SAFE
Safe Activities For Enhancement

INDICE

1. OBIETTIVO

Descrivere il metodo SAFE per la gestione delle minacce (threats) collegate ai progetti ed alle iniziative aziendali (di seguito chiamati tutti con il nome di "progetti").

2. APPLICABILITÀ

Progetti di natura organizzativa o di ICT.

3. DEFINIZIONI E ABBREVIAZIONI

ACRONIMI	DEFINIZIONI
PMI	Project Management Institute
PMP	Project Management Plan
TAR	Threat Action Report
TC	Threat Catalogue
TER	Threat Evaluation Report
TRP	Threat Response Plan

Azioni di prevenzione: azioni che vengono messe in atto prima che un evento rischioso si manifesti allo scopo di ridurne la probabilità di accadimento o di diminuirne l'eventuale danno in caso di manifestazione.

Azioni di sorveglianza: azioni che vengono messe in atto al fine di rilevare tempestivamente i segnali emessi dai sensori che sono stati progettati per rivelare l'eventuale accadimento di un evento rischioso.

Azioni di contenimento: azioni che vengono messe in atto solo nel momento in cui il rischio negativo (minaccia) si manifesta allo scopo di ridurne il danno associato.

Danno*:* è la combinazione dell'impatto oggettivo di una situazione rischiosa con la tolleranza ammessa dagli stakeholder per quel particolare impatto. Ad esempio, un ritardo di 3 settimane nella consegna di un prodotto (impatto oggettivo) potrebbe essere fatale per la riuscita di un progetto (tolleranza bassa e conseguente danno estremo) e del tutto accettabile per un altro progetto (tolleranza alta e conseguente danno limitato).

Impatto oggettivo*:* è la valorizzazione il più possibile oggettiva e/o condivisa delle disfunzioni e delle conseguenze che un determinato evento rischioso può provocare al progetto. Ad esempio un ritardo di 2 mesi su 10 rappresenta un impatto oggettivo del 20%.

Rischio: evento o condizione incerta che, se si dovesse verificare, avrebbe un effetto positivo o negativo sugli obiettivi di progetto. Il Rischio, secondo la definzione fornita dal Project Management Institute (PMI) può essere negativo (minaccia) o positivo (opportunità).

***Rischio Negativo (Minaccia)**:* in senso complessivo è la eventualità di non ottenere il successo del progetto cioè di non raggiungere gli obiettivi stabiliti per esso. In senso più particolare è il *valore atteso statistico* del danno di una situazione incerta cioè, in maniera semplificata, il prodotto della probabilità di occorrenza della minaccia moltiplicata per il valore previsto del danno. La valorizzazione di una minaccia può essere monetaria o non monetaria; nel primo caso assume il nome di "esposizione economica" e non è influenzata dalla tolleranza ammessa, nel secondo caso assume il nome di "valore convenzionale" in quanto è misurata su una scala numerica condivisa ed è, invece, influenzata dalla tolleranza ammessa.

***Rischio Negativo Incondizionato**:* è un rischio negativo (minaccia) a cui il progetto è sottoposto, valutato in assenza di specifiche azioni di gestione. In altri termini è il rischio negativo che il progetto correrebbe nell'ipotesi in cui tale evento rischioso non fosse stato individuato e potesse, quindi, manifestarsi in modo inatteso. La probabilità di manifestazione non è influenzata da alcuna prevenzione specifica così come il danno associato è valutato considerando le sole capacità ordinarie di reazione del progetto attivate in condizioni di emergenza.

***Rischio Negativo Residuo**:* è un rischio negativo (minaccia) a cui il progetto è sottoposto, valutato in presenza delle specifiche azioni di gestione per esso individuate. Tali azioni di prevenzione, sorveglianza e contenimento permetteranno, in genere, di ridurre la probabilità e/o il danno associato allo stesso rischio negativo considerato come "incondizionato". La differenza tra rischio negativo incondizionato e rischio negativo residuo rappresenta la quantità di rischio rimossa dal piano d'intervento immaginato.

***Rischi negativi tecnici**:* rischi negativi determinati, per esempio, dal ricorso a tecnologie innovative, da avarie di attrezzature, innovazione dei processi produttivi, etc.

***Rischi negativi gestionali**:* rischi negativi determinati, per esempio, da indisponibilità del personale di uno specifico profilo professionale, oppure dalla eccessiva necessità di riunioni progettuali o ancora dall'atteggiamento negativo di alcuni stakeholder. Le penali contrattuali rientrano in questa categoria, in quanto la motivazione di origine del pagamento di una penale è sempre legata al mancato rispetto di accordi contrattuali e quindi deriva principalmente da motivazioni gestionali.

***Rischi negativi economico/finanziari**:* rischi negativi dovuti per esempio a variazioni dei costi delle materie prime, rinnovi contrattuali collettivi, variazioni del tasso di sconto, modifiche dei tassi passivi praticati dagli istituti di credito, etc. Queste minacce sono tipicamente dovuti a fattori esterni e difficilmente governabili dall'Azienda, sono quelle minacce per le quali solitamente si ricorre a specifiche coperture assicurative.

***Stakeholder**:* sono tutti i cosiddetti "portatori d'interesse" progettuali; coloro i quali hanno un qualche interesse legittimo influenzato dal progetto in esame sia in senso positivo che negativo. Le principali classi di stakeholder sono: utenti diretti ed indiretti, management, personale tecnico coinvolto nella gestione del prodotto/servizio, committenti, sponsor, partecipanti al progetto, regolatori esterni (autorità, enti di normazione etc.).

***Tolleranza ammessa**:* Ogni progetto potrà avere delle diverse tolleranze rispetto al grado con cui ci si discosta dagli obiettivi di quantità, qualità, costi e tempi. La tolleranza ammessa influenzerà il valore della minaccia espresso su scala convenzionale ma non quello dell'esposizione economica che rimarrà determinato dal solo prodotto dell'impatto economico oggettivo moltiplicato per la probabilità di accadimento dell'evento.

4. CONSIDERAZIONI GENERALI

Gestire il rischio di un progetto significa occuparsi attivamente del suo successo. Un progetto è per sua natura uno sforzo complesso, temporaneo, innovativo, interdisciplinare, inusuale e talvolta unico. Per questi motivi esso è esposto ad eventi rischiosi in misura molto maggiore di quella relativa alle attività correnti e ripetitive di un'organizzazione. Come nelle attività imprenditoriali, del resto, rischi elevati sono in genere compensati da elevati vantaggi.

Nell'accezione terminologica introdotta dal PMI, il rischio è considerato sia nella sua accezione negativa (più comune ed intuitiva) che in quella positiva. Il rischio negativo prende il nome di minaccia, quello positivo di opportunità. In linea generale, la gestione del rischio dovrebbe tendere a minimizzare i rischi negativi e massimizzare i rischi positivi di un progetto.

Il presente metodo, nella versione attuale, si applica in modo specifico ai rischi negativi (minacce), sebbene l'approccio generale e i razionali alla base siano mutuabili anche ai rischi positivi (opportunità).
Nel seguito del documento si userà indistintamente il termine "minaccia" o "rischio negativo", in quanto i due termini sono da considerarsi sinonimi. Si userà invece il termine più generale "rischio" quando si vuole comprendere anche l'accezione positiva di un evento incerto.

Il rischio negativo (minaccia) è un elemento presente in tutti i progetti. Non dedicare tempo e risorse alla sua identificazione ed alla predisposizione pianificata delle adeguate misure di prevenzione e contenimento significa esporsi alla necessità di una gestione progettuale di tipo reattivo legata ad eventi imprevisti che fatalmente portano a danni ed erosione dei margini economici di commessa e/o della convenienza progettuale.

La disciplina che si occupa della gestione delle minacce di progetto è definita come Threat Management.

Il Threat Management permette di:

- ***Evitare le situazioni di Crisis Management*** *– più dispendiose e gravose della gestione preventiva degli eventi rischiosi.*
- ***Gestire i progetti nel rispetto dei tempi e dei costi previsti*** *(evitando le penali, ad esempio, e/o deviazioni negative registrate durante l'avanzamento che comportano l'aumentare di costi interni non previsti).*

La valorizzazione dei costi di gestione dei rischi negativi non riduce la competitività aziendale ma semmai rende più consapevole l'azienda sulla entità della eventuale erosione del margine di commessa stabilito a livello commerciale. L'aggravio dei costi portato dalla gestione dei rischi negativi, infatti, serve ad evitare ben maggiori aggravi di costi per la gestione delle emergenze che andrebbero ad erodere il valore prodotto dal progetto a condizioni commerciali o contrattuali ormai difficilmente modificabili. E' fondamentale riconoscere, d'altra parte, che le riserve di gestione dei rischi negativi non possono essere aggiunte in cascata da ogni partecipante al progetto in modo implicito perché questo porterebbe ad un eccesso di costo ingiustificato.

La gestione delle minacce, benché di precisa responsabilità assegnata al Project Manager, deve essere un processo partecipato in cui tutte le parti coinvolte contribuiscono all'analisi ed inseriscono "riserve di gestione" una sola volta per ogni minaccia identificata.

Per gestire le minacce bisogna innanzitutto essere in grado di comprendere e prevedere gli eventi rischiosi e le loro interazioni che, manifestandosi, possono ostacolare il raggiungimento degli obiettivi progettuali. Successivamente occorre progettare e mettere in azione un piano di sicurezza che permetta di intervenire nel modo più appropriato con attività di prevenzione, sorveglianza e contenimento sui singoli elementi di rischio negativo. Infine bisogna valutare sia a priori che sul campo l'efficacia del piano di azione adottato per poter operare le opportune modifiche al sistema di gestione delle minacce.

