La disciplina dell'analisi del rischio: la valutazione e la gestione

Quando parliamo di analisi dei rischi esaminiamo il cosiddetto concetto di information security risk management. Per information security risk management viene definito il processo di identificazione, controllo, eliminazione o minimizzazione di eventi incerti che possono danneggiare le risorse di un sistema IT. L'Information Security Risk Management dagli anni '70 è uno degli aspetti fondamentali della Corporate Governance. Si contrappone all'approccio basato sull'adozione di misure general pur pose (obiettivo generale). La sicurezza complessiva di un sistema è pari alla sicurezza dell'anello più debole della catena. Lo scenario normativo dell'analisi del rischio deve considerare i vincoli sul trattamento dei dati imposti da leggi e norme. Il Codice in materia di protezione dei dati personali (D. Lgs. 196/2003) sancisce l'obbligo di redigere un "Documento Programmatico sulla Sicurezza" contenente tra l'altro l'analisi dei rischi che incombono sui dati
Passiamo ora ad esaminare quali sono gli standard di riferimento. Nello specifico sono i seguenti:
1) ISO 27000;
2) ISO 27001 :"Information Security Management System requirements standard", in conformità con il quale si ottiene la certificazione;
3) ISO 27002 : ha sostituito la ISO 17799 e contiene un set di control objectives e di controlli mirati a raggiungere gli obiettivi ed inoltre contiene delle guide all'implementazione;
4) ISO 27003 che contiene una guida all'implementazione dell'ISMS;
5) ISO 27004 che contiene delle metodologie di metrica e misurazione dell'efficacia dell'ISMS;
6) ISO 27005: "Information Security Risk Management standard" in sostituzione della BS 7799 Part 3 e dell'ISO TR 13335 Part 3 più vari standard specifici di settore.
Nello specifico i riferimenti del Risk management sono i seguenti:
I**SO Guide 73:2002** – "Coordinated activities to direct and control an organization with regard to risk";
ISO 27001 – "Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies an objectives";
ISO 27005 (ex ISO 13335) – "Guidelines designed to assist the satisfactory implementation of information security based on risk management approach";
Passiamo ora ad esaminare il modello PDCA (Plan, Do, Check, Act) cioè pianifica, realizza, controlla ed agisci cosi visualizzato nella seguente figura:

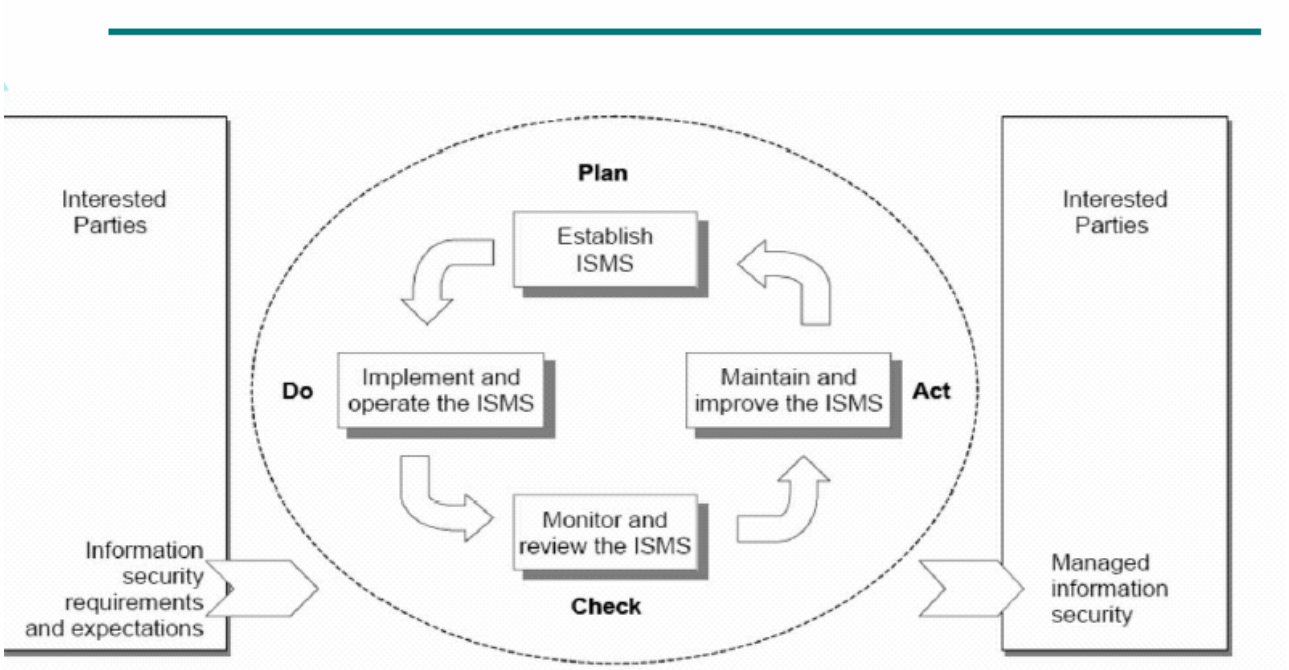


Figure 1 — PDCA model applied to ISMS processes

Passiamo ora ad esaminare quelle che sono le finalità del risk mangement cosi dettagliati:

a) Identificare i rischi potenziali;

b) Comprendere (e far comprendere) la probabilità e le conseguenze di questi rischi;

c) Stabilire una priorità per il trattamento dei rischi;

d) Individuare i controlli volti a limitare i rischi al di sotto di un valore accettabile.

