Requisiti per una metodologia di Risk Assessment

Requirements for Risk Assessment Methodologies

Giancarlo Butti ♦*, Alberto Piamonte* □

♦ *ISACA Chapter Milano*
□ *ISACA Chapter Roma*

Sommario

Questo articolo, ispirato alla Guida tecnica di Open Group (Requirements for Risk Assessment Methodologies), fornendo un elenco di criteri di valutazione e di requisiti indispensabili chiaramente definiti, identifica e descrive quali siano le principali caratteristiche che una metodologia di valutazione del rischio deve possedere per essere efficace.

Ne vengono in questo modo indicate, sia le caratteristiche da individuare, che il valore che esse rappresentano.

Abstract

This paper, inspired by an Open Group Technical Guide, identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.

1. Introduzione

Nel corso del tempo, sono stati sviluppati una varietà di metodi che consentono di analizzare e valutare i rischi presenti nell'ambito di un'organizzazione. Le esigenze alla base del metodo di valutazione scelto sono in genere molteplici e variabili, come risultato, l'approccio adottato varia ampiamente in termini di consistenza, accuratezza, ed utilizzo.

Questo articolo riprende una serie di concetti base dell'analisi dei rischi[1] e successivamente, *ispirandosi ad una analisi dell'organizzazione Open Group*[2]*,* si propone di individuare ed articolare gli aspetti più significativi e le caratteristiche delle metodologie utilizzate nella valutazione dei rischi.

2. Obiettivi

Nel complesso contesto della gestione del rischio, va sempre tenuto presente che il principale obiettivo dell'attività stessa è quello di individuare e stimare i livelli di esposizione ad eventi che possano causare danni di qualsiasi natura, in modo che i responsabili aziendali siano in grado di gestire questi rischi, accettandoli, o mitigandoli – con l'adozione di misure, ritenute sufficienti a ridurre la potenziale perdita ad un accettabile livello, oppure investendo in garanzie di carattere assicurativo.

Con questo in mente, le metodologie scelte dovranno, in particolare, garantire che:

- i risultati delle analisi possano, in modo affidabile, essere confrontati, sia tra diverse organizzazioni / scenari sia nell'ambito di una singola organizzazione,
- chi deve selezionare disponga di validi criteri di valutazione, in grado di differenziare tra le metodologie più efficaci e quelle meno efficaci,
- chi sviluppa le metodologie possa farlo tenendo conto di esigenze reali.

3. Utilizzo

Questo articolo può essere utilizzato per:

- valutare se una determinata metodologia di valutazione del rischio soddisfa le esigenze di gestione,
- dotarsi di elementi per poter differenziare le varie metodologie in modo per poter individuare quella che più da vicino soddisfi le nostre esigenze,

[1] Parte del testo, tabelle ed immagini sono tratte dal libro di G. Butti e A. Piamonte Governance del rischio - Dall'analisi al reporting e la sintesi per la Direzione ITER. 2020,

[2] Open Group è un consorzio globale nato con lo scopo del raggiungimento degli obiettivi di impresa attraverso gli standard tecnologici. é costituito da più di 800 organizzazioni include clienti, fornitori di sistemi e soluzioni, fornitori di strumenti, integratori, accademici e consulenti in più settori. Tra le quali: Fujitsu, HCL, Huawei, Intel, Micro Focus, Oracle, Accenture, Philips, Boeing, Capgemini, Microsoft, NASA, Google e molte altre

- verificare se una determinata metodologia valuta efficacemente il rischio (piuttosto che, semplicemente, alcuni sub-elementi di questo, quali ad esempio, il livello di implementazione dei controlli),
- costituire un riferimento per lo sviluppo o l'evoluzione di metodologie per la valutazione dei rischi.

4. Definizione dei termini

Questa guida utilizza la terminologia fornita in Open Group Standard Risk Taxonomy (O-RT), Version 2.0. Prendendo in prestito da quel documento, qui si applicano le seguenti definizioni chiave:

Risk	The probable frequency and probable magnitude of future loss.
Threat	Anything that can act in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.
Vulnerability	The probability that a threat event will become a loss event.[3]
Asset	Anything that may be affected in a manner whereby its value is diminished, or the act introduces liability to the owner. Examples include systems, data, people, facilities, cash, etc.

5. I limiti delle analisi dei rischi

Il primo aspetto da considerare è che l'analisi dei rischi non è una scienza esatta. Infatti, come evidenziato nel proseguo dell'articolo è opportuno considerare che il risultato che si desidera ottenere non è un valore preciso ed assoluto del rischio, ma una stima attendibile dello stesso.

Questo si traduce anche in una diversa modalità con cui rappresentare i risultati dell'analisi, che in luogo di valori assoluti si può esprimere, nel caso in cui si utilizzi una metodologia basata su valori quantitativi, con un range di possibili valori.

Nel caso si utilizzino metodologie basate su valori qualitativi, questi esprimono già un grado di incertezza, basato sulla scala di valori rappresentata nei termini.

Del resto, anche secondo la **ISO 31010** l'analisi dei rischi è caratterizzata da una serie di incertezze legate a numerosi fattori, fra i quali:

- le metodologie utilizzate,
- l'incertezza sul fatto che gli eventi futuri saranno simili al quelli del passato,
- la conoscenza imperfetta o incompleta delle minacce,
- le vulnerabilità ancora da scoprire,
- le dipendenze non riconosciute, che possono portare a impatti imprevisti.

[3] Questa definizione differisce da quelle date in altri documenti / standard

Analogamente il **NIST 800 30 R1** evidenzia che un'analisi del rischio non è uno strumento preciso ed è condizionata da:

- i limiti delle metodologie, degli strumenti e delle tecniche di valutazione specifici impiegati,
- la soggettività, la qualità e l'affidabilità dei dati utilizzati,
- l'interpretazione dei risultati della valutazione,
- le capacità e le competenze di quegli individui o gruppi che conducono le valutazioni.