Le minacce cambiano col passare del tempo nella loro natura, nella probabilità di manifestazione così come nella entità del danno che possono procurare ed è, quindi, necessario mantenere sempre vivo l'interesse per questo aspetto iterando più volte il processo descritto nel seguito. Le attività di threat management dovranno avvenire sia in particolari momenti canonici del Ciclo di Vita del progetto (Management Review in momenti sincroni) sia ogni qual volta lo si ritenga necessario per via della variazione delle condizioni progettuali o della diversa conoscenza che di esse si riesce ad avere nel corso del tempo (on demand).

Un importante risultato che l'azienda intende perseguire con una gestione esplicita delle minacce è l'apprendimento organizzativo collettivo determinato da una trasmissione di informazione tra progetti in modo da evitare di ricadere nei problemi che si manifestano in modo ricorrente nel contesto aziendale.
Un secondo vantaggio è quello di poter disporre di una stima globale del livello di esposizione alle minacce per l'intera azienda aggregando i vari rischi negativi progettuali a livello di portafoglio iniziative e con i rischi negativi provenienti dalle altri sorgenti (processi ripetitivi, asset generali etc.). Questo approccio più ampio è definito Enterprise Threat Management.

Il processo descritto nel seguito si applica a qualunque tipo di progetto, indipendentemente dalla sua taglia e criticità, in quanto è auto-tarante, si adatta cioè alle caratteristiche del progetto: piccolo progetto, piccolo sforzo di gestione delle minacce; grande progetto, grande sforzo di gestione delle minacce.

La gestione delle minacce è legata ad un approccio mentale orientato alla identificazione non tanto di cosa occorre fare per giungere al risultato finale (percorso progettuale) quanto di che cosa non deve accadere perché il risultato sia raggiunto (percorsi alternativi). In questo senso, attuare comunque i passi indicati nel seguito aiuterà il Responsabile del rischio progettuale a migliorare le probabilità di successo del progetto stesso, impegnando solo le risorse che saranno ritenute congrue con l'entità dell'impegno progettuale da governare.

Un'ultima annotazione è legata al fatto che così come accade per un'analisi costi-benefici, anche una valutazione delle minacce è condizionata dalla scelta di una prospettiva dalla cui angolazione osservare i danni.

Mescolare le prospettive non è mai una buona idea perché alcune cose che sono positive per un gruppo di stakeholder potrebbero essere negative per un altro gruppo di stakeholder. In particolare l'analisi di rischio vista dalla prospettiva del fornitore è diversa da quella vista dalla prospettiva cliente (ad esempio: un potenziale ritardo di pagamento può essere una minaccia per il fornitore ma un'opportunità di tesoreria per il cliente !).

5. PROCEDURA

In questo capitolo verranno descritti i passi per effettuare la gestione delle minacce di progetto secondo la presente procedura. Per l'operatività si utilizzeranno i moduli allegati.

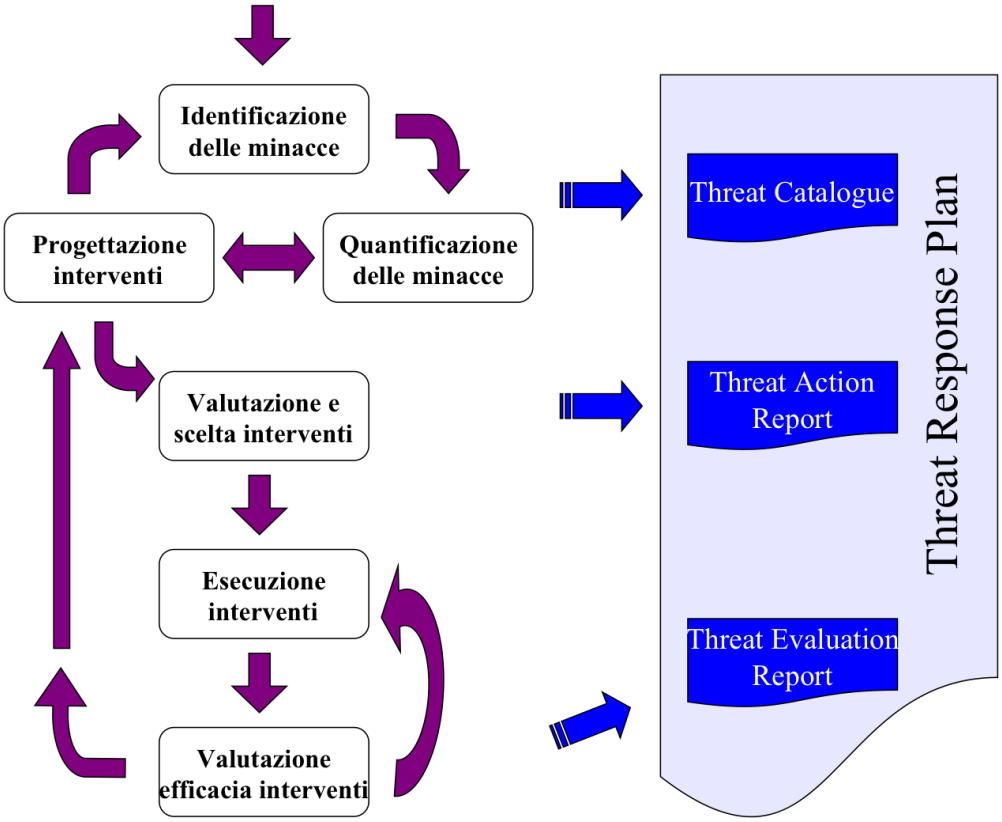


Figura 1

Le check-list e le tabelle richiamate nella presente procedura sono a supporto dei Project Manager e costituiscono la base per condurre il minimo insieme di attività richieste per l'analisi delle minacce di progetto.

Come indica la figura 1, la prima attività del processo di Threat Management è quella della Identificazione delle Minacce (Threat Activity n°1 – TA1), nella quale tutte le principali fonti di rischio negativo sono individuate, elencate ed entrano a far parte del

Threat Response Plan (TRP) che, nel caso più semplice, può essere un semplice foglio elettronico come quello fornito a corredo della procedura e descritto in allegato. Esso contiene tutte le informazioni rilevanti per l'applicazione di questo metodo. Tale attività può essere aiutata dalla esecuzione di un Threat Identification Workshop condotto con i principali stakeholder e conoscitori del contenuto del progetto.

Alla prima attività segue la Quantificazione delle Minacce (TA2) che permette di ottenere la visione più oggettiva possibile delle percezioni intuitive sulla rischiosità del progetto. Anche questa attività può essere aiutata dalla esecuzione di un Threat Quantification Workshop condotto con i principali stakeholder e conoscitori del contenuto del progetto oppure dall'utilizzo di metodi di stima cooperativa come il metodo Delphi o il metodo Shang.

Al termine di queste due attività può essere prodotta la bozza di una relazione sulla natura ed il livello di rischio negativo a cui il progetto è esposto (Threat Catalogue - TC).

Dopo la fase di diagnosi (TA1+TA2) si passa poi alla individuazione di strategie generali e particolari per ridurre i fattori di rischio negativo sia nella loro probabilità di accadimento che nella entità dei loro possibili effetti. Questo è possibile attraverso la Progettazione degli interventi (TA3) di gestione delle minacce che permette la formulazione di un Threat Action Report (TAR) contenente sia le indicazioni generali per la corretta impostazione del progetto sia una sezione in cui, per ogni fattore di rischio negativo su cui si ritiene opportuno intervenire, viene individuata una serie di interventi di: prevenzione, sorveglianza e contenimento. Scopo del TAR è quello di ridurre il Rischio Negativo Incondizionato (Unconditioned Threat) associato al progetto ad un Rischio Negativo Residuo (Residual Threat) che abbia un livello di accettabilità esplicitamente definito e documentato nel Threat Catalogue.
Esso viene così ad arricchirsi di una seconda sezione: quella relativa al rischio negativo stimato a posteriori dell'applicazione degli interventi progettati, valutata a seguito della conduzione per una seconda volta dell'attività TA2. E' possibile a questo punto, attraverso il confronto tra Rischio Negativo Incondizionato e Rischio Negativo Residuo, attribuire al Threat Response Plan generale un livello "a priori" di efficacia stimata nella gestione delle minacce. Occorre far presente che è possibile che, a seguito della individuazione di una serie di azioni tese a ridurre una certa minaccia, se ne possano generare di nuove che dovranno essere identificate e valorizzate al pari di tutte le altre e che concorreranno nella valutazione di praticabilità di una certa contromisura. Un Threat Response Workshop, condotto con i principali stakeholder e conoscitori del contenuto del progetto, può essere di aiuto nella individuazione di un piano di azione migliore.

A questo punto è possibile passare alla quarta attività di Threat Management consistente nella Valutazione e scelta degli interventi (TA4) da mettere in campo. Tale scelta dipende dalla efficacia ed efficienza presunta nella rimozione dei rischi negativi cioè dal confronto tra i costi stimati per le attività di gestione individuate (interventi prescelti) e l'entità dei risparmi legati al prevedibile abbassamento del rischio negativo. Questi ultimi dovranno essere espressi, quando possibile, in misura economica, per omogeneità di paragone e per facilitare il processo decisionale.

