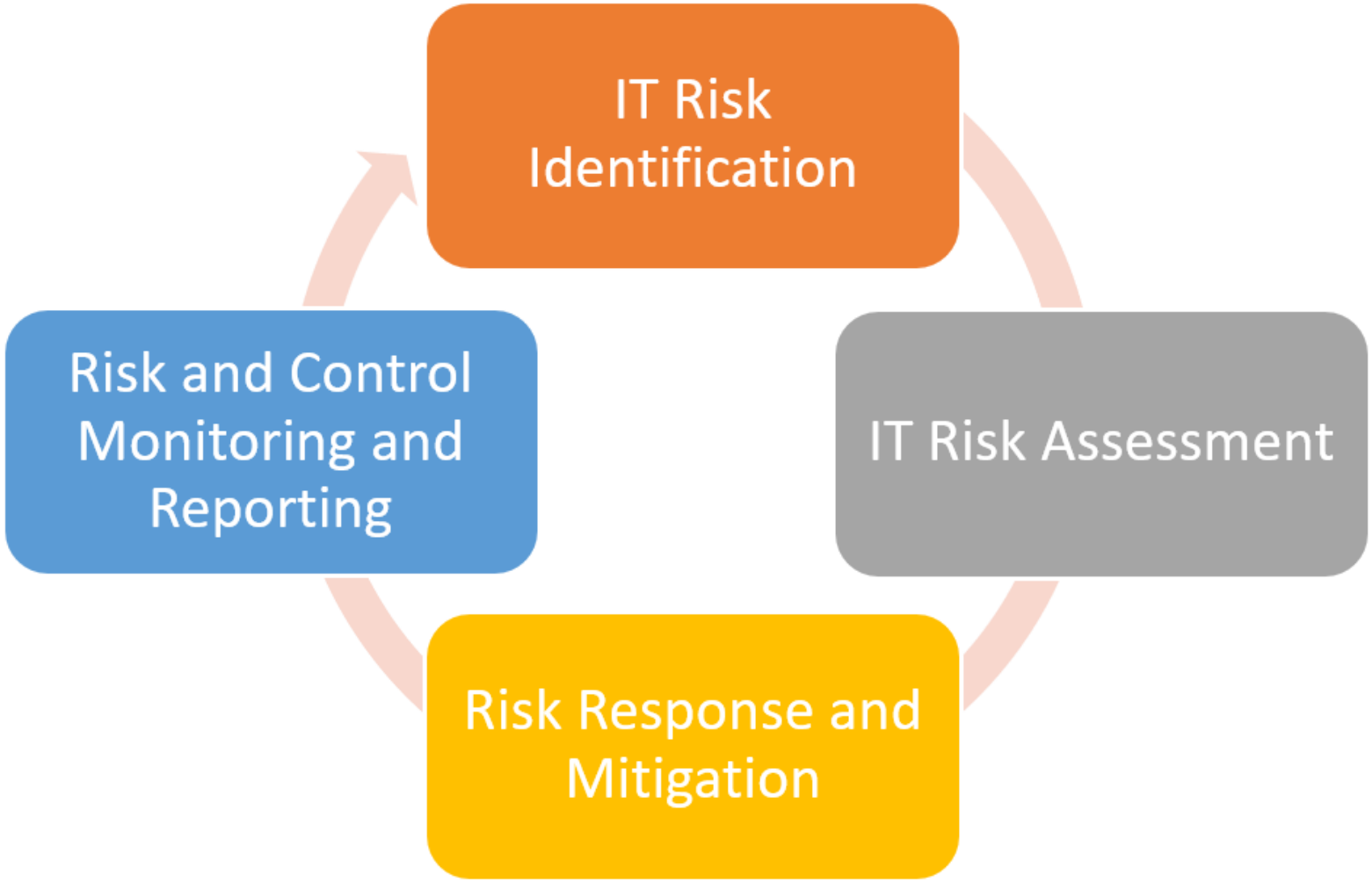
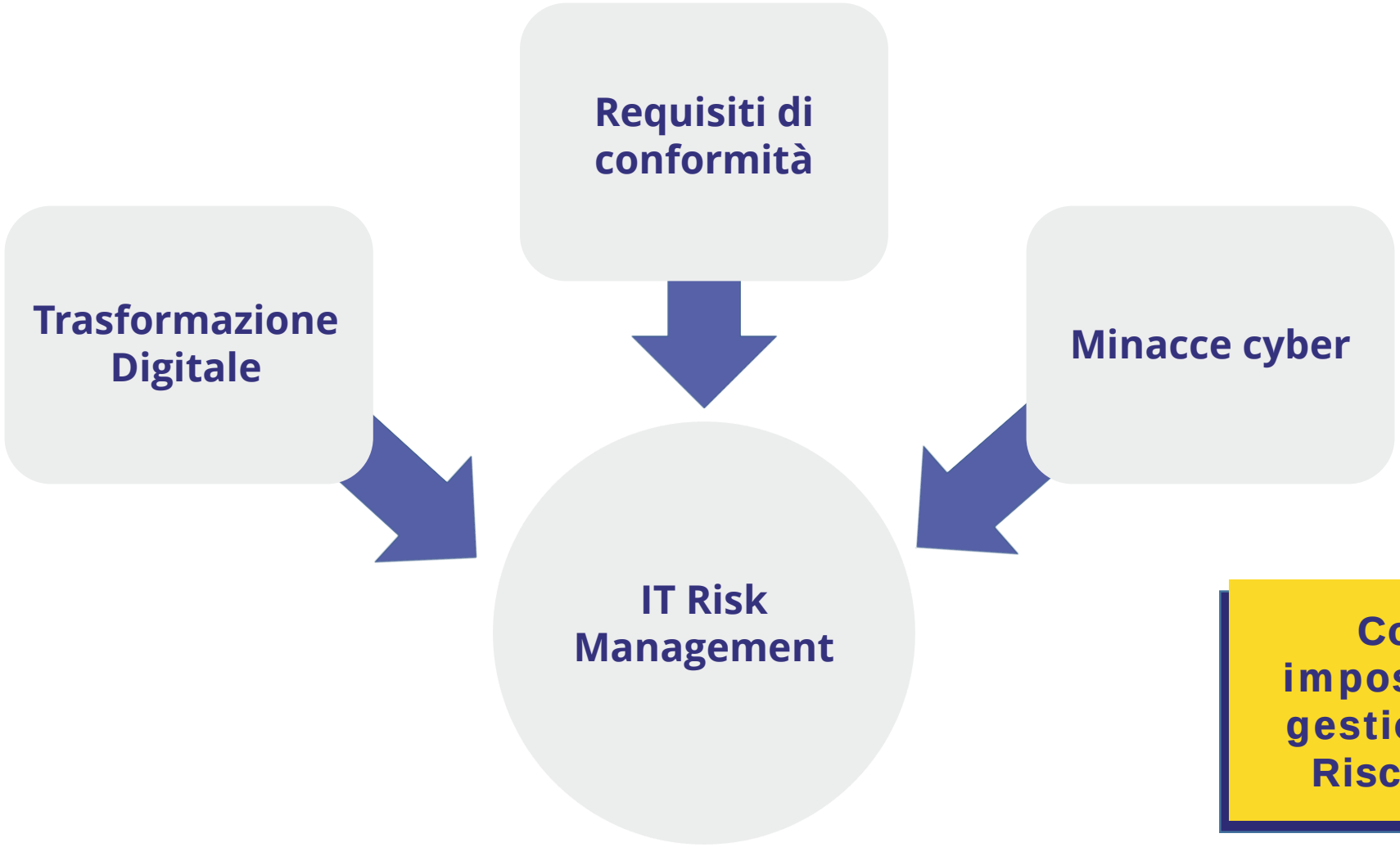
IT RISK MANAGEMENT