6. Documentare l'analisi dei rischi

Per quanto sopra è opportuno identificare e documentare le fonti di incertezza sia in merito ai dati utilizzati, sia in merito alle metodologie.

Dovrebbero essere adeguatamente documentate:

- le scelte effettuate,
- la metodologia scelta,
- il momento,
- il perimetro di indagine,
- la completezza,
- l'accuratezza con cui si è svolta l'analisi dei rischi.

È infatti opportuno ricordare che un'analisi dei rischi viene effettuata su un ambiente dinamico ed in continua evoluzione e che quindi ognuno degli elementi fino a qui identificati può variare nel tempo, modificando il livello di rischio.

Al riguardo anche il momento del ciclo di vita, ad esempio di un progetto o di un'applicazione determina il livello di accuratezza della valutazione.

Diverso è infatti il caso di un'analisi condotta su un sistema in produzione, per il quale possono esistere anche dei dati storici in merito ad anomalie ed incidenti occorsi, rispetto ad un sistema in fase di progettazione.

7. Qualitativo o quantitativo

Nel precedente articolo[4] sono state presentate diverse metodologie, sia di natura qualitativa, sia quantitativa. Queste hanno pregi e limiti come già evidenziato e come ricorda anche il NIST nella Tabella 1.

Tabella 1. Vantaggi e svantaggi dei metodi quantitativi e qualitativi

Risk Analysis	**Quantitative methods**	**Qualitative methods**
Chosen advantages	Provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls.	The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
Chosen disadvantages	The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to • An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year) • An approximate cost for each occurrence of the threat-source's exercise of the vulnerability • A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.	The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

Tratto da: NIST SP800 30

[4] G.Butti, A. Piamonte, Misurare la physical cyber security, Rivista - La Comunicazione - Note, Recensioni e Notizie 2016

In realtà tali metodologie devono essere considerate non come fra loro alternative, ma con finalità diverse: vanno quindi utilizzate in funzione del risultato che si desidera ottenere, anche congiuntamente.

Di fatto un'analisi dei rischi di tipo qualitativo può essere più veloce da svolgere e richiedere un numero più limitato di informazioni.

Può quindi essere molto utile per dare un inquadramento iniziale della situazione, ad esempio dei rischi relativamente ad una determinata categoria di asset.

In considerazione del costo e dell'impegno richiesto per un'analisi dei rischi puntuale, dopo questa prima valutazione ci si potrà concentrare, con analisi anche di tipo quantitativo, sulle aree di maggior rischio.

In tale contesto è particolarmente importante che, chi svolge l'analisi, sia cosciente dei limiti degli strumenti che decide di utilizzare, evitando di forzare l'uso di strumenti inadatti ai propri scopi.

Un errore questo che in realtà si riscontra molto frequentemente.

È emblematico in tale senso quanto sta accadendo con riferimento, ad esempio, al Regolamento Europeo sulla protezione dei dati (679/2016), il così detto GDPR.

Oltre a confondere l'analisi dei rischi (prevista obbligatoriamente da diversi articoli del GDPR, fra i quali il 24, 25 e 32 e per quanto riguarda gli aspetti di sicurezza in particolare da quest'ultimo) con la DPIA (articolo 35), moltissimi consulenti utilizzano per lo svolgimento dell'analisi quanto già messo in atto, ad esempio, la certificazione ISO 27001.

È evidente in questo caso l'errore del voler applicare una metodologia la cui finalità è valutare i rischi in merito alla sicurezza delle informazioni, ad un oggetto totalmente diverso, e cioè i diritti e le libertà delle persone fisiche: una notevole differenza.

La conoscenza delle possibilità e delle finalità degli strumenti utilizzati è quindi fondamentale e, come già indicato nei paragrafi precedenti, l'indicazione di tali informazioni dovrebbe essere parte integrante della documentazione a corredo dell'analisi dei rischi.

8. Informazioni per l'analisi dei rischi: metodi e fonti

Qualunque sia la metodologia utilizzata, l'analisi dei rischi si basa su una serie di informazioni che è necessario raccogliere e documentare.

Queste vanno dalla mappatura degli asset sui quali svolgere l'analisi, agli elementi che consentono di stimare l'impatto di un evento dannoso o la probabilità di accadimento dell'evento stesso.

È evidente che le varie metodologie di analisi dei rischi non fanno altro che mettere in relazione fra loro, secondo gli schemi e gli algoritmi che le contraddistinguono, le informazioni che sono state raccolte o elaborate; la qualità della valutazione dipenderà in larga misura dalla qualità delle informazioni raccolte, dalla loro completezza, aggiornamento, affidabilità, coerenza, etc..

Nessuna metodologia, per quanto complessa, può sopperire alla mancanza delle informazioni da cui partire; nemmeno metodologie basate sulla stima di esperti si sottraggono a questa regola.

Ci sono diverse pubblicazioni dedicate all'analisi dei rischi che suggeriscono modalità per la raccolta delle informazioni quali il **NIST 800 30** o la **Harmonized Threat and Risk Assessment (TRA) Methodology** realizzata fra gli altri dalla Royal Canadian Mounted Police.

Tabella 2. Tecniche per la raccolta di informazioni (Adattamento da NIST SP 800-30)

Questionnaire	To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.
On-site Interviews	Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.
Document Review	• Policy documents (e.g., legislative documentation, directives), • system documentation (e.g., system user guide, system administrative manual, • system design and requirement document, acquisition document), • security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the IT system. • An organization's mission impact analysis or asset criticality assessment provides information regarding system data criticality and sensitivity
Use of Automated Scanning Tool	Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Sebbene riguardi le attività di audit, alcuni suggerimenti su metodi e fonti di informazioni possono essere mutuati anche dalla ISO 19011 che cita ad esempio:

- interviste,
- osservazioni,
- documenti,
- registrazioni,
- sintesi dei dati,
- indicatori di prestazione,
- informazioni sui piani di campionamento,
- informazioni di ritorno dai clienti e fornitori,
- indagini e misurazioni esterne,
- banche dati,
- siti web,
- simulazione,
- elaborazione di modelli, etc..

