

Perdere un 10% nel prezzo percepito dal cliente per un prodotto o per una commessa non è cosa di poco conto! Il cliente potrebbe rivalutare fornitori britannici a discapito dell'attuale fornitore italiano.

Per questo, al fine di **non perdere il cliente**, occorre che le imprese italiane che riforniscono – direttamente o indirettamente – clienti inglesi cerchino di mantenere la propria competitività non abbassando i prezzi per sopperire alla diminuzione di valore della Sterlina, ma puntando su **qualità del prodotto e del servizio**, oltre che sull'organizzazione interna, cercando di **rendere i propri processi più efficienti**. Questo potrebbe essere ottenuto introducendo innovazioni nel processo produttivo, nella progettazione (ove presente) e nei processi di supporto, attraverso il miglioramento delle competenze del personale ed il ricorso a **sistemi informativi più moderni e performanti**, e perché no, ricorrendo anche ad **innovazioni tecnologiche** che rientrano nella sfera della cosiddetta "Industry 4.0".

Ottenere la certificazione ISO 9001 per chi non la possiede oppure migrare il sistema qualità alla ISO 9001:20015 sfruttando le opportunità di miglioramento fornite dalla nuova norma, o magari – per chi opera nel settore automotive – cercare di ottenere la certificazione ISO/TS 16949: queste sono alcune strade da percorrere per cercare di essere più competitivi ed apparire "più forti" nei confronti del cliente britannico che ha fatto della qualità il suo modus operandi ormai da decenni. E se per caso volesse venirci a visitare per fare un audit fornitore (si veda anche l'articolo "Il cliente straniero viene a fare un audit: che fare?") potremmo mostrare le capacità, l'organizzazione e l'affidabilità della nostra azienda.

Come applicare la ISO 9001:2015 – V parte

In questo quintoarticolo vedreno in dettaglio i requisiti del capitolo 9 (Valutazione delle prestazioni) e 10 (Miglioramento) della norma UNI EN ISO 9001:2015 con particolare riguardo alle novità introdotte rispetto alla precedente versione del 2008 ed alle possibili modalità di attuazione dei nuovi requisiti, per il passaggio del sistema di gestione per la qualità ISO 9001:2008 alla ISO 9001:2015.

9 Valutazione delle prestazioni

La sezione 9 della norma si suddivide in tre paragrafi

- 9.1 **Monitoraggio, misurazione, analisi e valutazione**
- 9.2 **Audit interno**
- 9. 3 **Riesame di direzione**

che rappresentano il "cuore" dell'attività di *quality management*, i cui compiti spesso sono completamente demandati alla funzione Qualità delle organizzazioni di medie e piccole dimensioni, sebbene il riesame del sistema rimanga una responsabilità della Direzione stessa.

Il punto 9.1 a sua volta è suddiviso in:

- 9.1.1 **Generalità**: l'organizzazione deve stabilire cosa, quando e come monitorare e misurare per garantire l'efficacia del sistema di gestione ed il soddisfacimento dei requisiti; inoltre deve stabilire come valutare i risultati del monitoraggio e delle misurazioni, conservandone informazioni documentate

come evidenze.
- 9.1.2 **Soddisfazione del cliente**: occorre monitorare la percezione che ha il cliente del rispetto delle sue esigenze ed aspettative, stabilendo metodi e criteri di valutazione dei risultati.
- 9.1.2 **Analisi e valutazione**: occorre analizzare e valutare i dati delle misurazioni e dei monitoraggi effettuati per valutare il raggiungimento degli obiettivi, la conformità dei prodotti, la soddisfazione delle esigenze del cliente, le prestazioni dei fornitori, la corretta attuazione di quanto pianificato, l'efficacia del sistema di gestione e delle azioni intraprese per il miglioramento, nonché per valutare le esigenze di miglioramento.

Anche su questi punti la domanda che ci si deve porre è: «quello che l'organizzazione ha stabilito di implementare è efficace e sufficiente per soddisfare i requisiti della norma?». Anche riguardo all'impiego di metodi statistici la norma offre la possibilità di utilizzarli, non certo l'obbligo.

Sicuramente traspare maggiore enfasi sul monitoraggio e la misurazione dei processi rispetto alle precedenti edizioni della norma ISO 9001, ma sarà sufficiente per imporre alle organizzazioni di adottare sistemi di misurazione e monitoraggio, nonché relativi indicatori, più efficaci e realmente vissuti come essenziali per governare i processi?

Il requisito 9.2 relativo agli **audit interni** (ex verifiche ispettive) non presenta significative differenze rispetto all'edizione del 2008: gli audit devono essere svolti per verificare la conformità alla norma ISO 9001 ed al sistema di gestione per la qualità, nonché l'efficacia dello stesso. Essi devono essere programmati secondo i medesimi criteri esposti in passato, anche con riferimento alla ISO 19011. Per dimostrare che si sono stabiliti requisiti di pianificazione e reporting la stesura o il mantenimento della procedura sulla conduzione degli audit interni è fortemente consigliata, anche se non più obbligatorio.

Occorre forse ribadire che la frequenza degli audit sui processi primari e più critici forse non è opportuno che sia di una sola volta all'anno, come per i processi secondari o di supporto. L'abitudine di molte organizzazioni di effettuare un solo audit completo poco prima che arrivi l'Ente di Certificazione non è proprio in linea con lo spirito della norma.

Nessuna novità rispetto al requisito di imparzialità ed indipendenza dell'auditor; piuttosto si enfatizza il fatto che correzioni e/o azioni correttive conseguenti ai rilievi dell'audit devono essere intraprese senza indebiti ritardi. Quanto tempo può essere concesso per chiudere i rilievi importanti emersi in fase di audit? L'inerzia di molti responsabili di funzione nel non voler affrontare "i problemi della qualità" dovrebbe essere adeguatamente sanzionata.

Infine il requisito 9.3 sul **riesame della direzione** (suddiviso nei paragrafi 9.3.1 **Generalità**, 9.3.2 **Input al riesame di direzione** e 9.3.3 **Output del riesame di**

direzione) è stato spostato dalle Responsabilità della Direzione della precedente edizione della norma a questo capitolo di Valutazione delle prestazioni del sistema di gestione per la qualità, anche se la responsabilità dei risultati del riesame ricade in capo all'alta direzione. Gli input al riesame sono stati estesi, naturalmente alla valutazione dei cambiamenti dei fattori interni ed esterni che influenzano il sistema di gestione ed all'efficacia delle azioni intraprese per affrontare rischi ed opportunità, ovvero alle principali novità della norma.

L'output del riesame deve trattare le modifiche che si rendono necessarie al sistema, le opportunità di miglioramento e le risorse necessarie.

Naturalmente sono richieste evidenze documentali dello svolgimento del riesame (dati in input, verbali di riunione di riesame del sistema, programmi di miglioramento, ecc.); la procedura non è necessaria (non lo era nemmeno nella precedente versione del 2008), ma chi ce l'ha se la tenga.

10 Miglioramento

Questa sezione si suddivide in tre paragrafi, nel primo 10.1 **Generalità** si riassume che il miglioramento deve riguardare:

- Prodotti e servizi erogati, non solo limitatamente al soddisfacimento delle esigenze attuali di conformità degli stessi, ma anche in previsione di esigenze ed aspettative future;
- Correzione, prevenzione e riduzione di ogni effetto indesiderato (NC, indicatori non soddisfacenti, ritardi di consegna, maggiori costi, ecc.);
- Il miglioramento delle prestazioni e dell'efficacia dello stesso sistema di gestione per la qualità che, dunque, deve essere dinamico e non statico nei secoli dei secoli.

Il successivo paragrafo 10.2 tratta le **Non conformità ed azioni correttive**, tornate di nuovo insieme per focalizzare l'attenzione sugli aspetti di miglioramento del processo di gestione delle NC, le quali, per la fase di gestione del trattamento, sono rimaste insieme ai processi produttivi (si veda § 8.7 "Controllo degli output non conformi").