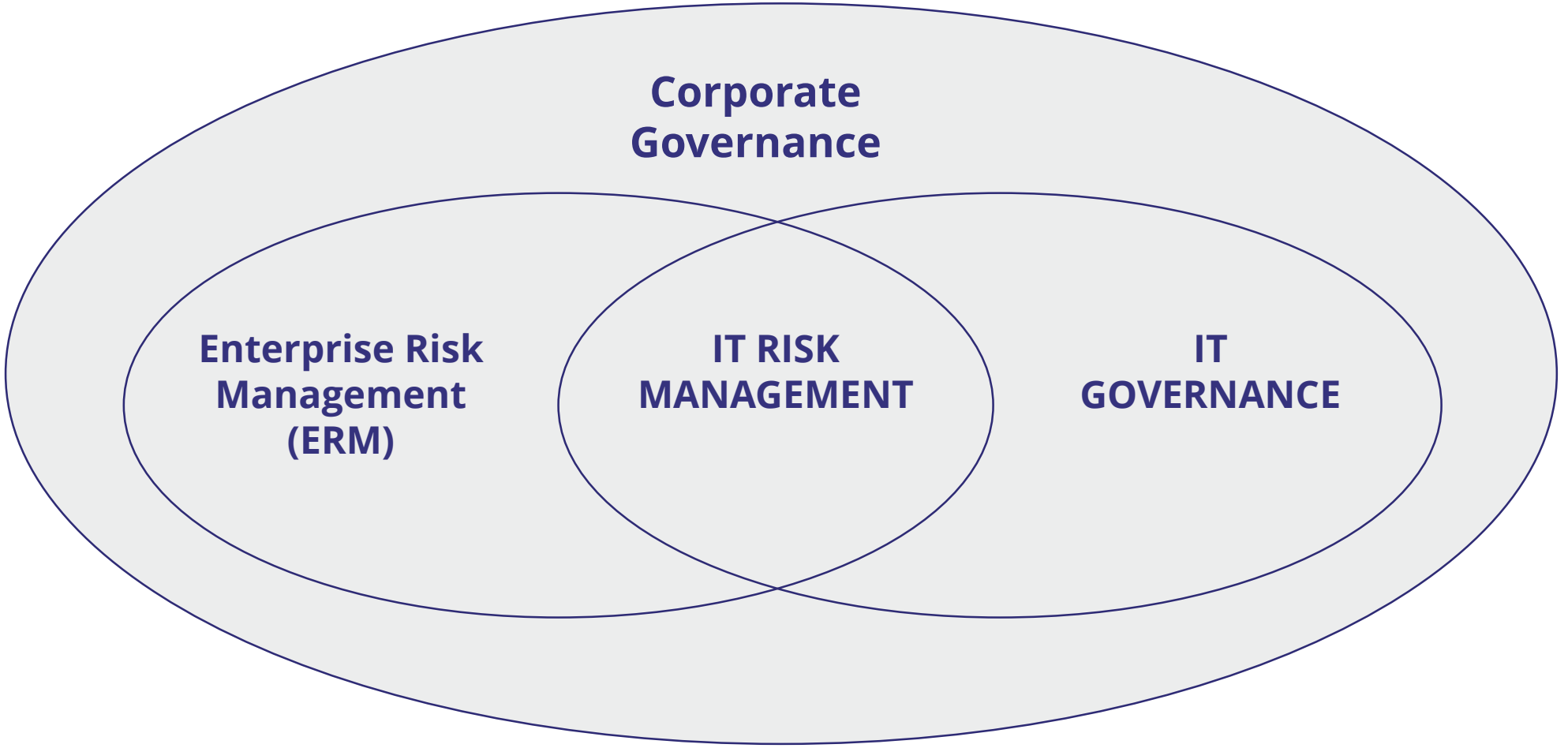
CREARE IL CONTESTO PER L'IT RISK MANAGEMENT

IT Risk Management. La rilevanza del tema.
3 Trend stanno portando attenzione sulla gestione del rischio IT



Come impostare la gestione dei Rischi IT?

Le aree da cui partire per impostare l'IT Risk Management in azienda



Enterprise Risk Management (ERM). Definizione.

L'Enterprise Risk Management (ERM), in linea con la definizione del Committee of Sponsoring Organizations of the Treadway Commission (COSO), ha l'obiettivo di portare coerenza nelle modalità con cui un'organizzazione gestisce il rischio:

*Enterprise risk management è un **processo**, governato dal **consiglio di amministrazione**, dal management e da altre figure dell'azienda, che ha l'obiettivo di **definire la strategia a tutti i livelli dell'azienda**, per identificare i **potenziali eventi** che possono avere un impatto sull'organizzazione, e gestire il rischio compatibilmente con il suo **livello di propensione** (al rischio), e fornire **ragionevoli garanzie** quanto al conseguimento degli obiettivi aziendali.*

Fonte: *Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework, 2004*

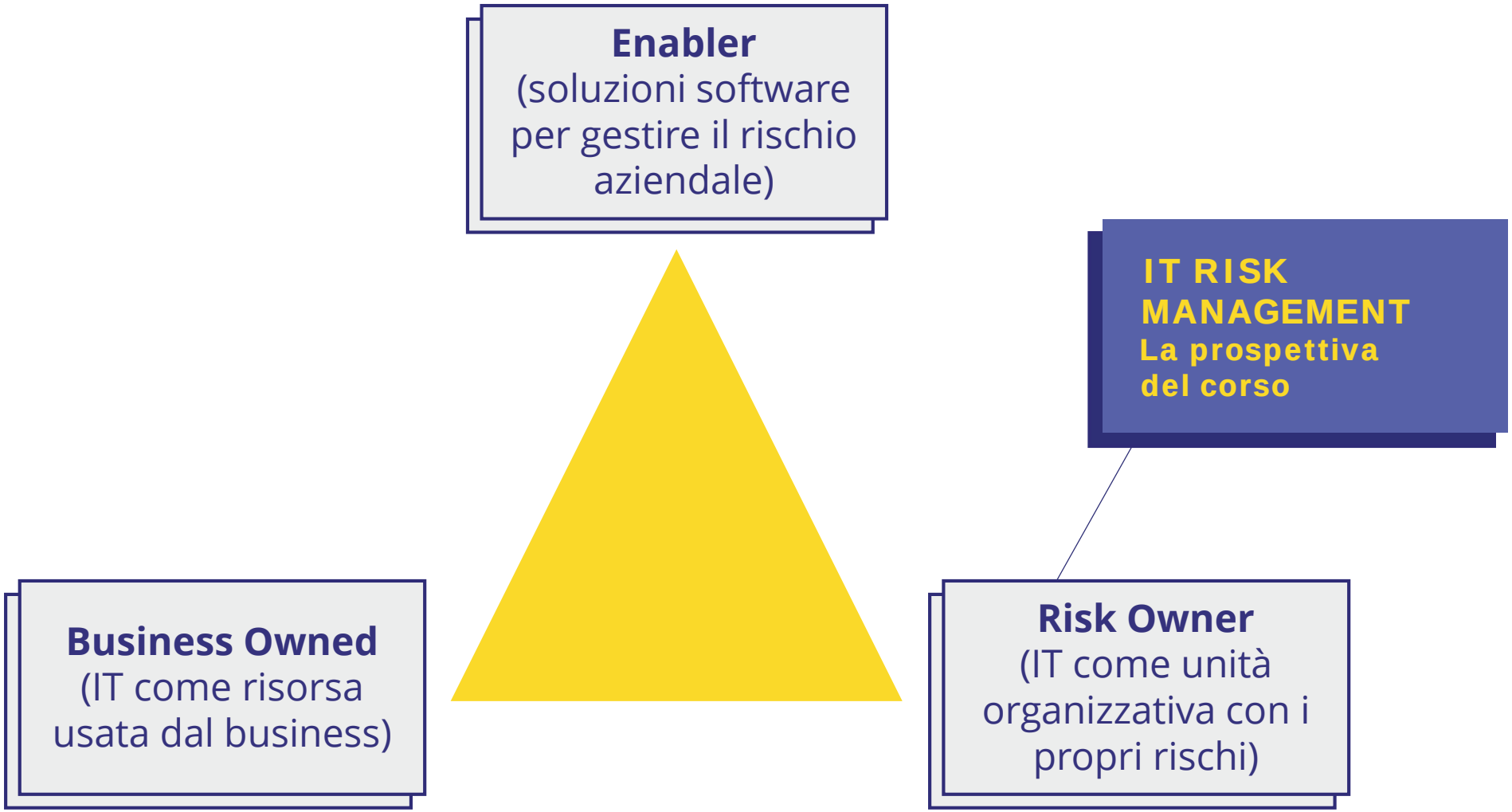
Enterprise Risk Management (ERM)

La definizione di ERM data dal COSO è intenzionalmente molto ampia.