Alcune di queste informazioni sono oggettive e relativamente semplici da individuare, come ad esempio l'elenco degli asset (anche se sarà possibile decidere il livello di granularità da utilizzare); se l'analisi dei rischi riguarda un sistema IT è indispensabile una profonda comprensione dell'ambiente di elaborazione ed al riguardo è utile rifarsi alla già citata norma NIST 800 30.

Tabella 3. Informazioni in ambito ICT (NIST 800 30)

Hardware
Software
System interfaces (e.g., internal and external connectivity)
Data and information
Persons who support and use the IT system
System mission (e.g., the processes performed by the IT system)
System and data criticality (e.g., the system's value or importance to an organization)
System and data sensitivity.
The functional requirements of the IT system
Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
System security architecture
Current network topology (e.g., network diagram)

Information storage protection that safeguards system and data availability, integrity, and confidentiality
Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
Management controls used for the IT system (e.g., rules of behavior, security planning)
Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
Physical security environment of the IT system (e.g., facility security, data center policies)
Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

Per altre informazioni, come ad esempio quelle utili a valutare probabilità ed impatto, la loro raccolta e valutazione sarà molto più complessa.

Come vedremo, in questo caso non sarà tuttavia necessario disporre di moltissime informazioni per fare una utile stima dei rischi, ma nondimeno tale stima richiederà che i parametri che entrano in gioco siano valutati da esperti. In altre parole, in assenza di dati oggettivi saranno i dati implicitamente presenti nel know how[5] degli esperti che consentiranno di ottenere un risultato valido.

Va puntualizzato al riguardo che le organizzazioni dispongono di molteplici fonti dati dalle quali possono ricavare informazioni utili, ad esempio, a valutare la probabilità che una minaccia si estrinsechi.

Il problema è che tali informazioni sono solitamente ignorate, non classificate, non collezionate.

Fra queste troviamo:

- quelle certamente riconducibili direttamente al sistema informativo, quali ad esempio:
  - la segnalazione di anomalie e malfunzionamenti da parte di utenti sia interni che esterni,
  - le richieste di interventi da parte degli utenti per risolvere tali situazioni (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdita ed alterazione di dati, rotture hw, etc.);

[5] Butti G., Tutela del capitale intellettuale e sistemi esperti: applicazioni pratiche di intelligenza artificiale, www.cybersecurity360

- quelle che possono in qualche modo derivare da problemi legati al sistema informativo, quali ad esempio:
  - reclami, in particolare dei clienti (ad esempio ritardi nelle consegne, errate evasione di un ordine, etc.);
  - reclami dei fornitori (ad esempio ritardi nei pagamenti).

Per poter fornire informazioni utili questi eventi vanno adeguatamente censiti in appositi database.

Per le segnalazioni direttamente riconducibili al sistema informativo le aziende più grandi dispongono di processi formalizzati e di apposite procedure per la gestione dei ticket di assistenza.

Tuttavia, spesso il livello di dettaglio con cui sono segnalati i problemi o meglio ancora il livello di dettaglio con cui viene censita l'identificazione della causa e la descrizione della soluzione non è sufficiente.

Si perde in questo modo la possibilità di effettuare un'analisi a posteriori di quali siano le aree del sistema informativo più esposte, piuttosto che le applicazioni più carenti.

Spesso chi analizza e risolve il problema è concentrato unicamente a fornire supporto nei tempi più rapidi possibili e non dedica un tempo adeguato alla fase, altrettanto importante, di corretta classificazione delle cause.

Tale mancanza è principalmente imputabile alla scarsa formazione del personale e alla bassa sensibilità del management aziendale che privilegia la soluzione immediata e "tattica" dei problemi, piuttosto che affrontarne alla radice le possibili cause.

Anche nel caso della gestione dei reclami provenienti dall'esterno, in particolare dai clienti, sono rari i casi in cui vi è una gestione informatizzata del processo di risoluzione.

Solo in aziende come le banche, che hanno specifici obblighi normativi, si procede di solito ad una gestione mediante un processo formalizzato che tiene traccia dell'iter seguito.

Anche in questo caso però è raro trovare un'idonea classificazione dei problemi e delle cause scatenanti, tali da poter effettuare un'analisi a posteriori delle aree più a rischio del sistema informativo.

I problemi in questo caso si pongono a diversi livelli; innanzi tutto ricondurre un reclamo esterno ad un malfunzionamento del sistema informativo non è immediato.

È necessario analizzare nel dettaglio il contenuto stesso del reclamo, interagendo da un lato con un cliente "ostile" e dall'altro con un insieme di strutture aziendali che partecipano al processo che non ha correttamente funzionato.

Restando in ambito bancario: un reclamo derivante da un errato calcolo della rata di un mutuo può derivare da diverse cause, una delle quali può essere un malfunzionamento

dell'applicazione che effettua il conteggio delle rate o di una qualunque delle applicazioni a monte e a valle della stessa.

Per verificare se si tratta effettivamente di un problema applicativo e non di un malfunzionamento isolato sarebbe necessario disporre di un sufficiente numero di segnalazioni opportunamente classificate cioè censite con modalità omogenee.

Le premesse per poter effettuare queste analisi sono comunque:

- una corretta segnalazione da parte dei clienti direttamente al call center o all'ufficio reclami della banca,
- una corretta segnalazione da parte della filiale nel caso in cui il cliente si rechi direttamente allo sportello.

Ulteriori fonti dati sono costituiti dai sistemi di monitoraggio; questi possono fornire dati in tempo reale o a scadenze prefissate, con diversi livelli di dettaglio ed aggregazione.