Alle organizzazioni è richiesto di reagire prontamente alle non conformità per tenerle sotto controllo e correggerle, anche al fine di evitare effetti negativi gravi, sia interni che esterni (dal cliente). Le fasi successive di analisi delle cause (di NC, problemi in genere, rilievi da audit, reclami, ecc.), determinazione delle azioni correttive, pianificazione ed attuazione delle stesse e, infine, di valutazione della loro efficacia, sono sostanzialmente le stesse rispetto alle edizioni precedenti della norma, ma con maggiore enfasi sul processo stesso di

gestione del ciclo di miglioramento che si avvicina al c.d. *metodo 8D* del settore automotive.

L'ultimo paragrafo della norma ISO 9001:2015 – il 10.3 **Miglioramento continuo** – si ricollega al punto 10.1 di cui sopra, ai risultati del riesame di direzione ed a tutte le informazioni derivanti dalla valutazione delle prestazioni del sistema di gestione per la qualità per determinare la necessità di migliorare in modo continuativo l'efficacia del sistema di gestione, considerando anche le opportunità di miglioramento emerse dalle altre attività del capitolo 9 della norma stessa.

Con questo articolo si conclude l'analisi dei requisiti della nuova norma ISO 9001:2015. Alcune interpretazioni soggettive potranno sicuramente essere smentite dai fatti a fronte di nuove interpretazioni ufficiali (al momento in Italia è disponibile solamente una Linea guida pubblicata da CONFORMA con il patrocinio dell'UNI) e prassi di fatto adottate dagli Organismi di Certificazione, comunque sotto il controllo di ACCREDIA. Vedremo anche se l'Ente di Accreditamento stesso vorrà replicare la pubblicazione delle linee guida (*Criteri per un approccio efficace ed omogeneo alle valutazioni di conformità alla norma ISO 9001:2008* "Sistemi di gestione per la qualità – Requisiti") emesse per le due precedenti edizioni della norma e, quindi, se saranno disponibili maggiori dettagli applicativi per gli auditor che dovranno valutare i SGQ delle organizzazioni.

Come applicare la ISO 9001:2015 – IV parte

In questo quarto articolo vedreno in dettaglio i requisiti del capitolo 8 (Attività operative) della norma UNI EN ISO 9001:2015 con particolare riguardo alle novità introdotte rispetto alla precedente versione del 2008 ed alle possibili modalità di attuazione dei nuovi requisiti, per il passaggio del sistema di gestione per la qualità ISO 9001:2008 alla ISO 9001:2015.

8 Attività operative

Le "*operations*" sono il cuore dei processi primari e della norma, ma forse il capitolo con minori modifiche rispetto alla edizione precedente della ISO 9001.

La **Pianificazione e controllo operativi** (8.1) non richiede nulla di più di quello che è necessario per pianificare e tenere sotto controllo i processi necessari al fine di garantire la conformità di prodotti e servizi. Le informazioni documentate da mantenere (procedure, programmi della produzione, piani della qualità, piani di controllo, piani di progetto, …) e conservare (rapporti di controllo, registrazioni di verifiche, controlli, validazioni, ecc.) sono "quelle che servono": come esposto in altri punti sta alla responsabilità dell'azienda dimostrare che realizza ciò che ha pianificato, ovviamente in conformità ai requisiti specificati.

Il punto **Requisiti per i prodotti e i servizi** (8.2) comprende tutti i requisiti relativi ai "processi relativi al cliente" della precedente edizione della norma ed amplifica il suo raggio di azione. I sotto paragrafi trattano i seguenti aspetti, tutti finalizzati ad un'appropriata definizione dei requisiti del prodotto e/o servizio:

- **Comunicazione con il cliente**: tratta la corretta gestione di tutte le informazioni che transitano fra organizzazione e propri clienti (offerte, ordini, contratti, cataloghi, listini, depliant, siti web, specifiche, reclami, segnalazioni, ecc.).
- **Determinazione dei requisiti relativi ai prodotti e servizi**: poche parole, ma molto chiare dovrebbero far capire che devono essere definiti requisiti per prodotti e servizi comprendenti aspetti cogenti e requisiti stabiliti dall'organizzazione stessa che deve poi dimostrare di essere in grado di offrire al cliente quello che promette.
- **Riesame dei requisiti relativi ai prodotti e servizi**: tutti i requisiti stabiliti dal cliente, dall'organizzazione e da normative cogenti devono essere riesaminati per assicurare di avere la capacità di soddisfarli.
- **Modifiche ai requisiti per i prodotti e servizi**: le variazioni ai requisiti del prodotto/servizio devono essere gestite aggiornando documentazione e trasferendo le informazioni necessarie a chi di dovere.

Anche in questo caso le informazioni documentate necessarie sono quelle che servono e la procedura documentata non è richiesta, ma opportuna nel momento in cui si vuole stabilire delle regole interne. L'audit di questo elemento non dovrebbe essere difficile, come non dovrebbe essere raro rilevare le promesse consapevolmente non mantenute o non mantenibili, le dichiarazioni di requisiti incomplete, le presentazioni eccessivamente autoincensanti, l'assenza di risorse adeguate per soddisfare i tempi di consegna confermati e così via. Il problema è capire se e come verranno registrate, ovvero qual è il limite fra la conformità e la non conformità?

Anche il punto 8.3 **Progettazione e sviluppo di prodotti e servizi** è una riscrittura, probabilmente più completa ed efficace, dell'ex punto 7.3 della norma del 2008.

I punti trattati sono i seguenti:

- **Generalità**: il processo di progettazione deve essere appropriato alla successiva

fornitura di prodotti e servizi conformi.

- **Pianificazione della progettazione e sviluppo**: non si rilevano particolari novità rispetto alla versione precedente, ma tutto deve essere considerato nel pianificare il processo di progettazione, comprese la partecipazione del cliente ai controlli della progettazione e le esigenze delle altre parti interessate (es. collettività ed utenti finali).
- **Input alla progettazione e sviluppo:** i dati di ingresso al processo di progettazione devono comprendere tutti gli aspetti importanti, comprese le potenziali conseguenze negative di un guasto sul prodotto e le norme ed i codici di condotta che l'organizzazione si è impegnata a rispettare.
- **Controlli della progettazione e sviluppo**: in un'unica voce ("controlli") sono compresi riesami, verifiche e validazioni delle precedenti edizioni della norma ISO 9001.
- **Output della progettazione e sviluppo**: anche per questo elemento non ci sono variazioni salienti rispetto alla ISO 9001:2008 in quanto è richiesto che gli elementi in uscita dalla progettazione siano completi e univoci e comprendano i criteri di monitoraggio e controllo del successivo processo di realizzazione.
- **Modifiche della progettazione e sviluppo**: nulla di significativamente diverso rispetto alla precedente edizione della norma, le modifiche progettuali devono essere gestite in modo adeguato.

Il successivo punto 8.4 **Controllo dei processi, prodotti e servizi forniti dall'esterno** equivale come contenuti al punto 7.4 (Approvvigionamento) delle edizioni precedenti (2000 e 2008) della norma.

Nel primo sottopunto (**Generalità**) viene chiarito che quando il prodotto/servizio di un fornitore esterno viene incorporato nel prodotto/servizio venduto al cliente, oppure viene fornito direttamente al cliente dal fornitore stesso (subappalto) o quando un processo o parte di esso viene fornito dal fornitore (in outsourcing), è necessario stabilire controlli efficaci su tali forniture, qualificare, valutare e rivalutare periodicamente il fornitore, ovvero monitorare costantemente le prestazioni dei fornitori e conservare informazioni documentate su tali attività.

Il **Tipo ed estensione del controllo** sul fornitore deve essere pianificato in funzione dell'influenza che la fornitura ha sulle capacità dell'organizzazione di fornire con regolarità prodotti e servizi conformi ai requisiti stabiliti.

Le **informazioni ai fornitori esterni** devono essere complete di tutti gli aspetti relativi alla fornitura, compresi specifiche di controllo, qualifiche del personale, tempi, requisiti di assicurazione qualità. Di fatto non ci sono state variazioni significative rispetto all'edizione del 2008.