A prescindere dalla metodologia utilizzata, esistono molti elementi e passaggi del processo di analisi dei rischi comuni a tutte le metodologie:

1) individuare, classificare e valorizzare i beni da proteggere;

2) individuare e valutare gli agenti ostili, minacce, vulnerabilità e il rischio;

3) definire quali minacce vanno fronteggiate e con quali contromisure (tecniche e non);

4) calcolare il rischio residuo, valutarne i livelli accettabili e definire le contromisure che permettono di mantenere il rischio entro questi livelli.

Esaminiamo ora le diverse metodologie di analisi dei rischi. Le metodologie esistenti in merito alla conduzione di un'analisi dei rischi sono molteplici e spesso si presentano con differenti obiettivi o caratteristiche, anche se si basano su alcuni concetti, elementi e passaggi procedurali comuni.

Nessuna è particolarmente migliore dell'altra. Però è importante comprendere quale tipologia di approccio sia più idonea utilizzare.

Ma quali sono le caratteristiche di duna determinata metodologia da usare. Nello specifico sono: 1) il livello di approfondimento dell'analisi, 2) la modalità di assegnazione dei valori (sistema di misurazione dei rischi), 3) la ripetibilità e frequenza del processo di analisi.

Livello di approfondimento

Se si considera il livello di approfondimento con cui si conduce un'analisi dei rischi, essa può essere concettuale, quando è destinata al management ed è orientata all'organizzazione e ai processi operativi, quando è destinata allo specialista o al responsabile dei sistemi informatici, e orientata, quindi, alla singole tecnologie e al contesto, appunto, operativo.

Una valutazione di tipo concettuale ad alto livello dei rischi consente di individuare il profilo di rischio a livello strategico e organizzativo, di definire le minacce all'organizzazione e quindi individuare le macro aree di criticità o contesti di rischio su cui intervenire nel tempo, di definire un piano di interventi immediati a livello di organizzazione, di definire la politica generale della sicurezza.

. Un'analisi di tipo operativo è più orientata alla valutazione dettagliata e approfondita della sicurezza delle singole tecnologie, sistemi e specifici ambiti di rete e si prefigge di (ad esempio):1) comprendere le vulnerabilità, minacce e rischi a cui sono esposte le singole tecnologie e le informazioni trattate, 2) definire architetture e standard tecnologici di sicurezza proporre percorsi operativi per la correzione delle debolezze riscontrate

Modalità di assegnazione dei valori del rischio

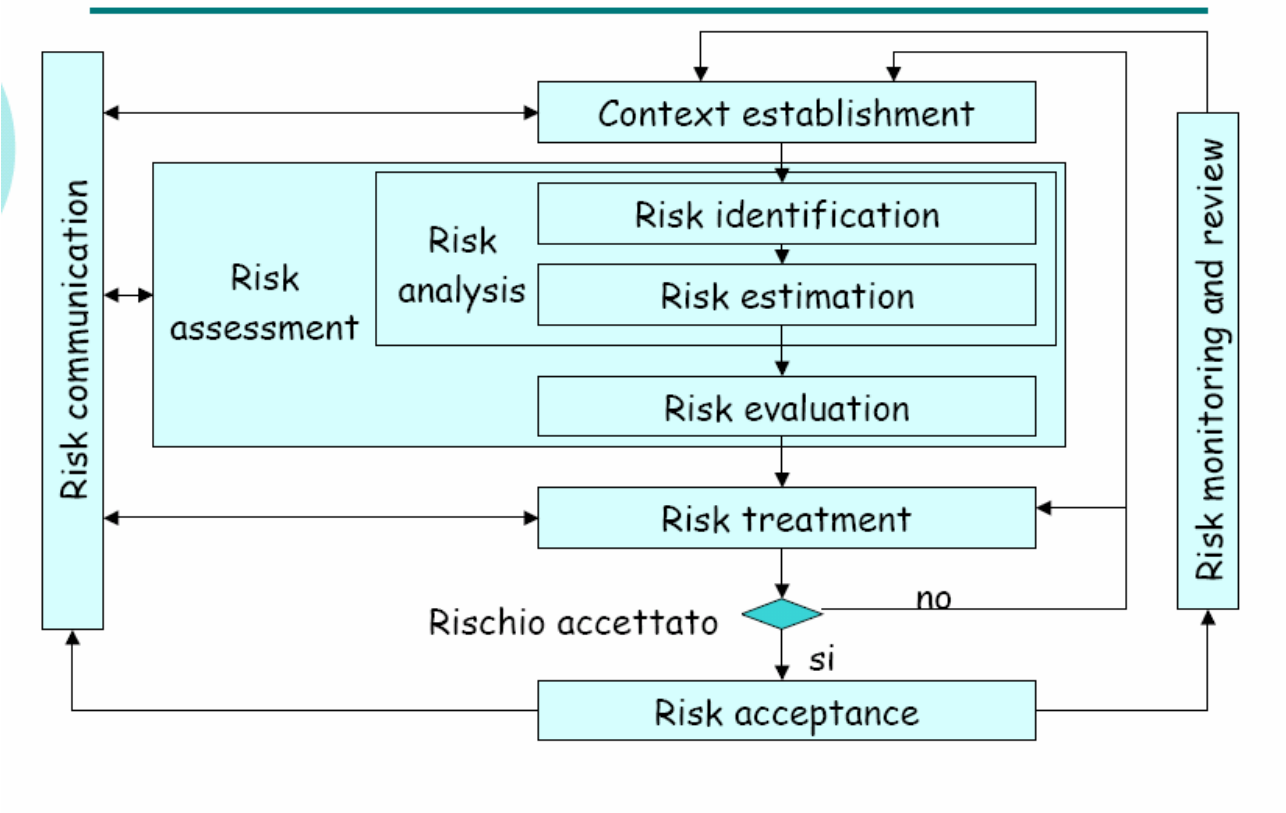
Nello scegliere una metodologia è importante scegliere una metrica. La misurazione di tipo quantitativo si basa su elementi monetari e statistici. Le metodologie qualitative in generale non richiedono dati statistici, e si basano su una scala di valori (basso, medio, alto, vitale, critico). Tali approcci, apparentemente più superficiali e meno precisi, in realtà si rivelano spesso più onesti

