Scheda informativa su nuove norme relative alla Gestione del Rischio

ISO Guide 73:2009 – ISO 31000:2009 - ISO/IEC 31010:2009

ISO/CD 22301

*Commenti redatti per **AICQ Centronord** a cura di: Gennaro Bacile di Castiglione – Consigliere del Comitato SGQ di AICQ, membro del Gruppo di Lavoro UNI sulla Gestione del Rischio e del "ISO TMB WG on Risk Management", oltre che coordinatore del Gruppo di Lavoro ristretto UNI che sta curando la traduzione della ISO 31000:2009.*

Sigla Norma	Stato	Titolo
ISO GUIDE 73:2009	pubblicata il 15/11/2009	Risk management — Vocabulary Management du risque — Vocabulaire *(edizione bilingue: inglese e francese)* *Non è attualmente prevista una traduzione italiana, ma si sta pensando ad una revisione della* UNI 11230:2007 (Gestione del rischio – Vocabolario)
ISO 31000:2009	pubblicata il 15/11/2009	Risk management — Principles and guidelines *È in fase di preparazione la traduzione italiana, che dovrebbe essere pubblicata nella prima metà del 2010*: UNI ISO 31000:2010 – Gestione del Rischio – Principi e linee guida
ISO/IEC 31010:2009	pubblicata il 01/12/2009	Risk management - Risk assessment techniques
ISO/CD 22301	In fase di bozza iniziale	Societal security – Preparedness and continuity management systems – Requirements

Nota: le traduzioni dei termini originali inglesi riportate di seguito non sono ancora "ufficiali"; in molti casi sono riportati ancora i termini inglesi per maggior chiarezza. Molte traduzioni fanno riferimento ai termini definiti nella UNI 11230:2007 (Gestione del rischio- Vocabolario). Nel testo sono anche messe in evidenza alcune delle principali difficoltà incontrate nella traduzione, sia già chiarite a fronte della UNI 11230:2007, sia in fase di elaborazione.

Sommario

0. Premessa alla ISO Guide 73:2009 ed alla ISO 31000:2009

Le due guide sono state sviluppate contemporaneamente dall'ISO TMB WG on Risk Management, un gruppo di lavoro che fa capo direttamente al Technical Management Board di ISO senza riferimento ad alcun specifico Comitato Tecnico (TC - technical committee). Si tratta di una prima edizione per la ISO 31000 e di una rivisitazione sostanziale della ISO/IEC Guide 73:2002 (Risk management -- Vocabulary -- Guidelines for use in standards).

Vengono trattate insieme in quanto strettamente collegate e tenendo conto del fatto che 29 dei 50 termini definiti nella ISO Guide 73:2009 sono riportati fedelmente ed integralmente nel punto 2 della ISO 31000:2009.

Gli aspetti terminologici sono di importanza fondamentale. Questa affermazione può sembrare una banalità assoluta, in quanto valida sempre nella normazione e non solo, ma a volte sottovalutata con la conseguenza di dare adito ad interpretazioni diverse, spesso contrastanti. Assume un rilievo forse ancora maggiore nel caso del termine rischio e della sua gestione, se si tiene conto che nel linguaggio ed immaginario comune il termine rischio è legato quasi esclusivamente al concetto di pericolo e di possibili danni. Spesso, inoltre, i termini "pericolo" e "rischio" sono utilizzati come sinonimi e non solo nella lingua italiana. Nel seguito proveremo a chiarire meglio questi aspetti che sono alla base delle due norme.

1. ISO Guide 73:2009 - Risk management — Vocabulary

1.1 Indice della ISO Guide 73:2009

Note:

- Al punto 1 è presente la sola definizione di "rischio"
- Al punto 2 la definizione di "risk management" più altre tre
- Il punto 3 è a sua volta suddiviso in:
  - 3.1 "Risk management process", con la sua sola definizione;
  - 3.2 "Termini relativi alla comunicazione e consultazione", con la definizione di "comunicazione e consultazione" più altre due;
  - 3.3 "Termini relativi al contesto", con la definizione di "establishing the context" (riconoscere, delimitare, definire il contesto) più altre tre;
  - 3.4 "Termini relativi alla valutazione del rischio (risk assessment)", con la sua sola definizione;
  - 3.5 "Termini relativi alla identificazione del rischio", con la definizione di "risk identification" più altre cinque;
  - 3.6 "Termini relativi alla analisi del rischio", con la definizione di "risk analysis" più altri otto;
  - 3.7 "Termini relativi alla ponderazione del rischio (risk evaluation)", con la definizione di "risk evaluation" più altri sette;
  - 3.8 "Termini relativi al trattamento del rischio", con la definizione di "risk treatment" più altri sette
  - 3.8.2 "Termini relativi al monitoraggio ed alla misurazione", con sei definizioni.

- In questo vocabolario sono quindi presenti in totale 50 definizioni, 29 delle quali sono riportate fedelmente ed integralmente nel punto 2 della ISO 31000:2009.

1.2 Introduzione e Scopo della ISO Guide 73:2009

La nuova edizione della guida, oltre che per modifiche più o meno significative alle definizioni in essa contenute, si differenzia dalla precedente anche per il fatto di essere destinata non più soltanto a fornire un riferimento per la stesura di norme sul risk Management, ma all'utilizzo da parte di tutti coloro che sono coinvolti nella gestione dei rischi, in modo da favorire una cultura comune, un approccio coerente e l'uso di una terminologia uniforme nella descrizione delle attività, processi e strutture organizzative che hanno a che fare con la gestione dei rischi.

Richiama espressamente la ISO 31000 per i principi e le linee guida sul risk management.

Richiama tra le altre, nella bibliografia, sia la ISO 9000 (*Quality management systems — Fundamentals and vocabulary*), sia la ISO/IEC Guide 51 (*Safety aspects — Guidelines for their inclusion in standards*) di cui è stato approvato da pochi mesi per la revisione della precedente edizione 1999.

Nell'introduzione si mette in evidenza che il risk management è un attività multi disciplinare e che si applica alle più svariate situazioni specifiche ed ai diversi aspetti dei processi gestionali, operativi e di supporto di un'organizzazione. Per questo in alcune circostanze può essere necessario integrare le voci riportate nella guida con ulteriori termini più specifici.

È fondamentale la differenza di base tra la ISO/IEC Guide 51 e le ISO Guide 73/ISO 31000.

I termini e le definizioni dati nella ISO Guide 73:2009 (come peraltro le linee guida ed i principi contenuti nella ISO 31000:2009), sono molto più ampi nei concetti e nell'applicazione di quelli contenuti nella ISO/IEC Guide 51, che si limita agli aspetti del rischio legati alla sicurezza, ovvero quei rischi con conseguenze negative o comunque indesiderabili.