Il punto 8.5 **Produzione ed erogazione dei servizi** è abbastanza simile al punto 7.5 della precedente versione della norma. Il sottopunto 8.5.1 (**Controllo della produzione e dell'erogazione dei servizi**) torna a distinguere fra processi produttivi e di erogazione di servizi e richiede esplicitamente informazioni

documentate per definire le attività da svolgere ed i risultati da conseguire: a seconda dei casi le organizzazioni dovranno definire procedure, programmi di produzione, piani di controllo, piani della qualità o quant'altro ritenuto necessario per tenere sotto controllo la produzione o il processo di erogazione del servizio. Fra gli aspetti nuovi si segnala la necessità di intraprendere azioni che prevengano gli errori umani: non si tratta dei "sistemi a prova di errore" della specifica tecnica ISO/TS 19649 per l'*automotive*, ma si va verso quella direzione.

Il successivo 8.5.2 (**Identificazione e rintracciabilità**) non presenta modifiche significative rispetto alla edizione 2008.

Invece le **Proprietà che appartengono ai clienti o ai fornitori esterni** (8.5.3) estendono il requisito della precedente edizione della norma alle proprietà dei fornitori (ma in realtà il materiale giunto non conforme dal fornitore andava notificato allo stesso anche nelle precedenti edizioni della norma), modernizzando un po' il requisito stesso in quanto oggi sono diventate sempre più importanti le proprietà intellettuali, la protezione dei dati personali ed in generale tutta la gestione delle informazioni in formato digitale, spesso gestite con troppa superficialità.

Nel sottopunto 8.5.4 viene trattato il requisito relativo alla **Preservazione** degli output dei processi produttivi e di erogazione dei servizi, impiegando un termine forse un po' infelice (in lingua italiana) per indicare, di fatto, gli stessi requisiti che comparivano nelle precedenti edizioni della norma quando si parlava di "conservazione dei prodotti", di "movimentazione", "immagazzinamento", "imballaggio", ecc., comprendendo anche le fasi di trasporto e consegna, quando sotto responsabilità dell'Organizzazione. Ora in due righe si sintetizzano tutti i concetti.

Le **Attività post-consegna** sono trattate al sottopunto 8.5.5 che rappresenta un requisito innovativo (per la verità implicito nella precedente edizione della norma), anche se di fatto viene ripristinato il requisito 4.18 dell'edizione del 1994 ampliandolo e non riducendolo solo all'assistenza. Oggi, infatti, l'assistenza post-consegna, che comprende assistenza in garanzia, su contratto, supporto nell'utilizzo del prodotto, gestione dell'eventuale smaltimento e di problematiche legate al ritiro dei prodotti non conformi, comunicazioni e così via, è diventata estremamente importante per la percezione di qualità che ha il cliente di un'organizzazione.

Il successivo sottopunto 8.5.6 (**Controllo delle modifiche**) costituisce un nuovo requisito che vuole porre l'attenzione delle organizzazioni sulla corretta gestione di tutte le modifiche (pianificate e impreviste) alle specifiche di un prodotto/servizio o alla sua realizzazione. Occorre definire compiti e responsabilità per il riesame delle stesse e conservare informazioni documentate per attestare la corretta gestione delle modifiche.

Nel paragrafo **Rilascio di prodotti e servizi** (8.6) la norma specifica che l'organizzazione deve verificare – in fasi appropriate – che sia stato attuato quanto pianificato nella produzione di prodotti ed erogazione di servizi. In particolare, prima di rilasciare il prodotto al cliente occorre accertarsi che tutto quanto era stato pianificato (lavorazioni, elaborazioni, controlli, test, ecc.) sia stato effettivamente completato soddisfacentemente per garantire la conformità del prodotto/servizio ai requisiti stabiliti. L'unica eccezione è data dall'approvazione di una "Autorità competente" o del cliente a rilasciare comunque un prodotto, ad esempio, non completamente controllato.

Su questo punto la norma richiede evidenze documentali:

- dei controlli effettuati, a fronte di criteri di accettazione stabiliti, per il rilascio dei prodotti;
- del riferimento alla/e persona/e che ha effettuato il rilascio del prodotto/servizio.

Questo requisito, come il successivo 8.7 (**Controllo degli output non conformi**), pur considerando le differenze di struttura tra le due edizioni della norma, sono stati di fatto spostati fra le Attività operative (ex capitolo 7) dalle Valutazioni delle prestazioni (analogo all'ex capitolo 8 dell'edizione del 20008 della norma).

Relativamente alle non conformità è stata esplicitata la necessità di intraprendere azioni correlate alla natura della non conformità ed ai suoi effetti; tra esse la semplice correzione, la segregazione, il contenimento degli effetti e l'informazione al cliente, ad esempio, che parte dei lotti consegnati possa risultare non conforme, se ci si accorge di un problema dopo la consegna del prodotto al cliente.

Naturalmente le NC vanno gestite anche durante lo svolgimento del processo produttivo o l'erogazione del servizio, in qualunque fase esse si verifichino. Infine, è necessario conservare informazioni documentate sulle NC rilevate e sulla loro gestione, come era richiesto nella precedente versione della norma.

(continua)

Come applicare la ISO 9001:2015 –

III parte

In questo terzo articolo affronteremo il capitolo 7 Supporto della norma UNI EN ISO 9001:2015 con particolare riguardo alle novità introdotte rispetto alla precedente versione del 2008 ed alle possibili modalità di attuazione dei nuovi requisiti, per il passaggio del sistema di gestione per la qualità ISO 9001:2008 alla ISO 9001:2015.

7 Supporto

Questa sezione, completamente nuova come titolo, ma non come contenuti, è direttamente figlia della HLS delle norme sui sistemi di gestione. Essa raccoglie diversi elementi afferenti ai cosiddetti processi di supporto di una organizzazione: gestione delle risorse umane, know-how, sistemi informativi, documenti e dati, dispositivi di monitoraggio e misura, macchinari/attrezzature ed altre apparecchiature hardware, ecc.

L'organizzazione deve sempre determinare le necessità di risorse per il funzionamento dei processi e metterle a disposizione, considerando le capacità delle risorse esistenti, i vincoli che gravano su di esse e ciò che può essere demandato a fornitori esterni.

Anche solo nel paragrafo **Generalità** di questa sezione si va più a fondo rispetto alle precedenti edizioni della norma su concetti fondamentali quali la disponibilità di risorse adeguate per perseguire gli obiettivi stabiliti, garantire la conformità dei processi e dei prodotti realizzati o servizi erogati. Forse parte delle PMI italiane non saranno pienamente conformi ai requisiti della norma, infatti chi ha messo a disposizione le risorse adeguate per soddisfare gli obiettivi?

Nei paragrafi successivi la norma ISO 9001:2015 non fa che ribadire che devono essere messe a disposizione le **Persone** (le risorse umane sono ritornate ad essere persone) e le **Infrastrutture** (edifici, macchinari, attrezzature, risorse tecnologiche, risorse per il trasporto…) necessarie per l'efficace attuazione del sistema di gestione per la qualità, il funzionamento e controllo dei processi e per ottenere la conformità dei prodotti e servizi ai requisiti.

Anche l'**Ambiente per il funzionamento dei processi** deve essere adeguato a quanto sopra ed addirittura la norma, nelle note esplicative per chiarire cosa si intende per "ambiente", fa riferimento a principi etici, aspetti sociali e psicologici, oltre che fisici (temperatura, illuminazione, rumore, ecc.). L'ambiente, infatti, comprende quelle variabile che possono influenzare il benessere ed il comportamento

delle persone che hanno relazione direttamente o indirettamente con l'impresa.