I sistemi di monitoraggio possono ad esempio verificare:

- la raggiungibilità di un sistema,
- l'esistenza in vita di un sistema,
- il corretto funzionamento di un sito web mediante robot di navigazione automatica che simulano un utente reale,
- la misurazione delle prestazioni della LAN,
- la misurazione delle prestazioni della WAN,
- la corretta replica dei dati verso i siti di DR.

In alcune aziende è formalizzata la gestione degli incidenti informatici, anche se con tale termine possono intendersi eventi molto diversi fra loro.

Ad esempio, un incidente potrebbe essere considerato un malfunzionamento applicativo che rende indisponibile l'applicazione per gli utenti, mentre a livello infrastrutturale si potrebbe considerare incidente ciò che provoca un disservizio generalizzato.

Anche in questo caso è importante censire correttamente le informazioni per procedere a posteriori con un'analisi delle stesse.

Ulteriori fonti informative sono costituiti da una serie di indicatori, quali ad esempio il numero di righe di codice modificate in un certo periodo, distinguendo fra quelle effettuate per attività di manutenzione risolutiva da quelle effettuate per attività evolutiva.

Nel primo caso gli interventi evidenziano la presenza di situazioni anomale che sono state o sono in fase di risoluzione. Il secondo caso introduce invece una possibile instabilità futura nei sistemi, a causa delle novità introdotte.

Il livello di obsolescenza di un sistema potrebbe renderlo inefficace rispetto ad una evoluzione delle esigenze introducendo elementi di rischio, quali ad esempio una caduta delle prestazioni in termini di capacità elaborativa, risorse disponibili, tempi di risposta, etc..

Si pensi ad esempio ad elaborazioni batch notturne che si allungano sempre di più e non rendono disponibile il sistema informativo in tempo per l'orario di apertura delle filiali di una banca.

Anche l'analisi dei log può essere utile per valutare a posteriori un incidente o comunque un evento insolito ed individuarne le cause.

Anche il sistema dei controlli interni (di linea e di secondo livello) e l'audit costituiscono, oltre che strumenti di controllo e di indagine, anche una fonte di informazioni per rilevare situazioni anomale, legate direttamente ai sistemi informativi ovvero potenzialmente derivanti da questi.

In realtà le attività di audit dovrebbero essere pianificate sulla base delle analisi delle informazioni precedentemente censite, le quali dovrebbero consentire l'individuazione delle aree del sistema informativo più a rischio, sulle quali è quindi maggiormente utile effettuare indagini.

Gli esempi riportati evidenziano tutti una serie di elementi comuni:

- la necessità di specifiche regole di rilevazione e classificazione (non interpretabili) degli eventi, ad esempio mediante strumenti che prevedano una adeguata alberatura che guidi nella compilazione coloro che effettuano la segnalazione e successivamente la risoluzione del problema,
- una corretta identificazione e classificazione delle cause,
- una analisi a posteriori dei dati raccolti, al fine di individuare la presenza di problemi endemici e non legati a fattori casuali, al fine di individuare le aree di rischio e predisporre opportuni interventi sia di controllo, sia correttivi,
- la necessità di adeguata formazione e sensibilizzazione di tutto il personale su questi temi,
- la necessità che il management aziendale dia adeguata importanza alla gestione di questi aspetti, affiancando alle soluzioni tattiche quelle strategiche.

Tabella 4. Possibili fonti dati per la valutazione delle probabilità

segnalazioni di malfunzionamenti da parte di utenti sia interni che esterni (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdite o alterazioni di dati, rotture…);
rapporti su incidenti
reclami dei clienti (per ritardi nelle consegne, errate evasioni di ordini…);
reclami dei fornitori (ad esempio ritardi nei pagamenti)
reclami dei dipendenti (ad esempio ritardi nei pagamenti degli stipendi, errori nei rimborsi spese)
rapporti di audit
analisi dei log
ticket: consentono di individuare i fattori di rischio e i difetti che possono preludere ad un incidente. supporto all'analisi delle cause

Nell'uso delle informazioni sopra citate devono comunque essere presi in considerazione importanti fattori; l'utilizzo di dati storici per la valutazione della probabilità, nasconde infatti delle insidie e pertanto è necessario valutare attentamente qual è la profondità storica con cui utilizzare tali dati. Questa non è assoluta, ma va determinata per ogni singola tipologia di evento, considerando il contesto di riferimento.

Ad esempio, una serie di incidenti di sicurezza derivanti dal malfunzionamento di un apparato o dalla mancanza di contromisure, non possono essere presi in considerazione se nel frattempo l'apparato è stato sostituito ovvero se sono state realizzate delle contromisure.

Non ha quindi senso definire a priori di prendere in considerazione tutti gli eventi anomali ed incidenti registrati, né che si prendano in considerazione ad esempio solo quelli degli ultimi 6 mesi.

Deve essere, infatti, presa in considerazione la serie storica di eventi che ha ancora valore, cioè che è applicabile ad una situazione (ad esempio un componente del sistema informativo) che non è stata cambiata nel tempo.

9. Calcolare la probabilità

Continuiamo l'articolo prendendo in considerazione, fra i parametri che entrano nella valutazione del rischio, la valutazione della probabilità.

Nei paragrafi precedenti si è dato per scontato che chi sta effettuando l'analisi sia in grado di valutare direttamente tale parametro in base alle informazioni disponibili ed alla propria esperienza.

In realtà le metodologie di analisi dei rischi, pur riconoscendo tale possibilità, introducono ulteriori parametri.

Ad esempio, nel caso di un evento che prevede l'intervento intenzionale di un attaccante, la valutazione deve anche considerare la sua motivazione che è a sua volta condizionata:

- dal valore intrinseco del bene che potrebbe sottrarre o del danno che potrebbe provocare,
- dalle vulnerabilità che potrebbe sfruttare,
- dalle contromisure in atto per contrastare le minacce.