Infatti oltre a gestire le **minacce** che potrebbero impedire di raggiungere i propri obiettivi, le organizzazioni stanno sempre più applicando i processi di risk management e sviluppando un approccio allo stesso per migliorare la gestione delle **opportunità** potenziali.[1]

1.3 Principali definizioni della ISO Guide 73:2009 e della ISO 31000:2009

Le definizioni sono scelte prevalentemente tra quelle riportate anche al punto 2 della ISO 31000:2009. L'ordine con cui vengono commentate nel seguito non è quello con cui sono presentati nella ISO Guide 73:2009, né nella ISO 31000:2009, peraltro in parte diverso tra le due.

Ad esempio si riportano qui di seguito per primi i commenti sulle definizioni e, in alcuni casi dubbi, sulle possibili traduzioni dei termini "event", "consequence" e "likelihood", per facilitare la comprensione dei commenti sulla definizione del termine "risk" che è riportata per prima in entrambe le norme.

Event - evento è definito come "il verificarsi o modificarsi di un particolare insieme di circostanze". In due note si precisa che "un evento può consistere in uno o più episodi, può avere diverse cause e può consistere nel **non verificarsi** di qualcosa". In altre due note si fa riferimento ai termini inglesi "incident" o "accident" cui talvolta ci si puo riferire al posto di utilizzare il termine "evento" ed al fatto che "un evento senza conseguenze può essere identificato come "near miss", "incident",

[1] Appare significativa un'interpretazione, controversa, che si dà del termine cinese "crisi", composto da due ideogrammi, di cui il primo rappresenta il pericolo, il secondo può rappresentare l'opportunità. Tale interpretazione ha ottenuto una vasta popolarità negli Stati Uniti, e non solo, dopo essere stata citata in un discorso di J. F. Kennedy del 1959.

"near hit" o "close call". Qui vi è un problema importante di traduzione relativamente al significato delle parole inglesi "incident", da intendersi come avvenimento o incidente che può avere o meno conseguenze negative, ed "accident" come un avvenimento che ha senz'altro avuto delle conseguenze negative (in italiano si potrebbe parlare di infortunio o, più in generale, di "sinistro". Questo è anche il senso dato ai termini "incident" ed "accident" nella OHSAS 18001:2007. Quanto alle espressioni anglosassoni "near miss", "near hit" o "close call", in italiano si parla in generale di "quasi incidente" o "mancato incidente" (termini che per quanto detto sopra rischiano di generare confusione) "quasi infortunio", "quasi perdita", "infortunio sfiorato", "perdita sfiorata".

Consequence – conseguenza, "esito di un **evento** che influenza gli obiettivi". Nelle note si precisa che:

- una conseguenza può essere certa o incerta e può avere **effetti** positivi o negativi sugli obiettivi;
- le conseguenze di un evento possono essere entro una gamma più o meno vasta ed essere espresse in modo quantitativo o qualitativo;
- le conseguenze iniziali possono aggravarsi attraverso **effetti** indiretti o effetto domino.

Likelihood : questo termine inglese è traducibile in italiano con "**verosimiglianza**" (traduzione utilizzata dai francesi "vraisemblance") o semplicemente con "**possibilità**". Il mio personalissimo parere è che sarebbe opportuno usare in italiano entrambi i termini, in quanto mi sembrerebbe più appropriato usare "possibilità" quando la "likelihood" è riferita ad un evento, mentre "verosimiglianza" quando è riferita alle conseguenze. La definizione è "chance of something happening", che potrebbe essere tradotta con "eventualità che accada qualcosa" o qualcosa di simile (nella sostanza: "plausibilità di un accadimento ipotizzabile"). Una prima nota chiarisce il concetto, mentre una seconda mette in evidenza le difficoltà di traduzione in altre lingue. Si riportano in modo integrale le due note tradotte liberamente:

NOTA 1 Nella terminologia della gestione del rischio, il termine "verosimiglianza" (o "possibilità") è utilizzato per riferirsi alla eventualità che qualcosa accada, sia esso definito, misurato, determinato oggettivamente o soggettivamente, qualitativamente o quantitativamente, e descritto utilizzando termini generici o in modo matematico (come probabilità o frequenza con riferimento ad un dato intervallo di tempo).

NOTA 2 Il termine anglosassone "likelihood" non ha un diretto equivalente in altre lingue; invece, è spesso usato il termine equivalente di "probability". Tuttavia, in lingua inglese, il termine "probability" è spesso interpretato in senso stretto come un termine matematico. Pertanto, nella terminologia della gestione del rischio, il termine "likelihood" è utilizzato con l'accezione più ampia, come ha il termine "probability" in altra lingue diverse dall'inglese.

Da notare che nella ISO Guide 73:2009 sono definiti anche i termini "probability" e "frequency" con le loro accezioni matematiche. L'uso di questi due termini non è presente nella ISO 31000:2009.

Risk – rischio. È definito come "effetto sugli obiettivi dell'incertezza". Si riportano integralmente le note:

NOTA 1 Un effetto è uno scostamento da quanto atteso – positivo e/o negativo.

NOTA 2 Gli obiettivi possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione).

NOTA 3 Il rischio è spesso caratterizzato dal riferimento a **eventi** potenziali e **conseguenze**, o una combinazione di questi.

NOTA 4 Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi i cambiamenti nelle circostanze) e della "**likelihood**" *(che qui tradurrei con "**possibilità**")* del suo verificarsi.

NOTA 5 L'incertezza è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro "**likelihood**" *(che qui forse tradurrei con "**verosimiglianza**")*.