In base alla definizione l'ERM è:

- un processo, continuo e trasversale
- che coinvoge tutte le persone di un'organizzazione
- applicato nella definizione delle strategie aziendali
- disegnato per identificare e gestire gli eventi che, al loro manifestarsi, avranno un impatto sull'azienda (positivo o negativo)
- in grado di fornire al management una ragionevole certezza di conseguire gli obiettivi aziendali
- in coerenza con il livello di propensione al rischio

Il ruolo dell'IT nell'ERM: un modello di riferimento



Cosa è la Governance dei Sistemi Informativi. Definizioni.

- IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of corporate governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives (Board Briefing on IT Governance, IT Governance Institute, 2001, www.itgi.org)

- IT governance is the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT (Van Grembergen et.al., 2003)

IT Governance e organi di Governance aziendale

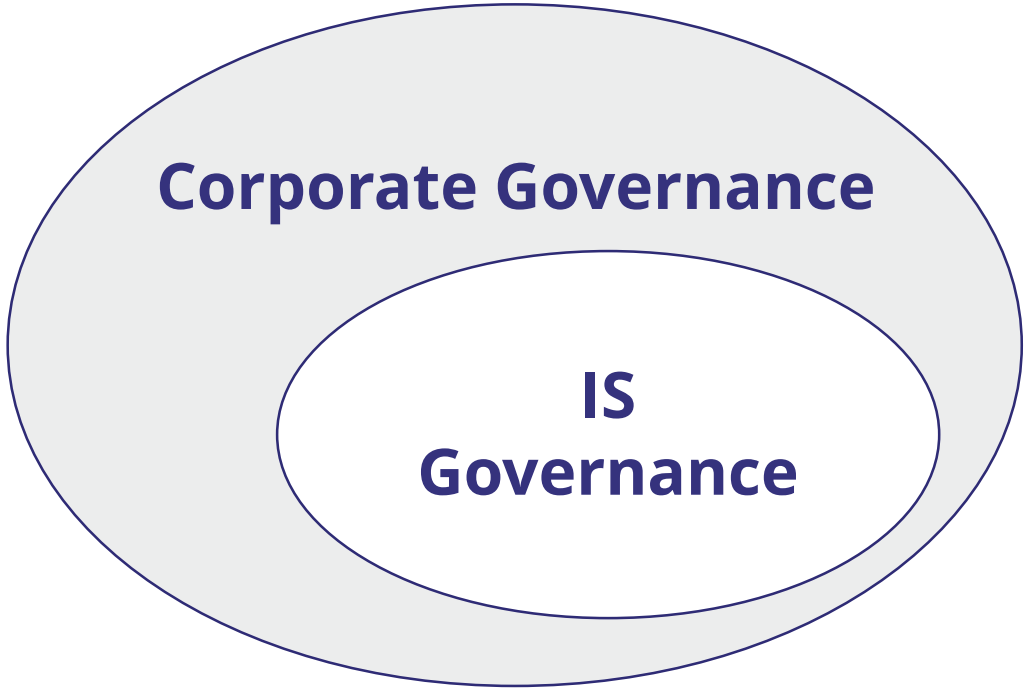
- Il filone della IT Governance, parallelamente agli adeguamenti normativi, hanno portato in evidenza l'importanza delle decisioni che riguardano l'assetto globale e i controlli relativi al Sistema Informativo.

- La presenza di rischi operativi, strategici e reputazionali collegati ai Sistemi Informativi richiedono una sempre maggiore attenzione da parte dei membri del Board.

- Sono sempre più frequenti e conosciuti i casi in cui la mancata identificazione dei rischi collegati ai sistemi informativi ha portato il Board ad essere esposto su temi che vengono trattati in sola logica emergenziale o con poca cognizione di causa.

Corporate Governance e IT Governance

Uno degli aspetti più importanti e determinanti in merito alla coerenza tra sistemi informativi e fabbisogni aziendali è la creazione di un legame forte ed esplicito fra Corporate Governance e IT Governance e fra IT Governance e IT Risk Management.



CORPORATE GOVERNANCE QUESTIONS		IT GOVERNANCE QUESTIONS
How do suppliers of finance get managers to return some of the profits to them?		How does top management get the CIO and IT organization to return some business value to it?
How do suppliersof finance make sure that managers do not steal the capital they supply or invest it in bad projects?		How does top management make sure that the CIO and IT organizations do not steal the capital it supplies or invest it in bad projects?
How do suppliers of finance control managers?		How does top management control the CIO and IT organization?

IT Governance e IT Risk Management

- L'IT Risk Management rappresenta uno dei processi fondamentali inclusi nella definizione di IT Governance: l'IT deve essere in grado di supportare ed estendere la strategia aziendale gestendo al contempo tutti i rischi che ne derivano.

- l'IT Governance deve rappresentare l'orientamento per l'azione dell'IT Risk Management:
  - collegando la gestione dell'IT e dei sistemi informativi agli organi apicali aziendali, in modo da settare i livelli di tolleranza al rischio allineati rispetto all'azione di governo (quando possiamo spingerci su certe scelte IT?);
  - definendo i meccanismi di delega e responsabilizzazione economica (chi decide cosa? In base a quali meccanismi?);
  - fungendo da raccordo rispetto agli orientamenti strategici aziendali, alla visione, agli obiettivi, alla strategia corporate e delle singole aree (dove dobbiamo concentrare prioritariamente l'attenzione?);
  - supportando l'individuazione dei perimetri di conformità aziendale che hanno un impatto diretto o indiretto sulla gestione dei sistemi informativi (a cosa dobbiamo stare attenti?).

INDIVIDUARE I DOMINI DEL RISCHIO IT

IT Risk Management. Definizione

Definiamo l'IT Risk Management come
*un **processo** finalizzato non solo a **individuare** e **trattare** (prevenire o mitigare) **gli eventi negativi** dovuti all'utilizzo dell'IT, ma anche a **concretizzare le opportunità** legate ai sistemi informativi per supportare al meglio l'azienda.*

Questa definizione richiama l'attenzione su alcuni elementi fondamentali:

- Primo, l'IT Risk Management è, come l'Enterprise Risk Management, un processo e non un'iniziativa spot o temporanea di natura progettuale. Si tratta invece di un insieme di attività continuative, che vedono i Sistemi Informativi da una prospettiva privilegiata.

- Secondo, l'IT Risk Management ha l'obiettivo di massimizzare l'utilità dell'impiego di tecnologie digitali per i Sistemi Informativi dell'azienda, da un lato riducendo la probabilità o minimizzando l'impatto di eventi negativi e dall'altro, massimizzando i benefici conseguenti alle opportunità offerte dall'ICT.

