LUISS

Tesi di laurea triennale

Dipartimento di Impresa e Management

Corso di laurea in Economia e Management

Cattedra: Matematica Finanziaria

Titolo:

"L'evoluzione del rischio operativo nei sistemi bancari, con focus sui rischi cyber"

Relatore:
Prof. Paola Fersini

Candidato:
Lavinia Conte
Matr. 261891

Anno Accademico 2022-2023

Indice:

Introduzione

Il sistema bancario è rappresentato dall'insieme delle istituzioni che si dedicano all'attività di intermediazione finanziaria, ovvero al collegamento all'interno del mercato di operatori che dispongono di liquidità in surplus ed operatori in deficit. La banca è l'istituto di credito per eccellenza ed ha come funzione principale quella di controllare e amministrare il denaro attraverso dei servizi offerti agli operatori.

Nello svolgimento di tali attività è probabile che le banche possano incorrere in rischi che vengono definiti "rischi bancari". Questi sono innumerevoli e dipendono da diversi fattori, sia interni che esterni. Una prima macro-classificazione dei rischi bancari ha identificato tre tipologie di rischio:

- il rischio economico che fa riferimento all'equilibrio tra costi e ricavi relativi alla gestione delle attività:
- il rischio finanziario, relativo alle entrate e uscite monetarie;
- il rischio patrimoniale, relativo alla solvibilità dell'ente.

Alla fine degli anni Novanta, date le numerose turbolenze sui mercati finanziari, le istituzioni hanno stimolato una crescente attenzione verso l'individuazione, la misurazione e la gestione dei rischi bancari e, in particolare, di nuove tipologie di rischio (vedi i rischi operativi) che erano man mano diventati sempre più rilevanti. Tra le principali motivazioni che hanno portato al riconoscimento della rilevanza di tali rischi si possono evidenziare:

- la crescita dimensionale delle banche e la sempre maggiore complessità organizzativa dovuta anche allo sviluppo di nuovi business;
- le numerose operazioni di fusione e acquisizione tra le banche che incrementa la probabilità di incorrere in rischi operativi vista la complessità nell'integrare due diversi sistemi informativi e operativi e quindi una più alta probabilità di incorrere in errori e disfunzioni;
- il sempre più crescente ricorso alla esternalizzazione di processi produttivi che introduce ulteriori rischi (es. rischi legali connessi all'incertezza sulla divisione delle responsabilità tra banca e outsourcer);
- l'evoluzione della tecnologia che ha spinto le banche ad innovare le loro modalità di svolgimento di determinate attività, iniziando a fare sempre più affidamento su sistemi di *information technology*. Se da una parte l'utilizzo della tecnologia consente alle banche di ottimizzare i processi operativi e di offrire servizi sempre più innovativi (vedi ad esempio i pagamenti on line e il mobile payment), dall'altra espone le banche a dei rischi nuovi non sempre conosciuti e completamente compresi (vedi i rischi Cyber)

L'obiettivo della tesi è quella offrire una panoramica dei rischi operativi nelle banche con un focus specifico sui Rischi Cyber vista la estrema rilevanza da questi assunta negli ultimi anni.

La tesi è pertanto strutturata in quattro capitoli:

- il primo capitolo "Introduzione" dove vengono illustrati obiettivi e struttura della tesi;
- il secondo capitolo "Il Rischio Operativo" dove viene fornita una panoramica sugli elementi caratterizzanti i rischi operativi nelle banche, le principali normative di riferimento, i principali metodi

di identificazione e valutazione di tali rischi, nonché le principali caratteristiche del processo di gestione;

- il terzo capitolo dedicato ai "Rischi Cyber" dove vengono illustrate le principali caratteristiche di questi rischi, le principali normative applicabili, sia italiane che europee, i principali metodi di identificazione e valutazione, nonché le principali caratteristiche del processo di gestione.
- Il quarto capitolo "Case Study: integrazione di rischi cyber nei rischi operativi delle banche" è dedicato alle metodologie ad oggi utilizzate per l'integrazione di tali rischi nei rischi operativi delle banche e le possibili evoluzioni future in ambito.

1 Il Rischio Operativo

I rischi operativi sono una categoria piuttosto ampia che racchiude al suo interno una moltitudine di eventi molto diversi tra loro e solo alcuni dei quali già noti nell'ambito bancario.
Tutto ciò ha comportato un aumento significativo degli scenari di rischio nei quali una banca potrebbe incorrere, molti dei quali dovuti a fattori esogeni non sempre noti e/o completamente compresi (a titolo esemplificativo, lo sviluppo dell'e-banking ed e-commerce ha aumentato in maniera esponenziale eventi di rischio connessi alle le frodi esterne e alla criminalità informatica).
Tutt'ora misurare e capire il rischio operativo rimane complicato e ciò vale sia per le autorità che per le banche. Questo è uno dei motivi tra i tanti che hanno reso tali rischi molto rilevanti da renderli secondi solo ai rischi di credito e comprendere una grande parte dei *risk-weight assets* delle banche.

1.1 Definizione di rischio operativo ed elementi caratterizzanti

Inizialmente il Comitato di Basilea aveva dato una definizione "negativa" del rischio operativo, ovvero esso corrispondeva a tutto ciò che non rientrava negli altri tipi di rischio e dunque non rientrava nelle categorie già note. Successivamente poi nel 2001, attraverso un "working paper", venne elaborata una nozione di rischio operativo in "positivo", definendolo come "*il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni*". Con il "Nuovo Accordo sulla Convergenza Internazionale della Misurazione del Capitale e dei coefficienti Patrimoniali" esso è diventato ufficialmente parte della gamma di rischi che le banche devono tenere obbligatoriamente conto e al quale corrisponde un coefficiente patrimoniale minimo specifico in base alla tipologia di rischio.

Una delle peculiarità del rischio operativo è connessa alla probabilità che vi siano delle oscillazioni di valore dovute a fattori non prevedibili i quali si manifestano durante la normale operatività della banca. Per analizzare in profondità questo rischio ci si deve chiedere innanzitutto da chi dipenda.

Come si evince anche dalla definizione, i fattori che determinano questo tipo di rischio (cd *risk driver*) sono principalmente persone, sistemi interni, processi e un contesto esterno.
Andando nel dettaglio:

- il fattore umano può generare una perdita operativa a cause di incompetenza, negligenza o mancanza di un'adeguata istruzione del personale. Il management delle risorse umane e il comportamento degli impiegati può diventare una delle maggiori fonti di rischio: avere un personale poco istruito oppure sovraccaricare di lavoro gli impiegati può esporre la banca ad eventi quali frodi, attività criminali, violazione di leggi, normative, regolamenti interni, etica. Anche la mancanza di una distinzione dei ruoli e delle responsabilità può generare un rischio operativo e anche un rischio legale.
- Nella definizione si parla si sistemi interni i quali possono racchiudere al loro interno una molteplicità di fattori, ma, considerata la vigente normativa degli ultimi anni, si evince che ci si riferisca soprattutto a sistemi di "*information and communication technology*" (I&CT). Essi si concretizzano in problemi di natura tecnica, interna alla banca; alcuni esempi sono il blocco/malfunzionamento/mancata disponibilità di hardware, software, information providers e telecomunicazioni, errori di programmazione, interruzioni della struttura di rete, caduta dei sistemi di telecomunicazioni, etc.
- Per quanto riguarda l'area di rischio connessa ai processi, ci si riferisce in particolare ad una erronea o mancata formalizzazione di procedure interne della banca, tra i quali rientrano controlli interni, attribuzione dei ruoli e responsabilità.
- Il contesto esterno fa riferimento a eventi esogeni, ovvero situazioni quali eventi naturali che potrebbero mettere in pericolo la sede fisica della banca (terremoti, alluvioni, incendi), ma anche pericoli connessi a soggetti esterni (furti, attacchi terroristici, vandalismo)

Da quanto scritto si evince come tale rischio abbia un impatto trasversale su ogni componente di business e non si presenta quindi come gli altri tipi di rischio.
Determinati i *risk driver*, si devono identificare gli eventuali scenari che questi possono produrre, ovvero i cosiddetti "*loss even type*", i quali rappresentano le tipologie di eventi pregiudizievoli che possono occorrere.
A seconda dei fattori di rischio (*risk driver*), si distinguono vari tipi di *loss even type.*
A titolo esemplificativo e non esaustivo, possibili *loss even type* possono essere:

- frodi interne/esterne: si hanno perdite dovute ad attività non autorizzate, appropriazione indebita, violazione delle leggi, regolamenti o direttive aziendali.
- contratto di lavoro e sicurezza sul posto di lavoro: perdite dovute da atti non conformi alla legge, risarcimento danni per lesioni personali, assenza di condizioni per la parità tra il personale, etc.
- clienti, prodotti, pratiche di business: perdite che derivano da una non adeguata professionalità del personale o del servizio prestato.

- danni a beni materiali: perdite dovute a danni ma anche perdita fisica dei beni facenti parte l'attività finanziaria.
- avarie e guasti ai sistemi: perdite generate dall'interruzione dell'operatività o dalla temporanea disfunzione dei sistemi.
- esecuzione, consegna e gestione del processo: perdite causate da un'erronea gestione dei processi e dal perfezionamento delle operazioni.

Dai *loss even type* si determinano l'impatto che questi provocano, ovvero i *loss effect type*. Alcuni esempi sono: responsabilità legale, l'azione da parte di un'autorità di regolamentazione, la perdita o il danno alle attività, le restituzioni/rimborsi, le perdite per errore non recuperate, etc.

Da quanto esposto in precedenza, emerge chiaramente che il rischio operativo è un tipo di rischio molto complesso per il quale risulta non molto semplice quantificare gli accantonamenti. Bisogna calcolare da un lato la probabilità con la quale l'evento rischioso si realizza e dall'altro la quantità di capitale assorbito a fronte di questi rischi. È essenziale inoltre stabilire le rispettive soluzioni per mitigare gli impatti dell'evento.
Gestire un rischio operativo significa quindi:

- identificare gli eventi generatori;
- misurare le probabilità essi si verifichino;
- osservare gli indicatori di rischio;
- attuare misure di mitigazione del rischio.

Il procedimento più complesso è senza dubbio l'identificazione degli eventi generatori perché, a differenza dei rischi di mercato o di credito, gli eventi che possono determinare l'occorrenza di uno scenario di rischio operativo sono numerosi, eterogenei e molto spesso poco conosciuti e compresi. Per classificare tali eventi è necessario uno studio approfondito dei processi aziendali in modo da stabilire una rilevazione sistematica degli *even type* a cui è associata la corrispondente probabilità di accadimento e il rispettivo ammontare di capitale. Ogni ente bancario dovrà scegliere, in maniera più approfondita, gli *even type* su cui focalizzarsi, considerando la natura del proprio operato, i propri processi aziendali e tutti i fattori di rischio che si considerano ad esso applicabili.
È buona prassi partire da modelli standardizzati e oggettivi con la quale è possibile considerare i rischi più comuni e, nel contempo, avere anche un confronto con le altre banche. Una classificazione causale potrebbe sembrare a primo impatto una buona scelta, ma spesso è complicato individuare tutte le cause alla quale è dovuta una perdita. Inoltre se si cominciasse ad inserire molti *even type*, si finirebbe per rendere la classificazione confusionaria e troppo complicata da applicare. Per tale ragione, una rilevazione basata sulla

natura degli *even type* consentirebbe di classificare i rischi in base alla natura dell'evento causato e quindi avere una classificazione più strutturata e un numero di eventi limitato.
Anche la misurazione della probabilità di tali eventi e la relativa misura delle perdite risulta complessa da calcolare il che risulta un problema poi per la successiva misurazione del requisito patrimoniale. Tuttavia, oggi le Autorità di Vigilanza preferiscono attuare misure prudenziali per contenere i vari rischi, a prescindere dalla loro quantità. Ciò è dovuto al fatto che, data la crescita continua della moderna attività bancaria, è impensabile analizzare ogni singolo rischio, perché ognuno avrebbe bisogno di un trattamento specifico.

1.1. Il quadro normativo: gli accordi di Basilea

Gli accordi di Basilea sono un insieme di accordi internazionali sui requisiti patrimoniali delle banche e sulla loro gestione del rischio. La loro storia risale agli anni '70, quando l'aumento della globalizzazione e degli scambi commerciali internazionali hanno reso necessaria una regolamentazione del settore bancario a livello internazionale. Il fatto decisivo che fece nascere gli accordi fu il fallimento di una banca tedesca, la *Herstatt Bank* nel 1974 che, a causa di investimenti sbagliati si trovò ad aver accumulato una perdita di dieci volte superiore al suo capitale. Ad aggravare la situazione ci fu il fatto che la banca avesse delle filiali negli USA e quando i regolatori nazionali imposero alla banca la liquidazione forzata, gli uffici all'estero continuarono ad operare perché non soggetti alla regolamentazione nazionale tedesca. Per tali motivi, nel medesimo anno del fallimento di questa banca, che in Germania aveva una certa influenza, venne fondato il Comitato per il Controllo Bancario Internazionale (BCBS). Esso è stato fondato dai governatori delle banche centrali dei paesi del G10, con lo scopo di migliorare la regolamentazione del settore bancario internazionale e di promuovere la stabilità finanziaria globale.

1.1.1. Basilea 1

Il primo accordo di Basilea, noto come Basilea 1, è stato siglato nel 1988 da rappresentanti di banche centrali e di regolamentazione finanziaria dei paesi del G10. L'accordo stabiliva un minimo requisito di capitale per le banche, in relazione ai loro rischi di credito e di mercato. Si parlava per la prima volta di "adeguatezza patrimoniale", con l'imposizione di coefficienti patrimoniali ponderati per il rischio, in modo tale che le banche disponessero di condizioni di solvibilità, in caso di perdite inattese e limitassero l'assunzione del rischio. L'accordo richiedeva alle banche di calcolare il rischio ponderato in base alla tipologia di prestiti, con prestiti a rischio maggiore che richiedevano più capitale di quelli a rischio minore. Con l'adozione di rapporti di capitalizzazione uniformi si è inoltre consentito il superamento di "distorsioni competitive" a favore di un "international level playing field". Tale primo accordo venne recepito dalle giurisdizioni solo nel 1992, anno in cui si può dire avvenne il passaggio da un tipo di vigilanza "strutturale", basata su autorizzazioni e controlli amministrativi, ad una vigilanza di tipo "prudenziale". Con vigilanza prudenziale ci si basa sull'assunto che il

conformarsi a un certo standard di capitale e a certi coefficienti di bilancio può diminuire il rischio e i costi di insolvenza. In Italia tale passaggio avvenne grazie al Testo Unico Bancario (TUB) emanato con decreto legislativo il primo settembre del 1993. Ad oggi, chi attua questo tipo di vigilanza alle banche è Banca d'Italia. L'accordo di Basilea 1, sebbene sia stato rivoluzionario nell'ambito bancario, presentò presto dei limiti. In primis, si era focalizzato sul rischio di credito, non considerando le altre tipologie di rischio, come ad esempio il rischio operativo. In secondo luogo, il sistema di ponderazione era troppo superficiale: non veniva considerata la diversificazione del portafoglio come elemento di riduzione del rischio, non veniva considerata la scadenza del prestito e non vi era differenziazione delle misure di rischio per la stessa tipologia di clientela.

1.1.2. Basilea 2

Fu proprio dai limiti di Basilea 1 e dalla sua revisione che nacque Basilea 2, nel 1999 e approvato poi definitivamente nel 2004. Basilea 2 si fonda su tre pilastri fondamentali:

- i requisiti patrimoniali;
- il controllo prudenziale;
- la disciplina di mercato.

Nel calcolo del requisito patrimoniale, non solo viene abolito il limite dell'8%, ma viene riformata la metodologia di calcolo dei requisiti patrimoniali, rendendola più sensibile al rischio dei singoli prestiti e consentendo l'utilizzo di giudizi assegnati dalla banca (rating).

Basilea 2 fu innovativa per la possibilità che diede alle banche di utilizzare non solo rating emessi da agenzie specializzate ma anche dalle banche stesse. Ciò con il fine di fornire più informazioni possibili che siano affidabili e veritiere, in modo da non concedere prestiti ad operatori di cui non si è certi della loro affidabilità. Quando la banca operava in attività di credito non complesse e dotate di sistemi di controllo semplificati, poteva far uso di misure del rischio di credito esterne, ovvero rating fatto da agenzie specializzate (questo approccio è definito metodo standardizzato). Vi era però la possibilità da parte delle banche di utilizzare rating interni (si parla di approccio "internal rating base" IRB); in tal caso la banca doveva sviluppare una propria procedura di valutazione e misurazione del rischio di credito, la quale necessitava di precisi requisiti in merito di dati utilizzati, modelli di calcolo e funzionalità operativa. Tramite un modello di valutazione del rischio si doveva andare a calcolare la specifica probabilità di insolvenza dell'ente alla quale si stava fornendo liquidità, nell'orizzonte temporale considerato per il pagamento.

Attraverso la metodologia IRB, per una corretta determinazione del rischio di credito, vennero introdotte 4 componenti nuove:

- la probability of default (PD) che misurava la probabilità di insolvenza del debitore;
- l'exposure at default (EAD) che misurava il rischio di un aumento dell'importo prestato;
- il loss given default (LGD) che misurava la percentuale di prestito che sarebbe andata persa a seguito dell'inadempienza (al netto dei recuperi);

- la maturity (M) ovvero la vita residua del prestito, la quale veniva presa di riferimento quando il rating del debitore peggiorava e si voleva calcolare di quanto si sarebbe ridotta la solvibilità del prestito.