Le tematiche esposte ai punti 7.1.2, 7.1.3 e 7.1.4 della norma sopra citati sono da considerarsi piuttosto delicate da verificare in fase di audit, perché si rischia di sconfinare nella normativa sul lavoro (Persone), sulla sicurezza (Persone e Infrastrutture) e sull'ambiente (Ambiente per il funzionamento dei processi e Infrastrutture). I confini fra i requisiti dei sistemi di gestione per la qualità ed i requisiti cogenti non inerenti i prodotti e servizi realizzati sono sempre stati mantenuti solidi e invalicabili da ACCREDIA e dagli Organismi di Certificazione, ma ora la norma del 2015 entra più nello specifico e ci pone degli interrogativi:

- Come è possibile essere conformi alla ISO 9001:2015 se non si rispettano le norme legate ai contratti di lavoro per fornire al cliente un servizio il cui livello qualitativo non può essere garantito dal personale incaricato in termini di risorse messe a disposizione, tempi di consegna, garanzia di continuità del servizio?
- Come si può pensare di garantire un ambiente di lavoro e relativi processi conformi alla ISO 9001:2015 se le apparecchiature non sono manutenute e gestite almeno osservando i requisiti cogenti del D.Lgs 81/2008 e s.m.i.?
- Quale conformità ai requisiti ISO 9001:2015 si può credere di garantire se le condizioni di lavoro del personale non sono coerenti con le norme sulla "sicurezza e salute dei lavoratori" e con principi etici condivisi (trattamenti discriminatori, rispetto della privacy, lavoro sotto stress eccessivo… la norma cita addirittura sindrome da *burnout*)?

È necessario stabilire con chiarezza fino a che punto spingersi in fase di audit di certificazione su questi aspetti e, soprattutto, quali saranno le competenze richieste agli auditor per eventualmente investigare su aspetti cogenti non di loro normale pertinenza.

Qualunque siano le eventuali specificazioni di ACCREDIA su questo argomento (in assenza di esse varrebbe quanto stabilito per le precedenti versioni della norma), certe situazioni "consapevolmente non conformi" per assenza di evidenze oggettive di conformità a requisiti cogenti, sarebbe corretto rilevarle.

Le **Risorse per il monitoraggio e la misurazione** del punto 7.1.5 della nuova norma sono gli ex "dispositivi di monitoraggio e misurazione" del § 7.6 della norma ISO 9001:2008, ovvero, per molte aziende, i classici **strumenti di misura**.

Nei sotto paragrafi **Generalità** e **Riferibilità delle misurazioni** di questo punto non vi sono particolari novità rispetto alla precedente edizione della norma: occorre

mettere a disposizione risorse adeguate (non solo legate alla strumentazione di misura) a garantire l'affidabilità delle misure e, ove richiesto, la riferibilità metrologica delle attività di taratura, calibrazione e controllo degli strumenti. Per dare evidenza di tutto ciò continuano ad essere richieste informazioni documentate.

Il punto 7.1.6 della norma tratta la **Conoscenza organizzativa** e costituisce una novità assoluta di questa edizione della norma, anche se alcuni concetti erano comunque insiti in altri punti della vecchia norma. Viene data l'importanza che merita alle conoscenze del funzionamento dell'organizzazione stessa e dei suoi processi da parte delle persone che vi operano, anche con ruoli di responsabilità. Il valore dell'esperienza delle persone, delle informazioni che costituiscono proprietà intellettuale dell'impresa e le conoscenze e capacità tecniche e gestionali che possono essere acquisite dall'esterno attraverso formazione, acquisizione di informazioni documentate o altro deve essere gestito in modo adeguato, identificando le necessità, colmando le carenze, proteggendo il know-how aziendale ecc.

Il requisito relativo alla **Competenza** delle persone non è sostanzialmente mutato rispetto alla precedente versione della norma, ma ora è più chiaro che è responsabilità dell'organizzazione assicurarsi che anche il personale esterno (collaboratori a contratto, consulenti) e del fornitore disponga delle competenze adeguate a svolgere le attività cui è preposto e, quindi, provvedere, se necessario, all'acquisizione delle competenze che risultano carenti. Su questo punto dell'acquisizione delle competenze la norma non prescrive di colmare le lacune solamente attraverso la formazione e l'addestramento del personale, questo è solo uno dei modi possibili.

Il requisito della **Consapevolezza**, senza variazioni significative rispetto alla versione 2008 della norma, viene enfatizzato (è elevato a requisito a sé): il personale deve essere consapevole degli effetti, sia positivi, che negativi, del suo operato sull'efficacia del sistema qualità e sul conseguimento della conformità dei prodotti e servizi.

La consapevolezza può essere ottenuta attraverso diversi metodi: riunioni, formazione, condivisione di non conformità e problemi rilevati (per imparare dall'esperienza), comunicazioni interne, ecc. Da parte dell'auditor, invece, la consapevolezza può essere dimostrata – oppure no – attraverso le interviste al personale e le verifiche incrociate con input/output di altri processi rispetto a quello sotto esame.

Anche la **Comunicazione** assume maggiore importanza in questa edizione della norma: l'organizzazione deve determinare cosa, come, quando, a chi e che cosa comunicare, sia internamente che esternamente alle parti interessate. Tutte le comunicazioni, interne ed esterne, dovranno essere coerenti con obiettivi ed altri requisiti del sistema di gestione.

Il punto 7.5 della norma tratta delle **Informazioni documentate**, ovvero dei documenti e delle registrazioni delle precedenti versioni della norma. In questa edizione, però, non è solo il nome a cambiare (il termine “informazioni” ricorda maggiormente le norme ISO 27000 sulla sicurezza delle informazioni), infatti il requisito lascia un maggior grado di libertà alle organizzazioni poiché il sistema di gestione per la qualità deve comprendere:

- le informazioni documentate richieste dalla norma, che sono in numero inferiore alle precedenti edizioni e non sono richieste procedure obbligatorie e nemmeno il manuale qualità lo è.
- Le informazioni documentate stabilite come necessarie dall’organizzazione.

Sebbene la norma lasci ad ogni singola organizzazione la scelta di quali documenti di tipo procedurale (manuale, procedure, istruzioni, piani della qualità, ecc.) mantenere in funzione delle dimensioni dell’organizzazione, della complessità ed articolazione dei processi, delle competenze delle persone, ecc. credo siano pochi i casi di aziende che possono ritenere non necessarie alcune procedure relative a processi primari o processi di supporto per i quali il personale non dispone di sufficienti competenze per gestirli in modo conforme alla norma.

La norma spiega in appendice (vedasi precedente articolo) la differenza fra “mantenere informazioni documentate” e “conservare informazioni documentate”. In ogni caso la norma indica puntualmente quali informazioni documentate è necessario conservare e non si riscontrano particolari differenze rispetto al passato.

Nei paragrafi 7.5.2 (Creazione e aggiornamento) e 7.5.3 (Controllo delle informazioni documentate) non sono riportate novità sostanziali rispetto alle precedenti edizioni della norma, ma solo una riscrittura dei requisiti in ottica più attuale, con maggiore enfasi sulla gestione sicura delle informazioni (va garantita la riservatezza e l’integrità, nonché il controllo delle versioni). Anche per le informazioni documentate di origine esterna (norme e leggi, specifiche del cliente, …) valgono le stesse regole. Da segnalare il fatto che non è più richiesto esplicitamente un tempo di conservazione per le informazioni documentate.

Rispetto al passato questo punto dovrà essere attuato con maggior rigore per quanto riguarda le informazioni in formato digitale, in quanto alcune di esse sono molto critiche per il funzionamento dei processi, per preservare il know-how aziendale e le proprietà del cliente.

Nel complesso la sezione 7 della norma ha migliorato significativamente l’omogeneità di gestione di tutti quei processi di supporto presenti in molte imprese che raccolgono le procedure (e relativi processi/attività) riguardanti: gestione delle risorse umane, gestione delle risorse tecniche/manutenzione attrezzature, gestione degli strumenti, gestionde della documentazione, comunicazioni interne, ecc..

(continua)

Come applicare la ISO 9001:2015 – II parte

In questo secondo articolo affronteremo i capitoli 5 Leadership e 6 Pianificazione della norma UNI EN ISO 9001:2015 con particolare riguardo alle novità introdotte rispetto alla precedente versione del 2008 ed alle possibili modalità di attuazione dei nuovi requisiti, per il passaggio del sistema di gestione per la qualità ISO 9001:2008 alla ISO 9001:2015.

5 Leadership

Questa versione della norma invoca, con maggior enfasi, la **Leadership e l'impegno dell'alta Direzione** sul sistema di gestione per la qualità: dalla definizione di politica ed obiettivi, all'assicurare l'efficacia del sistema stesso nel raggiungimento di suddetti obiettivi. Per garantire ciò la Direzione deve fornire supporto e motivazione a tutto il personale per l'attuazione dei requisiti del sistema qualità e deve mettere a disposizione risorse adeguate per il perseguimento degli obiettivi stabiliti.