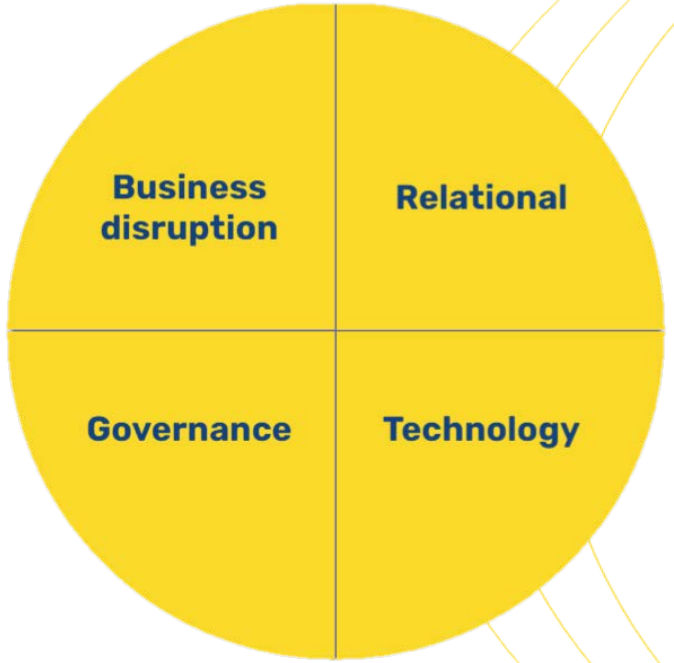
IT Risk Management. Definire il rischio IT.

L'oggetto del processo di IT Risk management è il rischio IT, definibile a sua volta come:
un rischio IT consiste nella possibilità di esposizione a perdite per l'organizzazione derivanti da un fallimento in ogni possibile aspetto del sistema informativo aziendale, e può rientrare in una delle seguenti classi di rischio: business disruption, relational, technology, governance.

Unendo le due definizioni possiamo subito notare come l'IT Risk Management sia un processo particolarmente complesso e articolato, che copre un ambito gestionale esteso a persone, tecnologie, risorse finanziarie, dati e informazioni, progetti, processi operativi, processi di gestione e di governance.

La tassonomia del rischio IT

- Una tassonomia preliminare dei possibili domini di rischio IT risulta fondamentale nell'impostazione del processo di risk management.
- In particolare, la classificazione proposta nella seconda definizione è tratta dalla tassonomia di Forrester Research.
- La tassonomia si basa sulla classificazione del rischio IT in 4 domini, come da definizione:
  - Rischi di business disruption;
  - Rischi di carattere relazionale (relational);
  - Rischi di carattere tecnologico (technology);
  - Rischi di governo (governance).
- Ognuno di questi domini è sua volta suddiviso in una serie di sotto-domini, che vanno in profondità rispetto alla specifica area.



IT Risk Domains. Business Disruption.

I rischi di business disruption hanno come effetto l'inoperatività (parziale o totale) del sistema informativo o la perdita (parziale o totale) di informazioni sensibili:

- Business Continuity, ossia l'incapacità dell'azienda di continuare a lavorare se informazioni o sistemi critici non sono disponibili (in toto o in parte). Un esempio è il rischio di non riuscire a lavorare dopo un disastro naturale che ha danneggiato i sistemi informativi.

- IT Security, ossia l'esposizione o la vulnerabilità dell'architettura informatica rispetto a minacce e attacchi provenienti dall'esterno o dall'interno ai confini aziendali. Ne sono esempi i rischi di hacking, i rischi di virus e malware, i rischi legati a comportamenti non sicuri da parte degli utenti (es. uso di drive esterni non controllati).

- Online, sono i rischi connessi alla presenza su canali Web e Internet da parte dell'azienda e possono essere legati a temi di hacking, privacy, reputazione, ecc.
- Information, sono i rischi legati all'inappropriato utilizzo di informazioni aziendali.

IT Risk Domains. Relational.

I rischi di relazione derivano dalle interazioni fra sistemi informativi e altre entità interne o esterne ai confini aziendali:

- Vendor Management, sono i rischi che derivano dalle relazioni con fornitori di software e hardware, con outsourcer e contractor, piuttosto che con società di consulenza,
- Third Party, sono i rischi che derivano dallo scambio o condivisione automatizzata di dati e informazioni con terze parti, come clienti e fornitori legati da flussi EDI o con ambienti applicativi distribuiti;
- Customer Satisfaction, sono i rischi che derivano dalla relazione con gli utenti aziendali, come per esempio il rischio di non raggiungere i livelli di servizio garantito (SLA).

IT Risk Domains. Technology.

I rischi tecnologici sono connessi alle scelte tecnologiche e architetturali dei sistemi informativi, così come alle capacità di gestione delle change e dei progetti:

- IT Agility, si ha un rischio di questo tipo quando i sistemi informativi non sono in grado di implementare e gestire le tecnologie di cui l'azienda ha bisogno per competere nel suo settore. L'obsolesenza di alcune applicazioni mission critical o la scelta di non adottare determinate soluzioni possono rallentare l'operatività aziendale rispetto ai concorrenti.
- IT Architecture, sono i rischi legati al disegno architetturale dei sistemi informativi, che può mancare del tutto o essere parziale, inefficace o senza standard aziendali di riferimento.
- Change Execution, il dominio include i rischi legati alla cattiva o non corretta gestione dei processi di change sugli ambienti tecnologici. Ne è un esempio la mancata comunicazione agli utenti di un'applicazione relativamente al lavoro di change sulla stessa.
- Project Development, sono i rischi connessi alla cattiva o non corretta gestione dei progetti di sistemi informativi.

IT Risk Domains. Governance.

I rischi di governo sono connessi alle scelte di governo dei sistemi informativi, per esempio in merito alla strategia o all'organizzazione IT, o ancora alla gestione delle risorse umane che lavorano in questo ambito:

- IT Strategy, i rischi legati alla strategia IT si sostanziano nell'assenza, completa o parziale, di allineamento fra requisiti aziendali e sistemi informativi, con una strategia IT che non soddisfa o eccede le richieste del business.

- IT Resources, questo dominio riunisce i rischi legati al cattivo utilizzo delle risorse umane e finanziarie a disposizione dei sistemi informativi.

- Compliance/legal, sono i rischi di non conformità dei sistemi informativi rispetto a requisiti di compliance di varia natura, così come i rischi derivanti dal non rispetto di condizioni o vincoli contrattuali che regolano il comportamento dei sistemi informativi vs l'esterno o terze parti.