Questo nuovo metodo comportò una critica da parte soprattutto delle piccole e medie imprese che, svantaggiate dalla loro dimensione, erano considerate non abbastanza affidabili e dunque faticavano di più a trovare istituti che le finanziassero.
All'interno del nuovo schema di calcolo dei requisiti patrimoniali, viene introdotto per la prima volta il rischio operativo e viene stabilito un accantonamento di capitale a fronte di perdite dovute a fattori esogeni, errori umani e malfunzionamenti dei sistemi e processi operativi.

Per quanto riguarda il secondo pilastro, ovvero il processo di controllo prudenziale, esso punta ad aumentare il controllo da parte delle Autorità di Vigilanza, le quali vanno a verificare che vi siano i requisiti minimi patrimoniali e che vengano correttamente applicate tutte le procedure organizzative e le politiche per la minimizzazione dei rischi. Venne previsto che il controllo prudenziale si articolasse in due fasi integrate: ICAAP (Internal Capital Adequacy Assessment Process) e SREP (Supervisory Review And Evaluation Process). Nella prima fase le banche effettuavano un controllo interno in maniera autonoma, valutando i requisiti patrimoniali e i vari rischi, in base alla propria situazione attuale e prospettica. Tale processo è di fondamentale importanza perché permette di verificare in maniera continua l'adeguatezza della dotazione patrimoniale della banca.
Il processo ICAAP, essendo interno, lascia molta libertà alle banche nella scelta di come valutare la propria adeguatezza patrimoniale; ad ogni modo Banca d'Italia fornisce degli strumenti utili per guidare al meglio e banche nelle loro scelte, considerando poi il processo SREP. Quest'ultimo è il processo di vigilanza fatto dalle Autorità, il quale mira a verificare che il processo precedente sia stato svolto in maniera adeguata. Attraverso la cosiddetta Risk Assesment System, le Autorità di Vigilanza fanno delle opportune analisi con le quali formulano un giudizio sulla banca. Vi è una duplice funzione di questo processo: un riesame delle strategie e dei meccanismi messi in atto dalle banche per uniformarsi alle normative e una valutazione dei rischi alla quale le banche sono sottoposte.

Il terzo pilastro del secondo accordo di Basilea è incentrato sul tema dell'asimmetria informativa. Tutti gli istituti di credito dovevano fornire maggiori informazioni al mercato, in modo tale da fornire agli investitori abbastanza informazioni per verificare la patrimonializzazione delle banche. In questa maniera, gli investitori potranno decidere in maniera più saggia dove investire la propria liquidità, andando a penalizzare banche con un alto tasso di rischio, chiedendo un tasso di interesse più elevato.

Basilea 2 ha comportato innumerevoli innovazioni però al contempo ha presentato innumerevoli criticità. Gli istituti di credito dovevano vincolare il proprio capitale per contrastare i rischi delle loro attività, i quali però

erano a loro volta strettamente collegati ai rischi delle imprese debitrici delle stesse banche. Esse, al fine di ridurre il loro rischio di credito (il che comporterebbe meno capitale da tenere a riserva e più possibilità di investimento), avrebbero chiesto alle imprese di diminuire il loro rischio di credito. Da ciò si deduce che con Basilea 2 i costi di finanziamento di un'impresa sono sempre più legati al rating dei prenditori di denaro, comportando che il contenimento di tali costi produca un aumento della patrimonializzazione e un miglioramento del rating aziendale.

1.1.3. Basilea 3

Gli accordi di Basilea nel loro insieme rappresentano un importante sforzo internazionale per regolamentare il settore bancario e promuovere la stabilità finanziaria globale. Tuttavia, la loro efficacia è stata messa alla prova durante la crisi finanziaria globale del 2008 e molte istituzioni finanziarie hanno dovuto affrontare sfide significative per soddisfare i nuovi requisiti patrimoniali. Il terzo accordo di Basilea, noto come Basilea 3, è stato introdotto nel 2010 per rafforzare ulteriormente i requisiti patrimoniali delle banche.
Le novità principali furono:

- introduzione di standard minimi di liquidità
- la definizione di capitale regolamentare e più elevati requisiti patrimoniali
- migliore copertura dei rischi di mercato e di controparte
- contenimento del livello di leva finanziaria
- misure anticicliche per ridurre la "prociclicità" delle regole prudenziali

Una delle novità principali di Basilea 3 fu proprio l'introduzione di standard minimi di liquidità che fino a quel momento non erano stato tenuti molto in considerazione. I due nuovi indicatori che vennero fissate dal nuovo accordo furono *il Liquidity Coverage Ratio (LCR)* e il *Net Stable Funding Ratio (NSFR)*, i quali sono due misure utilizzate per valutare la liquidità delle banche e la loro capacità di far fronte a situazioni di stress finanziario.
Il Liquidity Coverage Ratio (LCR) è una misura della liquidità a breve termine delle banche e misura la capacità delle banche di far fronte a situazioni di stress finanziario che possono verificarsi nel corso di un periodo di 30 giorni. Il rapporto è calcolato dividendo gli attivi liquidi (come contanti, titoli di Stato e altre garanzie di alta qualità) per i finanziamenti netti che si prevede di dover rimborsare nel periodo di 30 giorni successivi.
Il Net Stable Funding Ratio (NSFR) è una misura della stabilità del finanziamento a lungo termine delle banche e misura la capacità delle banche di far fronte a situazioni di stress finanziario a lungo termine, come una crisi finanziaria. Il rapporto è calcolato dividendo il finanziamento stabile a lungo termine per gli attivi stabili a lungo termine. Esso è stato creato per evitare il cosiddetto "effetto precipizio", ovvero la situazione che si

viene a creare dopo una crisi finanziaria nel lungo periodo. Il NSFR è stato creato come misura successiva al LCR.

Per quanto riguarda la definizione di capitale regolamentare, ne vengono definiti tre tipi:

- il Tier 1, che rappresenta il capitale di base di una banca e include gli azionisti, i profitti accumulati e gli strumenti finanziari di capitale di alta qualità;
- il Tier 2, che rappresenta il capitale supplementare e include strumenti finanziari di capitale di qualità inferiore;
- il Tier 3, che rappresenta il capitale complementare e include strumenti finanziari di breve termine che possono essere utilizzati solo in determinate circostanze.

In base ai requisiti patrimoniali di Basilea 3, le banche devono mantenere un minimo del 8% di capitale regolamentare rispetto ai loro attivi ponderati per il rischio. Tuttavia, le banche possono essere soggette a requisiti di capitale più stringenti a seconda dei loro profili di rischio e della loro esposizione ai mercati. Un'altra importante novità di Basilea 3 riguarda la leva finanziaria, la quale misura il grado di indebitamento di una banca rispetto al suo capitale regolamentare. In altre parole, la leva finanziaria rappresenta il rapporto tra gli attivi totali di una banca e il suo capitale regolamentare. Vennero introdotti nuovi requisiti sulla leva finanziaria delle banche, al fine di garantire una maggiore stabilità finanziaria del sistema bancario. Il nuovo requisito sulla leva finanziaria richiede alle banche di mantenere un rapporto tra i loro attivi totali e il loro capitale regolamentare del 3%. Ciò significa che una banca non può avere una leva finanziaria superiore a 33 volte il suo capitale regolamentare. Ad esempio, se una banca ha un capitale regolamentare di 100 milioni di dollari, il suo totale degli attivi non può superare i 3,3 miliardi di dollari.

La novità introdotta da Basilea 3 riguardo alla leva finanziaria è che questo requisito non si basa sui rischi associati ai singoli attivi, ma si applica a tutti gli attivi della banca. Inoltre, il requisito sulla leva finanziaria è più semplice e meno complesso rispetto ad altri requisiti di capitale, come i requisiti di capitale basati sul rischio. Questo requisito sulla leva finanziaria mira a limitare la leva eccessiva delle banche e a prevenire situazioni in cui una banca si indebita eccessivamente.

Per quanto riguarda la "prociclicità" delle regole prudenziali, ci si riferisce alla tendenza delle banche ad assumere rischi maggiori durante le fasi di espansione economica e a ridurre i rischi durante le fasi di recessione. Ciò può amplificare l'instabilità del sistema finanziario. Per ridurre questa prociclicità, Basilea 3 ha introdotto alcune misure anticicliche, tra cui il Buffer di Capitale Contro Ciclico (CCyB), ovvero una riserva di capitale che le banche devono accumulare durante le fasi di crescita economica per poi poter essere utilizzata durante le fasi di crisi. Ciò rende il sistema finanziario meno prociclico, poiché le banche avranno meno incentivi ad assumere rischi maggiori durante le fasi di espansione. Sono stati introdotti poi degli Stress Test che aiutano a valutare la capacità delle banche di resistere a scenari di crisi. Basilea 3 ha introdotto stress test più rigorosi e più frequenti per ridurre la prociclicità delle regole prudenziali.

Potremmo concludere dicendo che Basilea 3 segue una filosofia molto semplice: tutte le operazioni compiute dalle banche comportano rischi, i quali a loro volta generano perdite; maggiore è il rischio, maggiore è la perdita, maggiore è il capitale che deve essere accumulato dalle banche. A mano a mano che gli accordi di Basilea evolvono, vengono stabiliti sempre più alti accantonamenti che hanno come conseguenza un aumento delle commissioni e degli spread sui prestiti bancari. Le imprese subiranno sempre più esami per raggiungere una valutazione del rating più veritiera possibile, in modo da stabilire se e quanto denaro possono prendere a prestito e a quali costi. L'obbiettivo di Basilea è creare un sistema economico e finanziario più forte, con banche solide che possono resistere a crisi di ogni tipo.

1.1.4. Basilea e il Rischio Operativo

Tornando al tema centrale del rischio operativo, esso è diventato un tema sempre più importante negli accordi di Basilea nel corso degli anni. Nell'accordo di Basilea 1 del 1988, il rischio operativo non era esplicitamente menzionato e non era considerato nel calcolo dei requisiti di capitale delle banche. Con l'introduzione di Basilea 2 nel 2004, il rischio operativo è stato definito e incluso nel calcolo dei requisiti di capitale. Basilea 2 ha definito il rischio operativo come il rischio di perdite causate da una mancanza o da un'inadeguatezza dei processi interni, delle persone o dei sistemi, o da eventi esterni. L'accordo ha introdotto un approccio basato sulla valutazione standardizzata del rischio operativo, che prevedeva un calcolo dei requisiti di capitale in base al volume di affari della banca. Tuttavia, con Basilea 3 nel 2010, l'approccio standardizzato al rischio operativo è stato criticato e sono stati introdotti nuovi metodi per il calcolo dei requisiti di capitale. Basilea 3 ha introdotto un approccio basato sull'approccio avanzato, che prevede una valutazione più dettagliata del rischio operativo, in base ai dati storici della banca. Inoltre, Basilea 3 ha introdotto un'ulteriore categoria di rischio operativo, nota come rischio legale, che copre il rischio di perdite derivanti da controversie legali e da sanzioni. In generale, l'evoluzione degli accordi di Basilea ha portato a una maggiore attenzione al rischio operativo e alla necessità di gestirlo in modo efficace all'interno delle banche. Nonostante ciò, l'approccio alla gestione del rischio operativo è ancora in continua evoluzione e viene costantemente valutato in base alle esigenze del mercato e alle sfide emergenti.

1.1.5. Basilea e il rischio operativo: calcolo requisito patrimoniale

Una crescente complicazione del sistema finanziario con nuovi prodotti, connessioni internazionali tra istituzioni, un'ampia scala di fusioni e acquisizioni e il processo di globalizzazione, hanno avuto un'enorme influenza sul processo di misurazione e gestione del rischio nelle banche. Esso è diventato sempre più complicato ed è necessaria molta più attenzione per identificarlo, comprenderlo, calcolarlo e proteggerlo.
Il rischio operativo è uno dei principali rischi finanziari delle banche, insieme al rischio di credito e di mercato. Nonostante esso sia stato identificato abbastanza presto, la sua importanza è stata ampiamente riconosciuta

solo dopo la crisi del 2007-2009. Ad oggi però, stanno insorgendo nuove minacce, legate a un maggiore rischio geopolitico, progressi tecnologici (come l'e-banking e processi automatizzati). Tutto ciò rappresenta nuove sfide per il processo di misurazione e gestione del rischio operativo.

Il Comitato di Basilea per la vigilanza bancaria ad oggi riconosce il rischio operativo come tema fondamentale per calcolare il requisito patrimoniale, all'interno della quale si comprende sia il capitale regolamentare, inteso come importo minimo necessario per avere una licenza (che corrisponde ai rischi attesi), sia il capitale economico, ovvero l'importo necessario per essere e rimanere in attività.

La raccolta di dati che copre le perdite operative suggerisce di utilizzare una distribuzione delle perdite dalla coda pesante che mostra una probabilità di un evento di perdita estrema (con un'elevata gravità della perdita). Le banche devono coprire le perdite attese (EL: expected loss) che sono il risultato di fallimenti prevedibili, così come le perdite impreviste (UL: unexpected loss) dovute a grandi shock una tantum.

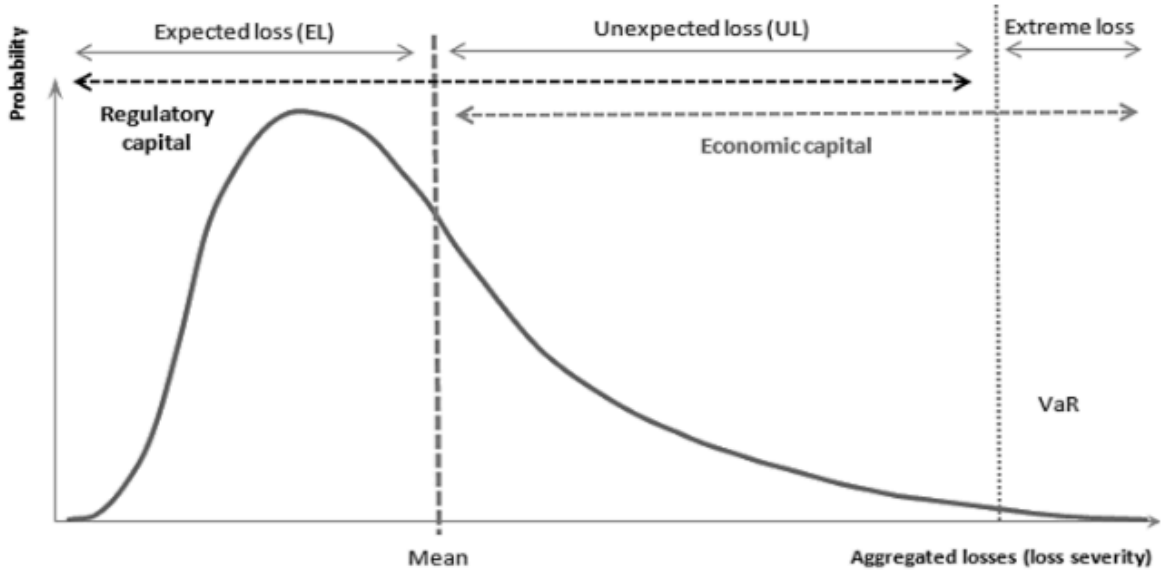


Figura 1 : Funzione di densità di probabilità delle perdite operative[1]

I metodi e gli strumenti che permettono di misurare il rischio operativo sono significativamente diversi da quelli dedicati ad altre tipologie di rischio. La mancanza di fonti di big data di perdite estreme e il loro comportamento anomalo, portano a una minore prevedibilità e difficoltà nella creazione di un modello. Non esiste una metodologia valida utilizzata per calcolare il capitale necessario per la protezione contro le perdite operative. Quelle che tutt'ora vengono applicate presentano sia vantaggi che svantaggi. I metodi porposti da Basilea sono:

- l'indicatore di base (*BIA: basic indicator approach*)
- l'approccio standardizzato (*SA: standard approach*)

[1] Fonte: "methods of measuring operational risk and their influence on the level of bank's capital adequacy", Ewa Dziwok, University of Economics in Katowice, 2018.

- i metodi avanzati (*AMA*: *Advanced Measurement Approaches*, tra i quali i 3 principali sono l'*Internal Measurement Approach* – IMA, il *Loss Distribution Approach* – LDA e lo *Scorecard Approach*)

Il modo in cui il rischio è gestito può seguire due diverse "direzioni": dall'alto verso il basso (top-down) o dal basso verso l'alto (bottom-up). Un approccio top-down consente di determinare la probabilità e l'entità delle potenziali perdite, nonché di identificare le minacce che potrebbero impedire all'ente di raggiungere i propri obiettivi. Questo approccio consente di misurare abbastanza facilmente il rischio per l'intera banca, ma è molto difficile da riformulare al livello unitario. I modelli top-down includono modelli di prezzo azionario multifattoriale, modello di capital asset pricing, modelli basati sul reddito, modelli basati sulle spese, modelli di leva operativa, analisi di scenario e stress test e anche modelli di indicatori di rischio.

Un approccio bottom-up si concentra principalmente sulle fonti di rischio che fanno riferimento al rapporto tra azioni umane, tecnologia e procedure in un'organizzazione, nonché a specifici eventi interni ed esterni. Il rischio viene misurato separatamente per ogni area di attività della banca (ogni unità di business) e sommandolo si ottiene il risultato per l'intera istituzione. I modelli bottom-up comprendono tre sottocategorie principali:

- modelli basati sui processi (modelli causali e reti di credenze bayesiane, modelli di affidabilità, fattori causali multifattoriali);
- modelli attuariali (modelli basati sulla distribuzione empirica delle perdite, modelli basati sulla distribuzione parametrica delle perdite, modelli basati su teoria del valore);
- modelli proprietari.