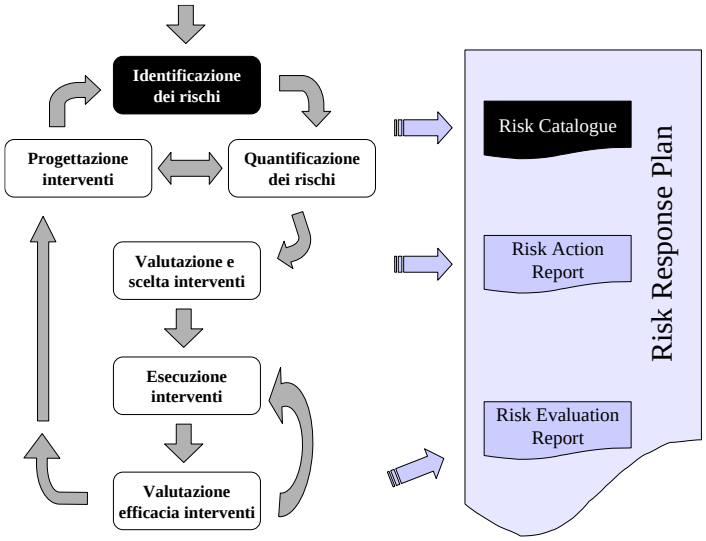
Il Threat Action Report (TAR) è un prezioso input per la modifica del piano generale di lavoro di progetto (PMP) col quale deve essere ovviamente coordinato, in quanto le attività di gestione delle minacce sono esse stesse attività progettuali e come tali vanno gestite nel quadro della pianificazione e controllo integrati. In particolare occorre osservare che le azioni di prevenzione e di sorveglianza, che hanno superato la verifica di convenienza, andranno comunque inserite nel PMP mentre quelle di contenimento saranno descritte accuratamente nel TAR e trasportate nel PMP solo su necessità determinata dall'accadimento dell'evento rischioso che intendono contrastare.

Alla progettazione degli interventi di gestione segue l'attività di Esecuzione degli interventi (TA5) nella quale si mettono in atto tutte le iniziative di prevenzione previste dal TAR, si attivano tutti i "sensori" progettati al fine di rilevare tempestivamente l'accadimento di un evento rischioso ed infine si adottano tutte le contromisure necessarie per contenere le minacce che si sono eventualmente tramutate in problemi da neutralizzare o almeno mitigare.

L'ultima attività prevista dal metodo proposto è quella di Verifica sul campo dell'efficacia degli interventi (TA6) messi in atto. Essa è necessaria al fine di confermare o contestare la validità del TAR in modo da prevedere eventuali nuovi interventi di prevenzione, sorveglianza o contenimento più efficaci di quelli adottati fino a quel momento. Il risultato di questa attività si può concretizzare in un documento chiamato Threat Evaluation Report (TER) che conterrà valutazioni sulle cose accadute, sull'efficacia della prevenzione eseguita e delle reazioni adottate. Questa attività potrà innescare nuovamente sia la fase di diagnosi (TA1 e TA2) sia la fase progettuale (TA3).

5.1 I PASSI IN DETTAGLIO

5.1.1 Identificazione delle minacce (TA1)



L'obiettivo di questa attività è quello di portare all'attenzione esplicita delle parti coinvolte nel progetto un insieme il più possibile completo di elementi di criticità che costituiscono la base per la valutazione del rischio negativo generale e per la predisposizione delle opportune risposte di governo. Nell'individuazione di tali elementi di base occorre rifuggire dalla tentazione scolastica di elencare le innumerevoli e normali circostanze da cui dipende l'esecuzione corretta del lavoro, per concentrarsi sui soli Fattori Critici maggiormente responsabili della sua riuscita o del suo fallimento, secondo la ben nota legge di Pareto (il 20% dei fattori porta l'80% dei problemi). D'altra parte non è neppure verosimile che un progetto di grosse dimensioni e di rilevanza per l'azienda possa annoverare nel suo catalogo di minacce solo un decina di fattori. L'identificazione dei fattori pertinenti è una delle fasi più importanti dell'intera gestione delle minacce in quanto solo gli elementi che sono stati portati alla consapevolezza collettiva possono essere affrontati efficacemente con la procedura illustrata nel seguito. Gli altri rischi negativi si manifesteranno come "imprevisti" da gestire in stato di "emergenza". Accontentarsi di identificare solo i primi rischi negativi che vengono alla mente non significa che non ve ne saranno altri, ma solo che quelli non identificati ci coglieranno alla sprovvista.

In termini poco rigorosi ma sintetici, una minaccia può essere considerata un problema che non si è ancora presentato ma potrebbe farlo. Il concetto di probabilità è intrinseco ed essenziale al concetto di minaccia. Il rischio negativo infatti è intimamente collegato all'incertezza più che alla complessità, per quanto la complessità – se non ben gestita - possa alimentare l'incertezza. Il rischio negativo è legato ad eventi negativi che si collocano su una scala ininterrotta che parte da quelli completamente sconosciuti (*minacce ignote*: si corrono senza neppure esserne consapevoli) a quelli conosciuti nella natura ma incerti (*minacce note* di cui si è consapevoli ma che sono comunque ipotetiche nel loro accadimento).

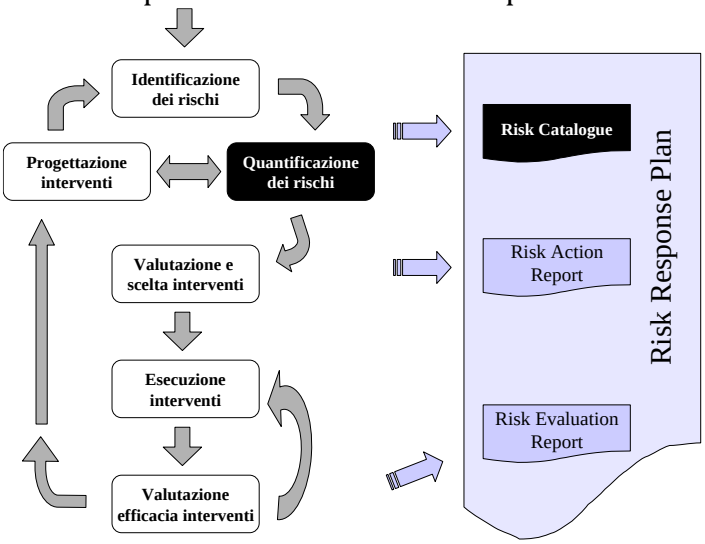
Per formulare descrittivamente ogni singolo elemento di rischiosità si dovrà adottare un approccio denominato CEC cioè Condizione-Evento-Conseguenza. La Condizione specifica una situazione il cui manifestarsi può portare, attraverso un Evento cui è associabile un grado di probabilità di accadimento, ad una Conseguenza indesiderata. In un approccio del genere la formulazione di un elemento di rischiosità può essere la seguente: "se si verifica la situazione A allora si potrebbe determinare la situazione indesiderata B". Ad esempio: "**se** la competenza tecnica del gruppo sulla tecnologia da

usare fosse bassa **allora** il prodotto realizzato potrebbe essere poco affidabile e robusto".

Nella individuazione dei singoli elementi rischiosi si potrà guardare "in avanti" ("forward chaining") - partendo dalla elencazione delle situazioni che si possono presentare con una certa probabilità alla ricerca dei possibili danni arrecati da queste al progetto - oppure "all'indietro" ("backward chaining") - partendo dalle conseguenze indesiderate alla ricerca delle situazioni che le possono generare.

Occorrerà evitare, nella identificazione delle minacce, l'uso di etichette e slogan difficilmente interpretabili al di fuori del contesto che li ha prodotti o a distanza di tempo. Ogni fattore critico dovrà essere il più possibile specifico e non generico. Nelle check list riportate in allegato, sono illustrati alcuni fattori che possono determinare incertezza per il progetto, divisi per classi. Tali liste di controllo potranno essere utilizzate, al pari di qualunque altra appropriata lista disponibile, per generare entrate nel Threat Catalogue di progetto. Le check list sono, quindi, solamente supporti per il responsabile del processo di Threat Management, al fine di individuare le minacce specifiche connesse al progetto e non devono essere considerate nè esaustive nè obbligatorie. Il responsabile può individuare minacce non previste dalle check-list stesse o non considerare fattori da esse citati.

Nell'identificazione delle minacce vanno specificate anche quelle che possono rivelarsi ricorrenti durante il progetto. In dettaglio, ciascuna di queste minacce va inserita nel Threat Catalogue aggiungendo tante righe con la stessa denominazione quante sono le possibilità di ripetizione della minaccia; la codifica delle ripetizioni manterrà la stessa numerazione con l'aggiunta di un codice alfabetico (1a, 1b, 1c, etc.). Per ciascuna minaccia ripetuta va effettuata la completa valutazione quantitativa.



5.1.2 Quantificazione della minaccia (TA2)

L'obiettivo di questa attività è quello di dare una base il più possibile misurabile alla valutazione delle singole minacce di progetto.

In un progetto, oltre che identificare quali cose possono andare storte, è necessario differenziare le cose importanti da quelle marginali. Ecco che allora la sola componente di eventualità per la definizione di minaccia non basta più. Occorre introdurre il concetto di "valore atteso" statistico: la minaccia, in prima approssimazione, è una quantità proporzionale al valore del danno causato da un certo problema moltiplicato per la sua probabilità di accadimento. In tale modo possiamo focalizzare le energie gestionali nel controllo di cose che siano davvero rilevanti per il progetto. Il concetto di danno, poi, va scisso nelle sue due componenti: impatto oggettivo e livello di tolleranza ammesso. La prima componente si riferisce alla capacità

di un evento rischioso di generare un oggettivo e misurabile impatto sul raggiungimento degli obiettivi progettuali in termini di tempo, costo, qualità e quantità di prodotto/servizio. Ad esempio, l'impatto oggettivo della mancanza di esperienza nella tecnologia di riferimento progettuale potrebbe essere quello di allungare i tempi di sviluppo, aumentare il livello di difettosità, generare conflitti tecnici interni etc. La seconda componente si riferisce al fatto che non tutti i progetti hanno lo stesso livello di tolleranza al manifestarsi di un identico impatto. Ad esempio, per un certo progetto "sforare" il budget di un 20% può essere una causa che può condurre alla cancellazione del progetto stesso mentre per un altro progetto lo stesso elemento non costituisce problema alcuno alla continuazione ed al raggiungimento dei fini progettuali. Non è possibile, quindi, definire un danno se non si conoscono gli obiettivi specifici di progetto e la tolleranza ammessa su ognuno di essi da parte degli stakeholder legittimi. Passo preliminare, dunque, alla gestione delle minacce di un progetto è la determinazione più precisa possibile degli obiettivi di quantità, qualità, tempo, costo e ricavo con i relativi margini di accettabilità. Assegnando valori di probabilità alle condizioni ed alle transizioni della formulazione CEC, nonché punteggi all'impatto delle conseguenze, si avrà la possibilità di valutare in modo completo le minacce del progetto.