Nel seguito dell'articolo verrà illustrata la metodologia **FAIR** (Factor Analysis of Information Risk), nella quale la valutazione della probabilità risulta essere una funzione di:

- frequenza della minaccia, a sua volta funzione della frequenza di contatto e probabilità di attacco,
- vulnerabilità, a sua volta funzione della capacità di attacco e azioni di contrasto.

Il **NIST Special Publication 800-30 Rev 1** propone invece una valutazione articolata in 3 fasi:

- in primo luogo, viene valutata:
  - nel caso di minaccia di tipo deliberato, la probabilità che eventi di minaccia siano messi in atto da parte di un attaccante,
  - nel caso di minacce accidentali, la probabilità che eventi di minaccia si verifichino;
- in secondo luogo, viene valutata la probabilità che gli eventi di minaccia, una volta messi in atto o verificatisi, comportino effettivamente degli impatti negativi sugli asset/processi dell'organizzazione;
- infine, viene valutata la probabilità complessiva come una combinazione della due precedenti secondo lo schema riportato in Figura 1.

Più dettagliatamente per quanto attiene gli atti deliberati, una valutazione della probabilità di accadimento si basa sulle caratteristiche di chi porta avanti l'attacco:

- le sue capacità e competenze,
- le sue intenzioni,
- i suoi obiettivi.

Al riguardo, il **NIST (800 30 RV1)** propone le tabelle, riportate come esempi mantenendo la denominazione originale, D3, G2, G4, G5.

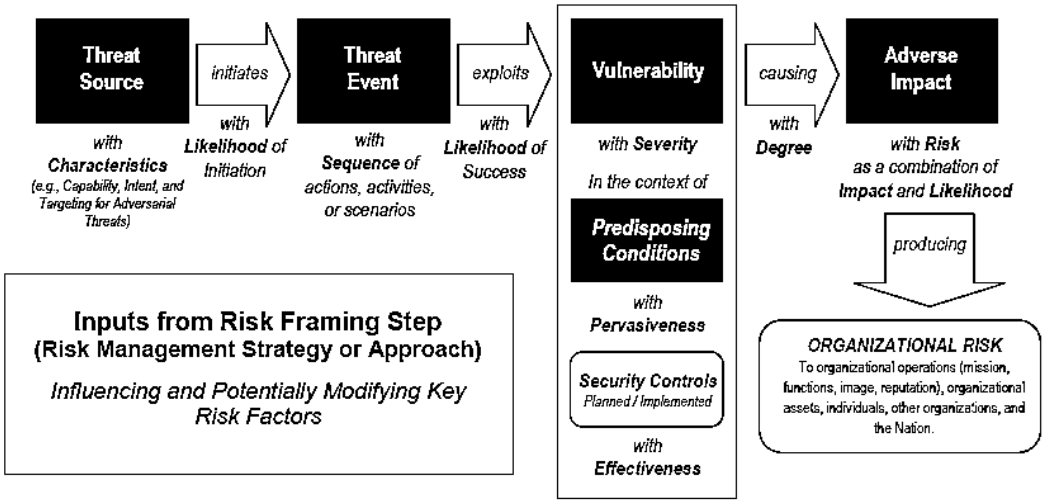

Figura 1

Per eventi diversi dagli atti deliberati, la probabilità che l'evento si verifichi si stima utilizzando:

- prove storiche,
- dati empirici o
- altri fattori.

Table D-3: assessment scale – characteristics of adversary capability

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Table G-2: assessment scale – likelihood of threat event initiation (adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Table G-4: assessment scale – likelihood of threat event resulting in adverse impacts

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Table G-5: assessment scale – overall likelihood

Likelihood of Threat Event Initiation or Occurrence		Likelihood Threat Events Result in Adverse Impacts			
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High

Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

La tabella G4 indica la probabilità che un evento, una volta avviato, possa provocare effettivamente un danno e la tabella G5 indica la probabilità complessiva.

Si rinvia al documento originale del NIST per una trattazione completa.

10. La metodologia FAIR: componente chiave: ontologia

In primo luogo, dobbiamo definire un modello che descriva come il rischio opera, indicandone i fattori costituenti e le loro relazioni. La descrizione, in termini matematici, di queste relazioni ci consentirà quindi di calcolare il rischio partendo dalla stima di tali fattori.

Nel paragrafo Ontologia FAIR saranno descritti in dettaglio i fattori che costituiscono l'ontologia sviluppata in ambito Open Group.

11. Aspetti salienti per la valutazione

Questo paragrafo descrive le caratteristiche che sono indicative di una buona metodologia di valutazione del rischio. L'insieme degli elementi considerati non è in alcun modo completo od esaustivo, ma vuole stabilire alcuni concetti fondamentali.

11.1 . Probabilistico

Uno studio ed un'analisi del rischio è un compito difficile, infatti, spesso si deve partire da ipotesi fondate su informazioni incomplete, che contengono quindi un certo livello di incertezza. Tale "incertezza" non va mascherata, ma costituisce essa stessa parte dell'informazione. Essa va quindi misurata e registrata perché divenga parte di una corretta analisi del rischio.

L'incertezza può e deve essere intesa come un attributo dell'informazione, piuttosto che un limite della stessa. La sua comunicazione e il suo uso possono ottimizzare la gestione del rischio ed in particolare quella degli eventi dannosi e delle loro conseguenze.

Solo trattando il rischio come un problema di previsione probabilistica si può aggiungere il necessario rigore, controllo e struttura al processo di analisi.

Una buona metodologia per la valutazione del rischio deve quindi fornire all'analista gli strumenti per la stima delle sue probabilità e di quelle dei fattori costituenti.