La metodologia quantitativa apparente ovvero semiquantitativa è un mix delle precedenti

Ripetibilità e frequenza del processo di analisi

A seconda della ripetibilità/frequenza del processo di analisi dei rischi, si possono distinguere le metodologie esistenti fra approcci statici e approcci dinamici/continuativi. Gli approcci dinamici non fotografano la situazione della sicurezza in un dato momento, ma danno gli elementi per analizzare e gestire continuamente e dinamicamente il rischio. In questo caso la valutazione e gestione dei rischi diventa parte integrante dei processi di implementazione, manutenzione e monitoraggio dei sistemi informativi e che comportano un decentramento in termini di responsabilità nella gestione dei rischi, con il coinvolgimento di tutte le funzioni aziendali a più livelli, e richiedono un mandato che parte dal Top-Management e che coinvolge tutta l'Organizzazione Gli approcci statici realizzano una fotografia dello stato attuale della sicurezza richiedono revisioni periodiche, con scadenze temporali diverse, a seconda del livello di profondità dell'analisi e normalmente sono gestiti sotto la responsabilità di funzioni aziendali specifiche, in genere in ambito ICT (ICT Manager, Security Officer, Comitato per la Sicurezza, ecc.); quindi le altre funzioni aziendali sono coinvolte solo passivamente.

Passiamo ora ad esaminare le diverse fasi del processo di risk management cosi evidenziato nella seguente figura:



Le fasi di tale processo sono le seguenti:

a) Individuazione del contesto;

b) Individuare i parametri fondamentali per gestire i rischi legati alla sicurezza;
c) Definire lo scopo e i confini del processo;
d) Definire un'organizzazione appropriata per il processo;
e) Istituire una struttura dettagliata per attuare il processo;
f) . Individuare i parametri fondamentali per gestire i rischi legati alla sicurezza;
g) Definire lo scopo e i confini del processo;
h) Definire un'organizzazione appropriata per il processo;
i) Istituire una struttura dettagliata per attuare il processo.

Passiamo ora ad esaminare i parametri fondamentali cosi elencati:

1) Criteri per la valutazione del rischio;
2) Valore strategico del processo informativo;
3) Criticità dei beni coinvolti;
4) Conseguenze finanziarie e di altra natura:
   • Obblighi legali o contrattuali;
   • Conseguenze operative della perdita di disponibilità, riservatezza o integrità dei dati;
   • Conseguenze sull'immagine.
5) Criteri per la valutazione dell'impatto;
6) Livello di classifica del bene compromesso;
7) Livello di sicurezza;
8) Operazioni compromesse (interne o di terze parti);
9) Scadenze o pianificazioni;
10) Danno alla reputazione
11) Criteri di accettazione del rischio;
12) Vincoli di operatività;
13) Vincoli tecnologici;
14) Vincoli economici;
15) Vincoli legali;
16) Risorse disponibili per: a) Effettuare la stima del rischio e attuare un piano di trattamento del rischio,b) definire e implementare le politiche e le procedure di sicurezza, c) monitorare l'attuazione delle politiche;
17) Individuare i parametri fondamentali per gestire i rischi legati alla sicurezza;
18) Definire lo scopo e i confini del processo;
19) Definire un'organizzazione appropriata per il processo;
20) Istituire una struttura dettagliata per attuare il processo.

Passiamo ora ad esaminare gli scopi ed i confini del processo

Nello specifico faremo riferimento all'ambiente in cui si applica il processo di risk management, ad i vincoli legali, alle politiche di sicurezza, ai confini geografici. L'oggetto del processo di risk management sarà costituito da un'infrastruttura IT, da un processo produttivo, da un ufficio.

Passeremo ad effettuare uno studio dell'organizzazione analizzandone in dettaglio i seguenti elementi:

1) lo scopo dell'organizzazione (cosa si propone di fare);
2) la competenza dell'organizzazione (il suo know-how);
3) i principi alla base dell'operatività (il suo codice di condotta);
4) la struttura dell'organizzazione (il suo organigramma);
5) la strategia (come intende migliorare).