Ogni minaccia, dunque, dovrà essere pesata con un voto. Tale voto esprimerà il giudizio circa il valore atteso del danno che il fattore critico potrebbe arrecare al progetto. E', in sostanza, un voto sulla pericolosità di ogni particolare elemento rispetto alla riuscita del progetto che si traduce, in ultima istanza, in un impatto sui suoi costi, tempi, qualità o quantità di requisiti implementati. I voti possono essere assegnati su una scala che assume valori da 1 a 5 dove 1 rappresenta il minimo danno (un incidente marginale) e 5 il massimo danno (il fallimento completo del progetto). E' necessario giungere a tale voto dopo aver stimato separatamente la probabilità di occorrenza (da 0 a 1) dell'evento ed il suo danno prevedibile in caso di manifestazione (da 1 a 5) e moltiplicando tra loro i due termini. Ricordiamo, infine, che il danno deve, a sua volta, essere valutato, anche se informalmente, in termini di impatto oggettivo (vedi definizione) e di tolleranza ammessa (vedi definizione).

Ad esempio: il fattore di rischio negativo precedentemente identificato come: "**se** la competenza tecnica del gruppo sulla tecnologia da usare fosse bassa **allora** il prodotto realizzato potrebbe essere poco affidabile e robusto", potrebbe essere valutato con il 30% di probabilità di accadimento (corrispondente ad un valore numerico pari a 0.3) ed un impatto oggettivo sulla qualità ritenuto alto (ad esempio intorno a 4). Considerando però, che in questa particolare situazione il livello di tolleranza sulla qualità del prodotto è abbastanza lasco, il danno atteso potrebbe ridursi a 3. Il rischio negativo incondizionato corrispondente si porta, dunque, a 0.3 x 3 = 0.9. Il contributo che questa minaccia porta al livello generale rischio negativo del progetto misurato su una scala convenzionale è pari a 0.9.

Una volta che i voti di tutti i rischi negativi in catalogo siano stati espressi sulla base della scala da 1 a 5 e ricordando che 5 rappresenta l'impatto massimo sul progetto, cioè il suo fallimento, potremo considerare le seguenti regole empiriche:

- totale dei voti tra 1 e 25: rischio negativo basso;
- totale dei voti tra 26 e 50: rischio negativo medio;
- totale dei voti maggiore di 50: rischio negativo elevato;

i seguenti casi particolari, però, annullano le precedenti regole:

- presenza di uno o più voti pari a 5: certezza di fallimento;
- presenza di più di un voto pari a 4: rischio negativo elevatissimo;
- presenza di un solo voto pari a 4 e di più di 5 voti tra 3 e 4: rischio negativo elevatissimo;
- assenza di voti pari a 4 e presenza di almeno 3 voti tra 3 ed 4: rischio negativo elevato;

Trattando una minaccia da un punto di vista quantitativo occorre evidenziare come la sua valorizzazione non sia assoluta ma dipenda da due fattori fondamentali: il tempo e le contromisure adottate. La prima dipendenza è legata al fatto che al semplice passare del tempo gli elementi di rischiosità tendono a mutare. Per il secondo aspetto, invece, occorre osservare che l'entità della minaccia dipende fortemente anche dalle strategie che vengono messe in atto per controllarlo. E' quindi possibile esprimere una valutazione degli elementi critici precedente ed una successiva rispetto all'adozione di un piano di azione specifico per la riduzione delle minacce (risultato della TA3). E' naturale aspettarsi, poi, che la valutazione iniziale sia significativamente superiore a quella successiva proprio in virtù dell'efficacia del piano di azione individuato. La prima valorizzazione sarà chiamata "Rischio Negativo Incondizionato", perché legato all'impatto che avrebbero i vari elementi di rischiosità se fossero lasciati liberi di agire incontrastati cioè senza alcuna specifica contromisura che non sia la gestione ordinaria del progetto. La seconda valorizzazione sarà chiamata "Rischio Negativo Residuo" e sarà svolta al netto delle azioni selezionate per essere inserite nel Threat Action Report. Il rapporto tra il rischio negativo dopo e prima della stesura del piano d'azione specifico potrà essere considerato un indicatore di massima dell'efficacia presunta del piano stesso.

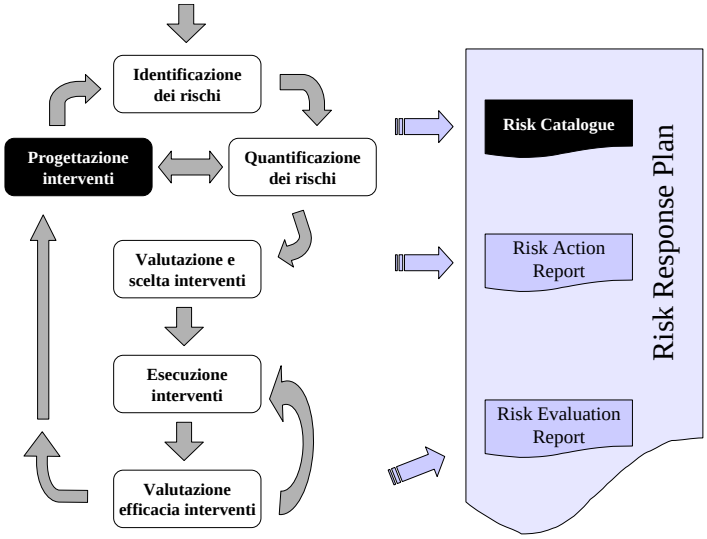
In parallelo alla valorizzazione convenzionale del rischio negativo (sempre obbligatoria) è consigliabile individuare una valorizzazione monetaria di ogni rischio negativo. Questa viene chiamata esposizione economica. E' obbligatorio individuare l'esposizione economica per quelle minacce che possono determinare extra costi significativi. La determinazione di questo valore a livello incondizionato e residuo, dovrà servire per valutare successivamente l'opportunità o meno di attuare una certa azione preventiva o di contenimento.

L'esposizione economica legata al fattore di rischio negativo si deve calcolare come il costo correlato al danno economico (nel caso il rischio negativo si dovesse verificare) moltiplicato per la percentuale di probabilità che il rischio negativo stesso si verifichi (esempio: costo correlato al rischio negativo: 100.000 Euro; fattore di probabilità di occorrenza pari al 35%; esposizione economica pari a 100.000 euro per 0.35 ossia 35.000 Euro). L'esposizione si suddivide in esposizione da fattori **tecnici**, dovuta ad elementi specifici ed individuabili del rischio, esposizione **gestionale**, che copre gli elementi più generali del rischio, oppure esposizione da fattori **economico/finanziari**.
E' essenziale non confondere il danno atteso con il costo delle azioni di prevenzione e recupero che potremmo immaginare per contrastare il rischio negativo stesso. Sarà proprio il confronto tra la riduzione del danno atteso ed il costo delle corrispondenti azioni per la sua gestione che darà la giustificazione economica del Threat Action Report. Ad esempio, il danno prodotto dalla rottura di un server sul quale si sta sviluppando un'applicazione critica è legato al costo delle disfunzioni derivanti dalle

operazioni correnti che non possono essere svolte, ad esempio al costo del ritardo di consegna prevedibile o di mantenimento di un team forzatamente inoperoso, mentre i costi di manutenzione preventiva del server e/o di riparazione urgente sono i costi del piano di gestione delle minacce. Se il costo della manutenzione preventiva e del canone di assistenza che è necessario pagare per ottenere un adeguato livello di servizio per interventi urgenti fosse superiore alla valorizzazione economica del danno associato ai tempi di fermo macchina e di ripristino stimati in condizioni di recupero "normali", allora sarebbe consigliabile non attivare alcuna azione di prevenzione particolare e sostenere il livello di rischio negativo stimato inizialmente nella situazione di recupero "ordinario" dei guasti di apparecchiature.

Nel fare la prima valutazione di esposizione incondizionata occorre, dunque, sforzarsi di non considerare le possibili contromisure che si possono adottare per mitigare il rischio negativo in quanto questo sarà espressamente oggetto della seconda valutazione: quella dell'esposizione residua.
Nel Threat Catalogue possono essere inseriti eventuali commenti per porre maggiormente in evidenza il percorso che ha portato all'individuazione ed alla pesatura di quei particolari rischi negativi.

5.1.3 Progettazione degli interventi (TA3)



L'obiettivo di questa attività è quello di fornire una lista appropriata di attività e responsabilità per il governo delle minacce nonché l'individuazione delle modalità di misura associate al controllo dei risultati.

Al termine di questa attività si disporrà di una preziosa lista di azioni e delle relative responsabilità organizzative che permetteranno di minimizzare l'impatto che i singoli elementi di rischio negativo possono avere sulla riuscita generale del progetto agendo sia sulla probabilità di accadimento che sull'entità del danno previsto per essi.