Tenendo presente che non esiste un approccio corretto, le istituzioni che devono affrontare la necessità di scegliere una metodologia di successo devono considerare fattori quali la disponibilità dei dati, le competenze del personale responsabile del calcolo del capitale, la cultura organizzativa e gli incentivi alla gestione del rischio e dei costi. Il Comitato di Basilea per la vigilanza bancaria non quantifica direttamente il rischio operativo, ma consente di designare il requisito patrimoniale per il rischio operativo nella banca.

In questi documenti sono presenti tre approcci fondamentali per la misurazione del rischio operativo: Basic Indicator Approach (BIA), Standard Approach (SA) e Advanced Measurement Approaches (AMA).

1.1.5.1. Basic Indicator Approach (BIA)

La metodologia del Basic Indicator Approach (BIA) è uno dei tre metodi di calcolo del rischio operativo previsti dal Comitato di Basilea per la vigilanza bancaria. Essa è la metodologia più semplice delle tre, che si basa sulla misura del reddito operativo lordo della banca come indicatore di base del rischio. La BIA parte dal presupposto che il rischio operativo di una banca sia direttamente proporzionale al reddito operativo lordo generato. Dunque, secondo tale approccio, le banche dovrebbero mantenere un capitale per coprire il rischio operativo pari a una quota fissa del loro reddito lordo.

Il valore totale del capitale è calcolato come:

$$K_{BIA} = \frac{\sum_{i=1}^{n} GI_i * \alpha}{n}$$

- K_{BIA}: requisito patrimoniale formulato secondo la metodologia BIA
- GI_i: margine di intermediazione (se è positivo, va riferito ai 3 anni precedenti)
- α: rapporto di copertura del rischio operativo (stabilito da Basilea come il 15%)
- n: numero di anni

Il margine di intermediazione è il soggetto principale di questo tipo di metodologia. Infatti, l'ammontare del capitale è calcolato in base a questo indicatore finanziario di esposizione al rischio, il quale rappresenta le dimensioni dell'attività della banca ed è dato dalla differenza tra il reddito operativo e i costi operativi. Il reddito operativo comprende tutte le entrate derivanti dall'attività bancaria (interessi, commissioni, trading, ecc.), mentre i costi operativi includono tutte le spese sostenute per svolgere l'attività bancaria (personale, affitto, forniture, ecc.). Dopodiché si ha α, il quale è un coefficiente di ponderazione che rappresenta il rapporto tra il rischio operativo e il reddito operativo lordo. Esso di default è previsto dal Comitato di Basilea ed è del 15%, ma le autorità di vigilanza bancaria possono richiedere alle banche di utilizzarne uno più elevato se lo ritengono opportuno. L'importo così ottenuto rappresenta il requisito minimo di capitale che la banca deve mantenere per coprire il proprio rischio operativo. In altre parole, se il rischio operativo di una banca aumenta, il suo requisito di capitale di base aumenta di conseguenza.

La BIA presenta alcuni vantaggi rispetto ad altri metodi di calcolo del rischio operativo, come ad esempio la sua semplicità e la sua facilità di applicazione. Tuttavia, sono innumerevoli gli aspetti negativi di questa procedura, infatti questo metodo era generalmente destinato a banche di piccole o medie dimensioni che non operano nei mercati internazionali. La BIA non richiede set di dati, personale altamente qualificato, è una metodologia che può essere applicata in breve tempo ed è facile da implementare. La criticità maggiore sta nel fatto che vi sia una forte dipendenza dal reddito operativo, come indicatore di base del rischio, il quale può essere facilmente influenzato da fattori esterni come l'economia generale. In sostanza, la metodologia BIA utilizza un approccio semplificato basato su indicatori di rischio che non riflettono accuratamente la complessità e la varietà dei rischi operativi che l'organizzazione potrebbe affrontare.

Oltre a una mancanza di precisione, la BIA pecca anche di flessibilità, non considerando la specificità dell'organizzazione e dei suoi processi aziendali, il che comporta una valutazione del rischio troppo generica e non adeguata alla situazione specifica dell'organizzazione. In aggiunta, il fatto che non esista un elenco definito di indicatori di rischio, rende tale metodologia difficilmente comparabile tra le diverse organizzazioni, il che complicherebbe il lavoro delle autorità, ma anche degli investitori, nel confrontare il rischio di diverse organizzazioni.

Inoltre, la BIA non tiene conto della diversità del portafoglio di attività e dei rischi specifici delle singole attività bancarie, il che può portare a una sottostima del rischio effettivo. In conclusione, è facile intuire come la BIA sia una metodologia di base per l'appunto, che può essere sfruttata da banche di piccola dimensione che dunque non corrono grandi rischi e alle quali peserebbe invece una metodologia più complicata.

1.1.5.2. Standardalised Approach (SA)

Per ovviare alle mancanze presenti nella metodologia BIA, Basilea 2 ne fornisce un'altra più completa, la quale rappresenta una sorta di evoluzione della BIA. La metodologia Standardalised approach si presenta come una metodologia più articolata, la quale riesce ad adattarsi alle diverse aree operative delle banche; infatti, già nelle prime righe in cui viene descritta da Basilea, è sottolineato che nella SA le banche dovranno mappare il totale delle loro attività annuali complessive in otto linee di business, che sono predeterminate dal medesimo accordo di Basilea. Le linee di business sono le seguenti:

Classificazione delle linee di *business*		
Livello 1	**Livello 2**	**Gruppi di attività**
Finanza di impresa	Finanza di impresa	Fusioni e acquisizioni (M&A), sottoscrizioni a fermo, privatizzazioni, cartolarizzazioni, attività di ricerca, emissioni obbligazionarie (debito pubblico, alto rendimento), aumenti di capitale, sindacati di collocamento e garanzia, offerte pubbliche iniziali, collocamenti titoli del settore privato
	Finanza pubblica e degli enti locali	
	Merchant banking	
	Servizi di consulenza	
Negoziazione e vendita	Collocamento	Reddito fisso, azioni, valute, merci, gestione del credito, *funding*, negoziazione c/proprio di strumenti finanziari, prestiti e PcT, raccolta ordini e negoziazione c/terzi di strumenti finanziari (verso "operatori qualificati" *), gestione del debito, *prime brokerage*
	Market making	
	Attività in proprio	
	Tesoreria	
Retail banking	*Retail banking*	Attività (principali e ancillari) rivolte alla clientela retail: prestiti e depositi, servizi bancari, gestioni fiduciarie e immobiliari
	Private banking	Attività (principali e ancillari) rivolte alla clientela privata: prestiti e depositi, servizi bancari, gestioni fiduciarie e immobiliari, consulenza agli investimenti
	Gestione di carte	Carte di credito e di debito per il settore commerciale e imprenditoriale, per la clientela *retail* e privata
Commercial banking	*Commercial banking*	Attività (principali e ancillari) rivolte alla clientela *corporate*: *project finance*, gestioni immobiliari, credito all'esportazione, credito alle attività commerciali, *factoring*, *leasing*, prestiti, fidejussioni, titoli cambiari
Servizi di pagamento e regolamento[254]	Clientela esterna	Pagamenti e incassi, trasferimento fondi, compensazione e regolamento (verso "operatori qualificati")
Servizi di agenzia	Custodia	Servizi di banca fiduciaria, banca depositaria e attività di custodia titoli (verso "operatori qualificati")
	Servizi di agenzia per la clientela *corporate*	Mandati di emissione e pagamento
	Amministrazione fiduciaria per la clientela *corporate*	
Asset management	Gestione fondi con mandato	In *pool*, separata, al dettaglio; in titoli pubblici, in fondi chiusi e aperti, in azioni del settore privato
	Gestione fondi senza mandato	In *pool*, separata, al dettaglio; in titoli pubblici, in fondi chiusi e aperti
Retail brokerage	*Retail brokerage*	Raccolta ordini, negoziazione c/terzi e collocamento di strumenti finanziari e prodotti assicurativi (verso "operatori non qualificati")

Figura 2 : Classificazione delle linee di business[2]

Tutte le attività della banca (bancarie e non) devono essere classificate nelle otto linee di business appartenenti al "livello 1", in modo tale da creare una precisa separazione delle attività per ogni categoria. Basilea sottolinea che nel caso di indecisione nella scelta della linea di business in cui collocare l'attività, venga usato un criterio oggettivo di classificazione e nel caso in cui l'attività rappresenti "una funzione ancillare di un'attività ivi compresa"[3], l'attività verrà inserita nella linea di business di riferimento. Rispetto alla BIA, dunque, la SA fa in modo che venga calcolato un diverso requisito patrimoniale per ogni linea di business e non uno solamente; ciò è stato fatto per ovviare alla diversa rischiosità delle attività operative svolte dalle banche. Nonostante tale

[2] Fonte: Comitato di Basilea per la vigilanza bancaria, Giugno 2006, "Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali

[3] Citazione presa dal testo "Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali", Comitato di Basilea per la vigilanza bancaria, Giugno 2006.

differenza, il margine di intermediazione è sempre presente e funge da livello massimo per ogni linea di business, impedendo alle banche di oltrepassarlo e dunque di esporsi proporzionalmente ad un rischio operativo più elevato.

A differenza della BIA però, questo valore cambierà in base alla linea di business. Nel caso in cui vi sia ulteriore indecisione nell'inserimento di un'attività in un alinea di business durante il processo di allocazione del margine di intermediazione, verrà scelta quella che comporterebbe un maggior requisito patrimoniale. Sempre durante il processo di allocazione del margine di intermediazione, le banche hanno la possibilità di usare metodi interni di pricing, a patto che "il margine di intermediazione totale della banca (risultante dal metodo base) sia equivalente alla somma del margine di intermediazione delle otto linee di business"[2]. Tutto il procedimento con la quale le attività verranno classificate deve fare riferimento alla tabella sovrastante e deve essere documentato, in modo tale da esplicare eventuali deviazioni alle regole e fornire un modello sufficientemente chiaro da poter essere usato anche da altre banche. Lo step finale starà nella revisione da parte di un ente indipendente, di tutto il procedimento di classificazione.

Per calcolare in requisito patrimoniale per linea di business si procede alla stessa maniera della BIA, ma essendoci più di una linea di business, quello che era indicato con alpha, ora è definito con β ("beta") ed indica la relazione tra le perdite per rischi operativi storicamente riscontrate in una determinata linea di business e il valore aggregato del margine di intermediazione per quella stessa linea. I valori di beta sono dettati anch'essi da Basilea e sono raffigurati nella figura sottostante.

Linea di business	Fattori β
Corporate finance (β_1)	18%
Trading and sales (β_2)	18%
Retail banking (β_3)	12%
Commercial banking (β_4)	15%
Payment and settlement (β_5)	18%
Agency services (β_6)	15%
Asset management (β_7)	12%
Retail brokerage (β_8)	12%

Figura 3 : Illustrazione del fattore beta per ogni linea di business[4]

La formula per calcolare il requisito patrimoniale è data dal calcolo della media aritmetica relativa agli ultimi tre anni della sommatoria dei requisiti patrimoniali calcolati per ciascuna unità di business in un anno. Essi derivano dal prodotto tra reddito operativo lordo di ciascuna linea di business e lo specifico coefficiente di rischio. Nel caso in cui in un esercizio uno o più requisiti patrimoniali siano negativi, ovvero il margine di intermediazione sia negativo, non è un problema, dal momento che vi si può attuare una compensazione con gli altri positivi. Tuttavia, se il requisito patrimoniale aggregato per tutte le linee di business fosse negativo, l'input del numeratore per quell'esercizio sarà posto uguale a zero. La logica di fondo della metodologia Standardised Approach implica dunque che, banche che operano su aree di attività maggiormente rischiose in

[4] Fonte: Comitato di Basilea per la vigilanza bancaria, Giugno 2006, "Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali".

termini di rischio operativo, debbano detenere un maggiore patrimonio a fronte di tale esposizione. La formula risulta la seguente:

$$K_{SA} = \frac{\sum_{i=1}^{n}\left(\sum_{j=1}^{8} GI_{i,j} * \beta_j\right)}{n}$$

- K_{SA}: requisito patrimoniale formulato secondo la metodologia TSA
- GI_i: margine di intermediazione per i-anno e j-linea di business (se è positivo, va riferito ai 3 anni precedenti)
- β_j: fattore beta per j-linea di business
- n: numero di anni

La metodologia SA è decisamente più puntuale della metodologia BIA: la distinzione in linee di business rende il calcolo del requisito patrimoniale molto più puntuale rispetto alla BIA e in alcuni casi conviene ad alcune banche che hanno le loro attività concentrate in linee di business con un coefficiente basso. Nonostante ciò, la SA presenta alcune criticità nella modalità di calcolo del requisito patrimoniale; oltre al fatto di usare il margine di intermediazione come parametro di esposizione al rischio, problema già presente nella BIA, l'ostacolo maggiore sta nel fatto che vengono usati coefficienti uguali per tutte le banche. Così facendo, è come se si stesse supponendo che vi sia perfetta correlazione tra gli eventi di perdita, non tenendo conto dell'effettiva incidenza che invece la perdita può avere sulla singola banca. In questa maniera si andrebbe ad azzerare la diversificazione tra diverse banche ed i benefici o gli svantaggi derivanti da ciò. In aggiunta, attraverso la SA non è possibile ottenere puntuali informazioni riguardo le cause della rischiosità operativa, ciò è di ostacolo per lo sviluppo di adeguate strategie e tecniche per fronteggiare il rischio operativo. Prendendo in considerazione gli aspetti positivi e negativi di questa metodologia di calcolo, sorgono dubbi in merito all'effettiva utilità della SA che, infondo, appare un metodo poco preciso ma che allo stesso tempo risulta complicato per quanto riguarda le rilevazioni richieste. È probabile che l'utilità della SA stia principalmente nel fatto che obblighi le banche a raccogliere dati sulle perdite in una maniera standardizzata, spingendo indirettamente le banche ad avere i requisiti necessari per adottare metodi di misurazione avanzati. Per applicare la metodologia standardizzata, vi sono dei requisiti particolari, i quali si suddividono in soglie quantitative, avere un efficace sistema di gestione dei rischi operativi e disporre di adeguati meccanismi di governo societario per i rischi operativi.

Per quanto concerne le soglie quantitative, possono accedere al metodo Standardizzato i gruppi bancari (banche individuali) che rientrano in almeno una delle due categorie:

- patrimonio di vigilanza maggiore o uguale a € 200 milioni ("soglia dimensionale");

- patrimonio di vigilanza maggiore o uguale a € 25 milioni e ammontare complessivo dell'"indicatore rilevante" delle "linee di business" diverse da "Retail Banking" e "Commercial Banking" pari ad almeno una determinata percentuale del totale ("soglia specialistica" pari a un contributo del 60% dell'"indicatore rilevante" totale).

Per quanto riguarda il sistema di gestione dei rischi operativi, si intende che la banca includa tutte le risorse e misure (attività/processi/strutture) adottate dalla banca per l'identificazione, il monitoraggio, il controllo, l'attenuazione e la valutazione dell'esposizione ai rischi operativi.

Nello specifico, le componenti di un sistema di gestione dei rischi operativi sono:

- il processo di raccolta dei dati rilevanti sui rischi operativi;
- il processo di valutazione dell'esposizione ai rischi operativi;
- il sistema di reporting;
- i criteri di classificazione delle attività nelle "linee di business" regolamentari.

È fondamentale che sia documentato nel dettaglio tale sistema di gestione e che siano specificate le responsabilità di ciascun membro all'interno del gruppo (banca individuale)[5].

Infine, l'ultimo requisito previsto per l'applicazione della metodologia riguarda i meccanismi di governo dei rischi operativi. Con ciò si intende la maniera con la quale avviene il processo decisionale, come esso è ripartito e come sono distribuite le responsabilità.

Una banca che vuole applicare la metodologia SA tendenzialmente ha i seguenti organi al suo interno:

- Consiglio di Amministrazione
- Alta Direzione
- Collegio Sindacale
- Internal Audit

In sintesi, le banche che desiderano utilizzare l'Approccio Standardizzato (SA) per il calcolo del rischio operativo devono soddisfare una serie di requisiti, come sopra citati, i quali sono richiesti in funzione di una corretta applicazione della metodologia.

Le metodologie SA e BIA, non essendo estremamente precise, tendono a sovrastimare il capitale necessario per la copertura del rischio, per tale motivo il Comitato di Basilea suggerisce di usare una versione alternativa del metodo standardizzato, ovvero il "metodo standardizzato alternativo" (ASA).

Adottare questa metodologia è facoltativo ed è dunque una scelta della banca se applicarla o meno anche se, una volta applicata, va mantenuta; non si può infatti tornare ad utilizzare l'approccio standardizzato senza l'approvazione dell'autorità di vigilanza.

[5] Informazioni prese dal documento "RECEPIMENTO DELLA NUOVA REGOLAMENTAZIONE PRUDENZIALE INTERNAZIONALE (NUOVO ACCORDO SUL CAPITALE DI BASILEA E NUOVA DIRETTIVA C.E. SUI REQUISITI DI CAPITALE DELLE BANCHE E DELLE IMPRESE DI INVESTIMENTO)", Banca d'Italia, Marzo 2006.