11.2. Accurato

Una buona metodologia di valutazione del rischio dovrebbe fornire risultati accurati. Mentre sembrerebbe ovvio che i risultati del rischio valutato dovrebbero essere precisi, molte metodologie di valutazione del rischio si focalizzano maggiormente sugli aspetti tecnici di debolezza del sistema (vulnerabilità), invece che sulle probabilità di accadimento di un evento dannoso e sul conseguente impatto.

11.2.1. Precisione e accuratezza

Uno dei maggiori ostacoli all'adozione di un'analisi del rischio è l'idea che sia richiesta precisione. La precisione nella misura è desiderabile, ma non è necessaria. La precisione è definita, in ambito dell'analisi dei rischi, come "la nostra capacità di fornire informazioni corrette ". Precisione, tuttavia, viene definita come "il grado di "convergenza" di dati rilevati individualmente (campione) rispetto al valore medio della serie cui appartengono". Poiché il rischio è un problema di probabilità, è estremamente difficile essere precisi nella misurazione, nel calcolo e nella rappresentazione, la precisione desiderata potrebbe non sempre essere raggiungibile.

Fortunatamente, per la maggior parte delle decisioni nella gestione del rischio delle informazioni non sono necessarie espressioni precise della probabile frequenza della perdita o della probabile entità della perdita, soprattutto quando la metodologia di valutazione del rischio è in grado di fornire costantemente risultati accurati. Uno degli obiettivi nella misurazione ed espressione del rischio dovrebbe essere quello di produrre e trasferire informazioni accurate.

Accuratezza e precisione sono due termini spesso utilizzati in modo errato nel contesto della misurazione, perciò è importante evidenziarne bene la differenza.

L'*accuratezza* indica quanto una misura è vicina al valore reale.

La *precisione*, invece, indica quanto vicini o quanto ripetibili siano i risultati. Uno strumento di misura preciso darà quasi lo stesso risultato ogni volta che viene utilizzato. In altre parole, la precisione di un esperimento, di uno strumento o di un valore è una misura dell'affidabilità e della coerenza.

Più in generale, l'accuratezza di un esperimento, di uno strumento o di un valore è una misura di quanto strettamente i risultati concordino con il valore vero. L'accuratezza si riferisce al grado di conformità e correttezza di qualcosa rispetto a un valore vero o assoluto, mentre la precisione si riferisce a uno stato di rigida precisione, cioè a quanto costantemente qualcosa è strettamente esatto.

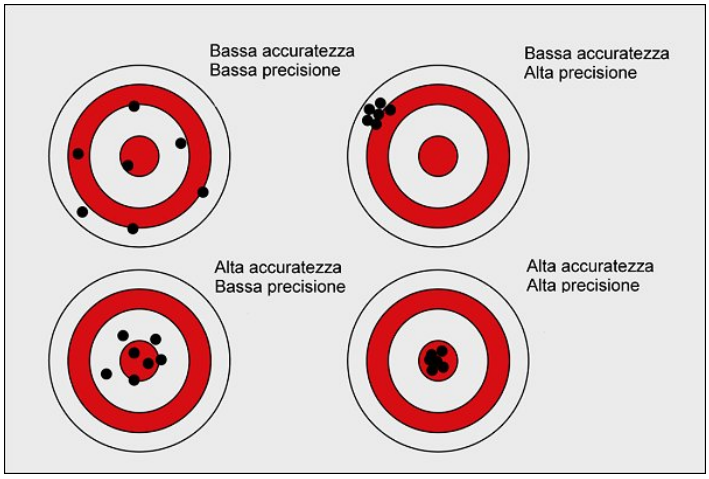

Figura 2 *- Accuratezza e precisione*

Quando una quantità viene misurata o calcolata, l'accuratezza della misurazione o il risultato calcolato danno il grado di vicinanza del valore al valore corretto. L'accuratezza, quindi, descrive una proprietà del *risultato*. La precisione, d'altra parte, quantifica il grado di efficacia con cui sono state effettuate le misure, o quanto bene sono stati effettuati i calcoli. La precisione dice qualcosa sul *processo di misurazione* o sul calcolo, ma non dice nulla sul risultato della misurazione o sul valore calcolato.

Spesso è possibile aumentare l'accuratezza di un risultato aumentando la precisione dello strumento di misura o del metodo di calcolo; tuttavia, se il modo di eseguire la misurazione o eseguire il calcolo non è corretto, aumentare la precisione non aumenterà necessariamente l'accuratezza del risultato. Inoltre, se il valore di una quantità è già noto con accuratezza, l'aumento della precisione non cambierà il suo valore.

11.3. Come riportare la precisione dei risultati

Esistono diversi modi per riportare (e valutare) la precisione dei risultati. Il più semplice è l'intervallo o *range* (ovvero la differenza tra i risultati più alti e quelli più bassi), spesso riportato come una differenza dalla media delle misure. Un modo migliore per evidenziare la precisione dei risultati – ma che richiede un'analisi statistica – sarebbe quello di valutare ed indicare la cosiddetta "deviazione standard".

La deviazione standard descrive come i risultati sono distribuiti intorno alla media. Se i risultati sono distribuiti normalmente, il 68% di questi sarà all'interno della deviazione standard. Una maggiore deviazione standard indica una maggiore dispersione nella precisione nei risultati. Una deviazione standard più piccola indica meno dispersione. Entrambe le serie di risultati hanno la stessa media.

11.3.1. Coerente (ripetibile)

Un indicatore significativo di una buona metodologia di valutazione del rischio è la ripetibilità delle misure. Essa consiste nel grado di concordanza tra una serie di misure della medesima grandezza quando le singole misurazioni sono effettuate lasciando immutate le condizioni di misura. In altre parole, se due analisti partono dalle medesime informazioni ed operano in modo indipendente dovrebbero arrivare a conclusioni simili.

Questa coerenza è importante per due motivi. In primo luogo, risultati ripetibili convalidano il grado di rigore e la logica della metodologia. In secondo luogo, rendono il risultato difendibile e credibile.