Il commento che riporto è non solo personale, ma in buona parte condiviso dal mirror-group italiano UNI: si tratta di una definizione a dir poco "insidiosa", anche se, per fortuna, è in parte chiarita meglio dalle note. Il riferimento, nella definizione base, alla incertezza, pur essendo condivisibile, non sembra essere la principale caratteristica del rischio e può ingenerare confusione con altri significati che allo stesso termine si danno nel linguaggio tecnico (ad es.: incertezza di misura). Sarebbe stato meglio inserirlo in una nota.
Inoltre parlare di "effetto" risulta oltremodo fuorviante, in quanto, con una definizione così formulata, il rischio può apparire come un sinonimo di "conseguenza". Si passa cioè dall'errore, che spesso si fa nel linguaggio comune, di usare come sinonimi "pericolo" e "rischio" a quello di rendere sinonimi "rischio" e "conseguenza".
Manca anche il riferimento al raggiungimento degli obiettivi che avrebbe potuto renderla più chiara.
Volendo mantenere a tutti i costi il riferimento all'incertezza nella definizione base, questa avrebbe potuto essere modificata in modo simile a quanto segue:
"*Condizione relativa alla possibilità e capacità di raggiungere gli obiettivi, risultante dall'incertezza sulle variabili coinvolte*".
La definizione originale può apparire ancora più incomprensibile o comunque fonte di notevoli fraintendimenti; "effect of uncertainty on objectives" che, tradotta in italiano mantenendo la stessa costruzione della frase, diventerebbe "effetto dell'incertezza sugli obiettivi". Qualcuno potrebbe essere portato a pensare che l'incertezza sia sugli obiettivi. In questo caso, cioè se un'organizzazione fosse incerta su quali siano i propri obiettivi, non saremmo di fronte solo ad un rischio, ma al "padre" di tutti i rischi! In alcune organizzazioni, però, non siamo troppo lontani una tale situazione.

Risk source - fonte di rischio, "elemento che da solo o in combinazione con altri possiede il potenziale intrinseco di originare il rischio". Una nota precisa "una fonte di rischio può essere materiale o immateriale (*tangibile o intangibile*).

Risk management - gestione del rischio, "attività coordinate per guidare e tenere sotto controllo una organizzazione con riferimento al rischio".

Risk management framework - struttura di riferimento per la gestione del rischio, "insieme di componenti che fornisce le fondamenta (comprendenti la politica, gli obiettivi, il mandato e l'impegno a gestire il rischio) e le disposizioni organizzative (comprendenti piani, relazioni, responsabilità, risorse, processi e attività) per progettare, attuare, monitorare, riesaminare e migliorare in continuo la gestione del rischio nell'intera organizzazione". Un'ulteriore nota precisa che il "risk management framework" è inserito all'interno delle politiche e prassi strategiche ed operative complessive dell'organizzazione.

Risk management process - processo di gestione del rischio, "applicazione sistematica delle politiche, procedure e prassi di gestione alle attività di comunicazione, consultazione, definizione del contesto e identificazione, analisi, ponderazione, trattamento, monitoraggio e riesame del rischio".

Stakeholder - portatore d'interesse, "persona od organizzazione che può influenzare, essere influenzata da, o percepire se stessa come influenzata da una decisione o attività". Una nota precisa che un "decision maker" può essere considerato uno "stakeholder".

È significativo notare che la condizione di "stakeholder" non è sempre qualcosa di oggettivo, ma può dipendere dalla **percezione** di un individuo, gruppo o organizzazione. Il termine "stakeholder" sembra coincidere con "interested party", espressione definita nelle norme delle Famiglie ISO 9000 ed ISO 14000, sia pure in modo leggermente diverso; non vi è più infatti la precisazione, presente

nella ISO Guide 73:2002, che *il termine "stakeholder" include ma ha un significato più ampio di "interested party" come definito in ISO 9000:2000*. Manca nelle definizioni Famiglie ISO 9000 ed ISO 14000 l'aspetto legato alla percezione, che, però, sarebbe da ritenere sottintesa, sicuramente in campo ambientale. Nessuna reale differenza tra "stakeholders" e "interested parties", confermata da un documento ISO, sia pur non ancora definitivo, sulla terminologia relativa ai sistemi di gestione, che inserisce i due termini con definizioni esattamente uguali e quasi identica a quella della ISO Guide 73:2009.

Per i portatori d'interesse è però necessario distinguere tra interessi "legittimi" o "illegittimi" e tra atteggiamento "benevolo" o "malevolo". Nella definizione del contesto occorre identificarle, valutandone correttamente legittimità e benevolenza per analizzare e trattare con proprietà i rischi correlati. Ad esempio è necessario contrastare gli interessi di criminali e terroristi, che a ben vedere ricadrebbero nella definizione. In alcuni casi interessi legittimi possono anche non essere benevoli: i concorrenti o la popolazione che è, o si ritiene, disturbata o danneggiata da attività ed emissioni di un'azienda. Tutto ciò va considerato attentamente nel processo di gestione del rischio.

Risk criteria - criteri di rischio, "termini di riferimento a fronte dei quali è ponderata (evaluated) la significatività del rischio". In due note si precisa che "possono aver origine da norme, leggi, politiche e altri requisiti" e che "si basano sugli obiettivi dell'organizzazione e sul contesto interno ed esterno", quindi anche sulle percezioni degli stakeholder.

Risk assessment - valutazione del rischio, "processo complessivo di identificazione del rischio, analisi del rischio e ponderazione (evaluation) del rischio"

Risk evaluation - ponderazione del rischio, "processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio e/o la sua magnitudo sia accettabile o tollerabile". Una nota precisa che " la ponderazione del rischio agevola la decisione circa il trattamento del rischio"

La traduzione di "risk evaluation" con "ponderazione del rischio" era stata definita già nella UNI 11230:2007 per evitare l'incongruenza presente in alcune traduzioni di norme precedenti relative alla gestione dei rischi, per specifici settori, in cui il processo complessivo di "risk assessment" ("valutazione del rischio") comprendeva tra le altre la fase di "risk evaluation", tradotta anch'essa con "valutazione del rischio".

risk treatment - trattamento del rischio, "processo per modificare il rischio". Si riportano le tre note significative:

NOTA 1 Il trattamento del rischio implica:

- evitare il rischio decidendo di non iniziare o non continuare l'attività che da origine ad esso;
- assumere o accrescere il livello di rischio al fine di cogliere un'opportunità;
- rimuovere la fonte di rischio;
- modificare la "likelihood";
- modificare le conseguenze;
- condividere il rischio con altra/e parte/i (compresi contratti e finanziamento del rischio); e
- ritenere il rischio con una decisione basata su conoscenze precise.

NOTA 2 I trattamenti del rischio che affrontano conseguenze negative sono talvolta denominati "protezione dal rischio", "eliminazione del rischio", "prevenzione del rischio", e "riduzione del rischio".

NOTA 3 Il trattamento del rischio può generare nuovi rischi o modificare rischi esistenti.

residual risk - rischio residuo, "rischio rimanente a seguito del trattamento del rischio". In due note si precisa che "può comprendere rischi non identificati" e che è noto anche come "rischio ritenuto".

ISO 31000:2009 - Risk management — Principles and guidelines

1.4 Indice della ISO 31000:2009

1.5 Introduzione e Scopo della ISO 31000:2009

La norma rappresenta l'evoluzione della cultura e delle prassi in atto a proposito di gestione del rischio. Prende le mosse dalla norma AS/NZS 4360 (Risk Management – emessa per la prima volta nel 1995, dagli Enti di normazione australiano e neozelandese, revisionata nel 1999 ed alla sua terza edizione nel 2004). AS/NZS 4360 è una guida generale accompagnata da una serie di altri documenti specifici di applicazione.