La banca che ha intenzione di usare tale metodo deve anche assicurare che ciò serva effettivamente a migliorare il calcolo del requisito patrimoniale. In particolare, l'ASA è destinato ad essere utilizzato dalle banche che non soddisfano i requisiti per l'utilizzo dell'approccio avanzato. Le banche che utilizzano l'ASA devono applicare una formula standardizzata per il calcolo del loro requisito patrimoniale, che tiene conto della dimensione dell'attività bancaria e di altri fattori. Non vi è particolare differenza tra il modello SA e ASA per quanto riguarda forma, vi è invece per quanto riguarda l'indicatore di esposizione da utilizzare nel calcolo del requisito patrimoniale per le linee *Retail Banking* e *Commercial Banking*. Le banche di dettaglio e commerciali, che solitamente hanno una dimensione inferiore rispetto alle banche d'investimento e di mercato, spesso utilizzano l'ASA come metodo di calcolo perché questo approccio standardizzato fornisce una formula di calcolo semplice che tiene conto di alcune caratteristiche dell'attività bancaria, come ad esempio il volume di affari.

Nel calcolo del capitale richiesto, il fattore beta è moltiplicato per il totale dei prestiti e delle anticipazioni anziché per il reddito lordo. Tale risultato "parziale" è poi moltiplicato per 3,5%. All'interno di questa metodologia i beta rimangono immutati, vi è però la possibilità di aggregare le varie linee di business sotto un'unica percentuale, come accade per esempio con le linee retail e commercial, le quali possono essere unite sotto un fattore beta pari al 15%. Nel caso in cui vi sia difficoltà anche per quanto riguarda la divisione delle restanti linee di business, esse si possono aggregare sotto l'unica percentuale del 18%. In tal caso la formula per il calcolo del requisito patrimoniale, seguendo le varie aggregazioni, diventerebbe:

$$K_{ASA} = \sum_{i=1}^{2} MI_i * \beta_i \; + \sum_{i=3}^{4} LA * \beta_i \; * m + \sum_{i=5}^{8} MI_i * \beta_i$$

- K_{ASA}: requisito patrimoniale formulato secondo la metodologia ASA
- MI_i: margine di intermediazione per i-linea di business (se è positivo, va riferito ai 3 anni precedenti)
- β_i: fattore beta per i-linea di business
- m: fattore dato dal Comitato di Basilea, pari a 3,5%
- LA: media dei prestiti e delle anticipazioni delle linee di business retail e commercial

1.1.5.3. Advanced Measurement Approach (AMA)

L'Advanced Measurement Approach è la terza metodologia di calcolo offerta dal secondo accordo di Basilea. Essa si compone di varie tipologie di calcolo; infatti si parla spesso della metodologia AMA al plurale, andando a configurarla con diversi metodi di calcolo. A differenza della BIA e della SA, le quali si caratterizzano come metodologie analitiche, per la quale si applica una formula generale, nel caso della metodologia AMA vi sono presenti numerosi modelli, che aumentano il grado di sofisticazione e personalizzazione nel calcolo del requisito patrimoniale.

Data la crescente diversificazione degli enti bancari, risulta sempre più complicato fornire metodologie di calcolo uguali per tutti. Per ovviare a questo problema ed ottenere modelli che si plasmano alla perfezione con i livelli di operatività della banca ed i connessi profili di rischio, sono stati studiati tali modelli, i quali si basano su un'analisi dei dati storici, la definizione di scenari di rischio e la modellizzazione matematica del rischio operativo.

Ciò che è innovativo nei modelli AMA è che sono costruiti su misura per la singola banca, di conseguenza la stima del requisito patrimoniale associato al rischio operativo diventa di gran lunga più precisa. Anche le metodologie in sé presentano delle novità nel calcolo che lo rendono estremamente più puntuale, evitando di sovrastimare il capitale necessario, come ad esempio l'uso di serie storiche e metodi statistici avanzati[6].

Per adottare tale metodologia è necessaria una previa autorizzazione dell'autorità di vigilanza e dei requisiti specifici, i quali possono essere classificati in:

- Soglia d'accesso
- Requisiti quantitativi
- Requisiti qualitativi
- Processo di convalida interna

Attraverso la "soglia di accesso" si intende stabilire una soglia minima in termini di dimensioni della banca perché, a banche con dimensioni significative, corrisponderanno più sofisticate tecniche di misurazione del rischio. Le soglie d'accesso al metodo AMA sono le stesse del metodo Standardizzato, dunque un patrimonio di vigilanza maggiore o uguale a € 200 milioni oppure un patrimonio di vigilanza maggiore o uguale a € 25 milioni e ammontare complessivo dell'"indicatore rilevante" delle "linee di business" diverse da "Retail Banking" e "Commercial Banking" pari ad almeno una determinata percentuale del totale.

Vi sono poi dei requisiti di tipo quantitativo che le banche devono rispettare per poter accedere all'utilizzo del modello AMA. I requisiti quantitativi si compongono di svariate sottocategorie; in primis si parla di requisiti generali, ovvero si fa riferimento a determinati dati storici che servono a fornire informazioni riguardo l'adeguatezza e la solidità del sistema con la quale viene calcolato il requisito patrimoniale e gli annessi risultati. Questa prima fase è denominata "Loss Data Collection" ed è fondamentale per costruire poi un modello di gestione del rischio operativo. In questa maniera la banca riesce a raccogliere dati sufficienti a collegare le stime del rischio alle perdite effettivamente subite. Nella selezione dei dati si cercherà di individuare la tipologia di evento pregiudizievole (ovvero ciò che specifica "cosa" sia accaduto), la tipologia di fattore di rischio (la quale rappresenta la "causa" dell'evento) ed infine la dimensione organizzativa. Per stabilire un "perimetro" di raccolta dei dati utili alla Loss Data Collection, vengono intese tutte quelle perdite che hanno un'incidenza sul conto economico della banca, non dovute a politiche commerciali o a compensazioni di costi e ricavi di esercizio che sono stati valutati incorrettamente in precedenza. Il processo

[6] Con la metodologia AMA vengono utilizzati metodi statistici avanzati come la distribuzione di Poisson e la distribuzione di Pareto, per calcolare la probabilità di accadimento del rischio.

di Loss Data Collection deve essere fatto in modo da essere guidato dagli eventi; dunque, il focus deve essere soprattutto sugli eventi, in modo tale da ricollegare più perdite operative, di diversa natura e quindi con effetti diversi, ad uno stesso evento.

In generale, i requisiti proposti da Basilea per l'applicazione del modello AMA sono stati fatti in modo tale che la banca sia spinta a seguire un framework generale che si sviluppa in una raccolta di dati, in modo da creare un database delle perdite operative, per poi svilupparsi in un processo di Loss Data Collection, dove vi è la ricerca, il censimento, la validazione, il monitoraggio e il reporting di questi dati, in modo tale da possedere informazioni che siano attendibili e delle serie storiche di dati di perdita che potranno poi essere utilizzate per lo studio del comportamento delle perdite e la predizione di esse. Tutto ciò è stato programmato con il fine di permettere alla banca di coprire le perdite globalmente e far si che ciò sia fatto con la massima tempestività. Passiamo ora alle componenti del requisito generale, le quali sono:

- Dati di perdita interni
- Dati di perdita esterni
- Dati generali da analisi di scenario
- Fattori del contesto operativo e del sistema dei controlli interni

Le informazioni relative a questi dati devono essere tenute a disposizione di Banca d'Italia nei 5 anni antecedenti. Dopodiché, l'intermediario deve decidere come definire i criteri di raccolta dei dati e documentare tutto il procedimento, compresa la gestione e conservazione dei dati. I dati interni di perdita sono il punto di partenza per un sistema di misurazione del rischio affidabile. In primis, vengono individuate delle soglie minime di perdita attraverso le quali vengono raccolti i dati; queste soglie dipendono dal profilo di rischio delle "classi" e vanno opportunamente calibrate in modo da essere giustificate all'autorità di vigilanza. Le soglie sono fondamentali perché attraverso esse vengono incluse le perdite ritenute significative per l'affidabilità e l'accuratezza della stima del rischio operativo. Per quanto concerne il periodo per la quale devono essere tenuti i dati, nel caso in cui una determinata "classe" presenti una bassa frequenza di eventi di perdita, il periodo storico preso in considerazione potrebbe aumentare; nel caso di mancanza di dati antecedenti, essi possono essere generati a partire da dati più recenti oppure vi è la possibilità di utilizzare dati esterni di altre banche con segmenti di operatività simili. Questi dati di perdita interni devono essere classificati in funzione delle linee di business (utilizzate già nel metodo standard) e delle annesse attività, tenendo in considerazione le tipologie di eventi di perdita fornite da Basilea. Tale insieme di dati è raggruppato in un data set di calcolo, dove le perdite sono inserite al lordo di ciò che si può recuperare (per esempio dalle polizze assicurative, ma sono inclusi anche altri tipi di recuperi), alla data di accadimento dell'evento e con annesse informazioni che descrivano le cause della perdita. I dati di perdita esterni sono secondi di importanza a quelli interni: sono fondamentali quando non si dispone di numerosi dati di perdita interni e quando l'intermediario pensa di poter andare incontro ad una perdita con un impatto elevato. Per tale ragione si deve disporre di un

criterio per la quale l'intermediario, in determinate situazioni, registrerà dati esterni e li utilizzerà nella valutazione del patrimonio minimo.

L'analisi dello scenario è anch'esso un dato importante, soprattutto dal momento in cui l'intermediario prevede una perdita con un impatto potenzialmente elevato, per la quale vi è scarsità di dati. Per registrare dati in merito all'analisi dello scenario devono essere stabiliti dei criteri con la quale si costruiranno degli scenari, dopodiché si farà un confronto dei risultati (con i dati interni ed esterni) per stabilire se si è rappresentato effettivamente il profilo di rischio calcolato. Infine, i fattori di contesto operativo e del sistema di controlli interni servono a rappresentare la "componente prospettica", ovvero la velocità con la quale il profilo di rischio peggiora o migliora a fronte di un evento che può variare le variabili legate ad un segmento di operatività, le risorse impiegate o il sistema di controlli interni. Questi fattori devono essere in grado di predire e rappresentare l'esposizione al rischio operativo dell'intermediario e per essere sicuri di ciò, va fatta continuamente un'attività di monitoraggio e reporting. Una caratteristica importante di questa metodologia è la granularità, la quale, in un sistema di misurazione die rischi operativi, si configura con il numero di classi di rischio operativo. Dato che il rischio operativo deriva da innumerevoli cause, più classi ci saranno a rappresentare la diversa natura del rischio, più il sistema si potrà considerare granulare. Per ogni classe vi corrisponderà una determinata distribuzione e/o misura di esposizione al rischio. L'obbiettivo di base è ridurre il grado di incertezza connesso al requisito patrimoniale e ciò viene fatto attraverso modelli statistici che, sotto richiesta di Basilea, devono avere un grado di confidenza del 99,9%. Ciò significa che, va stimato il valore del requisito patrimoniale e l'intervallo entro la quale questo valore si potrebbe aggirare; il grado di confidenza sta a rappresentare il livello di certezza/fiducia associato a questa previsione, ovvero la percentuale della probabilità che il risultato sia accurato. Durante l'analisi delle perdite si va ad individuare una distribuzione di esse; la difficoltà maggiore sta nel produrre una misura credibile della cosiddetta "coda" della distribuzione, ovvero la predizione delle perdite; si vuole dimostrare come si sia tenuto conto anche di eventi rari ad elevato impatto[7]. Un sistema di rilevazione delle perdite che sia efficiente ed abbastanza granulare, è in grado di individuare i fattori di rischio che influenzano la "coda" della distribuzione.

Si passa ora ai requisiti qualitativi, ovvero caratterizzati dal sistema di gestione dei rischi operativi e dai meccanismi di governo societario per i rischi operativi. Basilea propone un preciso sistema di gestione dei rischi operativi, che si caratterizza in:

- Processo di raccolta e conservazione dei dati relativi ai rischi operativi[8]

[7] Per eventi rari ad impatto elevato si può immaginare l'attacco terroristico negli USA, 11 Settembre 2001. Questo esempio è raffigurativo di evento raro ad impatto elevato, perché la prevedibilità di un evento smile è decisamente bassa ma, nonostante ciò, per una corretta stima delle perdite, va inclusa.

[8] In merito a questo punto, Basilea vuole focalizzarsi sui sistemi informativi degli intermediari finanziari, assicurandosi che abbiano banche dati in grado di reggere la grande mole di dati, che siano complete e affidabili. Inoltre, le banche devono possedere meccanismi di sicurezza informatica che preservino la riservatezza di tali dati. Basilea 2, all'epoca in cui è stata scritta, era molto improntata (relativamente ai sistemi di sicurezza informatica) alla continuità operativa; perciò, vi è menzionata tra i requisiti relativi alla sicurezza dei dati.

- Sistema di reporting: l'intermediario deve disporre di un sistema di reporting tale da fornire, a determinati soggetti, periodicamente, informazioni rilevanti, che siano coerenti in materia di rischio operativo.
- Utilizzo gestionale del sistema di misurazione: il sistema interno di misurazione dei rischi deve essere fatto in modo tale da garantirne un utilizzo continuato e funzionale, non limitandosi a determinare semplicemente il requisito patrimoniale.

Passiamo ora ai meccanismi di governo dei rischi operativi, ovvero tutte quelle modalità con la quale il rischio viene gestito, la suddivisione delle responsabilità, il processo decisionale ed in generale l'assetto organizzativo.

Gli organi e le funzioni centrali sulla quale questo requisito si sviluppa sono i seguenti:

- Consiglio di Amministrazione;
- Alta Direzione;
- Collegio Sindacale;
- Internal Audit;
- Funzione di controllo dei rischi operativi.

Tutte le funzioni che devono essere svolte e le varie responsabilità ad esse connesse sono stabilite all'interno del documento di Basilea 2, il quale segue un ordine prettamente gerarchico, per la quale risulta facile seguire il procedimento passo passo. Infine, il processo di convalida interna è un processo attraverso il quale le banche verificano l'efficacia e l'accuratezza del proprio sistema di gestione del rischio operativo, al fine di ottenere il riconoscimento delle autorità di vigilanza per l'utilizzo della metodologia AMA.

Il processo di convalida interna è composto da tre fasi;

- la prima è una fase di autovalutazione dove la banca deve autovalutarsi e valutare il proprio sistema di gestione del rischio operativo. Questa fase prevede l'identificazione delle fonti di rischio operativo, la valutazione del grado di copertura del rischio operativo da parte del sistema di gestione del rischio operativo e la valutazione dell'accuratezza dei dati utilizzati per la gestione del rischio operativo.
- Nella seconda fase si deve accertare l'efficacia del proprio sistema; dunque, si verifica la qualità dei dati utilizzati per la gestione del rischio, l'adeguatezza dei modelli utilizzati per il calcolo del capitale richiesto e la verifica della coerenza tra il sistema di gestione del rischio e quello di controllo interno.
- Nell'ultima fase, ovvero quella di verifica esterna, la banca deve sottoporre il proprio sistema di gestione del rischio ad una controparte esterna qualificata (External Validation). Al termine di queste fasi, la banca deve presentare alla propria autorità di vigilanza un report di convalida interna (Internal Validation Report) dove sono riportati i risultati delle verifiche effettuate durante tutto il processo di convalida.