Po sarà necessario passare all'analisi del contesto mediante:

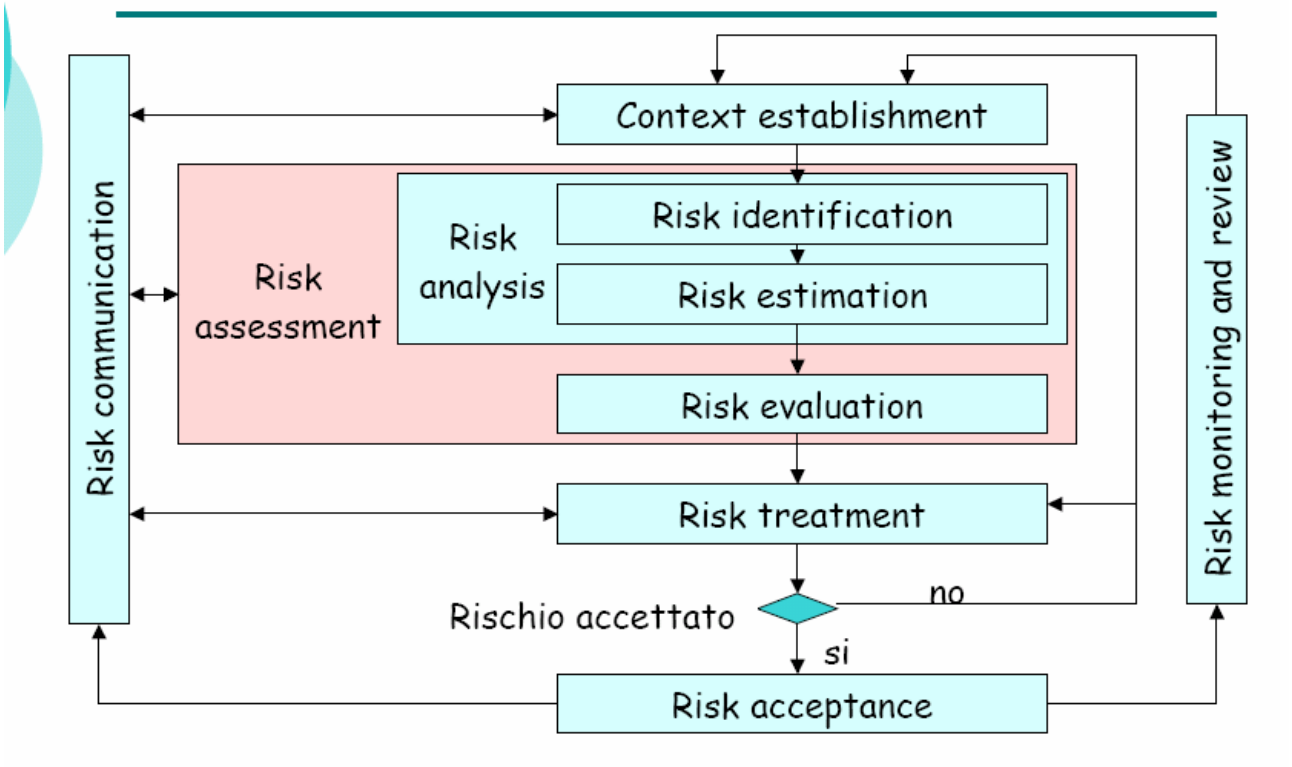
. 1) l'individuazione dei parametri fondamentali per gestire i rischi legati alla sicurezza;
2) la definizione dello scopo e i confini del processo;
3) la definizione di un'organizzazione appropriata per il processo;
4) l'istituzione di una struttura dettagliata per attuare il processo.

Successivamente si verificherà l'organizzazione appropriata per il processo cosi dettagliata nelle seguenti fasi:
1)Identificazione delle parti interessate:
2) Definizione dei ruoli e delle responsabilità;
3) Individuazione delle relazioni con altri processi aziendali e delle interfacce.

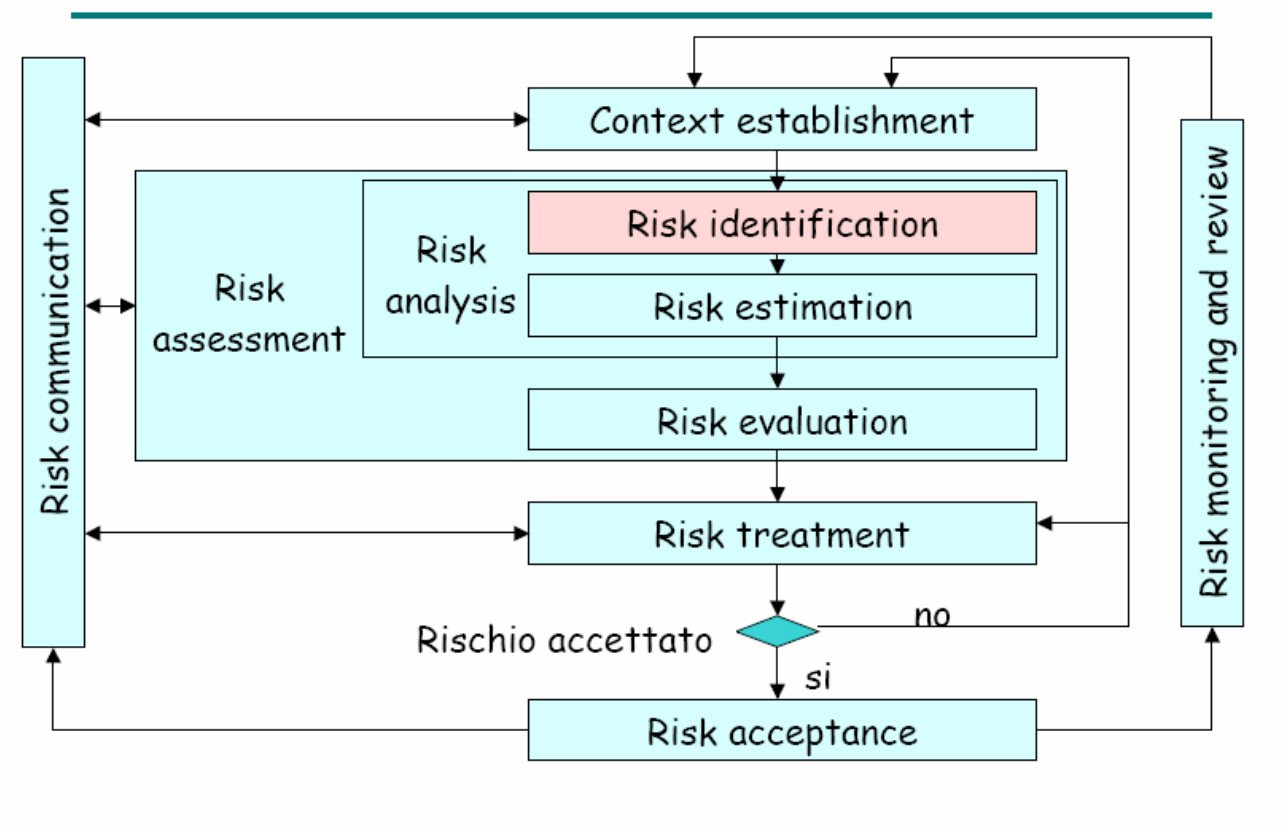
Si passerà poi alla fase di individuazione del contesto cosi dettagliata:
1) individuare i parametri fondamentali per gestire i rischi legati alla sicurezza;
2) definire lo scopo e i confini del processo;
3) definire un'organizzazione appropriata per il processo;
4) istituire una struttura dettagliata per attuare il processo.