11.3.2. Difendibile

Affinché la valutazione del rischio sia difendibile, i risultati devono apparire accurati e logici. In caso contrario, quanto emerge dalla valutazione nonché il valutatore stesso perderanno inevitabilmente di credibilità.

11.3.3. Logico

L'utilizzo di una ontologia per la definizione del rischio consente anche di dimostrare e giustificare la "logica" utilizzata per trarre le conclusioni relative al rischio sia in termini dei fattori considerati, sia della matematica utilizzata per metterli in relazione

Una valida misurazione del rischio non deve utilizzare operazioni matematiche prive di senso. Ad esempio, molti metodi di valutazione del rischio che utilizzano scale ordinali, utilizzano anche operazioni aritmetiche per mettere in relazioni tali valori, ignorando il fatto che l'impiego di aritmetica con tali scale non porta a risultati logici e che quindi non è né accettabile né giustificabile ed andrebbe evitata.

11.3.4. Incentrato sul rischio

Le uniche metriche che contano davvero sono la probabile frequenza dell'evento perdita e la probabile entità della perdita. Ne consegue che, qualsiasi valutazione che non possa essere espressa in questi termini non è in realtà una misurazione del rischio, e non fornisce le informazioni necessarie per prendere le decisioni migliori nella gestione del rischio.

11.3.5. Conciso e significativo

L'espressione del rischio deve fornire le informazioni appropriate per i vari destinatari. Ad esempio, mentre i dirigenti dovranno essere messi in grado di scegliere se accettare, mitigare o trasferire il rischio, le informazioni tecniche fornite dovrebbero invece consentire alle parti interessate (tecniche) di realizzare le soluzioni selezionate. I risultati della valutazione del rischio dovrebbero essere espressi nel modo più conciso possibile per ridurre la possibilità di confusione. Le elaborazioni tecniche sui controlli e le tecniche di attacco dovrebbero essere utilizzate con giudizio.

Infine per essere significative, le raccomandazioni dovranno anche essere praticamente realizzabili per consentirne un utilizzo diretto, senza ulteriori eccessive elaborazioni.

11.3.6. Economicamente giustificato

Migliorare il livello di accuratezza di una misura ha un costo che cresce, in genere con un andamento simile a quello indicato in figura 3.

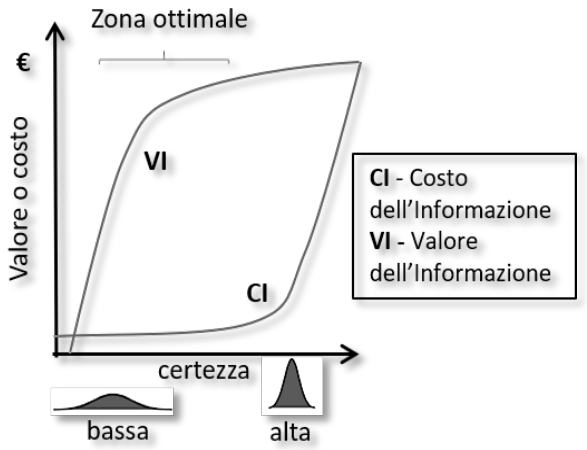

Figura 3 *- Costo / accuratezza analisi*

Migliorare le stime ha un costo progressivamente crescente. Di questo fenomeno va tenuto conto per evitare investimenti il cui ritorno, in termini di gestione del rischio, è progressivamente decrescente. In altre parole, esiste un livello di accuratezza oltre il quale non conviene andare.

11.3.7. Assegnazione delle Priorità

I risultati di una valutazione del rischio dovrebbero fornire chiare indicazioni relative alla priorità di intervento. La definizione delle priorità potrà essere basata sul rischio, sulle risorse necessarie per affrontare i problemi, e/o su altri criteri precedentemente previsti dal management.

12. Ontologia FAIR

L'ontologia FAIR costituisce la base per l'omonima metodologia e ne garantisce efficacia, praticità e concretezza. Detto semplicemente, possiamo affermare che l'ontologia costituisce un modello di come il rischio si genera, descrivendone i fattori costituenti e le loro relazioni. Queste relazioni possono essere descritte matematicamente consentendo quindi di calcolare il rischio partendo da misure e stime dei fattori stessi (v. Figura 4 e Figura 5).

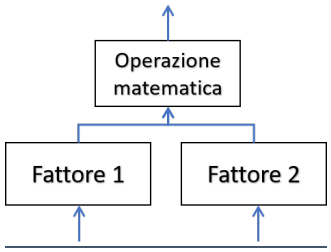

Figura 4 *- Relazione tra fattori FAIR*

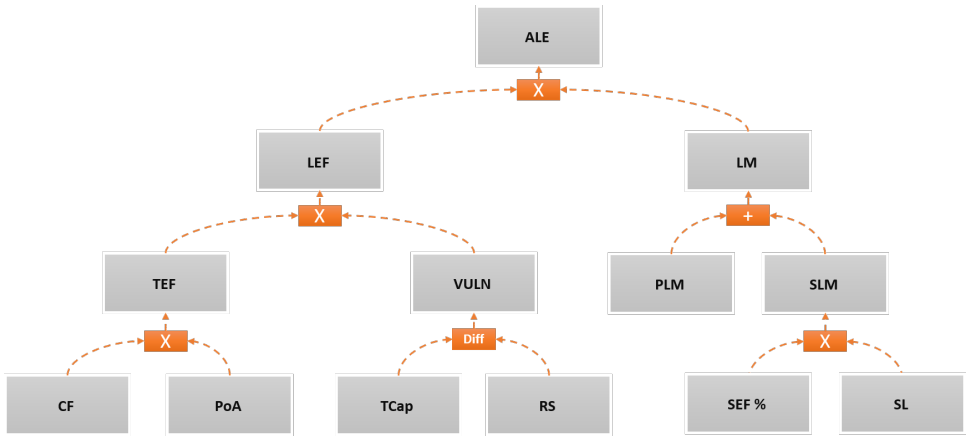

Figura 5*- Ontologia FAIR*

Tabella 5 - Fattori dell'ontologia FAIR

Sigla	Descrizione
ALE	**Annual Loss Excpectation** Perdita Totale Annua L'esposizione alla perdita totale è il rischio totale calcolato (valore della perdita atteso) che si verifica su base annua (se non è dimostrato che un evento di perdita si verifichi almeno una volta all'anno). Ciò significa che l'importo di un singolo evento di perdita viene ripartito negli anni precedenti. Gli scenari di rischio con eventi di perdita che si verificano una o più volte all'anno mostrano la somma degli eventi di perdita annuali.