Il coinvolgimento nel sistema di gestione per la qualità deve riguardare tutto il "*top management*" ("Persona o gruppo di persone che dirigono e controllano una organizzazione al più alto livello"), o Alta Direzione, e il sistema stesso deve essere integrato con il funzionamento dell'azienda.

Questi requisiti potranno essere verificati attraverso interviste al *top management*, verifica del riesame del sistema, verifica del coinvolgimento del personale – attraverso le interviste normalmente svolte durante l'audit e della Direzione stessa – nella qualità dei processi e dei prodotti, valutazione delle evidenze dei risultati degli indicatori di monitoraggio e misura dei processi e così via. Occorrerà solo vedere quanto il bravo auditor vorrà "ferire" in caso di rilevazione di carenze su questo punto.

Leadership ed impegno dovranno evidenziarsi anche nella **Focalizzazione sul cliente** che, rispetto ai requisiti rafforzati della precedente edizione, dovranno affrontare rischi ed opportunità che possono influenzare la conformità dei prodotti e dei servizi, oltre l'aumento della soddisfazione del cliente a cui bisognerà sempre tendere.

L'analisi dei rischi dovrebbe anche valutare possibili minacce al rispetto dei requisiti dei prodotti ed a quelli cogenti, nonché al rispetto dei requisiti del servizio, come i tempi di consegna. In ogni impresa tali possibili rischi sono innumerevoli e non sempre sono correttamente valutati ed affrontati dalla Direzione. In questo senso la norma ISO 9001:2015 va verso la normativa del settore automotive (ISO/TS 16949 e altri schemi) in cui vanno considerati anche fattori straordinari quali il fermo-macchina prolungato, catastrofi naturali, chiusura di fornitori critici, assenza di personale, ecc.

Il requisito successivo sulla **politica per la qualità** ha subito pochi cambiamenti, legati al fatto di essere legata al contesto dell'organizzazione ed essere coerente con strategie ed obiettivi dell'organizzazione. Quindi la politica per la qualità – comunicata all'interno ed all'esterno dell'organizzazione, disponibile anche alle parti interessate, per es. ai fornitori – dovrebbe essere dinamica, riesaminata più frequentemente che in passato per adeguarsi al mutato contesto dell'organizzazione.

La definizione, da parte del *top management*, di **Ruoli, responsabilità e autorità nell'organizzazione** non ha prescrizioni particolarmente differenti rispetto al passato, salvo constatare l'assenza del "Rappresentante della Direzione". Questa figura non è più necessaria, ma non è pensabile che un sistema di gestione per la qualità possa funzionare (soprattutto nel nostro Paese) senza un Responsabile Qualità che mantiene le fila di tutto il Sistema. Cade l'obbligo che il Rappresentante della Direzione sia un membro effettivo della Direzione che ha procurato numerosi problemi, soprattutto in organizzazioni di piccole dimensioni che avrebbero voluto delegare la qualità "al primo che capita".

In generale, sebbene non siano richieste informazioni documentate, la definizione di un organigramma funzionale e nominativo, unito alla presenza di un mansionario condiviso a tutti i livelli dell'organizzazione resta condizione imprescindibile per dimostrare quanto richiede la norma. Ovviamente possono sussistere altre forme di documentazione al riguardo, compreso il richiamo a procedure ed istruzioni per dettagliare compiti e responsabilità di ogni funzione, ma le responsabilità in azienda non possono essere solamente fondate sulla parola.

La verifica della coerenza di tutto quanto resta sempre una regola dettata dal buon senso per il bravo auditor.

6 Pianificazione

Questa sezione, un caposaldo della nuova struttura HLS, si basa sulle **Azioni per affrontare rischi ed opportunità**. Considerando il contesto dell'organizzazione descritto ai punti 4.1 e 4.2 l'organizzazione deve determinare rischi ed opportunità che influenzano la sua attività per:

- assicurare i risultati attesi del sistema di gestione per la qualità;
- accrescere gli effetti desiderati (derivanti dalle opportunità);
- prevenire gli effetti indesiderati (derivanti dai rischi);
- perseguire il miglioramento continuo.

Le azioni per affrontare rischi ed opportunità devono essere pianificate secondo modalità che assomigliano molto al vecchio paragrafo sulle azioni preventive e di miglioramento. Nella nuova edizione della norma tali azioni sono elevate di livello, derivano dalla valutazione di importanza di rischi ed opportunità, devono essere attuate integrandole nell'intero sistema e nei suoi processi e deve essere valutata l'efficacia di tali azioni.

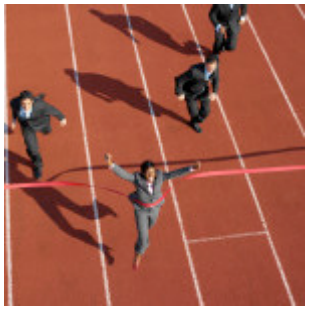
Le note riportate in questo paragrafo chiariscono le possibili alternative a fronte dell'identificazione di un rischio, tra cui l'assunzione dello stesso per cogliere un'opportunità di crescita.

D'altro canto le opportunità possono trovarsi nell'ambito dell'innovazione di prodotto e di processo, nelle relazioni con clienti e fornitori, nella creazione di nuovi prodotti e in molte altre situazioni.

Sebbene la norma non richieda espressamente una analisi del rischio documentata, riesce difficile comprendere come un'attività così complessa possa essere condotta senza redigere e riesaminare periodicamente un documento specifico, anche nelle organizzazioni più piccole.

Un minimo di classificazione e graduazione dei rischi, delle relative probabilità di accadimento e della gravità delle conseguenze in caso di verificarsi del rischio credo sia indispensabile per dare evidenza di una corretta gestione del rischio e dell'applicazione del *risk-based thinking*.

Al riguardo si segnala che l'ISO ha pubblicato un esempio applicativo della gestione dei rischi legati all'ISO 9001:2015, riportato in *allegato 3* della *Linea Guida Conforma sulla ISO 9001:2015*.



Relativamente agli **Obiettivi per la qualità e pianificazione per il loro raggiungimento** la nuova norma specifica che gli stessi devono essere pertinenti alla conformità dei prodotti e dei servizi ed al raggiungimento della soddisfazione del cliente. Dunque non bastano indici sulle vendite, sulla produttività e sul raggiungimento di obiettivi strategici aziendali, occorre considerare conformità/non conformità dei prodotti, resi, reclami, ritardi di consegna e soddisfazione del cliente.

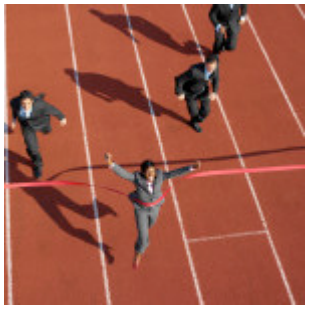
In più la nuova edizione della norma precisa che l'organizzazione deve pianificare cosa sarà fatto per raggiungere gli obiettivi, come sarà fatto, quali risorse saranno impiegate, quali saranno i responsabili delle azioni pianificate, quando si ritiene saranno completate e come si valuterà i risultati. Questi aspetti spesso sono richiesti dagli auditor degli Organismi di Certificazione, ora diventano un requisito non tanto facile da soddisfare, soprattutto per molte PMI con scarsa mentalità alla pianificazione delle risorse per il conseguimento degli obiettivi.

Questo punto della norma, se correttamente verificato e valutato in fase di audit, potrebbe mettere a nudo alcune carenze di numerose piccole organizzazioni che, da un lato documentano obiettivi di qualità dei prodotti e dei processi e dall'altro, nella pratica, spingono il personale solamente all'ottenimento del massimo fatturato al più presto possibile, per essere quindi pagati prima possibile, il tutto a discapito dei controlli e della qualità dei prodotti e servizi. Non è certo questa la filosofia della nuova ISO 9001:2015, ma bisognerà avere il coraggio di far capire alle organizzazioni le loro carenze manageriali.