L'introduzione ed il punto relativo allo scopo sono ampiamente dettagliati e riassumono in maniera efficace quello che poi è il corpo della ISO 31000:2009; perciò il presente paragrafo di questa scheda informativa sarà altrettanto dettagliato e, in parte, sopperirà alla sinteticità dei commenti sui paragrafi dal 3 in poi.

Tiene sostanzialmente conto dei più accreditati punti di vista sui rischi e sulla loro gestione ed è estremamente generale, tanto da poter essere utilizzata da qualsiasi tipo di organizzazione, pubblica o privata, da gruppi di persone associate in qualsiasi forma o da singoli individui, in qualsiasi settore di attività.

Parte dal presupposto che "le organizzazioni di tutti i tipi e dimensioni si trovano ad affrontare fattori ed influenze interni ed esterni che rendono incerta la realizzazione dei propri obiettivi". Tra le novità, rispetto alle norme nazionali che l'hanno preceduta, vi è proprio l'enfasi data al concetto di "incertezza", intesa come lo *stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della sua verosimiglianza*.

"Tutte le attività di un'organizzazione comportano dei rischi". Ritengo che questo concetto fondamentale debba essere esteso a qualsiasi attività anche del singolo individuo, non solo nella vita lavorativa, ma anche in quella strettamente personale, familiare, ecc. Dalla nascita, meglio dal concepimento, ciascun individuo è interessato da rischi: sino a quando una persona non inizia a ad acquisire una propria autonomia, la gestione dei suoi rischi è demandata ai propri tutori. Inoltre occorre tenere ben presente che non solo le attività, ma anche la **non attività** comporta dei rischi.

Scopo della ISO 31000:2009 è quello di mettere a disposizione di tutti i suoi lettori i "principi e le linee guida generali sulla gestione del rischio".

La norma può essere utilizzata da qualsiasi organizzazione pubblica o privata, a scopo di lucro o meno, associazione di qualsiasi tipo, gruppo o individuo e, pertanto, non è specifica per alcuna industria o settore. Si precisa in una nota che, con il termine generale "organizzazione", ci si riferisce a tutti i diversi potenziali utilizzatori della norma.

Può essere applicata a qualsiasi tipo di rischio, di qualsiasi natura e con conseguenze positive o negative. Può essere applicata lungo tutta la vita di un'organizzazione e ad un'ampia gamma di attività, processi (operativi, di supporto e gestionali, incluse strategie e decisioni), funzioni, progetti, prodotti, servizi e beni (assets).

È espressamente dichiarato che non è destinata ad essere utilizzata per la certificazione.

Ritengo importante precisare in questa sede che è stato sventato il pericolo di introdurre un ulteriore "Sistema di Gestione" (cosa desiderata da alcuni, ma che per fortuna la maggioranza dei paesi, tra cui l'Italia, sono riusciti ad evitare. Il "Risk Management" è un processo (un macro-processo) che si dovrebbe integrare con tutti gli altri processi dell'organizzazione ed essere un elemento fondamentale per una gestione consapevole e responsabile della stessa.

Tenendo conto di questo la ISO 31000:2009 "raccomanda che le organizzazioni sviluppino, attuino e migliorino in continuo una struttura di riferimento (framework) il cui lo scopo è integrare il processo per gestire il rischio nella governance complessiva dell'organizzazione, nella strategia e nella pianificazione, nella gestione, nei processi di reporting, nelle politiche, nei valori e nella

cultura", ed aiuta a mettere in pratica tale raccomandazione. Si ribadisce che "l'adozione di processi coerenti all'interno di una struttura di riferimento generale può contribuire ad assicurare che il rischio sia gestito efficacemente, con efficienza e in maniera coerente in tutta l'organizzazione".

Ogni settore od applicazione specifici del risk management ha proprie necessità, criteri, stakeholder ed interlocutori in genere con le loro percezioni in merito. Una caratteristica fondamentale delle norme generali sulla gestione del rischio, così come della ISO 31000:2009, è l'attività iniziale di "definire il contesto" ("establishing the context"). Questa fase iniziale consente di "cogliere gli obiettivi dell'organizzazione, l'ambiente in cui essa persegue tali obiettivi, i relativi stakeholder ed i diversi punti di vista su quelli che sono i criteri di rischio – elementi che contribuiscono tutti a rivelare e valutare la natura e la complessità dei propri rischi".

Tra i vantaggi di una gestione del rischio, attuata e mantenuta attiva in conformità alla ISO 31000:2009, sono riportati tra gli altri i seguenti:

- aumentare la probabilità di raggiungere gli obiettivi;
- incoraggiare una gestione proattiva volta a favorire le opportunità, a migliorare la prevenzione delle perdite e la gestione degli incidenti, per minimizzare i danni;
- favorire la consapevolezza della necessità di identificare e trattare il rischio nell'intera organizzazione;
- migliorare l'identificazione delle opportunità e delle minacce;
- aiutare a soddisfare i requisiti cogenti e le norme internazionali applicabili;
- migliorare il reporting sia cogente, sia volontario;
- migliorare la governance, l'efficacia e l'efficienza operative, i controlli e l'assegnazione di risorse per il trattamento dei rischi;
- incrementare la fiducia degli stakeholder;
- costituire una base affidabile per il processo decisionale e la pianificazione (decisioni basate su dati di fatto – uno degli otto principi alla base della famiglia ISO 9000);
- accrescere le prestazioni sia in ambito salute e sicurezza, sia in tema di protezione ambientale;
- migliorare la resilienza organizzativa (intesa come capacità di sopportare le avversità e reagire prontamente);

In uno schema (figura 1), che riprende le figure 2 e 3 riportate nel seguito, sono messe un evidenza le relazioni tra i principi, che influenzano prevalentemente gli aspetti legati al mandato ed all'impegno della direzione e l'attuazione del processo di "risk management".