Sigla	Descrizione
LEF	Loss Event Frequency Frequenza degli Eventi di Perdita La frequenza degli eventi di perdita è la frequenza probabile, entro un periodo di tempo, in cui una minaccia danneggerà un asset. Affinché questa misura abbia un significato, deve includere un periodo di tempo. Ex. quante volte all'anno gli hacker eseguono un attacco Denial of Service contro un sistema bancario online che si traduce in una perdita di utilizzo per i clienti o con la frequenza con cui i ladri rubano denaro.
TEF	Threat Event Frequency Frequenza degli Eventi Minaccia La frequenza degli eventi di minaccia è la frequenza probabile, entro un periodo di tempo, in cui una minaccia potrebbe causare una perdita. Rispetto alla LEF, questa misura descrive come una minaccia può, piuttosto che quanto spesso si tradurrà in una perdita. Ex. quante volte all'anno un ladro cerca di rubare i soldi o quante volte gli hacker eseguono un attacco Denial of Service al tuo computer.
CF	La Frequenza di Contatto (CF) è la frequenza probabile, entro un periodo di tempo, in cui una minaccia entrerà in contatto con una risorsa. Il contatto può essere fisico o "logico" (ad esempio, sulla rete).
PoA	La Probabilità di Azione (PoA) è la probabilità che una minaccia agisca contro una risorsa una volta che si verifica il contatto. Una volta che si verifica il contatto tra una minaccia e una risorsa, l'azione contro la risorsa può o meno aver luogo. Per alcuni tipi di agenti di minaccia, in particolare gli agenti di minaccia naturali, l'azione ha sempre luogo. Ad esempio, se un tornado entra in contatto con una casa, l'azione è una conclusione scontata. Tuttavia, le scansioni delle porte su un sito Web potrebbero non comportare ulteriori azioni da parte della minaccia.
VULN	La Vulnerabilità (VULN) è la probabilità che un evento di minaccia diventi un evento di perdita. La vulnerabilità esiste quando c'è una differenza tra l'attacco utilizzato dall'agente di minaccia e la capacità di una risorsa di resistere a quell'attacco. Un esempio di ciò è il malware rivolto a un server Windows senza patch.
TCap	La Capacità di Minaccia (TCap) è il probabile livello di forza che una minaccia è in grado di applicare contro una risorsa. Il contesto per questa misurazione è con le capacità e le risorse che una minaccia ha a disposizione per attaccare una risorsa. Nell'esempio degli attacchi degli stati-nazione, l'esperienza e la conoscenza dell'hacking definiscono le abilità e la quantità di tempo e denaro disponibile per finanziare gli attacchi sono le risorse.

Sigla	Descrizione
RS	La difficoltà misura la forza di un controllo rispetto al livello di sforzo richiesto dagli attacchi per una violazione riuscita. Ad esempio, un sistema bancario online che sfrutta l'autenticazione a più fattori ha una difficoltà maggiore per una comunità di hacker rispetto a uno protetto da una semplice coppia di nome utente e password.
LM	Loss Magnitude (LM) è la probabile entità della perdita risultante da un evento di perdita. L'altro lato della tassonomia in Frequenza degli eventi di perdita ha introdotto i fattori che determinano la probabilità che si verifichino eventi di perdita. Il lato Loss Magnitude della tassonomia descrive l'altra metà dell'equazione del rischio: i fattori che determinano l'entità della perdita quando si verificano gli eventi.
PL	La Perdita Primaria (PL) è il risultato diretto delle azioni di una minaccia su una risorsa e spesso rappresenta l'intenzione di agire contro la risorsa. Il proprietario degli asset interessati è considerato lo stakeholder principale in un'analisi. Ex. Il successo degli attacchi Denial of Service e della violazione dei dati di un sito di shopping online durante le festività natalizie si traduce in una perdita di entrate previste, che di solito si prevede saranno le più alte dell'anno, per l'azienda.
SL	Il Rischio Secondario (SL) è il risultato di stakeholder secondari, come clienti, azionisti, autorità di regolamentazione, ecc., Che reagiscono negativamente all'evento di perdita primaria che si traduce in un'ulteriore perdita per lo stakeholder principale. Un esempio sono i clienti che hanno fatto causa a un'azienda dopo una violazione dei dati o il costo dell'offerta di servizi di monitoraggio del credito ai clienti interessati da una violazione dei dati.

13. Conclusioni

Le organizzazioni di tutti i tipi hanno una crescente necessità di potersi avvalere di strumenti per una valutazione dei rischi che consenta loro di meglio indirizzare i propri investimenti in termini di sicurezza.

Nonostante le oggettive difficoltà, derivanti molto spesso dalla carenza delle informazioni necessarie allo scopo, sono oggi disponibili metodi che consentono, anche in tale contesto, di elaborare con relativa facilità e con l'uso di normali strumenti di office automation, risultati utili per tale finalità.

È quindi fondamentale che le organizzazioni rivedano il proprio approccio al rischio, per essere preparate ad affrontare le nuove sfide delle quali la recente pandemia costituisce un valido esempio.