Infine si analizza la struttura dettagliata per attuare il processo:
1) attribuzione dei compiti e delle attività del processo di gestione del rischio;
2) definizione dei decision escalation paths;
3)definizione della documentazione che deve essere conservata.

Passiamo ora ad esaminare il processo di risk management come raffigurato nel seguente disegno:



Risk assessment
Per risk assessment intenderemo l'identificazione, quantificazione, graduazione dei rischi secondo criteri e obiettivi stabiliti dall'organizzazione
. Risk analysis



Risk analysis

Nella risk analysis si passerà all'identificazione di: beni, minacce, vulnerabilità, impatto, controlli in atto.Un bene (asset) è una qualunque cosa che abbia valore per l'organizzazione e che quindi richieda protezione (non solo beni tangibili).Gli elementi essenziali relativi ai beni sono le attività e processi aziendali, le informazioni mentre gli elementi di supporto sono costituiti dall'hardware, dal software, dalle reti, dal personale e dalla sede.

Elementi essenziali

Sono funzioni la cui perdita o degrado impediscono o compromettono il raggiungimento degli obiettivi,funzioni che contengono segreti industriali,informazioni coperte dal segreto di Stato, informazioni vitali per il raggiungimento degli obiettivi, informazioni sensibili (ad es. dati personali), informazioni strategiche, informazioni "costose".

Elementi di supporto

Sono costituiti dall'Hardware (computer fissi e portatili, server, stampanti, supporti rimuovibili), dal software (sistemi operativi, applicativi generici, applicativi business standard o specifici), dalle reti (supporti, dispositivi, interfacce), dal personale (managers, utenti, operatori, sviluppatori) ed infine dalla sede (edifici dell'azienda o di terzi, linee telefoniche, impianti, forniture di servizi).

Passiamo ora ad esaminare e ad individuare le potenziali minacce. Una minaccia è una potenziale causa di incidente che potrebbe danneggiare un sistema o un'organizzazione. Una minaccia può essere di origine naturale o umana, e può essere accidentale o intenzionale.

Le minacce sono cosi catalogate nelle seguenti tabelle:

Danno fisico	Incendio	A,D,E
	Terremoto	E
	Eruzione vulcanica	E
	Allagamento	A,D,E
Mancanza di servizi essenziali	Interruzione dell'alimentazione	A,D,E
	Indisponibilità del servizio di telecomunicazione	A,D,E
	Interruzione del condizionamento dell'aria	A,D
Radiazioni	Radiazioni elettromagnetiche	A,D
	Rumore termico	A,D,E

Compromissione dell'informazione	Intercettazione (eavesdropping)	D
	Furto di documenti	A,D
	Furto di apparecchiature	D
	Divulgazione	A,D
	Manomissione dell'HW o del SW	A,D
	Ritrovamento di media eliminati	A,D
Guasti tecnici	Guasto di un dispositivo	A,D
	Malfunzionamento HW o SW	A
	Saturazione dello spazio di memoria	A,D

Azioni non autorizzate	Uso non autorizzato di dispositivi	D
	Copia di software	A,D
	Corruzione di dati	A,D
	Uso non autorizzato di applicativi	A,D
Compromissione di funzioni	Errore di utilizzo	A
	Abuso di privilegi	A,D
	Escalation di privilegi	D
	Denial of action	D

Esaminiamo invece ora le caratterizzazioni di un ipotetico attaccante cosi raffigurate nelle seguente tabella:

Fonte	**Motivazione**	**Minaccia**
Hacker	Sfida Ego	Hacking Intrusioni ~~Accesso non autorizzato~~
Criminale	Distruzione di informazioni Lucro	Computer crime Replay, impersonificazione, intercettazione Spoofing
Terrorista	Vendetta	Intrusione DDoS Corruzione di dati

Fonte	Motivazione	Minaccia
Spionaggio industriale	Competizione Spionaggio	Furto di informazioni Intrusione nei sistemi Social engineering
Personale interno	Curiosità Egocentrismo Vendetta Errori	Appropriazione di informazioni riservate Corruzione dei dati Intercettazione Vendita di informazioni Sabotaggio Accesso non autorizzato