La **Pianificazione delle modifiche** al sistema di gestione per la qualità deve essere ben ponderata, valutando le possibili conseguenze in situazioni di cambiamento quali introduzione di nuovi prodotti o servizi, apertura di nuovi mercati, introduzione di nuovi sistemi informativi o modifica degli esistenti, cambiamenti organizzativi, attuazione di nuovi requisiti cogenti, ecc. Anche se non presenta particolari novità rispetto all'edizione precedente della norma, il requisito risulta allineato ai nuovi concetti normativi.

continua

È uscita la ISO 9001:2015: che fare?



Lo scorso 22 settembre è stata pubblicata (in realtà retrodatata 15 settembre 2015) la nuova versione della norma **UNI EN ISO 9001:2015 "Sistemi di gestione per la qualità – Requisiti"**. Tale norma, come noto, regola i sistemi di gestione per la qualità e la relativa certificazione in Italia e nel mondo.

Premesso che non è intenzione di questo articolo entrare nel merito tecnico e sostanziale dei singoli capitoli della norma, per la cui analisi si rimanda a successivi articoli, vorrei esprimere alcune considerazioni generali sulle novità introdotte dalla revisione della norma sui sitemi di gestione per la qualità e, soprattutto, illustrare quale approccio dovrebbero tenere le organizzazioni certificate e certificande nei confronti della nuova edizione della norma ISO 9001.

I principali aspetti innovativi della norma sono probabilmente i seguenti:

- La nuova **struttura di alto livello** della norma illustrata nell'Annex SL (*High Level Structure* derivante dalla Direttive ISO/IEC, Parte 1, Annesso SL, Appendice 2);
- Un requisito esplicito che richiede l'adozione del ***Risk Based Thinking***;
- Introduzione di un capitolo dedicato al "**contesto organizzativo**";
- Maggiore **flessibilità sulla documentazione** ("informazioni documentate") inerente il Sistema di Gestione per la Qualità;
- Minori **requisiti prescrittivi**;
- Incremento dei **requisiti legati alla leadership** e maggiore enfasi sul **raggiungimento dei risultati** stabiliti negli obiettivi misurabili dei processi e dell'organizzazione.

In particolare i nuovi requisiti sulla comprensione del contesto dell'organizzazione, sulle esigenze delle parti interessate e sulla **valutazione di rischi ed opportunità** dovrebbero costringere le organizzazioni a vivere il sistema qualità come un "vero" sistema di gestione, calato a 360 gradi nella realtà aziendale e nel contesto in cui opera.

Di questi nuovi concetti sono pervasi tutti i punti della norma che sono stati riscritti in questa ottica. In pratica non viene più ritenuto necessario specificare in dettaglio requisiti puntuali su cosa si deve ritrovare nel sistema (procedure, istruzioni, piani, registrazioni particolari o altro) per essere conformi. La

struttura del sistema stesso, dal punto di vista documentale, è lasciata libera. Addirittura sono scomparse le prescrizioni sul **Manuale Qualità** e sulle **procedure documentate** minime che dovevano essere presenti in passato.

Da un lato la norma sembra dire alle organizzazioni: «analizzate il vostro contesto organizzativo (mercato, ambiente, esigenze di tutte le parti interessate, …), identificate e valutate tutti i rischi di *business* che potreste dover fronteggiare con idonee contromisure, stabilite i vostri obiettivi di breve, medio o lungo periodo, traduceteli in obiettivi dei processi aziendali misurabili tramite indicatori oggettivi, monitorate e misurate i processi e la soddisfazione del cliente pianificando ed attuando, quando necessario, idonee azioni correttive e di miglioramento e procedete così nell'ottica del miglioramento continuo e della prevenzione dei rischi, tenendo sempre sotto controllo i mutamenti che si manifestano all'interno ed all'esterno dell'organizzazione.»

Dall'altro ci dice di «progettare, attuare e mantenere sempre aggiornato un sistema di gestione per la qualità adeguato alle dimensioni ed al contesto dell'organizzazione, costituito dalle procedure e dai documenti che sono ritenuti necessari per garantire il rispetto delle regole stabilite ed il perseguimento degli obiettivi, richiedendo le registrazioni ritenute necessarie per dare evidenza – prima internamente alla Direzione ed ai vari Responsabili, poi esternamente agli auditor dell'Organismo di Certificazione – che le varie attività sono svolte come stabilito, al fine di garantire la qualità promessa dei prodotti/servizi venduti ed il rispetto di tutti i requisiti normativi e del cliente (tempi di consegna, modalità di erogazione dei servizi, imballaggi, ecc.). »

La norma, dunque, che nacque negli anni '80 come una norma che esprimeva regole dettate dal buon senso nella gestione della qualità in azienda, non fa altro che confermarsi come tale con i dovuti aggiornamenti e mutamenti intercorsi in questi anni nelle attività delle aziende e nelle organizzazione di ogni settore e dimensione.

Le aziende italiane, però, abituate a seguire una serie di prescrizioni ed a produrre un volume di documentazione che spesso non dipende dalle reali esigenze dell'organizzazione, ora si trovano un po', per così dire, spaesate. Che fare? Buttiamo via il manuale e tutte le procedure?

E gli auditor come faranno a decretare la conformità alla norma per la relativa certificazione ISO 9001 senza più disporre del manuale delle procedure documentate richieste dalla norma e delle altre prescrizioni che non sono più tali?

A queste domande, forse, sarà possibile rispondere solo fra qualche tempo, quando gli Organismi di Certificazione si saranno allineati alla nuova norma che dovrà essere supportata da linee guida ed interpretazioni ancora da definire da parte degli Enti competenti (EA, ACCREDIA, ecc.).

Per adesso pare che una descrizione del modo di procedere descritta a voce dall'interlocutore dovrebbe essere sufficiente all'auditor per capire il *modus operandi*. Fatto salvo poi verificare se tutti in azienda la pensano e la raccontano allo stesso modo e, soprattutto, fanno quello che dicono.

Dal punto di vista delle aziende certificate il consiglio che ci viene dalla norma è quello di **abbandonare sistemi di gestione per la qualità distanti dalla realtà aziendale**, costruiti ad uso e consumo del certificatore. Spesso tali sistemi sono alimentati solo in prossimità della visita di rinnovo della certificazione o di sorveglianza dell'Ente di certificazione, ma non danno un vero valore aggiunto all'azienda. O meglio lo potrebbero apportare, anche se non progettati al meglio e mal applicati, perché alcune informazioni le forniscono, peccato che restino confinate nell'ufficio del responsabile qualità! A proposito, non è più richiesta la figura del Rappresentante della Direzione, tanto discussa perché sovente veniva ricoperta da un membro effettivo della Direzione che poco sapeva di qualità, soltanto per evitare di dare uno stipendio da manager al responsabile qualità che "faceva tutto il lavoro".

Tutti questi sistemi qualità se non proprio fittizi, almeno inadeguati o comunque non applicati, potranno sopravvivere alla nuova edizione della norma ISO 9001:2015? Ai posteri l'ardua sentenza. La domanda in realtà va fatta alla Direzione di molte organizzazioni: perché mantenere sistemi qualità disallineati con la realtà solo per avere un bollino? Perché non fare le cose seriamente e costruire (o ristrutturare) un sistema qualità effettivamente applicato con efficacia che **ci fornisca indicazioni veritiere di dove sta andando l'azienda** e strumenti idonei a **migliorare l'efficacia e l'efficienza dei processi** interni, oltre che la soddisfazione del cliente?

Forse è l'ultima occasione per attuare principi universalmente condivisi che consentono di governare l'azienda verso obiettivi di miglioramento.

Soprattutto in questo periodo, ancora di crisi per alcuni e di ripresa più o meno lenta per altri, **la qualità paga sempre**.

La nuova norma da un lato ci dà **maggiori libertà** di definire e gestire le informazioni documentate di cui effettivamente necessitiamo, dall'altro ci fa capire che se vogliamo implementare un controllo sul nostro prodotto dovremo **descriverlo in qualche modo** affinché il personale preposto lo esegua correttamente e bisognerà esigere delle **registrazioni puntuali** di suddetti controlli se vogliamo essere sicuri che vengano eseguiti costantemente.