Finita la digressione in merito ai numerosi requisiti necessari per l'utilizzo della metodologia AMA, si può passare alla descrizione del procedimento in sé. Nell'utilizzo di questa metodologia, Basilea 2 propone 3 tipologie di approcci avanzati:

- *Internal measurement Approach* (IMA)
- *Scorecard Approach*
- *Loss Distribution Approach* (LDA)

Partendo dal metodo IMA, anch'essa come nel metodo standard fa riferimento a 8 linee operative, le quali però in questo caso fanno riferimento a diverse tipologie di "eventi di perdita" stabiliti dall'autorità di vigilanza, che la banca dovrà considerare. Per ciascuna linea operativa si deve fare la somma delle perdite attese e inattese, più specificamente, si presuppone tra esse vi sia una relazione lineare. Dunque, la banca procede a stimare l'importo delle perdite attese (Expected Loss Amount; ELA) per ogni "cella" della matrice di linee di business e tipi di eventi. Per stimare l'ELA, la banca fornisce un indicatore di esposizione (Expousure Indicator; EI) per ogni linea di business e stima la probabilità di perdita dell'evento (Probability of loss Event; PE) e la perdita data dall'evento (Loss Given Event; LGE) per ogni combinazione di linee di business e tipi di evento. Il prodotto di EI, PE e LGE produce l'ELA. Il capitale richiesto per ogni linea di business e per ogni combinazione di eventi sarà calcolato moltiplicando l'ELA per il fattore gamma (γ). Questo fattore gamma rappresenta una traduzione della stima della perdita attesa in funzione del requisito patrimoniale; infatti deve tener conto delle perdite inattese che sono state ipotizzate e messe in correlazione con quelle attese. I fattori gamma possono essere diversi a seconda delle linee di business e delle tipologie di evento, ma verranno applicati gli stessi fattori gamma a tutte le imprese. Per essere più precisi nel calcolo, si propone di utilizzare l'indice del profilo di rischio (Risk Profile Index; RPI) come fattore di aggiustamento in modo tale da tenere conto del diverso profilo di rischio della distribuzione delle perdite delle singole banche. Il requisito patrimoniale complessivo per la banca è la semplice somma di tutti i prodotti risultanti. Tale somma può essere espressa con la seguente formula:

$$K_{IMA} = \sum i \sum j \left[\gamma(i;j) * EI(i;j) * PE(i;j) * LGE(i;j) * RPI(i;j)\right]$$

dove:

- K_{IMA}: requisito patrimoniale ottenuto applicando la metodologia IMA
- $\gamma(i;j)$: fattore gamma per i-linea operativa e j-tipo di evento (è una percentuale fissa proposta dalle banche e accettata dall'autorità di vigilanza)
- $EI(i;j)$: Livello di indicatore di esposizione per i-linea operativa e j-tipo di evento
- $PE(i;j)$: Probabilità di un evento di perdita per i-linea operativa e j-tipo di evento
- $LGE(i;j)$: Ammontare della perdita in funzione dell'accadimento di un evento di perdita per i-linea operativa e j-tipo di evento
- $RPI(i;j)$: Indice di profilo di rischio per singola banca in base a i-linea operativa e j-tipo di evento

Si passa ora alla descrizione dello “Scorecard approach”, ovvero la seconda delle tre metodologie proposte dall’ Advanced Measurement Approach. Questo metodo di calcolo è definito “di matrice qualitativa” in quanto prevede che la banca ponderi il rischio in base a giudizi di esperti, i quali mediamente vengono raccolti attraverso questionari, che hanno lo scopo di analizzare le probabilità di eventi di perdita futuri, le cause di tali eventi e l’efficacia dei controlli interni. Dunque, tale modello si basa su un’autovalutazione fatta dalla banca, con sentiti pareri di esperti, i quali solitamente sono interni ad essa e rappresentano un’unità di business. Le dichiarazioni di autovalutazione possono essere raccolte e modellate per produrre una classifica dei vari rischi e un elenco prioritario di azioni per migliorare i controlli pertinenti. Per una valutazione complessiva del rischio operativo, le perdite percepite incluse nel modulo di autovalutazione possono essere presentate graficamente (ad esempio, un istogramma) per produrre una distribuzione empirica non parametrica. Da questa distribuzione si può ricavare una funzione di interesse, ad esempio il 99,9° percentile (VaR: Value at Risk). Il capitale da assegnare a ciascuna unità operativa (in base al suo profilo di rischio) è determinato dai risultati della scorecard, quindi, è necessario definire un insieme di indicatori che possano riflettere i diversi rischi di ciascuna area operativa. Di conseguenza, l'organizzazione dovrebbe sviluppare delle "scorecard" in grado di riflettere i rischi di ciascuna area di business e l'efficacia del sistema di controllo interno. Queste scorecard vengono regolarmente preparate dal personale di ogni unità operativa e riviste dalla funzione centrale di controllo dei rischi, che ne verifica l'accuratezza, anche confrontandole con i dati interni sulle perdite. Tra le categorie di rischi che vengono analizzate, le più comuni sono le frodi interne, le frodi esterne, le pratiche di impiego, i clienti, i prodotti, le pratiche commerciali, i danni alle attività fisiche, le interruzioni dell'attività, i guasti ai sistemi e la gestione dell'esecuzione, della consegna e dei processi. Si passa poi all’assegnazione di indicatori chiave di rischio (KRI: Key Risk Indicator) per ogni categoria di rischio, nella quale le banche definiscono specifici indicatori chiave di rischio. I KRI sono fattori misurabili che segnalano le variazioni dei livelli di rischio; degli esempi di KRI sono il numero di transazioni non andate a buon fine, i tempi di inattività del sistema o il tasso di turnover dei dipendenti. Successivamente vengono raccolti i dati storici rilevanti per ogni KRI. Questi dati possono essere ottenuti da fonti interne, come i registri delle transazioni e i rapporti di audit, o da fonti esterne, come i benchmark di settore o i rapporti normativi. A ciascun KRI viene assegnato un peso in base alla sua importanza per il profilo di rischio complessivo della banca. Le banche assegnano quindi un punteggio a ciascun KRI sulla base dei dati osservati, in genere utilizzando una scala predefinita (ad esempio, da 1 a 5 o da 1 a 10). I punteggi possono essere basati su metriche quantitative o su valutazioni qualitative. I punteggi ponderati per ogni KRI vengono combinati per calcolare un punteggio totale di rischio operativo per ogni categoria di rischio. Questi punteggi vengono poi analizzati per identificare le aree ad alto rischio o le tendenze emergenti del rischio. Infine le banche comunicano i risultati della valutazione della scorecard all'alta direzione (e ad altre parti interessate, come ad esempio il consiglio di amministrazione e le

autorità di regolamentazione) e sulla base dei risultati, le banche sviluppano e attuano strategie di mitigazione del rischio e piani d'azione per affrontare i rischi identificati.

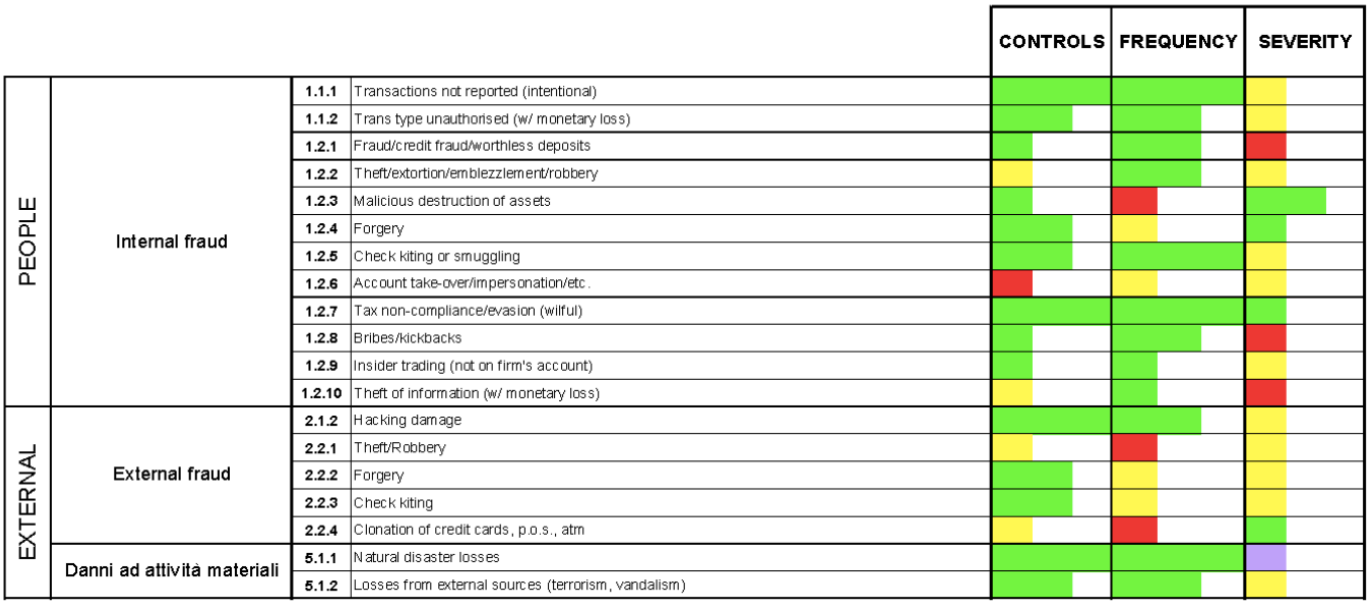
L'approccio della scorecard offre alle banche un modo strutturato e sistematico per monitorare e gestire il rischio operativo. Può aiutare le banche ad allocare le risorse in modo più efficiente, a dare priorità agli sforzi di mitigazione del rischio e a migliorare le pratiche generali di gestione del rischio. Tuttavia, l'efficacia dell'approccio delle scorecard dipende dalla qualità dei dati sottostanti, dall'accuratezza degli indicatori di rischio e dalla capacità della banca di intraprendere azioni appropriate sulla base dei risultati. Di conseguenza, i modelli di scorecard sono più utili per definire le priorità degli interventi sul sistema di controllo, in modo da ridurre efficacemente l'impatto dei rischi ex ante e non a posteriori.

Qui di seguito si riporta un esempio di **Modello di Scorecard**.

Supponiamo di avere a disposizione 80 eventi a rischio riconducibili a quattro cause principali di rischio operativo: persone, processi, sistemi ed eventi esterni. Supponiamo sia stato selezionato un campione di professionisti del settore bancario e che gli obiettivi del progetto del questionario sono stati già descritti. A ciascuno dei professionisti selezionati viene chiesto, per ogni evento di rischio, il suo parere su: frequenza, gravità ed efficacia dei controlli in atto per ciascun evento. Il numero di possibili classi di frequenza è pari a quattro: giornaliera, settimanale, mensile e annuale. Il numero di classi di gravità dipende dalle dimensioni del capitale della banca, con una media di 6/7 classi, che vanno da "una perdita irrilevante" a "una perdita catastrofica". Infine, le possibili classi di controllo sono tre: non efficace, da adeguare ed efficace. Una volta raccolte le interviste, l'obiettivo è assegnare un "rating" a ciascun evento di rischio, in base alla distribuzione delle opinioni sulla frequenza, sui controlli e sulla gravità. Nel seguente esempio viene utilizzata la classe mediana come misura di localizzazione di ogni distribuzione e l'indice di Gini normalizzato come indicatore del "consenso" su tale misura di localizzazione. Ne risultano tre misure di valutazione per ogni evento, espresse con le lettere: A per il basso rischio, B per il medio rischio, C per il rischio più elevato e così via. Mentre la mediana viene utilizzata per assegnare una misura "a lettera singola", l'indice di Gini viene utilizzato per raddoppiare o triplicare la lettera, a seconda del valore dell'indice. Ad esempio: se la mediana della distribuzione di frequenza di un certo tipo di rischio (ad esempio, furti e rapine) è "annuale", corrispondente alla categoria di rischio più bassa, si assegna una lettera A. Poi, se tutti gli intervistati concordano su tale valutazione (ad esempio, l'indice di Gini è pari a zero), A viene convertita in AAA; se invece tutti gli intervistati sono in disaccordo (ad esempio, l'indice di Gini è pari a uno), A rimane A. I casi intermedi riceveranno una doppia valutazione di AA. Lo stesso approccio può essere seguito sia per la gravità che per i controlli, portando a una scorecard completa che può essere utilizzata a fini di intervento. Per la visualizzazione, i colori possono essere associati alle lettere: il verde corrisponde ad A; il giallo a B; il rosso a C; e così via. La Figura riportata qui di seguito presenta i risultati di questo esempio di modello scorecard; risulta che all'evento 1.2.6 dovrebbe essere assegnata una priorità 1 di intervento, poiché i controlli non sono

efficaci e sia la frequenza che la gravità sono gialle. Altri eventi a rischio sono 2.2.1 e 2.2.4, che hanno una frequenza elevata e controlli di qualità media

Figura 4 : Illustrazione del fattore beta per ogni linea di business[9]



Il Loss Distribution Approach (LDA) è la terza metodologia di calcolo proposta da Basilea 2 tra i tre metodi AMA. Nonostante vengano previsti tre modelli per AMA, nella pratica si sono iniziati ad usare maggiormente lo scorecard approach e il LDA, i quali si focalizzano rispettivamente sulla perdita effettiva e sulla perdita attesa. Il metodo LDA fa principalmente affidamento sui dati di perdita interna per costruire una distribuzione relativa alla perdita, mentre gli altri due metodi AMA sono più utilizzati per "stressare" il sistema di misurazione del rischio. Il vantaggio di questo metodo sta proprio nel fatto di utilizzare i dati interni, i quali sono reali e connessi alla banca singolarmente; lo svantaggio però sta nel fatto di considerare come arco temporale di raccolta dei dati solo un anno quando, nella pratica, per raggiungere un livello alto di confidenza, ne servirebbero molti di più. Passando poi all'effettivo funzionamento, questo metodo utilizza un approccio di tipo statistico dove la banca stima, per ciascuna linea di business e tipologia di rischio, le funzioni di distribuzione di probabilità dell'impatto del singolo evento e la frequenza dell'evento per il successivo (un) anno utilizzando i propri dati interni, e calcola la funzione di distribuzione di probabilità della perdita operativa cumulativa. Andiamo per step:

- Modellazione della frequenza: viene stimata la distribuzione di frequenza degli eventi di perdita, ossia il numero di punti dati da osservare nell'orizzonte temporale considerato. Di solito, questo viene fatto adattando una distribuzione statistica (ad esempio, Poisson) al numero di eventi di perdita osservati in ciascuna categoria. La distribuzione di Poisson è la più utilizzata in quanto è relativamente semplice e

[9] Fonte: Paolo Giudici, "Scorecard models for operations management", 1° Novembre 2015, Dipartimento di Economia e Management, Università di Pavia

funziona bene nei casi in cui il numero di eventi è un numero intero e un periodo è probabilmente uguale a un altro. Si basa su un unico parametro λ, che rappresenta il numero medio di eventi per anno e coincide con la varianza dell'insieme di informazioni, ed è calcolato come segue:

$$f(n) = \frac{\left(\lambda^N e^{-\lambda}\right)}{n!} \quad ; per\ ogni\ n \in N$$

La distribuzione rappresenta in questa maniera la probabilità che una serie di eventi si verifichi in un determinato anno. Come mostrato nella figura seguente, valori piccoli di λ producono una distribuzione più obliqua rispetto a valori grandi:

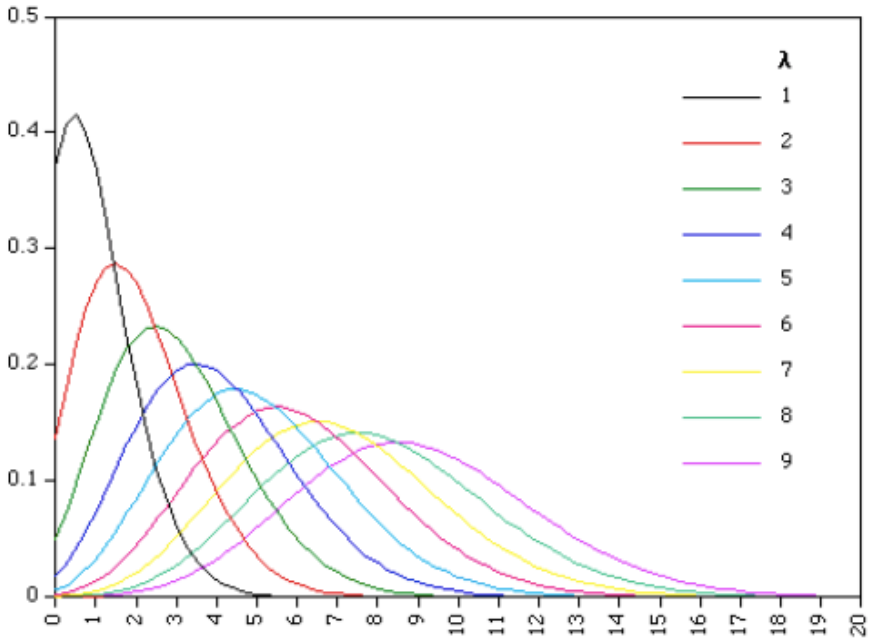


Figura 5 : Distribuzione di Poisson[10]

- Modellazione della gravità (anche chiamata "severity"): si stima la distribuzione della gravità degli eventi di perdita, ovvero il loro impatto. A tal fine, si applica una distribuzione statistica (ad esempio, Lognormale, Weibull, Pareto) alle perdite osservate in ciascuna categoria. Le distribuzioni di gravità rilevano l'entità delle perdite quando si verifica un evento di perdita. Il metodo più comune e più semplice è quello Lognormale, che si limita a modellare l'entità della perdita operativa in base alle medie e alle varianze dei dati storici, anche se per eventi più rari possono essere utili altri metodi come il gamma generalizzato, il beta trasformato, il Pareto generalizzato o il Weibull.
- Modellazione delle dipendenze: vengono poi valutate le dipendenze tra i diversi fattori di rischio, come le correlazioni tra le diverse linee di business e i tipi di eventi. A tal fine si possono utilizzare varie tecniche, come le copule o le matrici di correlazione.

[10] Fonte: Distribuzione creata attraverso il programma MATLAB

- Simulazione: successivamente vengono combinate le distribuzioni di frequenza e gravità utilizzando la simulazione Monte Carlo[11], in modo da generare un gran numero di scenari ipotetici di eventi di perdita per ogni categoria di rischio. Perciò, in ogni scenario, vengono combinate le distribuzioni di frequenza e gravità per stimare la perdita totale per ogni categoria. Si passa poi ad aggregare le perdite totali di tutte le categorie incorporando la struttura di dipendenza. In questo modo si ottiene una distribuzione simulata delle perdite operative totali per l'intera banca.