Identificazione delle vulnerabilità

Una vulnerabilità è una debolezza che può essere sfruttata da una minaccia per compromettere o danneggiare un bene. Una vulnerabilità costituisce un rischio solo se al sistema si applica una minaccia in grado di sfruttarla. Vediamo ora degli esempi di vulnerabilità nelle seguenti tabelle:

Vulnerabilità	Minaccia
Ambiente e infrastrutture	
Mancanza di protezione fisica all'edificio	Furto di dispositivi o di informazioni
Mancanza di controllo degli accessi fisici	Accesso non autorizzato alle informazioni
Collocazione in un sito soggetto ad allagamenti	Allagamento
Hardware	
Mancanza di un piano di sostituzione	Deterioramento dei media
Assenza di camera schermata	Emissione elettromagnetica

Vulnerabilità	Minaccia
Software	
Vulnerabilità note del software	Uso non autorizzato, scalata di privilegi
Interfaccia di utente complessa	Errore nell'utilizzo
Password non protette	Masquerading
Comunicazioni	
Trasferimento di password in chiaro	Masquerading
Linee non protette	Intercettazione

Vulnerabilità	Minaccia
Documenti	
Archivi non protetti	Furto, accesso non autorizzato
Incuria nell'eliminazione	Furto, accesso non autorizzato
Personale	
Addestramento insufficiente	Errori operativi
Reclutamento di personale non fidato	Danneggiamento intenzionale
Procedurale	
Mancanza di una procedura di verifica dei log degli eventi	Accesso non autorizzato

Ora risulta necessario effettuare una stima del livello di rischio cosi dettagliata:

1) Valutazione delle conseguenze dell'attacco sui beni;
2) Valutazione della probabilità delle minacce;
3) Valutazione della probabilità di sfruttamento della vulnerabilità;
4) Valutazione delle conseguenze dell'attacco.

Deve essere assegnato un valore ai beni individuati: (Bassissimo, basso, medio, alto, altissimo 1÷10). Per effettuare una Valutazione delle conseguenze dell'attacco devono essere considerati nel dettaglio i seguenti elementi:

a) gli aspetti di riservatezza, integrità, disponibilità;
b) eventuali dipendenze tra i beni
c) l'impatto di un incidente di sicurezza su ognuno dei beni che può essere diretto cioè con un costo economico della sostituzione del bene ed un costo dell'interruzione del servizio, indiretto cioè con un potenziale uso malevolo delle informazioni, con violazioni di leggi o obblighi e con violazioni di codici di condotta;
d) la probabilità che ogni minaccia venga attuata sulla base di: a) frequenza della minaccia, b) motivazione, capacità, risorse necessarie; c) fattori geografici o ambientali.

Nella tabella successiva vengono esaminate le caratteristiche dei metodi di stima del livello del rischio.

Metodi di stima del livello di rischio

Caratteristiche	Quantitativo	Qualitativo
Richiede calcoli complessi	Sì	No
Grado di intuitività e esperienza richiesti	Elevato	Basso
Volume di informazioni richieste	Elevato	Basso
Valorizzazione economica beni	Si	No
Richiede l'analisi costi e benefici	Si	No
Tempo richiesto	Elevato	Basso
Si basa su automatismi	Si	No

La stima del livello di rischio si divide in qualitativa (costituisce un utile strumento di pianificazione quando i beni o i dati non sono facilmente valutabili in termini economici, inoltre permette di individuare le priorità e le parti più a rischio del sistema, può essere seguita da una seconda iterazione a livello più dettagliato ed ha bassi costi di esecuzione) e quantitativa (richiede una conoscenza in dettaglio del sistema, C+comporta costi, tempi e esperienza considerevoli ed ha un vantaggio a lungo termine ripetibile e confrontabile
La stima quantitativa del rischio viene effettuata mediante la matrice con valori pre-definiti cosi dettagliata:

Matrice con valori pre-definiti

	Probabilità della minaccia	Bassa			Media			Alta		
	Probabilità della vulnerabilità	B	M	A	B	M	A	B	M	A
Valore del bene	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Mentre la classifica della minacce in base ai valori di rischio viene esaminata nella seguente tabella:

Classifica delle minacce in base ai valori di rischio

Descrittore della minaccia	Conseguenza (C)	Probabilità della minaccia (P)	Misura del rischio (C*P)	Classifica della minaccia
Minaccia A	5	2	10	2
Minaccia B	2	4	8	3
Minaccia C	3	5	15	1
Minaccia D	1	3	3	5
Minaccia E	4	1	4	4
Minaccia F	2	4	8	3