Le azioni conseguenti potranno essere di tre tipi: di **prevenzione**, di **sorveglianza** e di **contenimento**. La prevenzione tende ad evitare che un certo elemento critico si manifesti nella sua problematicità. La sorveglianza serve a rilevare che un certo elemento critico si sta avvicinando alla zona di pericolosità o si è verificato e che è necessario correre ai ripari. Il contenimento esprime la reazione alla problematicità concretizzatasi e tende ad annullare gli effetti negativi del problema stesso. La prevenzione agisce sia sulla probabilità dell'elemento di rischio negativo, cercando di ridurla, sia sull'entità del danno in caso di manifestazione dell'evento rischioso. Il contenimento agisce, invece, solo sugli effetti del danno cercando di minimizzarli o rimuoverli una volta che l'evento rischioso si sia manifestato. La sorveglianza non agisce

direttamente nè sulla probabilità nè sul danno ma amplifica la capacità di contenimento per via di una più tempestiva azione di innesco dello stesso (accorgersi di un incendio quando ha ormai bruciato tutto non favorisce le azioni di contenimento del danno). Per sorvegliare accuratamente un progetto occorre progettare e mettere in azione un insieme di "sensori" adeguati ai fenomeni da monitorare. Questi sensori possono essere sistemi socio-tecnici di vario tipo da quelli più meccanici a quelli più umani.

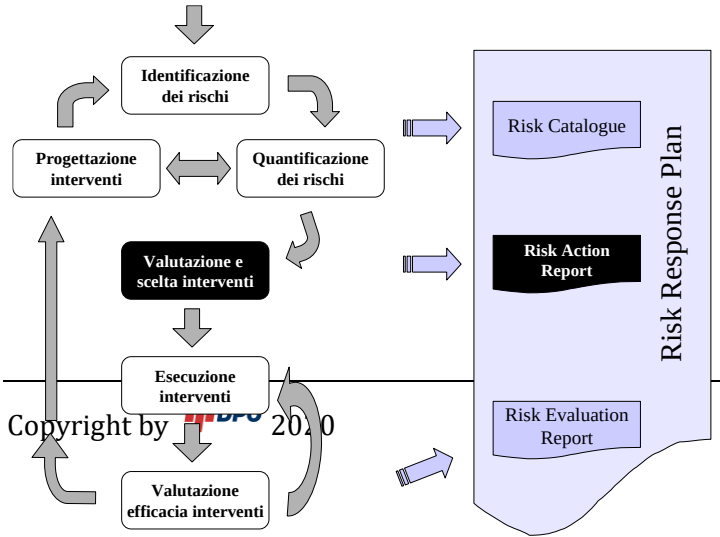
La risposta alle minacce può seguire diverse tecniche, in particolare quelle suggerite sono:

- **Avoidance**: es., evitare il rischio scegliendo una diversa strategia di sviluppo del sistema o un diverso sub-fornitore, tenendo conto che difficilmente una minaccia evidenziata in questa fase si può totalmente eliminare, ma il più delle volte si trasferisce semplicemente ad un'altro task
- **Reduction**: es. la riduzione può avvenire sia in termini di diminuzione della probabilità sia in termini di riduzione di impatto della minaccia correttamente individuato e gestito
- **Transfer**: es. trasferimento di tutto o parte della minaccia in qualche maniera contrattuale, come assicurazioni o verso un sub-fornitore
- **Acceptance**: es. una minaccia il cui impatto o la cui bassa probabilità di accadimento può essere ritenuto trascurabile in termini di conseguenze sul progetto in relazione alla soglia aziendale (o del cliente) di tolleranza.

Se il piano di azione viene ben pensato, messo in opera e seguito fedelmente rappresenterà una forma di assicurazione contro gli infortuni di progetto che potrà essere complementata dalla stipula di vere e proprie polizze assicurative che siano in grado di coprire minacce altrimenti ingestibili.

Naturalmente occorrerà che il piano di azione TAR sia sostenibile da parte dell'organizzazione nel senso che il suo costo sia rapportabile in modo positivo alla riduzione del danno derivante dal suo mancato impiego. Per fare questo occorrerà stimare in modo opportuno costi di gestione e perdite possibili utilizzando anche qui tecniche di analisi economica e finanziaria adeguate.

Tra i rischi negativi identificati verranno presi in considerazione tutti quelli con valore di "minaccia convenzionale" maggiore o uguale a 6. Su tali rischi negativi si procederà alla individuazione di interventi. Nel caso in cui i rischi negativi di livello 6 o superiore siano in numero minore di 10 verranno comunque presi in considerazione quelli appartenenti alla Top 10 (ossia le 10 minacce che hanno ottenuto un valore del fattore di rischio negativo ed esposizione più alto rispetto agli altri).



5.1.4 Valutazione e scelta degli interventi (TA4)

L'obiettivo di questa attività è di selezionare gli interventi di contrasto delle minacce che risultano giustificati ad un'analisi convenzionale od economica.

L'analisi convenzionale utilizza i valori numerici di minaccia mentre quella economica utilizza l'esposizione economica delle minacce ed il costo delle contromisure adottate. L'analisi convenzionale è la più difficile da giustificare perché richiede di paragonare variabili disomogenee: una riduzione del voto rappresentante una minaccia nella situazione precedente e in quella seguente all'applicazione di un intervento (espresso su una scala intera da 1 a 5) con la sua entità economica (espressa in termini monetari). Ad esempio decidere se è opportuno spendere 10.000 Euro per ridurre un fattore di rischio negativo da 5 a 3 può essere difficile e comunque relativamente soggettivo. D'altra parte molte decisioni manageriali sono basate su indicatori di massima dei fenomeni da gestire e sono migliorate da una valutazione quantitativa e non solo qualitativa.

Ad un'analisi convenzionale come quella proposta si può affiancare un'analisi economica in termini monetari se si è in grado di stimare le possibili perdite derivanti dall'accadimento di eventi rischiosi in modo da poterle confrontare successivamente con i costi di governo delle minacce derivanti dall'implementazione del piano di gestione relativo (TRP). L'analisi può essere condotta con le consuete tecniche di valutazione costi/benefici sulla base dei valori attesi delle perdite differenziali cioè:

(perdita possibile * probabilità di perdita)$_{prima}$ - (perdita possibile * probabilità di perdita)$_{dopo}$.

Tale valore dovrà essere superiore a:

(costi di prevenzione + costi di sorveglianza) + (costi di contenimento * probabilità di perdita $_{dopo}$)

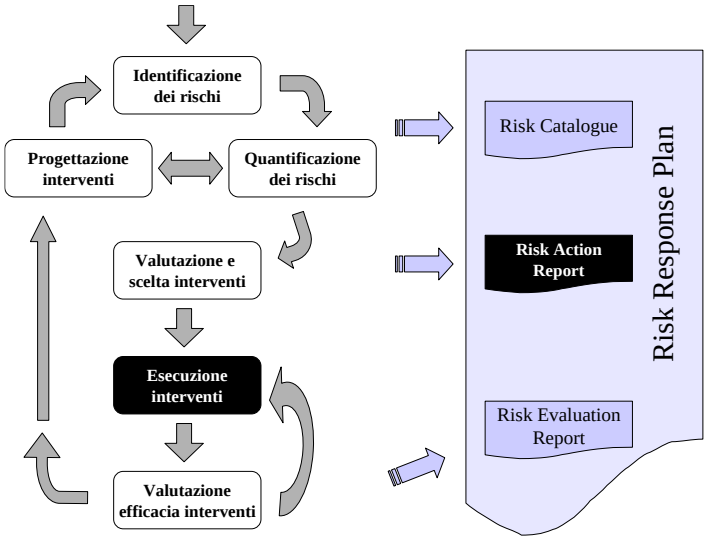
Occorre considerare che l'introduzione di azioni di gestione delle minacce potrebbe portare a identificare nuove minacce inesistenti precedentemente. Per valutare la convenienza delle azioni individuate occorre dunque quantificare l'impatto che queste nuove minacce possono avere sul progetto.

Una volta che l'azione ha superato il test di convenienza può essere registrata nel TAR (Threat Action Report). Il costo delle azioni contenute nel TAR và riportato, poi, nella pianificazione economico/finanziaria come illustrato in allegato. I risultati di questo passo vanno utilizzati per rivalutare se necessario la WBS/OBS ed il PMP.

Nel caso in cui venga accettata la minaccia e non vengano intraprese nè azioni preventive nè di contenimento, il valore dell'esposizione calcolato all'inizio andrà inserito nella pianificazione. Nel caso in cui l'evento dovesse accadere e non vengono intraprese azioni di contenimento il valore di esposizione da considerare è quello pari al valore intero (con valore della probabilità pari al 100%).

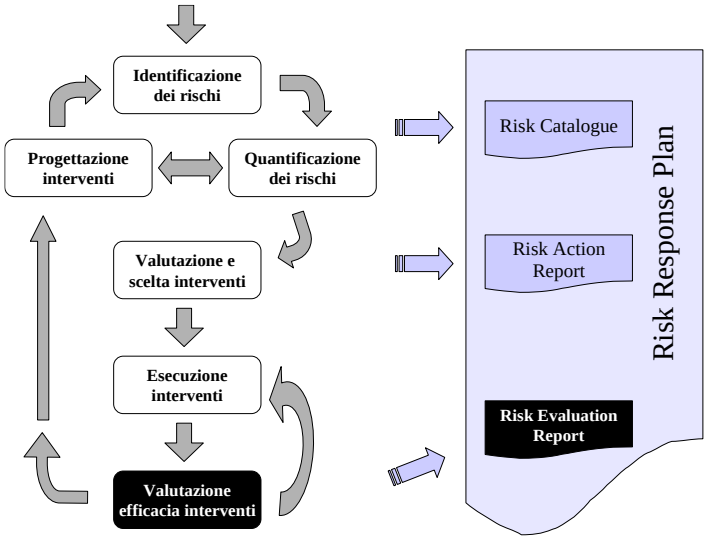
Il Risk Response Plan dovrà essere allegato al Project Management Plan.