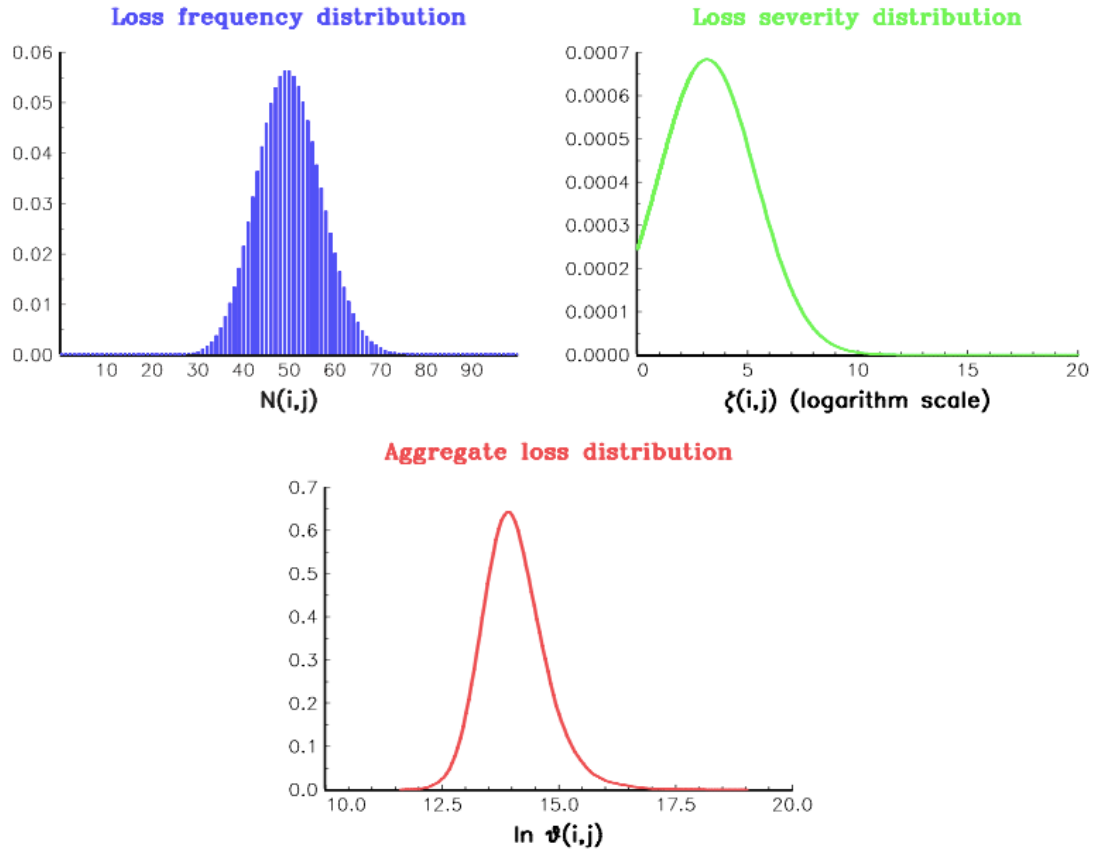


Figura 6 : Loss Distribution Approach[12]

- Metriche di rischio: infine vengono calcolate le metriche di rischio, come il Valore a rischio (VaR) e l'Expected Shortfall (ES), dalla distribuzione delle perdite aggregate. Il VaR rappresenta la massima

[11] La simulazione Monte Carlo è una tecnica computazionale utilizzata per risolvere problemi matematici e fisici attraverso simulazioni randomizzate o campionamento stocastico. Questo metodo si basa sull'idea di sfruttare la casualità per ottenere soluzioni approssimate, ed è particolarmente utile quando affrontare problemi complessi con molte variabili o incertezze.
Essa è stata inventata durante la Seconda Guerra Mondiale da Stanislaw Ulam, un matematico polacco-americano, e John von Neumann, un matematico e fisico ungherese-americano. Entrambi lavoravano sul Progetto Manhattan, il programma di ricerca statunitense che portò allo sviluppo delle prime bombe atomiche. L'idea di fondo fu di utilizzare il campionamento casuale per risolvere problemi complessi. Insieme, i due matematici, svilupparono la tecnica della simulazione Monte Carlo e la applicarono a vari problemi scientifici e ingegneristici.
[12] Fonte: A. Frachot, P. Georges e T. Roncalli, "Loss Distribution Approach for Operational risk", 25 Aprile 2001

perdita potenziale a un determinato livello di confidenza (99,9%), mentre l'ES è la perdita attesa oltre il VaR.

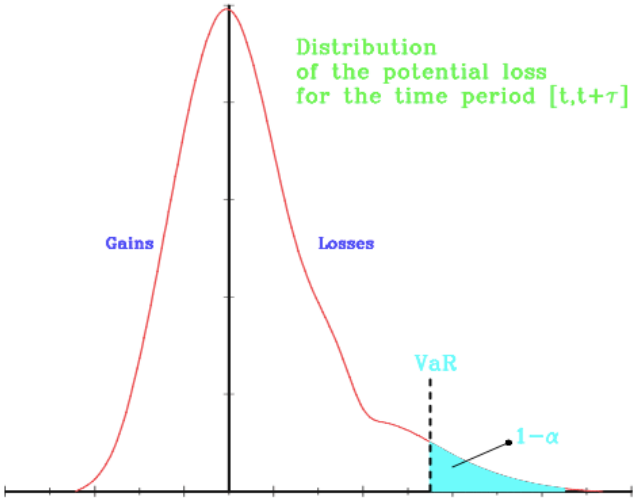


Figura 7 : Distribuzione delle perdite[13]

Dal punto di vista matematico, il procedimento può essere spiegato come segue:

- si individua la variabile aleatoria che rappresenta l'ammontare di un j-evento di perdita per la i-linea di business, la quale in questo caso indicheremo con: ζ (i, j).
- assumiamo implicitamente che le variabili casuali ζ (i, j) siano distribuite in modo indipendente e non dipendano dal numero di eventi.
- la distribuzione della gravità della perdita di ζ (i, j) è indicata da Fi,j
- supponiamo che il numero di eventi tra i tempi t e t + τ (dove r genericamente è uguale a un anno) sia casuale
- la variabile corrispondente a N (i,j) ha una funzione di probabilità pi,j
- allora la distribuzione di frequenza degli eventi di perdita Pi,j corrisponde a:

$$P_{i,j}(n) = \sum_{k=0}^{n} p_{i,j}(k)$$

- Dunque, la perdita per i-linea di business e j-evento di perdita è:

$$\vartheta(i,j) = \sum_{n=0}^{N(i,j)} \zeta_n(\mathrm{i},\mathrm{j})$$

- Se indichiamo con $G_{i,j}$ la distribuzione della perdita, otteniamo che:

[13] Fonte: A. Frachot, P. Georges e T. Roncalli, "Loss Distribution Approach for Operational risk", 25 Aprile 2001

$$G_{i,j}(x) = \begin{cases} \sum_{n=1}^{\infty} p_{i,j}(n) F_{i,j}(x) & x > 0 \\ p_{i,j}(0) & x = 0 \end{cases}$$

- si ottiene poi la distribuzione aggregata delle perdite combinandole: con ζ (i, j) ~ LN (i, j) e N (i, j) ~ P (n)
- utilizzando il metodo Monte Carlo, la distribuzione Gi,j viene "approssimata" dall'insieme S⟨θ(i,j)⟩ = {θs (i, j) , s = 1, . . . S} di valori simulati della variabile casuale θ (i, j). Una stima di Gi,j viene quindi ottenuta dalla distribuzione empirica di S ⟨θ (i, j)⟩.

La LDA offre un quadro completo e flessibile per la quantificazione del rischio operativo nelle banche. Consente di incorporare il giudizio degli esperti, le prove di stress e l'analisi di scenario, rendendola uno strumento prezioso per la gestione del rischio e l'allocazione del capitale. Tuttavia, è essenziale tenere presente che l'LDA dipende in larga misura dalla qualità dei dati e dalle ipotesi formulate durante il processo di modellazione.

1.1.6. Evoluzione di Basilea: verso Basilea 4

Da qualche anno a questa parte è stato coniato il termine "Basilea 4", il quale rappresenta una maniera informale per indicare un insieme di riforme regolamentari proposte per il settore bancario internazionale a seguito del trattato *"Basilea 3- Schema di regolamentazione internazionale per il rafforzamento delle banche e dei sistemi bancari."*. Si tratta di un'estensione e un rafforzamento degli accordi di Basilea 3, che sono stati introdotti dopo la crisi finanziaria del 2007-2008 per migliorare la stabilità finanziaria e la resilienza delle banche. La terminologia "Basilea 4" non è un'etichetta ufficiale adottata dal Comitato di Basilea per la vigilanza bancaria (BCBS), l'organismo internazionale responsabile dell'elaborazione degli accordi di Basilea. Tuttavia, il termine è comunemente usato nel settore per riferirsi a una serie di riforme che mirano a ulteriormente rafforzare il quadro prudenziale bancario. Le riforme associate a "Basilea 4" affrontano diverse aree chiave, tra cui:

1. Miglioramento della qualità e della consistenza del capitale delle banche, aumentando i requisiti minimi di capitale e introducendo nuovi strumenti di capitale.
2. Rafforzamento delle regole per il calcolo dei rischi ponderati per attività (RWA), che sono alla base del calcolo dei requisiti di capitale delle banche. Questo include modifiche alla metodologia standardizzata e all'approccio basato sui rating interni per il calcolo dei rischi di credito, di mercato e operativo.
3. Introduzione di un "pavimento" per i rischi ponderati per attività, che stabilisce un limite minimo per i RWA calcolati utilizzando i modelli interni delle banche. L'obiettivo è ridurre la variabilità dei risultati tra le banche e aumentare la comparabilità.

4. Implementazione di nuovi standard per la gestione del rischio di liquidità, come il rapporto di copertura della liquidità (LCR) e il rapporto di finanziamento stabile netto (NSFR), per garantire che le banche abbiano risorse sufficienti per far fronte a potenziali crisi di liquidità.
5. Rafforzamento delle norme relative alla leva finanziaria, come il rapporto di leva finanziaria (Leverage Ratio), per ridurre il rischio di eccessivo indebitamento delle banche.

Le riforme che fanno parte della denominazione di "Basilea VI" mirano a creare un sistema bancario più stabile e resiliente, riducendo la probabilità e l'impatto di future crisi finanziarie. Tuttavia, l'implementazione di queste riforme può comportare sfide per le banche, come l'adeguamento dei loro modelli di business e l'aumento dei costi di conformità.

Nel contesto di tali riforme e del rafforzamento del quadro regolamentare bancario, il rischio operativo riceve particolare attenzione, poiché è stato identificato come uno dei fattori chiave nelle crisi finanziarie passate. Per affrontare tale rischio, sono stati proposti diversi cambiamenti e aggiornamenti alle metodologie e ai requisiti di capitale. Innanzitutto, è stata fatta una revisione degli approcci per la misurazione del rischio operativo, infatti "Basilea IV" propone di semplificare il quadro per la misurazione del rischio, eliminando i precedenti approcci Basilea II (Approccio Indicatore di Base, Approccio Standardizzato e Approccio con Misurazione Avanzata) e introducendo un unico Approccio Standardizzato per il calcolo del rischio operativo (*Standardized Measurement Approach*, SMA). Questo nuovo metodo dovrà essere adottato obbligatoriamente da tutti gli intermediari bancari, sia quelli "less significant" che "significant". Il nuovo Approccio Standardizzato SMA combina due componenti: una basata sul volume dell'attività (Business Indicator Component, BIC) e un'altra basata sulla storia delle perdite operative (Loss Component, LC). Lo SMA mira a fornire una misurazione più semplice, trasparente e comparabile del rischio operativo tra le banche. Vi saranno dei cambiamenti nella ponderazione delle perdite, infatti lo SMA assegna un peso maggiore alle perdite operative più recenti e rilevanti nel calcolo dei requisiti patrimoniali. Questo approccio mira a garantire che le banche mantengano un livello adeguato di capitale per far fronte a potenziali perdite operative future, comportando però un aumento dei requisiti di capitale per il rischio operativo, in particolare per le banche con un profilo di rischio più elevato. L'obiettivo è di garantire che le banche abbiano un'adeguata copertura di capitale per far fronte a potenziali perdite operative e con il rafforzamento del quadro regolamentare, esse saranno incoraggiate a migliorare le loro pratiche di gestione del rischio operativo, adottando processi e controlli più efficaci e promuovendo una cultura del rischio a tutti i livelli dell'organizzazione. Poiché tutte le banche utilizzeranno lo stesso approccio standardizzato, ci sarà una maggiore comparabilità e trasparenza nella misurazione e nella comunicazione del rischio operativo e con ciò si contribuirebbe a rafforzare la fiducia degli investitori e delle autorità di regolamentazione nel settore bancario.

Questi cambiamenti rappresentano un importante passo avanti nella regolamentazione del rischio operativo e mirano a creare un quadro più semplice, coerente e robusto. Tuttavia, le banche potrebbero dover affrontare

sfide nell'adeguamento ai nuovi requisiti, come la modifica dei loro sistemi di gestione del rischio e la raccolta di dati più dettagliati sulle perdite operative

1.2. Il processo di Operational Risk Management

Il processo di Operational Risk Management (ORM) consiste nell'identificazione, valutazione, monitoraggio e mitigazione dei rischi operativi all'interno di un'organizzazione. Questi rischi, come spiegato da Basilea, possono derivare da inadeguatezze o fallimenti nei processi interni, persone, sistemi o eventi esterni, e possono avere un impatto negativo sulle performance finanziarie e sulla reputazione dell'organizzazione
La gestione del rischio operativo è oggi un processo essenziale per garantire il corretto funzionamento delle funzioni di controllo di un'organizzazione bancaria. Il rischio, infatti, è insito nella progettazione e nella gestione dei processi e, in particolare, nel modo in cui ciascun attore svolge i propri compiti. Imparare a gestire il rischio in modo dinamico richiede quindi di studiare la fisiologia di ogni attività e di raccogliere e catalogare i dati relativi a tutte le attività per elaborare mappe dettagliate dei possibili scenari. Inoltre, queste mappe sono in continua evoluzione, poiché le variabili del sistema e i sistemi di riferimento cambiano frequentemente. Sulla base delle mappe così prodotte, i risk manager possono avviare fasi cicliche di valutazione e aggiornare periodicamente le priorità da tenere in considerazione e, naturalmente, i rischi per la banca. In altre parole, la prospettiva è cambiata radicalmente: invece di cercare di ridurre le minacce potenziali, di sviluppare piani per affrontarle o di stimare l'entità dei danni causati da un incidente, ci si concentra sull'ottimizzazione dei processi in modo che il risultato finale sia il più lontano possibile da quello che ci si potrebbe aspettare anche nello scenario peggiore.
Sintetizzando, il processo di ORM può essere suddiviso in cinque fasi principali:

1. Identificazione dei rischi: In questa prima fase, si identificano e si registrano i rischi operativi presenti nell'organizzazione. Questo può includere l'analisi dei processi interni, dei sistemi informativi, delle risorse umane e dei fattori esterni. Si può utilizzare un mix di approcci qualitativi e quantitativi per identificare i rischi, come ad esempio workshop, interviste, revisioni di documentazione e analisi storiche.
2. Valutazione dei rischi: Una volta identificati i rischi, si procede con la valutazione della loro gravità in termini di probabilità di occorrenza e impatto potenziale sull'organizzazione. Questo permette di classificare i rischi in base alla loro priorità e di focalizzare le risorse e gli sforzi sulle aree più critiche. La valutazione dei rischi può essere effettuata utilizzando metodi qualitativi (come matrici di valutazione del rischio) o quantitativi (come modelli di simulazione e analisi di scenario).
3. Mitigazione dei rischi: In questa fase, si sviluppano e si attuano strategie per ridurre la probabilità di occorrenza dei rischi o per limitarne l'impatto. Le opzioni di mitigazione possono includere la modifica dei processi interni, l'implementazione di nuovi sistemi o tecnologie, la formazione del personale, l'adozione di politiche di sicurezza e la stipula di contratti di assicurazione. La scelta delle misure di

mitigazione dovrebbe basarsi su un'analisi costi-benefici, considerando l'efficacia delle soluzioni proposte e le risorse necessarie per implementarle.

4. Monitoraggio dei rischi: Una volta implementate le strategie di mitigazione, è importante monitorare continuamente i rischi operativi per verificare l'efficacia delle misure adottate e per identificare nuovi rischi emergenti. Il monitoraggio può essere effettuato attraverso il controllo di indicatori chiave di rischio (KRI), l'analisi di incidenti e la conduzione di audit interni o esterni.
5. Reporting e comunicazione: Infine, è fondamentale comunicare i risultati del processo di ORM ai vari livelli dell'organizzazione, inclusi i membri del consiglio di amministrazione e i dipendenti. Il reporting può includere la presentazione di report periodici sullo stato dei rischi, l'aggiornamento delle mappe dei rischi e la diffusione di informazioni e linee guida per la gestione dei rischi operativi.

Nel 2013 venne emanata la Circolare 285 della Banca d'Italia, la quale indicava 3 tipi di funzioni di vigilanza che una banca doveva detenere:

- la prima categoria, anche detta di primo livello, consiste nella vigilanza diretta, volta ad assicurare il corretto svolgimento delle operazioni. In questo caso il controllo viene svolto dalle stesse entità operative, comprese le unità che svolgono esclusivamente compiti di vigilanza e che rispondono ai responsabili delle entità operative, o da unità di back-office. Durante questo processo, i controlli dovrebbero essere integrati il più possibile nelle procedure informatiche. Le unità operative sono le principali responsabili del processo di gestione del rischio: esse devono identificare, misurare o valutare, monitorare, attenuare e segnalare i rischi derivanti dalle normali attività commerciali nell'ambito dell'operatività quotidiana, in conformità al processo di gestione del rischio; devono rispettare i limiti operativi loro assegnati in conformità agli obiettivi e alle procedure che definiscono il processo di gestione del rischio.
- Il secondo livello di controlli è sui rischi e sulla conformità; esso mira a garantire la corretta applicazione del processo di gestione dei rischi, il rispetto dei limiti operativi assegnati alle varie attività e la conformità delle attività dell'azienda ai requisiti normativi, compresa l'autoregolamentazione. Le funzioni responsabili di questi controlli sono separate dalle funzioni produttive e partecipano alla definizione della politica di gestione del rischio e del processo di gestione del rischio.
- Infine, esiste una funzione di revisione interna (terzo livello di controllo) la quale detiene la responsabilità di rilevare le violazioni delle procedure e delle norme e di valutare regolarmente la completezza, l'adeguatezza, l'efficacia (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e delle informazioni.