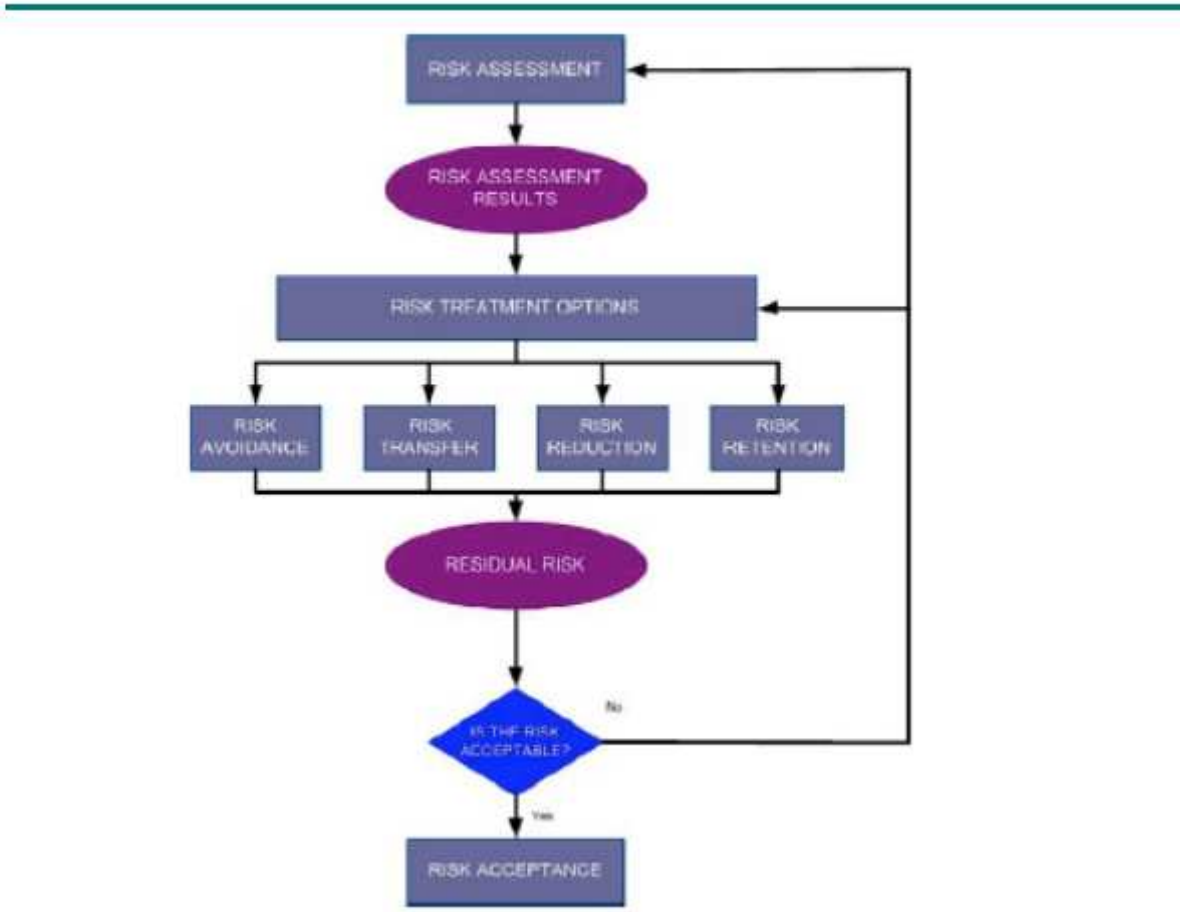
Valutazione del rischio

Il livello di rischio ottenuto deve essere confrontato con i criteri di valutazione stabiliti dall'organizzazione in fase di definizione del contesto. Si utilizzano i risultati dell'analisi del rischio per decidere circa le azioni future: e un rischio necessita di essere trattato, e con quale priorità, quali azioni si devono intraprendere.

Trattamento del rischio

Nel trattamento del rischio devono essere individuate e implementate le misure idonee per modificare il rischio, si deve passare alla rimozione (eliminare la causa del rischio), al trasferimento (assicurazioni, outsourcing…), alla riduzione (controlli appropriati, SOA) ed alla ritenzione. Si veda in proposito il grafico successivo:

Trattamento del rischio



Nella rimozione del rischio deve essere eliminata la condizione o l'attività che dà origine al rischio in esame. L'eliminazione del rischio può comportare la terminazione o lo spostamento di attività che comportano un rischio ritenuto troppo alto. Nel trasferimento del rischio il rischio deve essere trasferito ad un soggetto che sia in grado di gestirlo. Il trasferimento del rischio può comportare nuovi rischi, o modificare quelli esistenti. Nella ritenzione del rischio si decide di assumere il rischio senza implementare misure di alcun tipo. Infine nella riduzione del rischio deve essere ridotto l'impatto di un particolare rischio in modo che il rischio residuo risulti tollerabile ed inoltre devono essere selezionati i controlli idonei, tenendo in considerazione i vincoli esistenti:di tempo, di budget, tecnici, culturali e legali.