1.6 Principi (ISO 31000:2009)

a) Risk management creates and protects value. Contribuisce in misura dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto, gestione dei progetti, efficienza nei processi produttivi, governance e immagine/reputazione.

b) Risk management is an integral part of all organizational processes. È parte integrante di tutti i processi di un'organizzazione (gestionali, di supporto e operativi, inclusa la pianificazione strategica e la gestione dei progetti anche di cambiamento e miglioramento), rientra tra le responsabilità della direzione.

c) Risk management is part of decision making. Aiuta a stabilire una scala di priorità, a distinguere tra line d'azione alternative e ad effettuare scelte consapevoli (decisioni basate su dati di fatto).

d) Risk management explicitly addresses uncertainty. Si ribadiscono concetti espressi nell'introduzione e nella definizione di rischio.

e) Risk management is systematic, structured and timely. Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.

f) Risk management is based on the best available information. Occorre porre una particolare attenzione alle fonti di dati ed informazioni e valutarle criticamente, tenendo conto di qualsiasi limitazione nei dati utilizzati o della possibilità di divergenza di opinione tra gli stakholder e/o tra specialisti interpellati.

g) Risk management is tailored. Deve essere "su misura", ovvero in linea con il contesto esterno ed interno e con il profilo di rischio (descrizione dell'insieme dei rischi) dell'organizzazione.

h) Risk management takes human and cultural factors into account. Occorre individuare capacità, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.

i) Risk management is transparent and inclusive. Il coinvolgimento tempestivo ed appropriato degli stakeholder e, in particolare, dei decision maker, assicura che la gestione del rischio sia sempre pertinente ed aggiornata. Il coinvolgimento, inoltre, fa sì che gli stakeholder siano opportunamente rappresentati ed i loro punti di vista presi in considerazione nel definire i criteri di rischio.

j) Risk management is dynamic, iterative and responsive to change. Il monitoraggio ed il riesame fanno sì che il quadro dei rischi siano sempre aggiornati al modificarsi del contesto interno e/o esterno: possono emergere nuovi rischi, alcuni modificarsi ed altri scomparire.

k) Risk management facilitates continual improvement of the organization. Si dovrebbero sviluppare ed attuare strategie per migliorare la maturità della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione (con rif all'Appendice A).

1.7 Struttura di riferimento (Framework - ISO 31000:2009)

In questo punto della norma si chiarisce meglio il ruolo della struttura di riferimento indicata tra le definizioni. Come sempre l'impegno della direzione è fondamentale, così come la definizione di indicatori di prestazione relativi al risk management e di una politica ed obiettivi per la gestione del rischio, in linea con la cultura dell'organizzazione, con la politica generale e con gli altri obiettivi.

Si ribadisce l'importanza del rispetto dei requisiti cogenti, dell'assegnazione di responsabilità e di adeguate risorse.

La figura 2 illustra come i componenti del framework sono in relazione sequenziale tra loro mette in evidenza il ciclo PDCA che sta alla base del miglioramento continuo di qualsiasi processo e struttura gestionale.

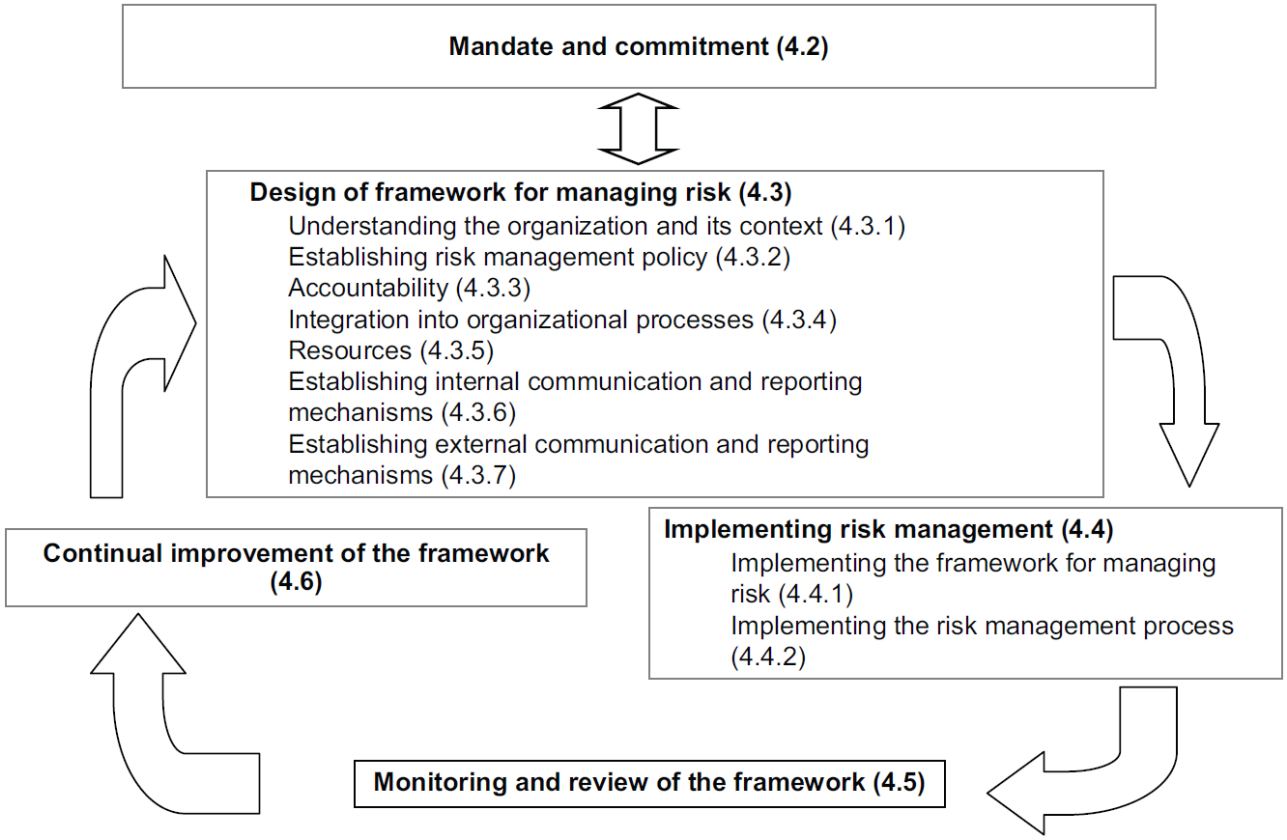

Figure 2 — Relationship between the components of the framework for managing risk

La progettazione (design of framework) prende le mosse dalla comprensione e definizione del contesto interno ed esterno e, oltre a quanto già ricordato a proposito di politica, responsabilità, assegnazione risorse ed integrazione in tutti gli altri processi e prassi dell'organizzazione, insiste sulla determinazione di meccanismi adeguati di comunicazione e reporting interni ed esterni.

Dalla progettazione (fase Plan del ciclo PDCA) si passa all'attuazione di quanto pianificato/progettato, framework e processo di risk management (fase Do) e, successivamente, al monitoraggio e riesame (fase Check) ed al miglioramento continuo del frame work (parte della fase Act).