Le principali funzioni di controllo a cui può essere applicato il nuovo approccio alla gestione del rischio operativo, come funzioni di secondo livello, vi sono le funzioni di compliance e antiriciclaggio (AML), quelle di terzo livello invece sono, per esempio, l'audit.

La Circolare 285, come la 263 del 2006, ha comportato, nell'ambito dei controlli, una grande estensione, in particolare alle attività aziendali responsabili delle attività di controllo di secondo livello, le quali prevedono la presentazione al Consiglio di Amministrazione, e successivamente all'Autorità, di una relazione annuale sui risultati dei controlli effettuati nel corso dell'anno. Nell'ambito dei rischi operativi, si segnala che, soprattutto negli ultimi anni, è aumentato il numero di rischi legati all'IT, per i quali è fondamentale sviluppare e implementare strategie strutturate di gestione dei rischi operativi.

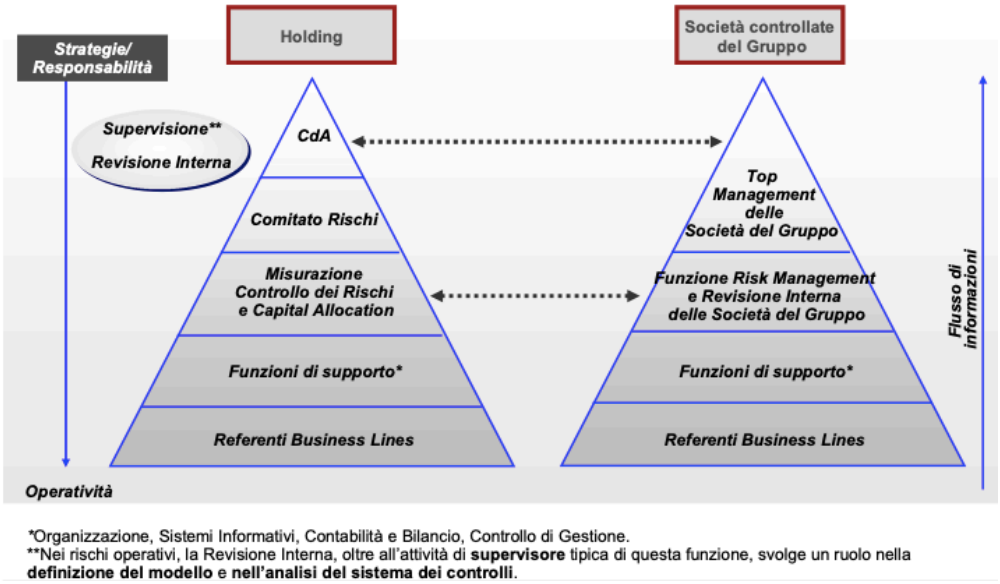


Figura 8 : Il processo di Operational Risk Management: struttura organizzativa e ruoli[14]

1.3. Modelli di identificazione dei rischi operativi

I modelli di identificazione dei rischi operativi sono tutti quegli strumenti e metodi che sono utilizzati per rilevare e analizzare i rischi operativi all'interno di un'organizzazione. Vi sono innumerevoli maniere per identificare questi tipi di rischio; si andrà però ad analizzare le forme più comuni e diffuse all'interno dei sistemi bancario. Il brainstorming e i workshop sono metodi partecipativi, ovvero che coinvolgono gruppi interdisciplinari di esperti e rappresentanti dell'organizzazione in sessioni di discussione per identificare potenziali rischi operativi. La peculiarità di questi metodi è che permettono di condividere esperienze, conoscenze e intuizioni, generando una vasta gamma di rischi identificati.

Un altro metodo ampliamente utilizzato sono le interviste, le quali possono essere strutturate o semi-strutturate con dipendenti, manager e altre parti interessate e possono rivelare rischi operativi specifici e le loro possibili

[14] Fonte: Andrea Giacchero, "Definizione, contesto normativo e classificazione dei rischi operativi", Roma, Giugno 2010.

cause. Similmente, i questionari sono usati per raccogliere informazioni in modo più sistematico e su larga scala, consentendo un'analisi più approfondita dei dati raccolti. Tra i modelli più usati vi sono sicuramente le analisi dei dati storici e degli incidenti passati, con lo studio delle cause e degli effetti degli incidenti.

Ad oggi il modello più usato nell'identificazione dei rischi operativi è sicuramente l'analisi di scenario. Questo metodo prevede la creazione di scenari ipotetici per valutare l'impatto di eventi avversi sulle operazioni dell'organizzazione. L'analisi di scenario può aiutare a identificare vulnerabilità e rischi nascosti che potrebbero non emergere attraverso metodi più tradizionali.

Per utilizzare questo metodo, si identificano i fattori chiave (o driver) che influenzano l'organizzazione e il suo contesto operativo. I driver possono essere interni (ad esempio, processi, sistemi, risorse umane) o esterni (ad esempio, contesto economico, politico, tecnologico). La comprensione dei driver è fondamentale per lo sviluppo di scenari plausibili e pertinenti. Dopodiché, basandosi sui driver identificati, si creano diversi scenari che riflettono possibili evoluzioni future del contesto operativo; scenari che dovrebbero essere diversi tra loro per coprire un ampio spettro di possibili situazioni e sfide (in genere, si sviluppano tra tre e cinque scenari, che variano da ottimistici a pessimistici, passando per scenari intermedi).

Per ogni scenario si analizzano le possibili conseguenze per l'organizzazione in termini di rischi operativi e opportunità. Ciò può includere l'identificazione di vulnerabilità nei processi interni, potenziali fallimenti nei sistemi o nella catena di approvvigionamento, e minacce esterne come disastri naturali o cambiamenti normativi. L'analisi può essere sia qualitativa (ad esempio, attraverso discussioni e valutazioni esperte) che quantitativa (ad esempio, utilizzando modelli di simulazione o analisi di impatto). Dall'analisi degli scenari, si valuta poi la probabilità di occorrenza e l'impatto potenziale dei rischi identificati. Questo permette di stabilire le priorità dei rischi e di concentrare gli sforzi di gestione sui rischi più significativi e urgenti. Una volta ottenuti i risultati dell'analisi di scenario, si elaborano strategie di risposta per affrontare i rischi identificati, le quali possono includere la mitigazione dei rischi attraverso l'adattamento dei processi interni, l'investimento in nuove tecnologie o la formazione del personale, oppure l'adozione di "strategie di trasferimento del rischio" le quali corrisponderebbero alle assicurazioni.

Infine, se si considera che tale analisi non è un processo statico, vi sono delle seguenti fasi di monitoraggio e aggiornamento con la stesura di report periodici, in modo tale da comunicare i risultati dell'analisi. Nonostante essa sia uno dei metodi più utilizzati, l'analisi di scenario non fornisce previsioni assolute sul futuro, ma piuttosto una serie di possibili risultati che possono aiutare le organizzazioni a prepararsi e a prendere decisioni più informate.

Altri metodi che meritano di essere nominati sono:

- Root Cause Analysis: Questo metodo si concentra sull'identificazione delle cause fondamentali dei problemi o dei rischi, piuttosto che limitarsi ai sintomi. L'analisi "delle cause radice" può includere tecniche come il diagramma di Ishikawa (o diagramma a lisca di pesce) e l'analisi dei Five Whys, che aiutano a identificare i fattori che contribuiscono ai rischi operativi.

- Risk Breakdown Structure (RBS): L'RBS è una rappresentazione gerarchica dei rischi che suddivide i rischi operativi in categorie e sottocategorie. Questa struttura facilita l'identificazione e la comprensione dei rischi a vari livelli dell'organizzazione, permettendo una gestione più mirata e organizzata.
- Indicatori Chiave di Rischio (KRI): I KRI sono misure quantitativa o qualitativa che forniscono informazioni sulla probabilità di occorrenza o sull'impatto dei rischi operativi. Monitorando i KRI nel tempo, è possibile identificare tendenze e anomalie che possono indicare l'emergere di nuovi rischi o l'evoluzione di rischi esistenti.
- Benchmarking e best practices: Il confronto delle pratiche e delle performance di un'organizzazione con quelle di altre organizzazioni simili o leader del settore può rivelare aree di rischio e opportunità di miglioramento. Il benchmarking può aiutare a identificare best practices per la gestione dei rischi operativi e promuovere l'adozione di soluzioni più efficaci.

È importante notare che l'identificazione dei rischi operativi può richiedere un approccio combinato che utilizzi diversi di questi metodi per ottenere una comprensione completa e accurata dei rischi esistenti e potenziali. L'uso di più strumenti e tecniche consente di compensare le limitazioni di ciascun metodo e di ottenere una visione più olistica dei rischi operativi.

2 I rischi cyber

Nell'ultimo decennio l'economia globale si è trasformata da un'economia basata sui tradizionali beni capitali (terra, capitale, lavoro) in un'economia digitale in cui l'informazione e un modello di business basato sull'elaborazione elettronica dei dati sono i più importanti. Lo sviluppo di tecnologie avanzate, le soluzioni cloud, le comunicazioni 5G, i mezzi di trasporto autonomi e l'intelligenza artificiale, nonché l'uso della robotica nei processi di produzione automatizzati, l'acquisizione di enormi quantità di dati (big data) grazie alla comunicazione onnipresente su Internet e ai dispositivi mobili inerenti, contribuiscono all'espansione dell'economia digitale. La digitalizzazione dell'economia e delle relazioni sociali non è l'unica fonte di enormi opportunità di sviluppo e di innovazioni, ma anche una fonte di gravi e completamente nuove minacce. Le informazioni digitali sono esposte a una perdita di disponibilità, integrità e riservatezza a causa di incidenti informatici, sia accidentali che intenzionali.

I rischi cyber e/o rischi ICT e di Sicurezza, di seguito indicati genericamente come rischi cyber, possono essere visti come un sottoinsieme dei rischi operativi e sono spesso citati come una minaccia importante per il sistema finanziario. Questa minaccia si estende ben oltre la finanza man mano che l'interesse per il cyber è gradualmente aumentato nel tempo. All'incirca a partire dal 2017, i ministri delle finanze del G20 e i governatori delle banche centrali hanno notato che "l'uso dannoso di sistemi di *information and communication technology* (ICT) potrebbero interrompere i servizi finanziari cruciali per i sistemi finanziari nazionali e internazionali, minando alla sicurezza, e mettendo in pericolo, la stabilità finanziaria". L'attenzione

su questa tipologia di rischi è cresciuta a partire dalla fine degli anni '90 e all'inizio del 2000, con l'aumento dell'adozione di Internet e l'evoluzione delle tecnologie digitali. Tuttavia, la consapevolezza e l'attenzione ai rischi cyber sono aumentate notevolmente negli ultimi 10-15 anni, a causa di diversi fattori. In primis, la crescente digitalizzazione dei servizi bancari, come l'introduzione del mobile banking, l'online banking e i pagamenti digitali, ha portato a una maggiore esposizione a potenziali minacce e vulnerabilità. Tutto ciò si traduce in un esponenziale aumento di attacchi informatici, i quali sono diventati più sofisticati e frequenti, con un aumento dei casi di frode, violazioni dei dati, ransomware e altri tipi di attacchi che coinvolgono istituzioni finanziarie. In secondo luogo, l'interconnessione tra i sistemi finanziari a livello globale ha aumentato la probabilità che un attacco informatico in un Paese o in una singola Istituzione abbia ripercussioni su altre istituzioni o sui mercati finanziari globali.

Oltre ai danni effettivi che la banca può subire, sono da considerare anche i "danni" dovuti alla reputazione. Gli incidenti di sicurezza informatica possono avere un impatto significativo sulla reputazione e sulla fiducia dei clienti nelle istituzioni finanziarie, il che può influenzare negativamente il loro valore e la loro quota di mercato. A causa di questi fattori, le banche e altre istituzioni finanziarie hanno iniziato a prestare maggiore attenzione ai rischi cyber e ad adottare misure proattive per proteggere i loro sistemi e dati sensibili.

Figura 9: numero di attacchi gravi di dominio pubblico per semestre[15]

Come si può osservare dalla figura, tra gennaio 2018 e dicembre 2022 si sono verificati in Italia un totale di 9.633 cyber attacchi. In particolare, nell'ultimo anno si sono registrati 2.489 incidenti, il numero maggiore di sempre ed è interessante notare come nel 2022 la realtà abbia superato le previsioni indicate in grigio dalla linea di tendenza.

[15] Fonte: Rapporto Clusit sulla Sicurezza ICT - 2023

2.1 Definizione di rischi Cyber ed elementi caratterizzanti

Il rischio informatico (detto anche rischio ICT e di sicurezza o rischio cyber) può essere definito come "rischi operativi per le risorse informatiche e tecnologiche che hanno conseguenze sulla riservatezza, la disponibilità o l'integrità delle informazioni o dei sistemi informativi"[16].

Banca d'Italia, nella Circolare 285, riprende la definizione data dalla European Banking Aithority (EBA) e definisce il "rischio ICT e di sicurezza" come "il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata. Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici."

Il rischio cyber rappresenta quindi il rischio di perdite finanziarie, interruzioni o impatti negativi sulla reputazione a causa di un guasto ai sistemi informatici, che sia dovuto a persone, processi o tecnologie. Secondo il CRO Forum (2016), il rischio informatico comprende:

- qualsiasi rischio derivante dall'uso di dati elettronici e dalla loro trasmissione, compresi gli strumenti tecnologici come Internet e le reti di telecomunicazione
- i danni fisici che possono essere causati da attacchi informatici
- le frodi commesse attraverso l'uso improprio dei dati
- qualsiasi responsabilità derivante dall'uso, dall'archiviazione e dal trasferimento dei dati
- disponibilità, integrità e riservatezza delle informazioni elettroniche, siano esse relative a individui, aziende o governi.

Il rischio cyber dipende dalle minacce dolose (o non dolose) che l'organizzazione deve affrontare e dal modo in cui le organizzazioni mitigano tali rischi attraverso decisioni aziendali e strategiche.

Il rischio cyber può avere un impatto sia sul primo (l'obiettivo) sia su terzi (una controparte dell'obiettivo). D'altro canto, le perdite dovute al rischio cyber sono spesso piccole e indipendenti, ma potrebbero anche avere una bassa frequenza e un elevato impatto ("scenario di blackout").

La nozione di rischio cyber combina due aspetti: tecnico ed economico. Dal punto di vista tecnico, è caratterizzato da un'elevata complessità progettuale, dal comportamento (ri)programmabile dei componenti in rete e da una superficie di minaccia dinamica globale (detta anche superfice di attacco). Per quanto riguarda l'aspetto economico, l'incompletezza delle informazioni, le esternalità e la correlazione causata da fattori di rischio comuni sono le caratteristiche principali del rischio informatico.

[16] Definizione data da Cebula e Young (2010).

Nonostante ciò, una quantificazione accurata dei rischi cyber è impegnativa, in quanto non esiste una definizione precisa degli eventi informatici. Si deve quindi fare affidamento su una serie di presupposti. In particolare, si utilizzano definizioni di tipo di evento e si considerano gli eventi informatici come una sottoclasse di eventi di rischio operativo.

Per promuovere una maggiore consapevolezza dei rischi cyber come parte del rischio operativo, è importante definire e introdurre un quadro di analisi all'interno del quale sviluppare scenari in modo coerente.

Una tassonomia comune è di fondamentale importanza per garantire la coerenza nella progettazione e nella parametrizzazione degli scenari relativi al rischio cyber. Esiste una serie di materiali disponibili pubblicamente che mirano a dare coerenza a questa discussione. Principalmente sono due le fonti specifiche da cui si prendono materiali di analisi:

- CRO concept paper
- NIST

Il National Institute of Standards and Technology Cybersecurity Framework ("framework NIST") è stato sviluppato per fornire standard, linee guida e best practice per la gestione dei rischi cyber. Fornisce una guida alle organizzazioni del settore privato statunitense per valutare e migliorare la loro capacità di identificare, prevenire, rilevare, rispondere e recuperare dagli attacchi informatici.

Il concept paper del CRO Forum propone invece una metodologia per la categorizzazione del rischio cyber. L'obiettivo del documento è quello di contribuire all'acquisizione dei dati relativi agli incidenti informatici. In particolare, il concept paper propone delle categorizzazioni per:

- incidente informatico
- tipo di evento
- cause principali
- attori della minaccia
- tipo di impatto

Tali categorizzazioni si sono rivelate utili nel considerare la progettazione e il corrispondente impatto economico degli scenari operativi. Le categorizzazioni del CRO Forum sono state quindi utilizzate come base per la tassonomia dei costi e degli impatti utilizzata nell'ambito del lavoro di questo gruppo di ricerca.