5.1.5 Esecuzione degli interventi (TA5)



L'obiettivo di questa attività è di mettere in pratica le azioni che sono state progettate al fine di governare le minacce ed in particolare quelle di prevenzione, di sorveglianza ed, eventualmente, di contenimento. Saranno rilevate tutte le misure necessarie a valutare l'efficacia e l'economicità del piano di gestione delle minacce (TRP).

5.1.6 Verifica sul campo dell'efficacia degli interventi (TA6)



L'obiettivo di questa attività è di valutare in campo l'efficacia e l'efficienza dimostrata dal piano di gestione delle minacce (TRP) al fine di confermarne la validità o di innescare una fase di revisione del sistema di gestione delle minacce. Da questa attività si potrà procedere ad una nuova fase diagnostica (TA1 e TA2) oppure alla definizione di nuove e più efficaci azioni di governo (TA3).

La verifica del piano di gestione delle minacce viene effettuata attraverso lo stato di avanzamento da parte del responsabile. Eventuali rivalutazioni dell'analisi delle minacce verranno effettuate durante le Review di passaggio di fase.

ALLEGATI

ALLEGATO 1 – THREAT CATALOGUE & THREAT ACTION REPORT

Gestione Minacce PROGETTO				PRIMA															RISPOSTA						DOPO			
				Variabili impattate									Periodo di esposizione		P		D	MC	Azioni						P		D	MC
				Responsabilità legali	Brand	Relazioni Esterne	Organizzazione	Conto Economico	Finanza	Quantità	Qualità	Scadenze			Probabilità		peso (da 1 a 5)	peso composto	Azione	Tipo	Assegnata a:	Data inizio	Data fine	Stato	Probabilità		peso (da 1 a 5)	peso composto
N	🗎	Owner	Minaccia										da	a	da 0 a 100	da 1 a 5									da 0 a 100	da 1 a 5		
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0	0	0
																0		0								0		0
																0		0								0		0
																0		0								0		0
																0		0								0		0
																0		0								0		0

Danno	DC
0	0

Danno	DC
0	0

Efficienza
#DIV/0!

ALLEGATO 2 – ESEMPIO DI TRATTAMENTO DEI COSTI DI GESTIONE DELLE MINACCE

CASO 1

Esposizione totale (Danno)	Probabilità accadimento	Esposizione ponderata	Costo azioni preventive	Costo azioni di contenimento	Esposizione residua
100	25%	25			

In tale situazione si decide di accettare la minaccia senza pianificare alcun tipo di azione. Occorrerà inserire 25 nel preventivo come generica contingenza. Si tenga presente che, qualora la minaccia si verificasse, si dovrà tener conto di un totale costi che, se ben stimati, potrebbero essere pari a 100. Se la minaccia non si verifica si dovrà evidenziare un surplus/accantonamento di 25, cioè il 25 non può essere "speso" per altre cose.

CASO 2

Esposizione Totale	Probabilità accadimento	Esposizione ponderata	Costo azioni preventive	Costo azioni di contenimento	Esposizione residua
100	25%	25	2		20

In tale situazione si decide di pianificare delle azioni preventive che portano l'esposizione residua ad un valore pari a 20.
Occorrerà inserire a preventivo il valore 22 (20+2): 20 come generica contingenza e 2 in corrispondenza dell'azione di prevenzione.
Si tenga presente che, qualora la minaccia si verificasse, si dovrà tener conto di un totale costi pari a 102. Se la minaccia non si verifica si dovrà evidenziare un surplus/accantonamento di 20, cioè il 20 non può essere "speso" per altre cose.

CASO 3

Esposizione Totale	Probabilità accadimento	Esposizione ponderata	Costo azioni preventive	Esposizione residua dopo aver intrapreso azioni di prevenzione	Costo azioni di contenimento	Danno economico dopo aver intrapreso azioni di contenimento
100	25%	25	2	20	10	5

In tale situazione si decide di pianificare sia delle azioni preventive che delle azioni di contenimento che portano il danno residuo ad un valore pari a 5.
Occorrerà in fase di pianificazione iniziale, dove è prevista la sola azione di prevenzione, inserire **22 (2+20).**

Occorrerà in fase di aggiornamento della pianificazione, nel caso di accadimento della minaccia e quindi di attivazione dell'azione di contenimento, inserire **17 (2+10+5):**
Si tenga presente che, qualora la minaccia si verificasse, sempre nell'ipotesi di averne ben stimato il valore, si dovrà tener conto di un totale costi pari a 17 (azioni prevenzione 2, azioni contenimento 10, danno residuo 5).

ALLEGATO 3 – THREAT EVALUATION REPORT

Il THREAT EVALUATION REPORT riporta una storia degli eventi significativi relativi alle minacce accadute in corso d'opera con le associate azioni intraprese e la valutazione della loro efficacia ed efficienza tecnica ed economica.

L'obiettivo del TER è quello, da un lato, di mantenere traccia degli accadimenti, delle decisioni prese, dell'appropriatezza delle azioni intraprese nello specifico progetto; dall'altro di alimentare la base di conoscenza necessaria ad uno sviluppo complessivo delle capacità di gestione delle minacce dell'intera azienda (Knowledge Management).

La struttura del documento può essere:

1. Considerazioni generali sull'efficacia e l'efficienza del processo specifico di threat management
2. Elenco delle minacce trasformatisi in problemi
3. Per ogni minaccia accaduta:
    a. codice identificativo
    b. descrizione testuale
    c. azioni previste a piano
    d. azioni effettivamente messe in campo
    e. costi attesi e costi consuntivi
    f. efficacia delle azioni intraprese
    g. danni manifestatisi
    h. lezioni apprese

ALLEGATO 4 – THREAT RESPONSE PLAN

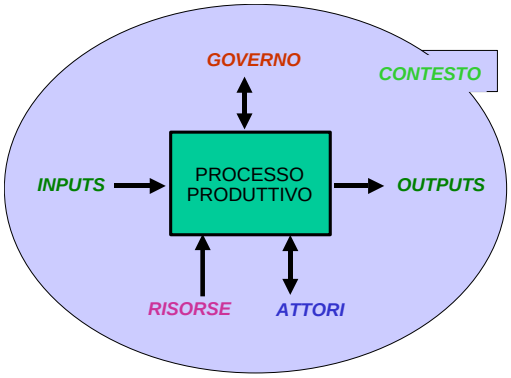
Nel presente capitolo verrà indicata la struttura del Piano di gestione delle Minacce. In generale, il Piano di gestione delle minacce descrive gli obiettivi della gestione delle minacce stesse per i differenti attori, l'identificazione delle aree a più alto rischio negativo, le procedure, i metodi e gli strumenti utilizzati nell'ambito del progetto per la gestione delle minacce.

La struttura documentale è:

1. Management Overview
    a. Sintesi degli obiettivi e delle strategie di gestione delle minacce
    b. Livello generale di minaccia incondizionata
    c. Potenziale danno economico massimo
    d. Esposizione economica incondizionata
    e. Costo del piano di gestione delle minacce
    f. Livello generale di minaccia residua
    g. Esposizione economica residua
    h. ROI del piano di gestione
2. Obiettivi della gestione delle minacce per il progetto
3. Strategie generali di gestione
    a. Approcci utilizzati
    b. Ruoli coinvolti
4. Processo adottato
    a. Standard
    b. Personalizzato (descrivere)
5. Modalità di verifica del piano
    a. Revisioni
    b. Auditing
6. Threat Catalogue
7. Threat Action Report
8. Threat Evaluation Report

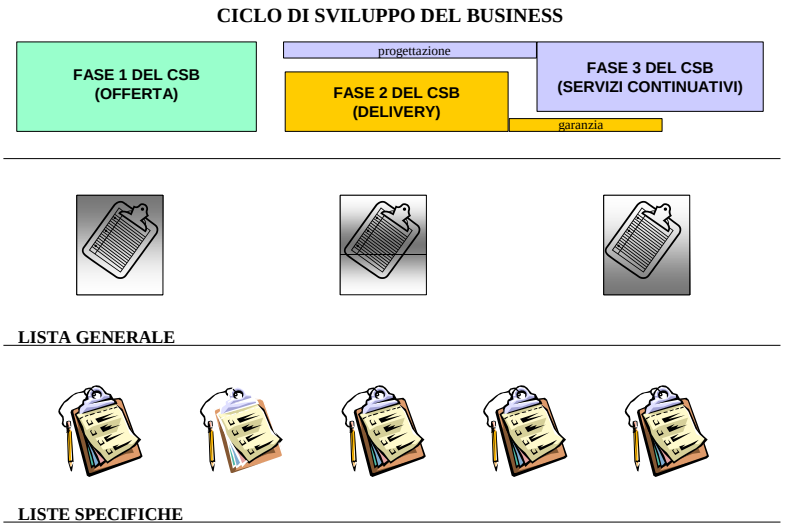
ALLEGATO 5 – CHECK LIST GENERALE DI IDENTIFICAZIONE DEI FATTORI DI RISCHIO NEGATIVO

MODELLO DI BASE



La check list generale di supporto alla individuazione dei fattori di rischio negativo è stata organizzata intorno al modello indicato nella figura accanto. Ogni etichetta corrisponde ad un'area in cui ricercare potenziali elementi di criticità per il progetto o per l'intervento di interesse. A queste si aggiunge un'area di fattori derivanti dalla interazione di variabili appartenenti ad aree diverse; ad esempio il fattore espresso come: "se le risorse economiche a disposizione non consentissero l'implementazione di tutti i requisiti richiesti allora il contratto potrebbe essere risolto a nostro danno" non appartiene nè all'area "requisiti" neè a quella "economico-finanziaria" ma alla combinazione di entrambe in quanto è il rapporto tra le due quantità (requisiti da una parte e risorse economiche dall'altra) ad essere eventualmente fonte di criticità.