1.8 Processo (ISO 31000:2009)

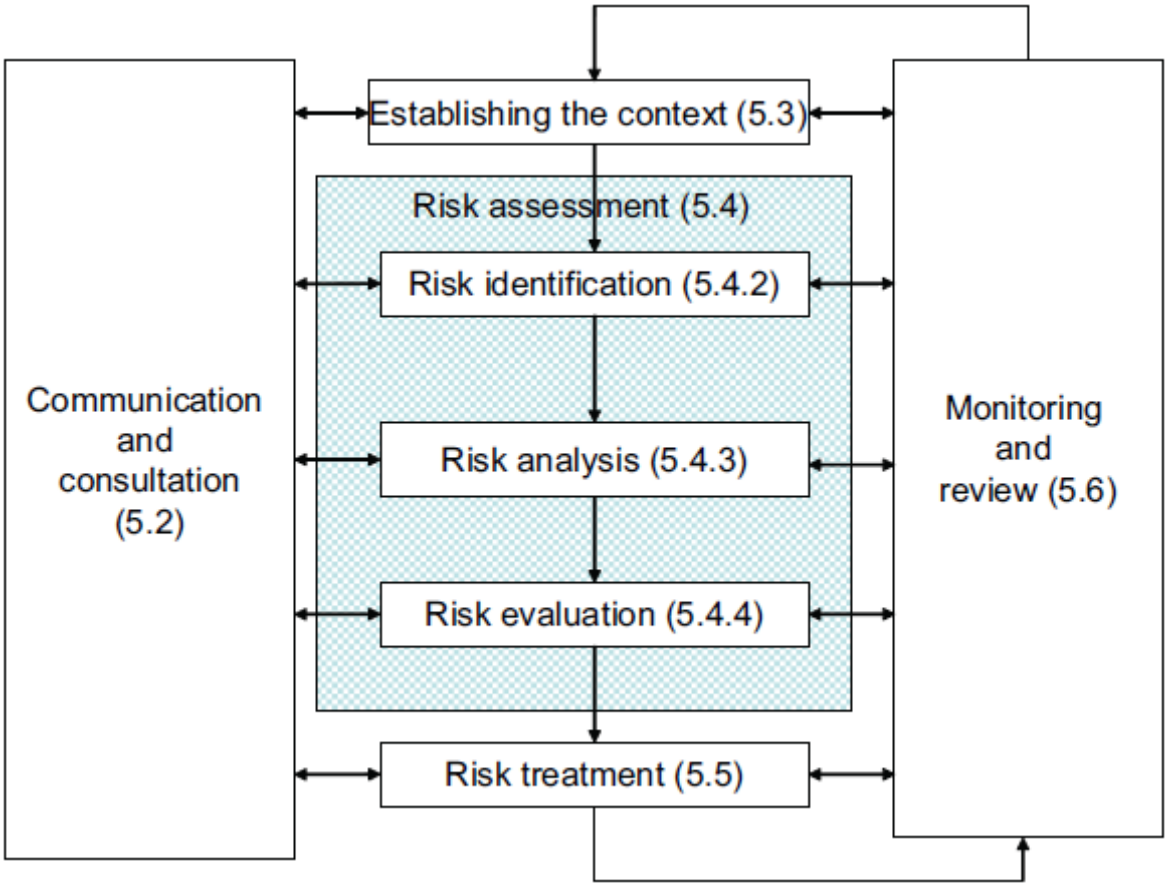

Figure 3 — Risk management process

Al punto 5 viene descritto in dettaglio il processo di risk management ed i suoi diversi sotto-processi. Si insiste sull'importanza della comunicazione e consultazione per tutti gli altri sotto-processi di risk management, in particolare per definire il contesto ed i criteri di rischio (da utilizzare per valutarne la significatività), quindi per tutte le fasi del risk assessment e, successivamente, sul trattamento. La comunicazione e la consultazione con i portatori di interesse sono importanti poiché i loro giudizi sul rischio si basano sulle proprie percezioni.

Per il trattamento si descrivono, tra l'altro, le modalità per la scelta tra le varie opzioni (descritte anche nella definizione riportata prima), mettendo in evidenza la necessità del bilanciamento dei valori e percezioni degli stakeholder, oltre che dei costi e degli sforzi di attuazione a fronte dei benefici derivanti, con considerazione dei requisiti cogenti e di altra natura, come la responsabilità sociale e la protezione dell'ambiente. Si passa poi ad esaminare la predisposizione ed attuazione dei piani per il trattamento dei rischi.

Si tratta, poi, del monitoraggio e riesame dei rischi, del processo e del framework di risk management.

Infine si introduce l'aspetto relativo alla registrazione nell'ambito del processo di risk management, non presente negli schemi delle figure, ma importante per assicurare la rintracciabilità delle decisioni ed attività e per garantire la disponibilità di dati ed informazioni che costituiscono la base per il miglioramento nei metodi e negli strumenti, così come nel processo complessivo.

1.9 Appendice A (informativa - ISO 31000:2009)Caratteristiche di una gestione del rischio avanzata (enhanced)

Nell'appendice A si illustrano quelli che possono essere considerati degli attributi che consentano di raggiungere i risultati chiave nella gestione dei rischi e si danno alcuni suggerimenti per poter definire indicatori in grado di fornire una misura delle prestazioni del processo di risk management, nell'ambito di ciascun attributo.

Gli attributi descritti sono:

- miglioramento continuo;
- piena responsabilità per i rischi;
- applicazione della gestione del rischio nell'intero processo decisionale;
- comunicazione continua;
- piena integrazione nella struttura di governance dell'organizzazione.

2. Informazioni sintetiche sulla ISO/IEC 31010:2009

Titolo: Risk management - Risk assessment techniques
(Gestione del Rischio – Tecniche per la valutazione del rischio)

2.1 Indice (ISO/IEC 31010:2009)

Bibliography

2.2 Introduzione e scopo (ISO/IEC 31010:2009)

L'introduzione richiama molti dei concetti riportati nell'introduzione della ISO 31000:2009. Tra gli scopi c'è quello di essere di supporto alla ISO 31000:2009 nella fase centrale di risk assessment.

Si precisa anche quello che è al di fuori dello scopo e campo di applicazione della norma:

- non è prevista per la certificazione, utilizzo in campo regolamentato o contrattuale;
- non fornisce specifici criteri per identificare la necessità di analisi dei rischi, né specifica il tipo di analisi del rischio richiesta per una particolare applicazione;
- non riporta né si riferisce a tutte le tecniche esistenti; l'omissione di qualche tecnica non vuol dire che non sia valida; il fatto che un metodo sia applicabile ad una particolare circostanza non vuol dire che debba essere necessariamente applicato
- non tratta specificamente di sicurezza; in quest'ultimo caso si rimanda alla ISO/IEC Guide 51 attualmente in fase di revisione.