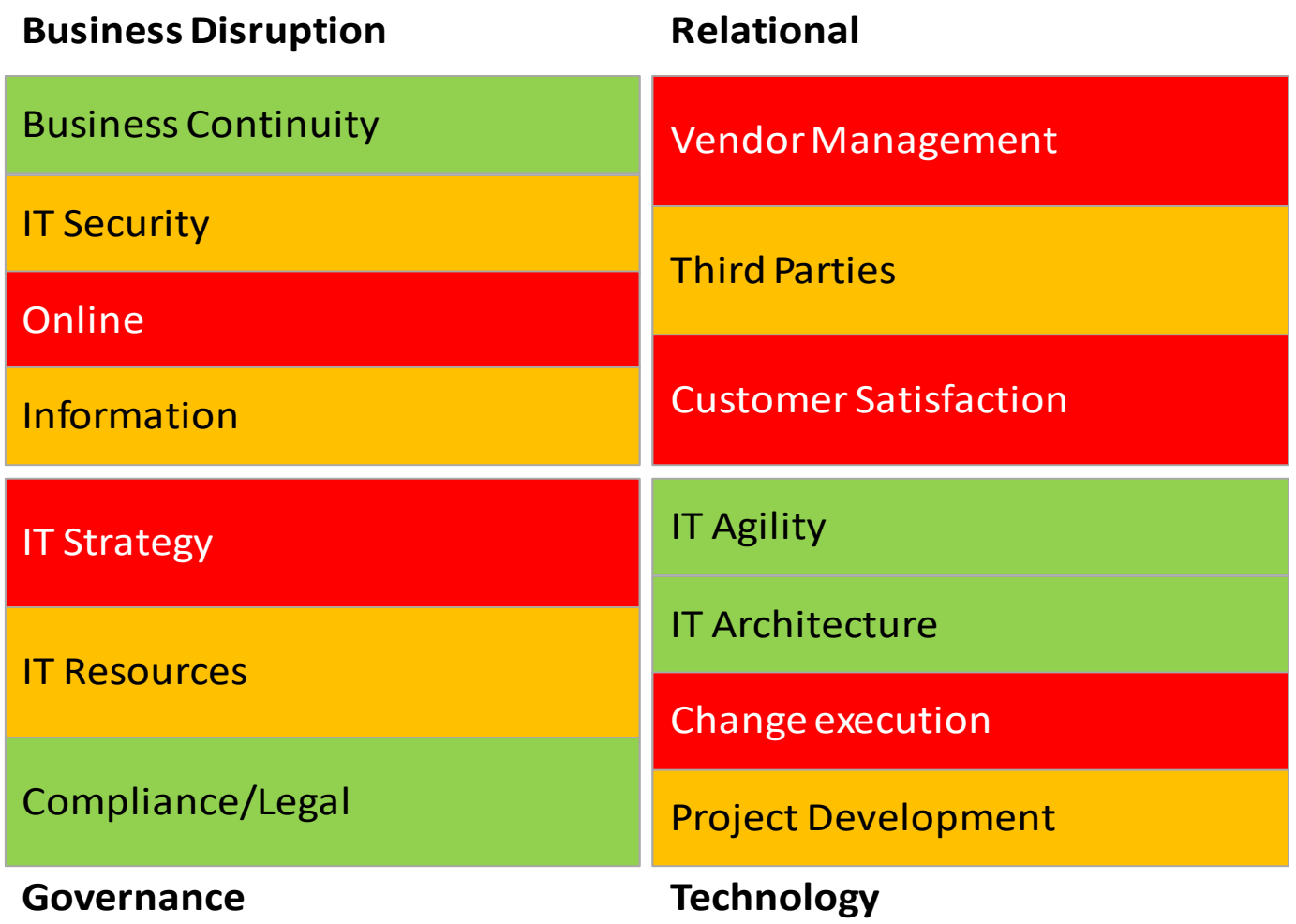
Vantaggi e attenzioni nell'utilizzo di una tassonomia del rischio IT

La tassonomia del rischio IT è infatti particolarmente utile e vi consentirà di:

- conoscere l'ampiezza complessiva del fenomeno, indirizzando tutti i possibili domini da considerare senza dimenticare elementi importanti, così da guidare la fase di identificazione;
- svolgere sotto-classificazioni per ogni dominio, in modo da segmentare il rischio in modo più granulare;
- fornire una logica di rappresentazione del rischio in ampiezza e in profondità, utilizzando domini e sottodomini come aree di possibile presidio su cui costruire sistemi di reportistica;
- costruire uno strumento di comunicazione facilmente comprensibile al di fuori dei confini della funzione Sistemi Informativi, soprattutto verso strutture di controllo, organismi di governo e entità manageriali apicali.

Ovviamente, come tutte le tassonomie, anche quella qui proposta per la gestione del Rischio IT non va presa in modo acritico.
Alcuni domini e sotto-domini sono infatti delle macro-aggregazioni che andrebbero ulteriormente dettagliati per adattarli al contesto specifico di applicazione.

Un possibile utilizzo della tassonomia per reporting sullo stato del Rischio IT (logica *dashboard*)



COMPRENDERE LA NATURA DEL RISCHIO IT

Soluzione dei casi «i Grandi disastri IT»
Il caso «Chi sbaglia in fretta piange adagio»

Il caso ci porta sul sottodominio Technology-Project Development: la scelta di comprimere un progetto troppo complesso in tempi non compatibili è il tipo errore di scoping del project management. Ovviamente si trova sempre un fornitore che promette di farcela, ma il vendor management qui è più una conseguenza che una causa. Anche in questo caso la strategia non è il problema: vien fatto quello che deve essere fatto, sbagliando però completamente lo scoping e il piano di progetto.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Quando la punteggiatura fa la differenza»

Il caso lascia pochi dubbi: nessuno ha testato il sistema prima di rilasciare le modifiche in produzione, peraltro su un applicativo utilizzato direttamente dai clienti finali.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Dov'è finito il paziente?»

Il caso può generare un dubbio fra Relational-Vendor Management e Technology-Architecture. Assumendo che il progetto complessivo sia stato messo a gara, visto l'ambito pubblico, probabilmente in questa gara pubblica si è optato per la frammentazione del progetto su "n" lotti e "n" fornitori per evitare problemi di tipo relazionale. L'architettura dei servizi a monte poteva anche essere solida, il problema è nato dalla frammentazione dell'opera complessiva su troppi interlocutori. Da li sono venuti anche i problemi progettuali citati nel caso.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Quando l'utente resta al buio»

Il problema cruciale in questo caso riguarda il difetto di comunicazione fra l'IT – che si accorge di un mal funzionamento di una componente del sistema di alert – e gli utenti, che non sono contattati a valle del ripristino per sapere se tutto funzionava regolarmente. Il processo di esecuzione di un intervento sui sistemi è mal gestito, siamo nel dominio Technology-Change execution, dove per change ricordiamo che nella tassonomia parliamo indistintamente di qualsiasi intervento (e non di interventi a seguito di change request).

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Al fuoco!»

Se analizziamo quello che è successo risulta evidente come ci si trovi in un perimetro al di fuori dei Rischi IT. Probabilmente Vendor-Management sarebbe una collocazione corretta, ma nella matrice dei rischi del responsabile della produzione dell'azienda di PC, non in quella del CIO.

NON IT

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Problemi con un boccone troppo grosso»

Nel caso McDonald's il problema che si genera risale a una strategia IT sovra-dimensionata rispetto a quella aziendale: l'IT lancia l'implementazione di un sistema ERP centralizzato su una serie di processi e funzioni che non richiedono centralizzazione. Siamo nel dominio Governance-Strategy. Non cadiamo nella trappola Technology-Project Development: qui il progetto non è mai partito. È rimasto solo su costosissimi fogli di carta.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Uno scandalo pubblico»

Il caso della Child Support Agency è un tipico caso di cambiamento dei requisiti durante l'implementazione di un sistema. Siamo nel dominio Technology-Project Development: una fattispecie di rischio di progetto molto comune è non considerare nello scoping iniziale eventuali eventi o fabbisogni che potrebbero cambiare in corso di implementazione. Potreste avere avuto un dubbio relativo a Governance-Compliance, ma qui la compliance a cui si fa riferimento è aziendale non specifica dei sistemi informativi.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Nubi all'orizzonte»

In questo caso i requisiti normativi che cambiano non hanno un impatto sulle funzionalità del sistema informativo, ma solo sul fatto che si presenteranno più persone allo sportello per chidere il passaporto. Questo, unito al rilascio di un nuovo software che non è stato adeguatamente insegnato ai dipendenti pubblici coinvolti, ha generato le file interminabili di cui si parla nel caso. Dove sta il rischio non gestito: mai rilasciare un software senza opportuno training agli utenti. Siamo nel dominio Relational-Customer Satisfaction. Customer inteso come utente interno dei Sistemi Informativi, anche se poi l'impatto si è esteso ai cittadini.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «Due metà imperfette»

Il caso delle due metà imperfette (Airbus) è il caso da manuale di non compatibilità fra due componenti software: qui sì, siamo nel dominio Technology-Architecture.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

Soluzione dei casi «i Grandi disastri IT»
Il caso «L'FBI infrange la legge dell'IT»

Gli elementi forniti sono piuttosto esplicative e non è difficile ricondurre ciò che è accaduto alla decisione di implementare una soluzione "custom" per un processo su cui si stavano affermando sul mercato delle soluzioni di tipo "buy".
Siamo nel dominio Technology e nel sotto-dominio Agility: l'IT di FBI ha optato per una tecnologia che sarebbe risultata obsoleta al termine (se mai ci fosse stato) dell'implementazione.