La check list generale, inoltre, si mappa su un Ciclo di Sviluppo del Business (CSB) nel senso che ad ogni fase del ciclo si può associare una diversa enfasi per sezioni diverse della lista stessa, come suggeriscono le diverse sfumature di colore nella figura sottostante. Ad esempio nella Fase 1 del CSB (fase di offerta verso il cliente) sarà maggiore l'enfasi su aree quali "requisiti di fornitura" e "aspetti legali" mentre nella Fase 2 del CSB (delivery) sarà maggiore l'enfasi su classi quali "tecnologie di produzione". Occorre evidenziare che quanto scritto non significa in alcun modo che quando si imposta un'analisi delle minacce nelle prime fasi di vita dell'iniziativa (ad esempio nella fase di offerta) si debba tenere conto solo dei fattori pertinenti a quella fase in quanto la valutazione quantitativa ed economica delle minacce ne risulterebbe fortemente penalizzata e falsata. La valutazione deve in ogni momento riferirsi all'intera estensione del progetto ancora da percorrere. E' ovvio che, invece, minacce appartenenti ad una fase ormai superata e non verificatisi saranno da escludere dalla rivalutazione delle minacce dell'iniziativa condotta nelle fasi successive.



Alla check list generale – valida per la maggior parte dei progetti/interventi – si potranno associare check list specifiche di settore con validità limitata a particolari aree o tipi di interventi.

Sia la check list generale che quelle specifiche sono frutto della capitalizzazione dell'esperienza maturata in vari ambiti settoriali e vanno considerate come spunti di analisi e non come fonti di elementi obbligatori da inserire nel catalogo delle minacce di uno specifico intervento. Esse sono evolutive e possono giovarsi di un meccanismo di editing e condivisione informatico che renda più flessibile sia la ricerca dei fattori pertinenti che la memorizzazione delle esperienze fatte in un'ottica di Knowledge Management.

STRUTTURA DELLA CHECK LIST GENERALE

1. INPUT DI PROCESSO
   a. REQUISITI DI FORNITURA
   b. MATERIALI UTILIZZATI
   c. SEMILAVORATI

2. PROCESSO PRODUTTIVO
   a. FLUSSI DI LAVORO
   b. METODI DI LAVORO
   c. ORGANIZZAZIONE INTERNA
   d. TECNOLOGIE DI PRODUZIONE
      i. Logistica
      ii. Macchinari
   e. TECNOLOGIE DI ESERCIZIO
      i. Logistica
      ii. Macchinari
   f. ASPETTI COMUNICATIVI
   g. ASPETTI TEMPORALI
      i. Schedulazione attività
      ii. Sincronizzazione esterna

3. RISORSE DI PROCESSO
   a. FORZA LAVORO
      i. Interna
      ii. Esterna
   b. ENERGIA
   c. RISORSE ECONOMICO-FINANZIARIE

4. STRUTTURA DI GOVERNO
   a. MANAGEMENT
   b. ASPETTI LEGALI
      i. Contratti in input
      ii. Contratti in output
      iii. Altri aspetti legali

5. ATTORI (STAKEHOLDER)
   a. CLIENTE
   b. AZIENDA
      i. Management
      ii. Personale operativo
   c. SUBFORNITORI
   d. REGOLATORI ESTERNI

6. CONTESTO AMBIENTALE

7. FATTORI COMBINATI

Licenza

Attribuzione - Non opere derivate 2.5 (ITALIA)

L'OPERA (COME SOTTO DEFINITA) È MESSA A DISPOSIZIONE SULLA BASE DEI TERMINI DELLA PRESENTE LICENZA "CREATIVE COMMONS PUBLIC LICENCE" ("CCPL" O "LICENZA"). L'OPERA È PROTETTA DAL DIRITTO D'AUTORE E/O DALLE ALTRE LEGGI APPLICABILI. OGNI UTILIZZAZIONE DELL'OPERA CHE NON SIA AUTORIZZATA AI SENSI DELLA PRESENTE LICENZA O DEL DIRITTO D'AUTORE È PROIBITA.

CON IL SEMPLICE ESERCIZIO SULL'OPERA DI UNO QUALUNQUE DEI DIRITTI QUI DI SEGUITO ELENCATI, TU ACCETTI E TI OBBLIGHI A RISPETTARE INTEGRALMENTE I TERMINI DELLA PRESENTE LICENZA AI SENSI DEL PUNTO 8.e. IL LICENZIANTE CONCEDE A TE I DIRITTI QUI DI SEGUITO ELENCATI A CONDIZIONE CHE TU ACCETTI DI RISPETTARE I TERMINI E LE CONDIZIONI DI CUI ALLA PRESENTE LICENZA.

1. Definizioni. Ai fini e per gli effetti della presente licenza, si intende per

a. **"Collezione di Opere"**, un'opera, come un numero di un periodico, un'antologia o un'enciclopedia, nella quale l'Opera nella sua interezza e forma originale, unitamente ad altri contributi costituenti loro stessi opere distinte ed autonome, sono raccolti in un'unità collettiva. Un'opera che costituisce Collezione di Opere non verrà considerata Opera Derivata (come sotto definita) ai fini della presente Licenza;
b. **"Opera Derivata"**, un'opera basata sull'Opera ovvero sull'Opera insieme con altre opere preesistenti, come una traduzione, un arrangiamento musicale, un adattamento teatrale, narrativo, cinematografico, una registrazione di suoni, una riproduzione d'arte, un digesto, una sintesi, o ogni altra forma in cui l'Opera possa essere riproposta, trasformata o adattata. Nel caso in cui un'Opera tra quelle qui descritte costituisca già Collezione di Opere, essa non sarà considerata Opera Derivata ai fini della presente Licenza. Al fine di evitare dubbi è inteso che, quando l'Opera sia una composizione musicale o registrazione di suoni, la sincronizzazione dell'Opera in relazione con un'immagine in movimento ("synching") sarà considerata Opera Derivata ai fini di questa Licenza;
c. **"Licenziante"**, l'individuo o l'ente che offre l'Opera secondo i termini e le condizioni della presente Licenza;
d. **"Autore Originario"**, il soggetto che ha creato l'Opera;
e. **"Opera"**, l'opera dell'ingegno suscettibile di protezione in forza delle leggi sul diritto d'autore, la cui utilizzazione è offerta nel rispetto dei termini della presente Licenza;
f. **"Tu"/"Te"**, l'individuo o l'ente che esercita i diritti derivanti dalla presente Licenza e che non abbia precedentemente violato i termini della presente

Licenza relativi all'Opera, o che, nonostante una precedente violazione degli stessi, abbia ricevuto espressa autorizzazione dal Licenziante all'esercizio dei diritti derivanti dalla presente Licenza.

2. Libere utilizzazioni. La presente Licenza non intende in alcun modo ridurre, limitare o restringere alcun diritto di libera utilizzazione o l'operare della regola dell'esaurimento del diritto o altre limitazioni dei diritti esclusivi sull'Opera derivanti dalla legge sul diritto d'autore o da altre leggi applicabili.

3. Concessione della Licenza. Nel rispetto dei termini e delle condizioni contenute nella presente Licenza, il Licenziante concede a Te una licenza per tutto il mondo, gratuita, non esclusiva e perpetua (per la durata del diritto d'autore applicabile) che autorizza ad esercitare i diritti sull'Opera qui di seguito elencati:

a. riproduzione dell'Opera, incorporazione dell'Opera in una o più Collezioni di Opere e riproduzione dell'Opera come incorporata nelle Collezioni di Opere;
b. distribuzione di copie dell'Opera o di supporti fonografici su cui l'Opera è registrata, comunicazione al pubblico, rappresentazione, esecuzione, recitazione o esposizione in pubblico, ivi inclusa la trasmissione audio digitale dell'Opera, e ciò anche quando l'Opera sia incorporata in Collezioni di Opere.
c. Al fine di evitare dubbi è inteso che, se l'Opera sia di tipo musicale
    i. **Compensi per la comunicazione al pubblico o la rappresentazione o esecuzione di opere incluse in repertori.** Il Licenziante rinuncia al diritto esclusivo di riscuotere compensi, personalmente o per il tramite di un ente di gestione collettiva (ad es. SIAE), per la comunicazione al pubblico o la rappresentazione o esecuzione, anche in forma digitale (ad es. tramite webcast) dell'Opera.
    ii. **Compensi per versioni cover.** Il Licenziante rinuncia al diritto esclusivo di riscuotere compensi, personalmente o per il tramite di un ente di gestione collettiva (ad es. SIAE), per ogni disco che Tu crei e distribuisci a partire dall'Opera (versione cover).
d. **Compensi per la comunicazione al pubblico dell'Opera mediante fonogrammi.** Al fine di evitare dubbi, è inteso che se l'Opera è una registrazione di suoni, il Licenziante rinuncia al diritto esclusivo di riscuotere compensi, personalmente o per il tramite di un ente di gestione collettiva (ad es. IMAIE), per la comunicazione al pubblico dell'Opera, anche in forma digitale.
e. **Altri compensi previsti dalla legge italiana**. Al fine di evitare dubbi, è inteso che il Licenziante rinuncia al diritto esclusivo di riscuotere i compensi a lui attribuiti dalla legge italiana sul diritto d'autore (ad es. per l'inserimento dell'Opera in un'antologia ad uso scolastico ex art. 70 l. 633/1941). Al Licenziante spettano in ogni caso i compensi irrinunciabili a lui attribuiti dalla medesima legge (ad es. l'equo compenso spettante all'autore di opere musicali, cinematografiche, audiovisive o di sequenze di immagini in movimento nel caso di noleggio ai sensi dell'art. 18-bis l.633/1941).