La norma ci consentirebbe di eliminare tutte le procedure che abbiamo: del resto la certificazione ISO 9001 è stata sempre accusata di produrre carta inutile. Probabilmente un po' di carta inutile si è prodotta solo da parte di aziende che non hanno progettato bene il proprio sistema, non dedicandoci il tempo e le risorse che meritava, magari con la collaborazione di consulenti improvvisati o mal pagati che

non avevano tempo, voglia e capacità di analizzare i processi con la dovuta cura; tanto sono sempre bastate procedure standard e moduli standard per ottenere e mantenere la certificazione. Ed era proprio questo che la Direzione voleva: ottenere la certificazione spendendo poco, sia in termini di risorse interne, sia di costi per consulenti e Organismo di Certificazione. Ma questo non è stato il bene delle aziende.

Ci sono molti sistemi qualità ben fatti che non vengono applicati, anche perché non sono diffusi all'interno dell'organizzazione e non adeguatamente "spinti" dalla Direzione. Basterebbe condividerne i principi con le varie figure chiave dell'organizzazione e cercare di aggiornarli e migliorarli per ottenere evidenti benefici per l'impresa. Questo ci invita a fare la ISO 9001:2015.

Dunque non è opportuno gettare via tutta la documentazione prodotta negli anni. Spesso le procedure sono comunque necessarie per avere una ragionevole certezza che le persone facciano quello che si è stabilito di fare. Addirittura anche se l'impresa è di piccole dimensioni, a maggior ragione è necessario documentare attraverso procedure come si desidera siano svolte le varie attività.

Lo stesso Manuale, visto anche come documento di presentazione, può essere utile per illustrare come è stata declinata la norma ISO 9001 all'interno dell'organizzazione e come documento base da cui sono richiamati tutti gli altri, procedure, istruzioni, ecc.

Il messaggio da trasmettere con la nuova norma ISO 9001:2015 alle imprese certificate ed a quelle in corso di certificazione è proprio questo: **costruite o ricostruite sistemi adeguati all'organizzazione**, effettivamente applicati e monitorati, finalizzati al perseguimento degli obiettivi reali dell'impresa.

Molto arduo sarà il compito degli auditor degli enti di certificazione per verificare che ciò avvenga, proprio perché non sarà sufficiente raccogliere evidenze documentali (come sembrava negli ultimi anni fosse la principale preoccupazione degli auditor), ma bisognerà capire se quello che l'organizzazione sta facendo è efficace per il raggiungimento degli obiettivi ed è conforme ai principi e requisiti normativi.

Infine qualche considerazione sul periodo transitorio. Tutte le organizzazioni certificate dovranno adeguare il loro sistema qualità entro il 15/09/2018; il consiglio è di fare la conversione della certificazione in occasione del prossimo rinnovo, salvo che esso non capiti fra pochi mesi, per dare comunque tempo agli organismi di Certificazione di allinearsi alle nuove metodologie.

Le novità della UNI ISO 27001:2014

La norma ISO 27001 pubblicata nel 2013 è stata tradotta in italiano e convertita in norma UNI nel marzo 2014 come UNI CEI ISO/IEC 27001:2014 – *Tecnologie informatiche – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti*. Essa specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un **sistema di gestione per la sicurezza delle informazioni** nel contesto di un'organizzazione, includendo anche i requisiti per **valutare e trattare i rischi** relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione.

La nuova ISO 27001 non riporta termini e definizioni, ma richiama la ISO 27000.2014 (scaricabile gratuitamente da http://www.iso27001security.com/html/27000.html e curiosamente venduta dall'UNI a € 138) per tutti i termini utilizzati nelle norme della serie ISO 27k.

Si segnala che nel capitolo introduttivo della ISO 27001 è scomparso il paragrafo "Approccio per processi", sebbene venga sottolineata l'importanza che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione.

La norma ISO 27001 riprende la nuova struttura di tutte le norme sui sistemi di gestione e, pertanto, al capitolo 4 tratta il "contesto dell'organizzazione". In questo capitolo viene esposto che per **comprendere l'organizzazione e il suo contesto** (4.1) occorre determinare i fattori esterni ed interni pertinenti alle finalità dell'organizzazione stessa e che influenzano la sua capacità di conseguire i risultati previsti per il proprio sistema di gestione per la sicurezza delle informazioni e che per **comprendere le necessità e le aspettative delle parti interessate** (4.2) occorre individuare le parti interessate al sistema di gestione per la sicurezza delle informazioni ed i requisiti delle stesse attinenti ad esso.

Anche la determinazione del **campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni** (SGSI o ISMS, *Information Security Management System*) è un'attività inerente la comprensione dell'organizzazione ed il suo contesto. In questo ambito l'organizzazione deve determinare i **confini di applicabilità** del sistema di gestione per la sicurezza delle informazioni ISO 27001 al fine di stabilirne il campo di applicazione, in modo analogo a quanto avveniva nella versione precedente della norma, considerando anche i **fattori esterni ed interni** ed i **requisiti delle parti interessate** esposti ai paragrafi precedenti.

Il capitolo 5 **“Leadership”** rispecchia anch’esso la nuova struttura delle norme sui sistemi di gestione. In esso, al paragrafo 5.1, viene indicato quali modalità l’alta direzione deve attuare per dimostrare leadership e impegno nei riguardi del sistema di gestione per la sicurezza delle informazioni. In analogia con altri sistemi di gestione, l’alta direzione deve stabilire **politica** ed **obiettivi**, mettere a disposizione le **risorse necessarie** per l’attuazione del SGSI, **comunicare** l’importanza di **un’efficace gestione della sicurezza delle informazioni** e dell’essere **conforme ai requisiti** del SGSI stesso; deve, inoltre, assicurare che il SGSI ISO 27001 consegua i risultati previsti, fornire guida e sostegno al personale per contribuire all’efficacia del sistema di gestione della sicurezza delle informazioni e, naturalmente, deve promuovere il miglioramento continuo.

Il paragrafo 5.2 tratta della **politica per la sicurezza delle informazioni** per la quale i requisiti sono analoghi a quelli presenti negli altri sistemi di gestione: naturalmente la politica deve essere documentata, comunicata all’interno dell’organizzazione ed essere disponibile a tutte le parti interessate.

Anche il paragrafo 5.3 – che riguarda **ruoli, responsabilità e autorità nell’organizzazione** – è molto simile a quanto riportato nelle altre norme sui sistemi di gestione; in particolare, il fatto che la l’alta direzione debba assegnare responsabilità e autorità per assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti della norma e per riferire alla direzione stessa sulle prestazioni del sistema di gestione per la sicurezza delle informazioni, se non definisce la **nomina di un responsabile per il sistema di gestione della sicurezza delle informazioni** poco ci manca. Pur non essendo richiesto un rappresentante della direzione (non lo era neanche nella versione 2005 ISO e 2006 UNI della norma) viene rafforzato il concetto che è necessario assegnare responsabilità precise, all’interno o all’esterno dell’organizzazione (consulente), per garantire la conformità del SGSI.

Il capitolo 6 “**Pianificazione**” tratta, nel paragrafo 6.1, quali azioni occorre attuare per affrontare **rischi ed opportunità**. Infatti sulla base di quanto emerso dall’analisi del contesto dell’organizzazione occorre determinare i rischi e le opportunità che è necessario affrontare per assicurare che il sistema possa conseguire i risultati previsti, possa prevenire, o almeno ridurre, gli effetti indesiderati e realizzare il miglioramento continuo. Le **azioni per affrontare rischi ed opportunità** devono essere **pianificate**, così come le modalità per **integrare ed attuare** le azioni stesse nei processi del proprio sistema di gestione per la sicurezza delle informazioni e per **valutare l’efficacia** di tali azioni.

La **valutazione dei rischi relativi alla sicurezza delle informazioni** è trattata al paragrafo 6.1.2, dove sono riportati i requisiti per il **processo di valutazione del rischio** relativo alla sicurezza delle informazioni. Il processo di valutazione del rischio dovrà comprendere le seguenti attività

- Stabilire e mantenere i criteri di rischio relativo alla sicurezza.