BUSINESS DISRUPTION	RELATIONAL	TECHNOLOGY	GOVERNANCE
Business Continuity	Vendor Management	Agility	Strategy
Security	Third-Party	Architecture	Resources
Online	Customer Satisfaction	Change execution	Compliance Legal
Information		Project Development	

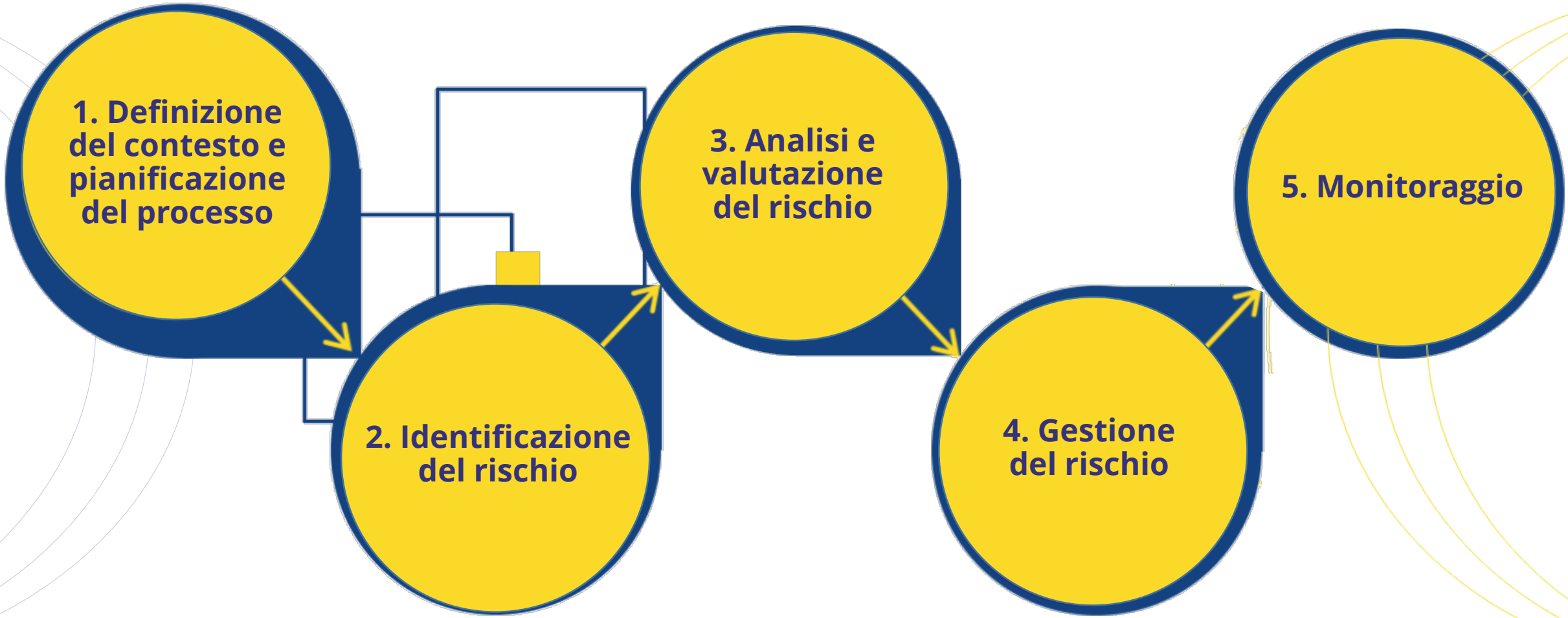
I grandi disastri e la tassonomia del rischio IT

La simulazione e l’applicazione della tassonomia ai casi che abbiamo affrontato ti hanno permesso di:

- applicare a casi concreti la tassonomia di classificazione del rischio IT;
- comprendere la rilevanza dell'identificazione "ex-ante" del rischio IT;
- distinguere in modo chiaro le cause dalle conseguenze legate a situazioni critiche in ambito IT.

IL PROCESSO DI IT RISK MANAGEMENT

Il processo di gestione del Rischio IT



1. Definizione del contesto e pianificazione del processo

- In questa fase del processo di gestione dei rischi dei sistemi informativi vengono idealmente creati i collegamenti con il più ampio contesto dell'Enterprise Risk Management.
- Grazie all'ERM l'azienda dovrebbe aver definito il grado di tolleranza del rischio e dovrebbe aver predisposto le metodologie e gli strumenti per l'applicazione dei principi di gestione del rischio a tutte le aree e livelli aziendali.
- In questa fase è fondamentale trovare un raccordo rispetto a quanto stabilito su questi aspetti dall'ERM.
- È inoltre la fase in cui si attribuiscono le responsabilità delle attività di IT Risk Management e si acquisiscono le risorse necessarie alle fasi successive del processo.

2. Identificazione del rischio - 1

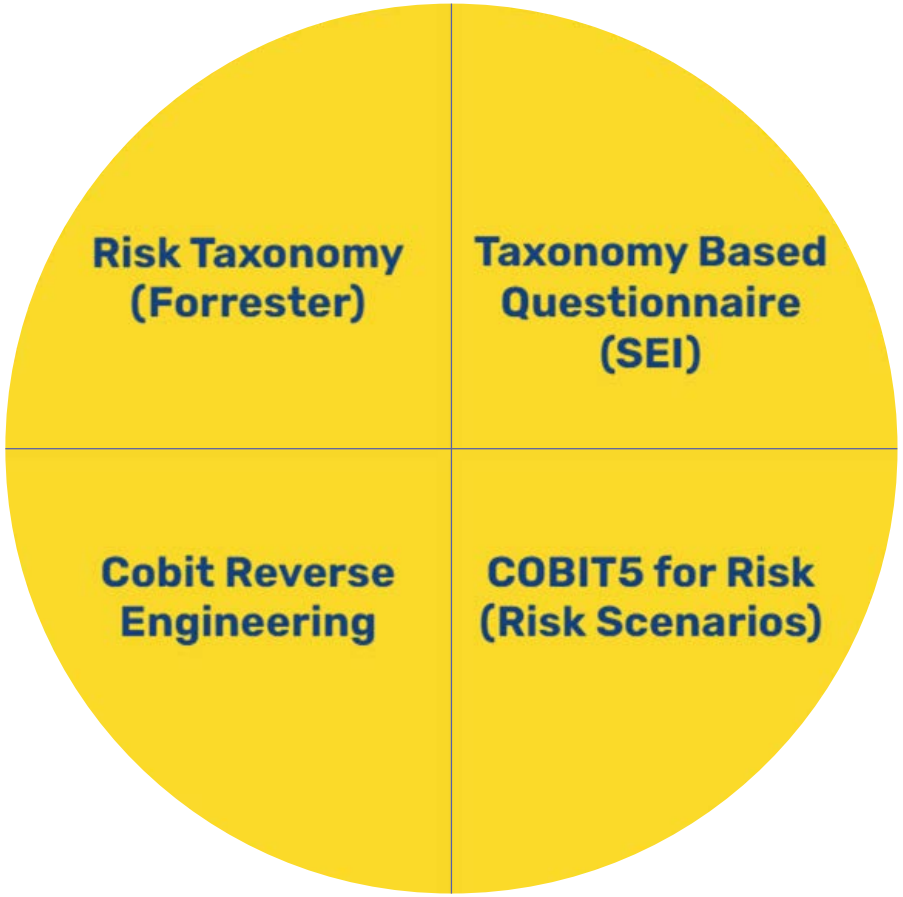
È considerata la fase più critica nel processo di IT Risk Management perché l'individuazione del rischio è la precondizione per poterlo gestire.