I diritti sopra descritti potranno essere esercitati con ogni mezzo di comunicazione e in tutti i formati. Tra i diritti di cui sopra si intende compreso il diritto di apportare all'Opera le modifiche che si rendessero tecnicamente necessarie per l'esercizio di detti diritti tramite altri mezzi di comunicazione o su altri formati, ma a parte questo non hai

diritto di realizzare Opere Derivate. Tutti i diritti non espressamente concessi dal Licenziante rimangono riservati.

4. Restrizioni. La Licenza concessa in conformità al precedente punto 3 è espressamente assoggettata a, e limitata da, le seguenti restrizioni:

a. Tu puoi distribuire, comunicare al pubblico, rappresentare, eseguire, recitare o esporre in pubblico l'Opera, anche in forma digitale, solo assicurando che i termini di cui alla presente Licenza siano rispettati e, insieme ad ogni copia dell'Opera (o supporto fonografico su cui è registrata l'Opera) che distribuisci, comunichi al pubblico o rappresenti, esegui, reciti o esponi in pubblico, anche in forma digitale, devi includere una copia della presente Licenza o il suo Uniform Resource Identifier. Non puoi proporre o imporre alcuna condizione relativa all'Opera che alteri o restringa i termini della presente Licenza o l'esercizio da parte del beneficiario dei diritti qui concessi. Non puoi concedere l'Opera in sublicenza. Devi mantenere intatte tutte le informative che si riferiscono alla presente Licenza ed all'esclusione delle garanzie. Non puoi distribuire, comunicare al pubblico, rappresentare, eseguire, recitare o esporre in pubblico l'Opera, neanche in forma digitale, usando misure tecnologiche miranti a controllare l'accesso all'Opera ovvero l'uso dell'Opera, in maniera incompatibile con i termini della presente Licenza. Quanto sopra si applica all'Opera anche quando questa faccia parte di una Collezione di Opere, anche se ciò non comporta che la Collezione di Opere di per sé ed indipendentemente dall'Opera stessa debba essere soggetta ai termini ed alle condizioni della presente Licenza. Qualora Tu crei una Collezione di Opere, su richiesta di qualsiasi Licenziante, devi rimuovere dalla Collezione di Opere stessa, ove materialmente possibile, ogni riferimento in accordo con quanto previsto dalla clausola 4.b, come da richiesta.
b. Qualora Tu distribuisca, comunichi al pubblico, rappresenti, esegua, reciti o esponga in pubblico, anche in forma digitale, l'Opera o Collezioni di Opere, devi mantenere intatte tutte le informative sul diritto d'autore sull'Opera. Devi riconoscere una menzione adeguata rispetto al mezzo di comunicazione o supporto che utilizzi: (i) all'Autore Originale (citando il suo nome o lo pseudonimo, se del caso), ove fornito; e/o (ii) alle terze parti designate, se l'Autore Originale e/o il Licenziante hanno designato una o più terze parti (ad esempio, una istituzione finanziatrice, un ente editoriale) per l'attribuzione nell'informativa sul diritto d'autore del Licenziante o nei termini di servizio o con altri mezzi ragionevoli; il titolo dell'Opera, ove fornito; nella misura in cui sia ragionevolmente possibile, l'Uniform Resource Identifier, che il Licenziante specifichi dover essere associato con l'Opera, salvo che tale URI non faccia alcun riferimento alla informazione di protezione di diritto d'autore o non dia informazioni sulla licenza dell'Opera. Tale menzione deve essere realizzata in qualsiasi maniera ragionevole possibile; in ogni caso, in ipotesi di Opera Derivata o Collezione di Opere, tale menzione deve quantomeno essere posta nel medesimo punto dove viene indicato il nome di altri autori di rilevanza paragonabile e con lo stesso risalto concesso alla menzione di altri autori di rilevanza paragonabile.

5. Dichiarazioni, Garanzie ed Esonero da responsabilità

SALVO CHE SIA ESPRESSAMENTE CONVENUTO ALTRIMENTI PER ISCRITTO FRA LE PARTI, IL LICENZIANTE OFFRE L'OPERA IN LICENZA "COSI' COM'E'" E NON FORNISCE ALCUNA DICHIARAZIONE O GARANZIA DI QUALSIASI TIPO CON RIGUARDO AI MATERIALI, SIA ESSA ESPRESSA OD IMPLICITA, DI FONTE LEGALE O DI ALTRO TIPO, ESSENDO QUINDI ESCLUSE, FRA LE ALTRE, LE GARANZIE RELATIVE AL TITOLO, ALLA COMMERCIABILITÀ, ALL'IDONEITÀ PER UN FINE SPECIFICO E ALLA NON VIOLAZIONE DI DIRITTI DI TERZI O ALLA MANCANZA DI DIFETTI LATENTI O DI ALTRO TIPO, ALL'ESATTEZZA OD ALLA PRESENZA DI ERRORI, SIANO ESSI ACCERTABILI O MENO. ALCUNE GIURISDIZIONI NON CONSENTONO L'ESCLUSIONE DI GARANZIE IMPLICITE E QUINDI TALE ESCLUSIONE PUÒ NON APPLICARSI A TE.

6. Limitazione di Responsabilità. SALVI I LIMITI STABILITI DALLA LEGGE APPLICABILE, IL LICENZIANTE NON SARÀ IN ALCUN CASO RESPONSABILE NEI TUOI CONFRONTI A QUALUNQUE TITOLO PER ALCUN TIPO DI DANNO, SIA ESSO SPECIALE, INCIDENTALE, CONSEQUENZIALE, PUNITIVO OD ESEMPLARE, DERIVANTE DALLA PRESENTE LICENZA O DALL'USO DELL'OPERA, ANCHE NEL CASO IN CUI IL LICENZIANTE SIA STATO EDOTTO SULLA POSSIBILITÀ DI TALI DANNI. NESSUNA CLAUSOLA DI QUESTA LICENZA ESCLUDE O LIMITA LA RESPONSABILITA' NEL CASO IN CUI QUESTA DIPENDA DA DOLO O COLPA GRAVE.

7. Risoluzione

a. La presente Licenza si intenderà risolta di diritto e i diritti con essa concessi cesseranno automaticamente, senza necessità di alcuna comunicazione in tal senso da parte del Licenziante, in caso di qualsivoglia inadempimento dei termini della presente Licenza da parte Tua, ed in particolare delle disposizioni di cui ai punti 4.a e 4.b, essendo la presente Licenza condizionata risolutivamente al verificarsi di tali inadempimenti. In ogni caso, la risoluzione della presente Licenza non pregiudicherà i diritti acquistati da individui o enti che abbiano acquistato da Te Collezioni di Opere, ai sensi della presente Licenza, a condizione che tali individui o enti continuino a rispettare integralmente le licenze di cui sono parte. Le sezioni 1, 2, 5, 6, 7 e 8 rimangono valide in presenza di qualsiasi risoluzione della presente Licenza.
b. Sempre che vengano rispettati i termini e le condizioni di cui sopra, la presente Licenza è perpetua (e concessa per tutta la durata del diritto d'autore sull'Opera applicabile). Nonostante ciò, il Licenziante si riserva il diritto di rilasciare l'Opera sulla base dei termini di una differente licenza o di cessare la distribuzione dell'Opera in qualsiasi momento; fermo restando che, in ogni caso, tali decisioni non comporteranno recesso dalla presente Licenza (o da qualsiasi altra licenza che sia stata concessa, o che sia richiesto che venga concessa, ai termini della presente Licenza), e la presente Licenza continuerà ad avere piena efficacia, salvo che vi sia risoluzione come sopra indicato.

8. Varie

a. Ogni volta che Tu distribuisci, o rappresenti, esegui o reciti pubblicamente in forma digitale l'Opera, il Licenziante offre al destinatario una licenza per l'Opera nei medesimi termini e condizioni che a Te sono stati concessi dalla presente Licenza.

b. L'invalidità o l'inefficacia, secondo la legge applicabile, di una o più fra le disposizioni della presente Licenza, non comporterà l'invalidità o l'inefficacia dei restanti termini e, senza bisogno di ulteriori azioni delle parti, le disposizioni invalide o inefficaci saranno da intendersi rettificate nei limiti della misura che sia indispensabile per renderle valide ed efficaci.
c. In nessun caso i termini e le disposizioni di cui alla presente Licenza possono essere considerati rinunciati, né alcuna violazione può essere considerata consentita, salvo che tale rinuncia o consenso risultino per iscritto da una dichiarazione firmata dalla parte contro cui operi tale rinuncia o consenso.
d. La presente Licenza costituisce l'intero accordo tra le parti relativamente all'Opera qui data in licenza. Non esistono altre intese, accordi o dichiarazioni relative all'Opera che non siano quelle qui specificate. Il Licenziante non sarà vincolato ad alcuna altra disposizione addizionale che possa apparire in alcuna comunicazione da Te proveniente. La presente Licenza non può essere modificata senza il mutuo consenso scritto del Licenziante e Tuo.
e. **Clausola i Commons.** Questa Licenza trova applicazione nel caso in cui l'Opera sia utilizzata in Italia. Ove questo sia il caso, si applica anche il diritto d'autore italiano. Negli altri casi le parti si obbligano a rispettare i termini dell'attuale Licenza Creative Commons generica che corrisponde a questa Licenza Creative Commons iCommon