2.3 Riferimenti normativi e definizioni (ISO/IEC 31010:2009)

I riferimenti normativi richiamati come indispensabili per l'applicazione della ISO/IEC 31010 sono la ISO 31000 e la ISO Guide 73; quest'ultima è l'unico riferimento per le definizioni.

2.4 Risk assessment concepts (ISO/IEC 31010:2009)

Si ribadiscono concetti espressi nella ISO 31000:2009 a proposito del "framework" e del processo di risk management in generale.

2.5 Risk assessment process (ISO/IEC 31010:2009)

Si entra nel merito processo di risk assessment approfondendolo molto di più di quanto espresso nella ISO 31000:2009, soprattutto per la fase di risk analysis. Si insiste sulla necessità di documentare il processo di risk assessment e sul monitoraggio e riesame dello stesso. L'ultimo paragrafo di questo punto è dedicato all'applicazione del risk assessment durante le fasi del ciclo di vita di attività, progetti e prodotti: dall'idea iniziale, alla realizzazione ed al completamento finale, che potrebbe includere la messa fuori uso e lo smaltimento delle attrezzature.

Può essere applicato in tutte le fasi del ciclo di vita, con modalità e grado di dettaglio diversi in relazione alle esigenze di ciascuna fase. Nella fase iniziale di un'idea, durante lo studio di fattibilità, può essere molto utile per decidere se procedure o meno. Quando siano disponibili più opzioni, si può utilizzare il risk assessment per ponderare le diverse alternative in modo da essere aiutati nell'identificare quella che presenta il miglior rapporto tra rischi positivi e negativi.

Nella fase di progettazione e sviluppo, contribuisce, tra l'altro, ad assicurare che i rischi siano ad un livello tollerabile, ad ottenere il miglior rapporto costi-benefici possibile, ad identificare rischi che potrebbero avere un impatto sulle fasi successive del ciclo di vita.

2.6 Selection of risk assessment techniques (ISO/IEC 31010:2009)

In questo punto vengono analizzate le modalità e le motivazioni che possono portare alla scelta di una particolare tecnica piuttosto che un'altra. Alcuni concetti esposti sono:

- Il risk assessment può essere effettuato con diversi gradi di approfondimento e dettaglio, utilizzando uno o più metodi che spaziano dal semplice al complesso.
- La forma ed i suoi risultati dovrebbero essere coerenti con i criteri sviluppati nella fase di definizione del contesto.

- Le tecniche per essere considerate adeguate dovrebbero:
  - essere giustificabili ed appropriate alla situazione dell'organizzazione che si sta considerando;
  - fornire risultati in una forma tale da accrescere la comprensione della natura del rischio e di come possa essere trattato;
  - poter essere utilizzate in modo da risultare tracciabili, ripetibili e verificabili.
- Alcuni fattori che possono influenzare la scelta sono:
  - gli obiettivi della valutazione.
  - le esigenze dei decision-makers.
  - il tipo e la gamma dei rischi da analizzare;
  - l'ampiezza potenziale delle conseguenze. La percezione iniziale può essere modificata man mano che lo studio avanza;
  - il grado di perizia, le risorse umane e di altro tipo richieste;
  - la disponibilità di informazioni e dati;
  - la necessità di modificare/aggiornare la valutazione del rischio (alcune tecniche rendono più facile le modifiche successive);
  - qualsiasi requisito legale o contrattuale.

2.7 Appendici A e B (informative) e Bibliografia

Nell'appendice A vi è un confronto tra le varie tecniche descritte successivamente nell'appendice B. Vi è una tabella sull'applicabilità delle tecniche esaminate nelle varie fasi del risk assessment: risk identification, analysis and evaluation. La risk analysis è suddivisa in ulteriori sotto-fasi (consequence analysis; qualitative, semi-quantitative or quantitative probability estimation; assessing the effectiveness of any existing controls; estimation the level of risk). Una seconda tabella indica e classifica gli attributi delle varie tecniche che possono influenzarne la scelta.
Le tecniche descritte con un certo dettaglio in appendice B sono le seguenti:

1. Brainstorming	16. Cause and consequence analysis
2. Structured or semi-structured interviews	17. Cause-and-effect analysis
3. Delphi	18. Layer protection analysis (LOPA)
4. Check-lists	19. Decision tree
5. Primary hazard analysis	20. Human reliability analysis
6. Hazard and operability studies (HAZOP)	21. Bow tie analysis
7. Hazard Analysis and Critical Control Points (HACCP)	22. Reliability centred maintenance
	23. Sneak circuit analysis
8. Environmental risk assessment	24. Markov analysis
9. Structure « What if? » (SWIFT)	25. Monte Carlo simulation
10. Scenario analysis	26. Bayesian statistics and Bayes Nets
11. Business impact analysis	27. FN curves
12. Root cause analysis	28. Risk indices
13. Failure mode effect analysis	29. Consequence/probability matrix
14. Fault tree analysis	30. Cost/benefit analysis
15. Event tree analysis	31. Multi-criteria decision analysis (MCDA)

Nella bibliografia sono riportate alcune norme IEC ed ISO collegate ad alcune delle tecniche illustrate in appendice B.

3. Cenni sulla ISO/CD 22301

Titolo: Societal security – Preparedness and continuity management systems – Requirements

Questa norma è ancora in una fase di Committee Draft, ovvero una bozza che potrebbe ancora subire significative modifiche.

3.1 Indice della bozza attuale

0 Introduction (General, The Plan-Do-Check-Act (PDCA) cycle)
1 Scope
2 Normative references
3 Terms and definitions
4 Establish the PCMS (Preparedness and Continuity Management Systems)
4.1 General requirements
4.2 Management responsibility
4.3 PCMS requirements
4.4 Business impact analysis and risk assessment (Legal and other requirements, Business impact analysis, Risk assessment)
4.5 Documentation requirements
4.6 Planning (Objectives and plans to achieve them, Provision of resources)
5 Implement and operate the PCMS
5.1 Selection of risk treatment options (Establishing resource requirements, Protection and mitigation)
5.2 PCMS competence and awareness
5.3 Preparedness and continuity procedure requirements (General, Protection and mitigation, Communication and warning, Response, Recovery)
5.4 Exercising and testing preparedness and continuity arrangements
6 Monitor and review the PCMS
6.1 Performance measurement and monitoring
6.2 Evaluation of preparedness and continuity arrangements
6.3 Audit of PCMS
6.4 Management review of PCMS (Input to management review, Output from management review)
7 Maintain and improve the PCMS
7.1 Continual improvement
7.2 Nonconformity, corrective action and preventive action
8 Annex A (normative) Consistency to ISO 9001, ISO 14001 and ISO 27001
Bibliography

3.2 Considerazioni

Deriva in prima battuta dalla BS 25999-2:2007 Business Continuity Management – Requirements.