- L'identificazione del rischio richiede:
  - l'individuazione degli eventi che hanno potenzialmente un impatto negativo sui processi e sugli obiettivi aziendali.
  - La documentazione delle loro caratteristiche.
  - Il coinvolgimento di diversi attori aziendali portatori di diversi punti di vista (persone IT e persone del business).

- L'identificazione del rischio deve tenere in considerazione fattori interni ed esterni.

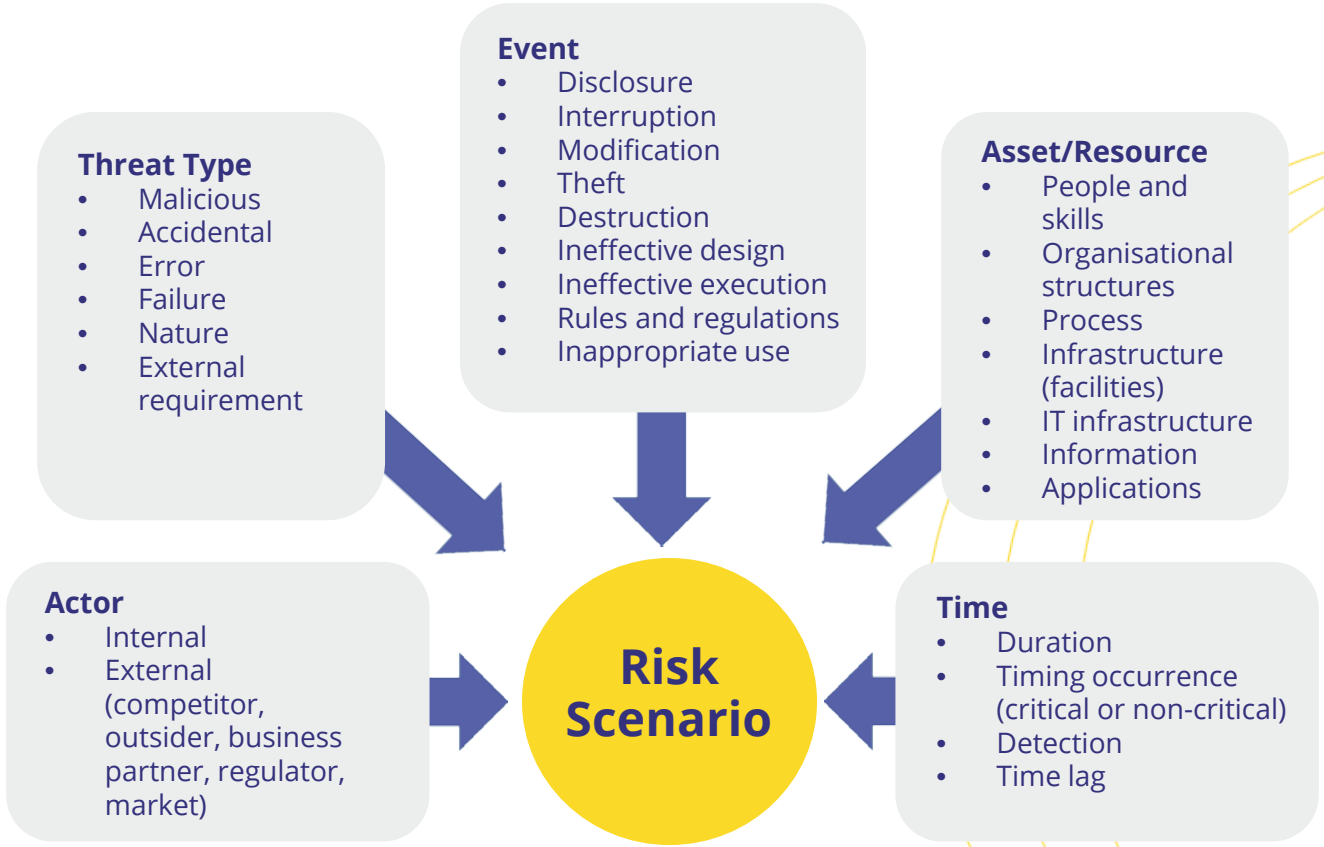
2. Identificazione del rischio – 2 Il toolkit proposto dal corso

Nel mondo dei Sistemi Informativi e dell'IT abbiamo a disposizione diverse raccolte di buone prassi e framework strutturati che ci aiutano nell'identificazione del rischio.



2. Identificazione del rischio. Risk Scenarios

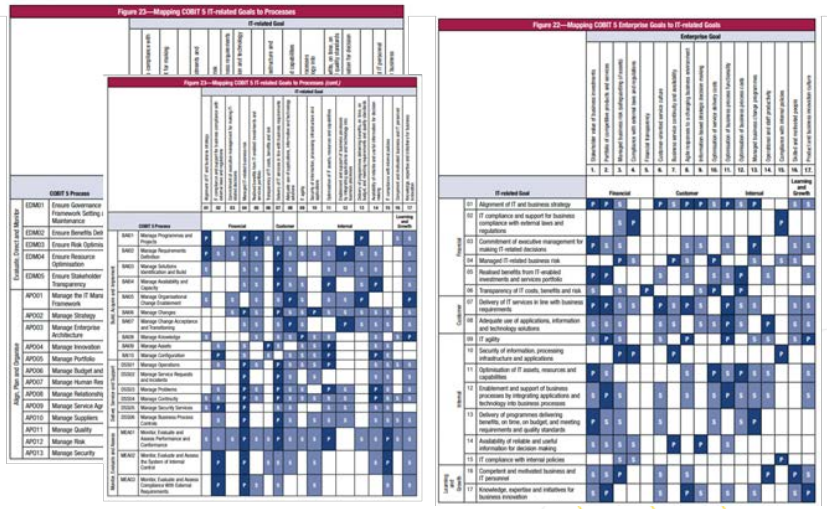
- Gli scenari di rischio possono essere creati a partire da una serie di "componenti" dati che includono tutti i possibili asset/risorse su cui è possibile svolgere un'attività di identificazione del rischio (persone e organizzazione, processi, infrastrutture, applicazioni, informazioni, ecc).
- In teoria gli scenari derivano da tutte le possibili combinazioni dei valori delle variabili di scenario (attore, evento, risorse…), ma nella realtà devono essere ricondotti ad un numero gestibile;
- Si potrebbe partire da scenari generici per poi definire scenari di dettaglio in funzione delle esigenze contingenti;



- Partire da scenari generici garantisce una certa flessibilità in un ambito, quello del risk management, estremamente variabile nel tempo;
- Lo sviluppo di scenari significativi richiede il coinvolgimento di diversi punti di vista (Senior management, Business management, IT Management e Risk management).

2. Identificazione del rischio. Cobit Reverse Engineering

- Una modalità particolarmente utile per elaborare una mappa complessiva dei rischi IT legati agli obiettivi di business è rappresentata dall'utilizzo delle matrici finali presenti nel Cobit19 (Appendice A).
- Queste matrici mettono in relazione gli obiettivi aziendali (EG) con gli obiettivi (AG) e i processi IT (Governance and Management Objectives) necessari per conseguirli.
- A partire dai processi IT è poi possibile utilizzare le prassi di controllo messe a disposizione dal framework per individuare i rischi di processo che possono inficiare il raggiungimento di uno o più obiettivi IT e, per tal via, di uno o più obiettivi aziendali.
- Questa modalità ha il grande pregio di essere pronta per l'utilizzo, salvo adattamenti allo specifico fabbisogno e contesto aziendale.