Accettazione del rischio

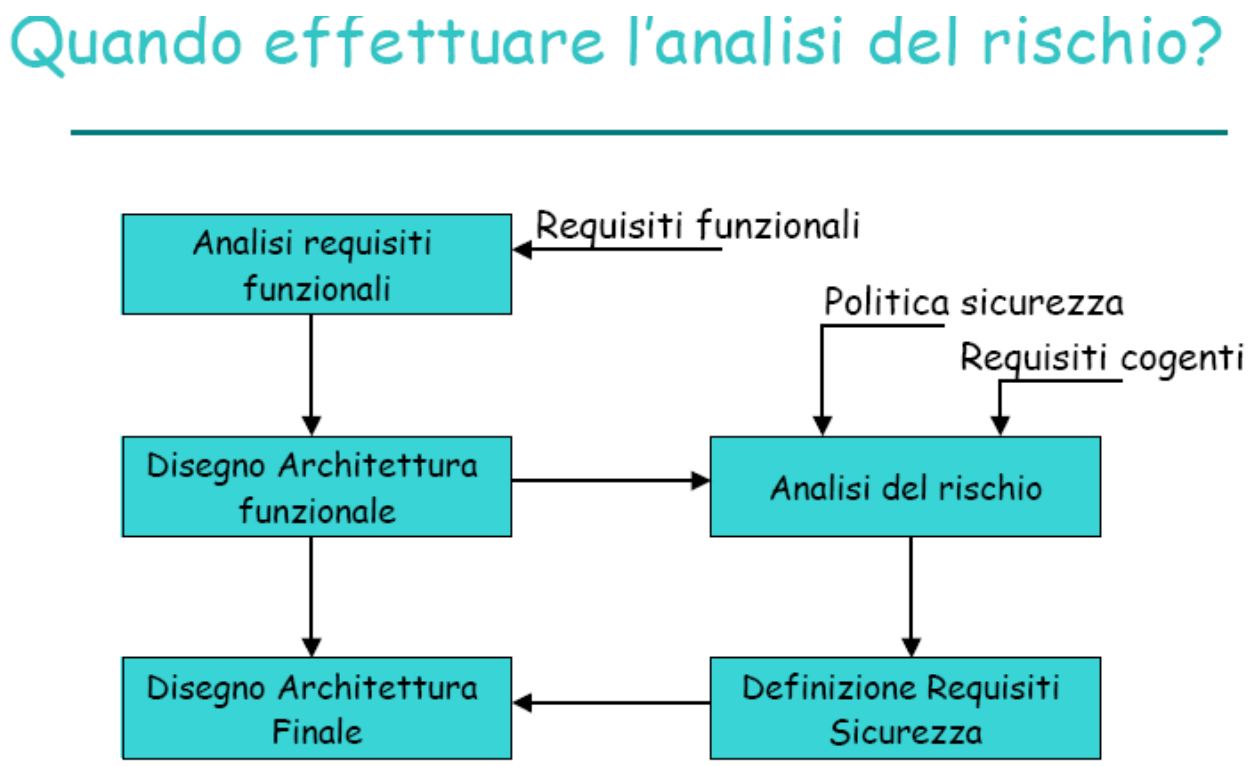
Viene presa la decisione di accettare i rischi perché il rischio è compatibile con i criteri adottati e perché il costo del trattamento del rischio è ritenuto troppo elevato.

Comunicazione del rischio

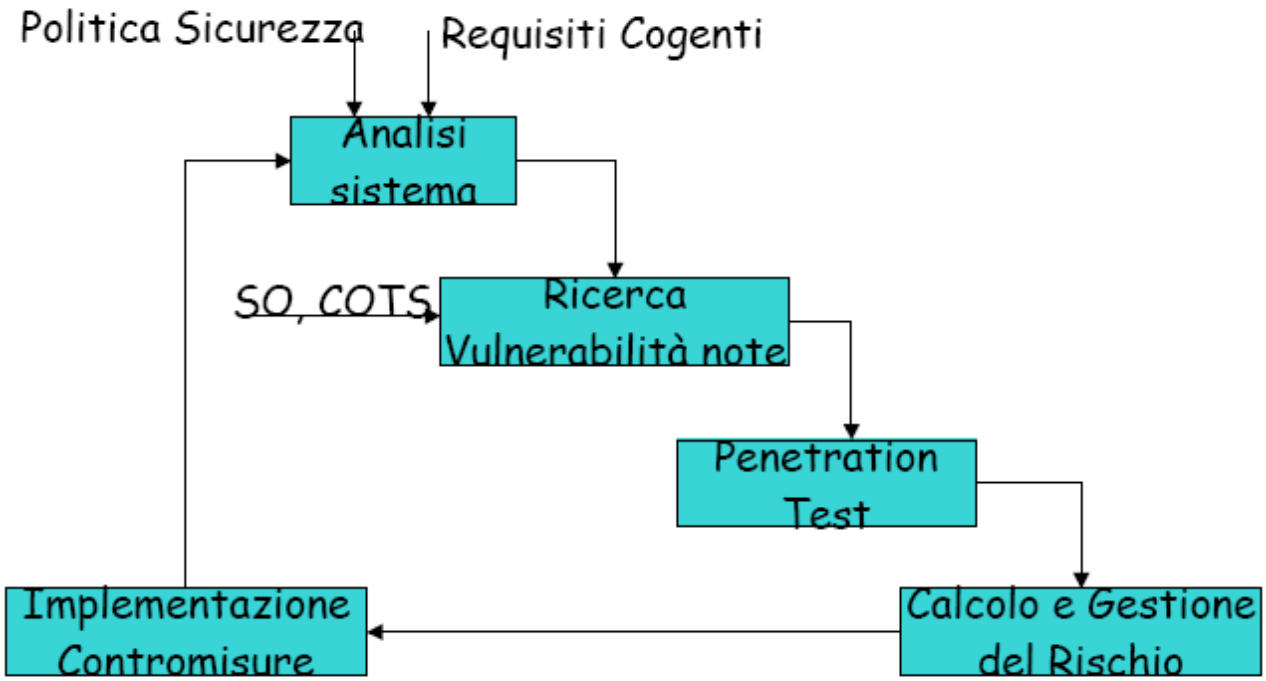
Deve essere definita una procedura per la comunicazione del rischio verso le parti interessate all'interno e all'esterno dell'organizzazione. Questo garantisce che i responsabili dell'implementazione del piano di gestione del rischio comprendano gli elementi su cui sono basate le decisioni e che richiedono di intraprendere determinate azioni.

Monitoraggio e revisione del rischio

I rischi, i beni, le minacce, le vulnerabilità devono essere monitorati e rivisti per identificare immediatamente cambiamenti significativi, tenendo in considerazione dei vincoli legali, degli aspetti di competizione, del valore dei beni, dei criteri di accettazione del rischio
Passiamo ora ad esaminare il timing temporale di effettuazione dell'analisi del rischio che si evince dal seguente schema:



Esaminiamo in successione l'analisi del rischio in fase di esercizio:



Dottor Antonio Guzzo
Responsabile CED del Comune di Praia a Mare