- Assicurare che le ripetute valutazione del rischio producano risultati coerenti, validi e confrontabili tra loro (il metodo usato deve essere ripetibile e riproducibile con risultati coerenti come se fosse un dispositivo di misurazione sotto conferma metrologica).
- Identificare i rischi relativi alla sicurezza.
- Analizzare i rischi individuati, valutando le possibili conseguenze che risulterebbero se tali rischi si concretizzassero e valutando la verosimiglianza realistica di concretizzarsi dei rischi identificati, ovvero la probabilità che essi accadono, e, infine, determinando i livelli di rischio.
- Ponderare i rischi comparando i risultati dell'analisi dei rischi con i criteri stabiliti e definendo le priorità di trattamento dei rischi precedentemente valutati.

Naturalmente **la valutazione dei rischi deve essere documentata.**

Il **trattamento del rischio** relativo la sicurezza delle informazioni (6.1.3) deve essere definito ed applicato attraverso un processo del tutto similare a quello stabilito nella versione precedente della norma, anche se esposto in modo differente. Oltre a selezionare l'opzione di trattamento dei rischi consuete occorre determinare i controlli necessari per attuare le opzioni selezionate per il trattamento del rischio, tenendo presente controlli riportati nell'appendice A e meglio dettagliati nella norma ISO 27002 (anch'essa tradotta finalmente in italiano come UNI CEI ISO/IEC 27002:2014 – *Tecnologie informatiche – Tecniche per la sicurezza – Raccolta di prassi sui controlli per la sicurezza delle informazioni*) al fine di non omettere controlli che potrebbero essere necessari.

Resta la necessità di redigere una **Dichiarazione di Applicabilità** che riporti:

- i controlli selezionati come necessari (che siano attuati o meno) e la relativa giustificazione per l'inclusione;
- i controlli presenti nell'Appendice A della ISO 27001 stessa eventualmente esclusi con le giustificazioni per la loro esclusione
- i controlli selezionati attualmente applicati.

Quest'ultimo punto costituisce una novità nel testo della norma che chiarisce e sancisce una prassi comunemente adottata dagli Organismi di Certificazione, ovvero quella di accettare una dichiarazione di applicabilità di determinati controlli di sicurezza la cui attuazione è stata pianificata, ma deve ancora venire.

Infine occorre predisporre un **piano di trattamento dei rischi** relativi alla sicurezza delle informazioni che dovrà essere approvato dalla Direzione, comprendente anche l'accettazione dei rischi residui che si è deciso di non trattare.

Anche questo **processo di trattamento del rischio dovrà essere documentato**.

Il sistema di gestione per la sicurezza delle informazioni ISO 27001 dovrà porsi degli **obiettivi** e **pianificare le azioni adeguate per conseguirli** (paragrafo 6.2). Le caratteristiche degli obiettivi sono le stesse degli altri sistemi di gestione (devono essere coerenti con la politica, misurabili, ecc.).

La pianificazione delle azioni poste in essere per conseguire gli obiettivi per la sicurezza delle informazioni deve comprendere le **azioni** pianificate, le **risorse** necessarie, le **responsabilità**, i **tempi** di completamento delle azioni, e le **modalità** di **valutazione dei risultati**.

Il capitolo 7 "**Supporto**" non presenta novità significative rispetto all'analogo capitolo delle altre norme relative ad altri sistemi di gestione. Pertanto i paragrafi **Risorse** (7.1), **Competenza** (7.2) Consapevolezza (7.3) e **Comunicazione** (7.4) non presentano sorprese di sorta, ma solo una esplicitazione più chiara rispetto al passato di cosa ci si dovrebbe attendere da un sistema di gestione per la sicurezza delle informazioni.

Il paragrafo 7.5 "**Informazioni documentate**" con i suoi sotto paragrafi descrive i requisiti relativi a **documenti** e **registrazioni,** secondo la dizione delle precedenti norme sui sistemi di gestione. Anche in questo caso i requisiti non presentano novità rispetto al passato, ma solo un diverso ordine di esposizione ed una maggior chiarezza nel descrivere che cosa ci si aspetta da un sistema di gestione documentato.

Non sono richieste procedure particolari, né un manuale del sistema di gestione ISO 27001, ma solo le informazioni documentate indicate nei vari punti della norma.

Il capitolo 8 "**Attività operative**" dispone requisiti relativi ai punti:

- pianificazione e controlli operativi (8.1);
- valutazione del rischio relativo la sicurezza delle informazioni (8.2);
- trattamento del rischio relativo la sicurezza delle informazioni (8.3).

In questo capitolo non ci sono novità rispetto alla versione precedente della norma, ma solo una riscrittura secondo la nuova struttura delle norme sui sistemi di gestione di quanto era già prescritto in passato. I contenuti, in verità, sono alquanto scarni, infatti viene prescritto di mantenere sotto controllo i processi operativi dell'organizzazione (processo produttivo o erogazione del servizio, approvvigionamenti, commerciale, ecc.) attraverso l'attuazione di tutti i controlli di sicurezza pianificati, monitorando ogni cambiamento e rivalutando periodicamente i rischi secondo le modalità già descritte nei paragrafi deò capitolo 6.

Il capitolo 9 "**Valutazione delle prestazioni**", riporta i requisiti per il **monitoraggio**, la **misurazione**, **l'analisi** e la **valutazione** (9.1) del SGSI, per gli **audit** interni (9.2) e per il **riesame della direzione** (9.3). Anche in questo capitolo non sono presenti novità sostanziali rispetto alla precedente versione della norma,

ma solo una riscrittura del testo in modo più chiaro. In particolare viene indicata la necessità di monitorare e misurare l'efficacia dell'attuazione dei controlli di sicurezza e tutti i processi che forniscono evidenza del buon funzionamento del SGSI.

Nel capitolo 10 "**Miglioramento**" sono trattate **non conformità**, **azioni correttive** e **miglioramento continuo**. Anticipando quello che avverrà per la prossima versione della norma ISO 9001:2015, si rileva l'eliminazione delle requisito riguardante le **azioni preventive** che vanno a confluire insieme a tutte le azioni di miglioramento non legate a non conformità o incidenti sulla sicurezza delle informazioni.

È curioso il fatto che mentre nella versione precedente la norma ISO 27001 non dedicava un paragrafo alle non conformità, che venivano citate nel testo, ma erano citati anche gli **incidenti** per la sicurezza delle informazioni, questa nuova versione non tratta gli incidenti – se non nei controlli dell'appendice A – e dedica il paragrafo 10.1 alle non conformità ed alle azioni correttive attuate per eliminarle.

Si ricorda che ACCREDIA ha disposto che Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27001:2005 dovranno essere ritirate entro il 1° ottobre 2015; oltre tale data potranno sussistere solo certificazioni secondo la nuova ISO 27001:2013. Pertanto restano pochi mesi per convertire i vecchi SGSI alla nuova norma. Probabilmente la stragrande maggioranza delle organizzazioni con SGSI certificato o certificando ISO 27001 dispongono già della certificazione ISO 9001 per la qualità, ma la nuova norma ISO 9001:2015, la cui struttura è allineata alla ISO 27001:2013 deve ancora essere ufficialmente emessa.

Il consiglio per le organizzazioni che si stanno adeguando alla 27001:2013 è quello di strutturare il sistema di gestione integrato secondo il nuovo schema, dunque allineare anche il sistema di gestione per la qualità sulla base delle indicazioni disponibili dalla bozza di ISO 90001:2015. Così facendo si avrà un sistema di gestione integrato ISO 9001-27001 omogeneo e meglio gestibile nell'immediato.

Questo probabilmente comporterà ristrutturare il manuale del sistema di gestione, anche se non esplicitamente richiesto dalla nuova norma, al fine di mantenere una continuità con il passato e garantire il controllo su tutta la documentazione del sistema di gestione.

Le modifiche al SGSI non sono sostanziali e riguardano più che altro i 114 controlli di sicurezza dell'appendice A e della ISO 27002 che naturalmente impattano sul trattamento dei rischi e sulla Dichiarazione di Applicabilità (*Statement of Applicability*, SoA).