- L'utilizzo di Cobit e dei suoi obiettivi di controllo consente di coprire in una logica di ampiezza i principali processi dei sistemi informativi.
- Tuttavia, la strumentazione alla base del framework è molto focalizzata sulla dimensione di processo e poco si presta per l'individuazione di rischi connessi ad altri ambiti o oggetti da controllare, come i progetti, gli asset tecnologici, ecc.

3. Analisi e valutazione del rischio

La fase di valutazione ha l'obiettivo di posizionare i rischi individuati nel passaggio precedente in termini di probabilità e impatto. Questo tipo di attività può essere supportata sia da strumenti e metodologie di natura quantitativa, sia da logiche di tipo qualitativo.
In genere la gestione dei rischi IT si affida a valutazioni di carattere qualitativo, ossia si cerca di posizionare ogni rischio in termini di probabilità e di impatto utilizzando una scala del tipo: "Alto", "Medio", "Basso".

METODI QUALITATIVI

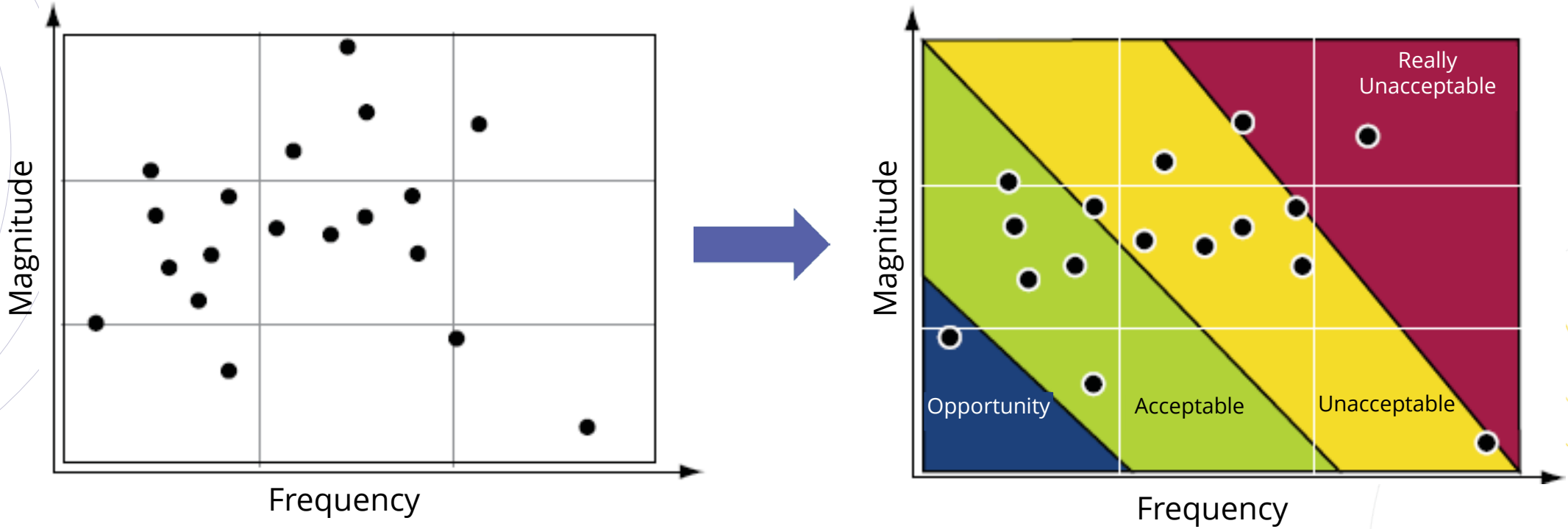
- Valutazioni di impatto e probabilità espresse con etichette qualitative (A/M/B).
- Utilizzato laddove le informazioni disponibili sono limitate o di bassa qualità.
- Alto livello di soggettività nelle valutazioni.
- Più semplice.
- Meno costoso.

METODI QUANTITATIVI

- Valutazioni di impatto e probabilità basate su metodi di calcolo statistici.
- Necessita di dati completi e affidabili relativi agli eventi passati che non sono facilmente disponibili.
- Necessita di competenze statistiche per il calcolo.
- Valutazioni più oggettive perché basate su dati empirici.
- Alcuni impatti sono difficilmente quantificabili (che valore ha la perdita di reputazione?).

3. Analisi e valutazione del rischio. La mappa dei rischi IT

Per ottenere una visualizzazione sintetica dei rischi IT, viene generalmente utilizzata una mappa che rappresenta ogni rischio nelle sue dimensioni di probabilità/frequenza di accadimento e impatto.
La valutazione del rischio IT associata alla tolleranza dell'azienda al rischio consente di fornire una prima evidenza dei rischi prioritari da gestire.



4. Gestione del rischio

Risk Avoidance (Evitare)	Risk Reduction/ Mitigation (Mitigare)	Risk Sharing/Transfer (Trasferire)	Risk Acceptance (Accettare)	Risk Monitoring (Osservare)	Risk Investigation (Indagare)
Richiede la dismissione delle attività fonte di rischio. **Esempio**: trasferire un data centre in una regione estranea a disastri naturali oppure decidere di non imbarcarsi in un progetto di grandi dimensioni se il business case evidenzia un elevato rischio di fallimento.	Richiede azioni finalizzate a ridurre la probabilità e/o la frequenza di un rischio. Azioni di controllo COBIT (policy, procedure, ecc)	Comporta la riduzione della frequenza e/o dell'impatto del rischio trasferendo o condividendo una porzione del rischio con terze parti. Le tecniche più comuni sono l'assicurazione e l'outsourcing. **Esempio**: Copertura assicurativa del data center in caso di incendio del building, outsourcing di attività IT, o condivisione del rischio di progetto con il fornitore definendo dei contratti fixed price.	Comporta la totale accettazione del rischio e delle perdite da esso derivanti.	Il rischio viene semplicemente osservato per valutarne l'evoluzione. E' tipicamente la strategia di default su rischi poco importanti. Si può anche applicare quando, prima di prendere altre decisioni, si vuole capire se la situazione rischiosa sta degenerando o migliorando.	Rispetto al caso precedente si adotta un approccio più attivo, orientato a meglio comprendere le caratteristiche del rischio (cause, probabilità, impatto, etc.).

5. Monitoraggio del rischio.

- L'IT Risk Management è un processo continuo e iterativo. Come si è visto nel paragrafo precedente, le azioni di gestione e i controlli implementati per dar loro seguito non annullano completamente la probabilità e l'impatto dei rischi IT. Il livello di rischio che permane dopo aver implementato una serie di azioni e controlli si definisce "rischio residuo" e va monitorato in modo costante per verificare l'efficacia delle azioni poste in essere e del sistema di controllo.

- Inoltre, parallelamente all'evoluzione del contesto aziendale di riferimento, possono sorgere nuovi rischi legati al governo e alla gestione dei sistemi informativi, a nuovi asset acquisiti, a nuovi progetti avviati, ecc.

- Le azioni di monitoraggio sono condotte sia da chi ha la responsabilità quotidiana di gestire i rischi IT, sia da funzioni indipendenti o esterne di IS Audit, in modo da garantire l'oggettività di giudizio e supportare il miglioramento continuo delle attività di gestione del rischio dei sistemi informativi.

Vincenzo Calabro'

Information Security Officer & Digital Forensics Analyst | Researcher | Trainer

WWW.VINCENZOCALABRO.IT