Entrambe possono essere oggetto di certificazione, contribuendo ad aumentare la fiducia delle parti interessate, tra cui i clienti per i quali può essere fondamentale la garanzia della continuità nelle forniture, soprattutto nel caso di servizi di primaria importanza.

Riguarda la preparazione e la risposta alle emergenze ed alle situazioni di crisi in generale, ed i piani per ristabilire la piena operatività dell'organizzazione dopo una crisi.

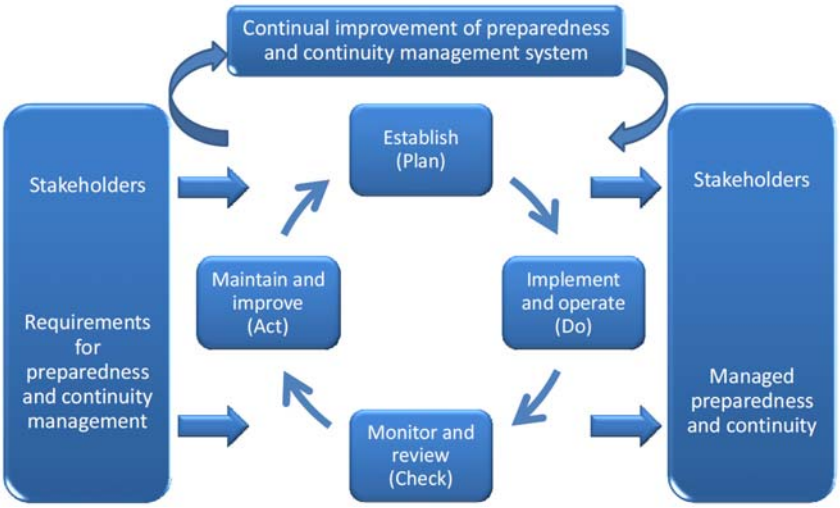

Figura 1 Ciclo PDCA applicato ai processi del Preparedness and Continuity Management System

Un commento puntuale a tale norma appare premature. Si riportano comunque due figure presenti nella bozza attuale che forniscono un'idea di quelli che potranno essere i contenuti.

Anche in questo caso è chiaramente richiamato il ciclo PDCA.

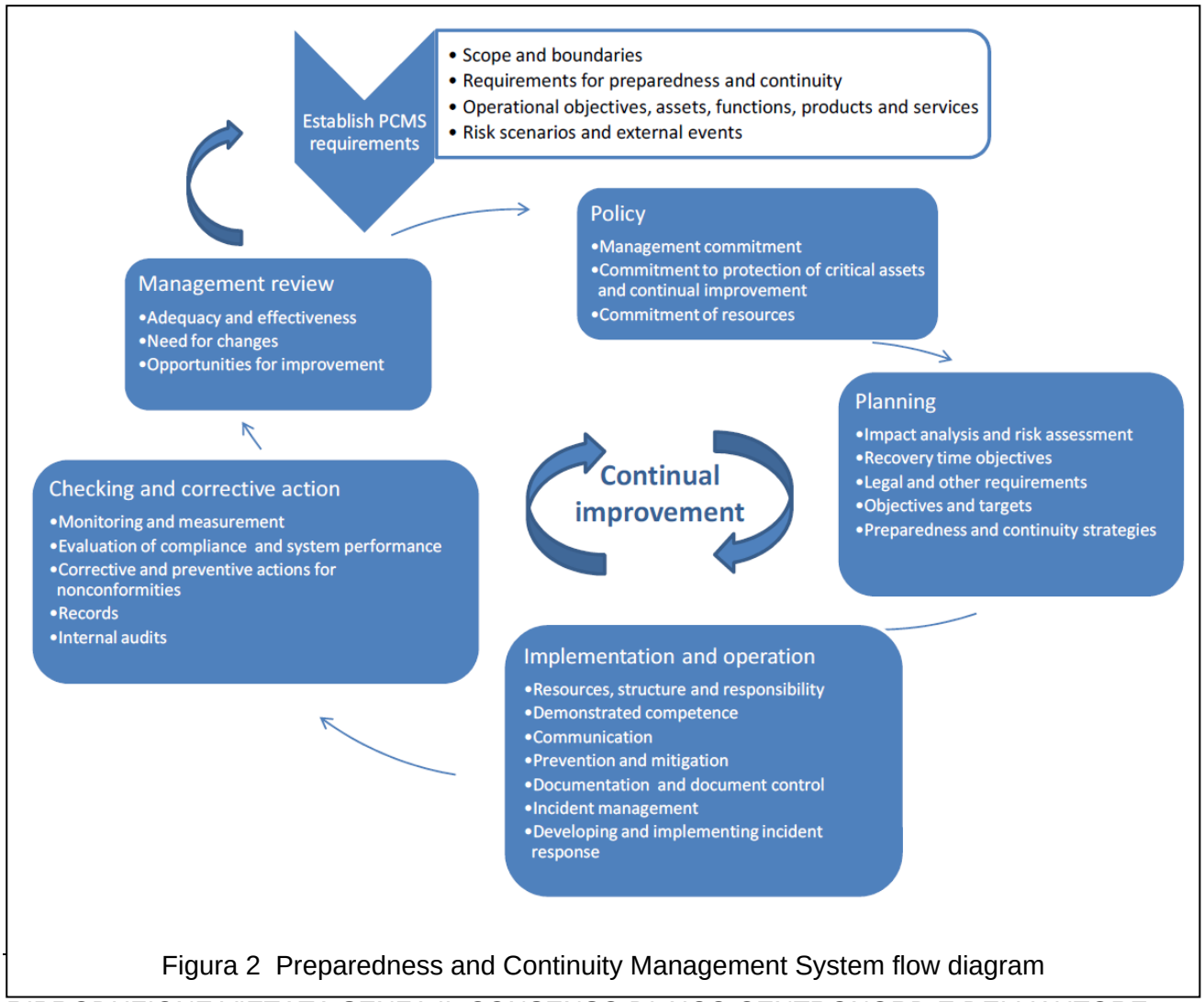

Figura 2 Preparedness and Continuity Management System flow diagram