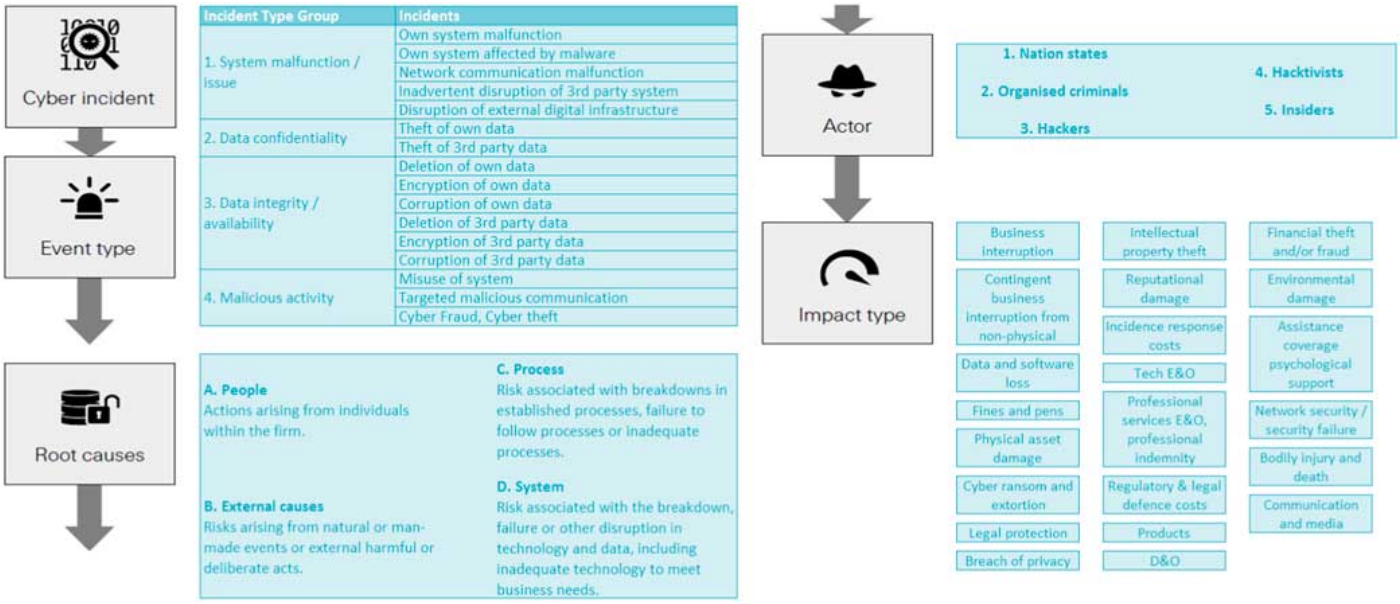


Figura 10: CRO concept paper[17]

Una volta concordata una tassonomia comune, gli scenari di rischio cyber possono essere sviluppati in modo coerente all'interno di un quadro semplice, il quale è indipendente da ogni singolo scenario.

Quando si definisce uno scenario, l'organizzazione deve innanzitutto definire la propria visione del rischio cyber e considerare come eventuali perdite tangibili o intangibili potrebbero derivare da fallimenti nei propri processi legati al cyberspace. Una parte fondamentale di questa valutazione è quella di considerare gli asset di alto valore e/o le debolezze/dipendenze chiave che potrebbero portare a un impatto aziendale significativo se si concretizzasse un rischio informatico. Per definire uno scenario di rischio cyber-operativo è fondamentale avere una comprensione accurata della maturità organizzativa in tutti i campi del framework proposto dal NIST. Una volta definiti i principali asset tangibili e intangibili dell'organizzazione, è possibile sviluppare scenari pertinenti per comprendere gli impatti delle principali minacce per l'azienda.

Ogni scenario viene valutato rispetto a un framework NIST aggregato che comprende un totale di 22 categorie di controllo per le cinque funzioni principali: Identificare, Proteggere, Rilevare, Rispondere e Recuperare. Per un determinato scenario, vengono quindi eseguite le seguenti fasi per ogni categoria di controllo:

1. Si valuta se una categoria di controllo è rilevante o meno per lo scenario.
2. Valutazione dei tipi di costo che potrebbero essere impattati dal fallimento della categoria di costo in questione.
3. Valutazione qualitativa dell'impatto potenziale dell'evento di fallimento di un controllo; si tiene conto sia della frequenza dell'evento che della sua gravità.

[17] Fonte: "Cyber operational risk scenarios for insurance companies", R. Egan, S. Cartagena, R. Mohamed, V. Gosrani, J. Grewal, M. Acharyya, A. Dee, R. Bajaj, V.-J. Jaeger, D. Katz, P. Meghen, M. Silley, S. Nasser-Probert, J. Pikinska, R. Rubin and K. Ang, Institute and Faculty of Actuaries' Cyber Risk Investigation Working Party, Londra, Ottobre 2017

2.2 Il Quadro Normativo

Negli ultimi anni, il settore bancario ha subito una rapida digitalizzazione, con l'adozione di tecnologie avanzate e l'espansione dei servizi online. Sebbene queste innovazioni abbiano migliorato l'efficienza e la convenienza per i clienti attraverso la fruizione di servizi sempre più innovativi, hanno anche esposto le banche a nuovi rischi, in particolare ai rischi cyber. Per affrontare queste minacce emergenti e garantire la stabilità del sistema finanziario, le autorità di vigilanza a livello globale e nazionale hanno introdotto una serie di normative specifiche per i rischi cyber nel settore bancario.

Queste normative hanno lo scopo di garantire che le istituzioni finanziarie adottino misure adeguate a identificare, prevenire e mitigare i rischi cyber, proteggendo al contempo i dati sensibili dei clienti e mantenendo la fiducia del pubblico nel sistema finanziario. Tra le principali normative pubblicate in materia di rischi cyber, figurano i principi e gli standard emessi da organismi nazionali ed internazionali, come il Comitato di Basilea per la vigilanza bancaria, Banca d'Italia e l'EBA.

Le normative in materia di rischi cyber nel settore bancario coprono una vasta gamma di aspetti, tra cui la governance, la gestione dei rischi, la protezione delle infrastrutture critiche, la prevenzione delle frodi, la resilienza operativa e la collaborazione tra le parti interessate. Tra le principali disposizioni, vi sono l'obbligo per le banche di stabilire un quadro di governance adeguato ad affrontare i rischi cyber, di effettuare valutazioni regolari dei rischi, di sviluppare piani di risposta agli incidenti e di garantire la formazione e la consapevolezza del personale in materia di sicurezza informatica.

Le normative in materia di rischi cyber nel settore bancario sottolineano inoltre l'importanza della collaborazione tra le istituzioni finanziarie, le autorità di vigilanza e altre parti interessate, al fine di condividere le migliori pratiche, le informazioni sulle minacce e le lezioni apprese dagli incidenti di sicurezza. Inoltre, le autorità di vigilanza sono sempre più attente alla supervisione delle terze parti e dei fornitori di servizi, poiché rappresentano un potenziale punto di ingresso per gli attacchi informatici.

In sintesi, le normative in materia di rischi cyber nel settore bancario rappresentano un passo cruciale nella creazione di un ambiente finanziario più sicuro e resiliente, garantendo al contempo la protezione dei dati dei clienti e la stabilità del sistema finanziario nel suo complesso. Tra le normative che hanno segnato un cambiamento in tema di sicurezza informatica nei sistemi bancari, si hanno la Circolare 285 di Banca d'Italia, la direttiva europea PSD2 e, tra le più recenti, il Digital Operational Resilience Act (DORA), ovvero il nuovo regolamento europeo sulla resilienza digitale per il settore finanziario.

2.2.1 La Circolare 285 di Banca d'Italia

La Circolare n. 285 di Banca d'Italia è una normativa stabilisce disposizioni in materia di vigilanza per le banche e gli standard regolamentari previsti da Basilea III. La prima e ufficiale versione di questa circolare risale al 17 dicembre 2013, ma esistono innumerevoli e periodici aggiornamenti. Prima che fosse emanata tale

circolare, le banche facevano riferimento alla circolare 263 di Banca d'Italia, la quale recepiva le norme comunitarie sull'accesso all'attività degli enti creditizi e al suo esercizio, e sull'adeguatezza patrimoniale delle imprese di investimento e degli enti creditizi, in attuazione degli indirizzi stabiliti con gli accordi di Basilea II.

Come detto precedentemente, la Circolare n. 285 stabilisce i requisiti di vigilanza prudenziale per le banche; essa contiene disposizioni su vari aspetti della gestione dei rischi, tra cui i rischi operativi e i rischi cyber.

La Circolare 285, nella parte prima, Titolo IV, richiede alle banche di adottare un approccio strutturato per identificare, valutare e gestire i rischi operativi con adempimenti specifici per i rischi cyber (vedi Capitoli 4 – "Il sistema informativo" e Capitolo 5 – "La continuità operativa").

In particolare, la circolare richiede alle banche di:

1. Implementare un sistema di governo dei rischi operativi che include politiche, procedure e responsabilità chiare.
2. Valutare regolarmente i rischi operativi, compresi quelli legati ai rischi cyber, e segnalare i risultati al consiglio di amministrazione e agli organi di controllo.
3. Adottare misure di prevenzione e mitigazione dei rischi, come il rafforzamento delle misure di sicurezza, la formazione del personale e la definizione di piani di continuità operativa e di ripristino dei servizi in caso di incidenti.
4. Monitorare e testare periodicamente le misure di sicurezza e i piani di risposta agli incidenti, al fine di verificarne l'efficacia e l'adeguatezza.

Le banche sono tenute a considerare i rischi cyber, come parte integrante della loro gestione dei rischi operativi e a implementare misure appropriate per ridurre la probabilità e l'impatto degli incidenti informatici.

L'approccio utilizzato da Banca d'Italia per lo sviluppo della Circolare 285 è stato quello di allineare gli adempimenti di tale Circolare a quelli richiesti dagli standard europei che man mano venivano emessi da EBA. Tra questi si evidenziano:

- le Linee Guida EBA in materia di esternalizzazione che introducono degli adempimenti nell'utilizzo di terze parti e/o esternalizzazioni di funzioni aziendali considerate importanti (indicate come FOI – Funzioni Operative Importanti):
- le Linee Guida EBA in materia di segnalazione dei gravi incidenti ai sensi della direttiva PSD2: inizialmente emessi nell'ambito della Direttiva PSD2, Banca d'Italia ha esteso tali adempimenti a tutti gli incidenti ICT definendo delle istruzioni operative su come classificare e comunicare tali incidenti differenziandoli per banche Significant, banche Less Significant, Istituti di Pagamento (IP) e Istituti di Moneta Elettronica (IMEL)[18];

[18] Per gli IP e gli IMEL, Banca d'Italia ha emesso apposito Provvedimento contenente le Disposizioni di Vigilanza per gli Istituti di Pagamento e gli Istituti di Moneta Elettronica (ultimo aggiornamento: 02/11/2022)

- le Linee Guida EBA sulla Gestione dei Rischi ICT e di Sicurezza: anche queste linee guida, emesse in ambito PSD2, sono state estese a tutto il sistema informativo attraverso il loro recepimento nel Capitolo 4 della Circolare 285 e, per gli IP e gli IMEL, nel relativo Provvedimento.

Andando nel dettaglio dei Capitoli 4 e 5 della Circolare 285, si evidenzia quanto segue:

- il Capitolo 4 della Circolare 285 è denominato "Il sistema Informativo" contiene degli adempimenti specifici inerenti le infrastrutture ICT gestite dalla banca e, in particolare:
  - i compiti degli organi aziendali per i profili ICT con particolare riferimento all'Organo con Funzione di Supervisione Strategica (in genere il Consiglio di Amministrazione della Banca), l'Organo con Funzione di Gestione (in genere l'Amministratore Delegato della Banca) e le Funzioni di Controllo (Risk, Compliance e Internal Audit). L'organizzazione della funzione ICT della banca che è deputata alla gestione del sistema informativo della banca e la funzione di controllo dei rischi ICT e di Sicurezza che è dedicata alla gestione di tali rischi[19].
  - La gestione del rischio ICT e di Sicurezza dove è richiesta la predisposizione di un framework completo per la gestione di tali rischi, nonché adempimenti sulla sua implementazione e reportistica da produrre per il management aziendale;
  - la gestione della sicurezza delle informazioni e delle operazioni ICT dove sono stati recepiti, con il 40° aggiornamento della Circolare, gli adempimenti specifici previsti dalle Linee Guida EBA sulla gestione dei rischi ICT e di Sicurezza;
  - la gestione dei progetti e dei cambiamenti ICT dove sono previsti degli adempimenti, anch'essi derivanti dal recepimento delle Linee Guida EBA citate al punto precedente, sulla gestione dei progetti e dei cambiamenti afferenti al sistema informativo aziendale. Particolare enfasi viene posta sulla valutazione dei rischi associati ai progetti e ai cambiamenti ICT e di come questi possano modificare il profilo di rischio degli asset ICT che compongono il sistema informativo aziendale.
  - Il sistema di gestione dei dati che contiene adempimenti inerenti la qualità dei dati aziendali e della relativa reportistica;
  - L'esternalizzazione del Sistema Informativo e il Ricorso a Soggetti Terzi per la Prestazione di Servizi ICT dove vengono ripresi gli adempimenti sulle esternalizzazioni previsti al Capitolo 3 della Circolare 285 e personalizzati ai fornitori ICT;
  - Le Disposizioni Specifiche in Materia di Prestazione di Servizi di Pagamento dove vengono recepiti nella Circolare 285 i principali adempimenti in ambito ICT derivanti dalla normativa secondaria prodotta in ambito Direttiva PSD2.
  - Tutti i documenti che devono essere obbligatoriamente prodotti dalla banca con indicazione del soggetto aziendale che li approva e la frequenza di emissione e aggiornamento.

[19] I compiti previsti per questa funzione possono essere ripartiti tra le funzioni di Compliance e Risk qualora la banca non decida di crearla

- Il Capitolo 5 della Circolare 285 è denominato "La Continuità Operativa" contiene degli adempimenti specifici inerenti per garantire la continuità operativa della banca, incluso quella del suo sistema informativo. Tale capitolo deriva da una prima normativa emessa da banca d'Italia nel 2004 che è stata negli anni incorporata nella Circolare 263, poi nella Circolare 285 e man mano aggiornata e integrata con nuovi requisiti derivanti dalla normativa secondaria della PSD2 che sono stati estesi, così come per il Capitolo 4, a tutto il sistema informativo. I principali adempimenti contenuti in tale capitolo sono relativi a:
    - Predisposizione di un Piano di Continuità Operativa che identifichi i principali scenari di crisi cui la banca è soggetta, i principali attori coinvolti, le soluzioni che si intendono adottare, le procedure di escalation per gestire le potenziali crisi e un piano di comunicazione da attuare durante gli stati di crisi;
    - Business Impact Analysis sulla quale deve basarsi l'identificazione degli scenari di crisi cui è soggetta la banca incluso le persone, i processi e gli asset coinvolti;
    - Predisposizione di un Piano di Disaster Recovery dell'IT on adempimenti sulla dislocazione dei siti (primario e secondario), gli asset ICT impattati e la frequenza e modalità dei backup;
    - Adempimenti relativi alla esecuzione di verifiche periodiche (almeno annuali) sulle soluzioni e processo di continuità operativa predisposte, incluso la simulazione di potenziali crisi;
    - Requisiti particolari per la continuità operativa dei processi a rilevanza sistemica[20].

2.2.2 La Direttiva Europea Payment Service Directive 2 (PSD2)

La Payment Services Directive 2 (PSD2) è una direttiva dell'Unione Europea che nasce per regolamentare i servizi di pagamento elettronico all'interno del Mercato Unico Europeo. Entrata in vigore nel 2018, la PSD2 è stata adottata per promuovere l'innovazione, la concorrenza e la sicurezza nel settore dei pagamenti. Essa ha introdotto alcuni cambiamenti significativi rispetto alla sua versione precedente, PSD1, e ha aperto la strada a nuovi servizi e fornitori di servizi di pagamento. Come obbiettivo principale, la PSD2 vuole aumentare l'estensione del cosiddetto Level Playing Field, ovvero il campo di competizione dei diversi attori, sempre all'interno del settore dei servizi di pagamento. Data la continua nascita di nuovi Player all'interno del settore e di conseguenza di nuovi servizi, la PSD2 cerca di proteggere e assicurare gli utenti di questi nuovi soggetti, chiamati anche Third Party Services Providers (TPP), definendo dei requisiti che garantiscano in primis la trasparenza e la sicurezza delle transazioni di pagamento.

[20] Si definiscono processi a rilevanza sistemica questi processi ad alta criticità nel sistema finanziario italiano che, per un effetto di contagio, possono provocare il blocco dell'operatività dell'intera piazza finanziaria nazionale si concentrano nei sistemi di pagamento e nelle procedure per l'accesso ai mercati finanziari (vedi Circolare 285 – Capitolo 5)

La PSD2 introduce il concetto di "open banking", che consente a terze parti di accedere ai dati dei conti bancari dei clienti con il loro consenso. Questo accesso è fornito attraverso tre nuovi tipi di servizi: Account Information Service Providers (AISP), Payment Initiation Service Providers (PISP) e Card Issuers Service Providers (CISP).

Gli AISP forniscono servizi di consolidamento delle informazioni sui conti di pagamento online; in questa maniera si possono avere tutte le informazioni riguardanti uno o più conti dell'utente, anche se si trovano in diverse banche. La comodità sta proprio nel fatto di avere, su un'unica piattaforma, tutte le informazioni relative ai propri conti[21].

I PIPS sono dei servizi che offrono all'utente la possibilità di effettuare pagamenti per suo conto, attraverso una previa autorizzazione, senza che egli debba accedere al portale online della banca. Questa pratica si è diffusa molto e in maniera celere, data la forte crescita di pagamenti online e ha reso il procedimento più veloce e flessibile, semplificando la procedura che l'utente avrebbe dovuto fare.

Per quanto riguarda i CISP, essi sono dei servizi che permettono a soggetti terzi di emettere carte di debito appoggiate a conti che sono stati aperti in un altro istituto. In sostanza, offrono servizi di conferma di disponibilità di fondi, in modo tale che, quando l'utente fa un acquisto online con una carta di debito emessa da un operatore diverso da quello presso cui si detiene il conto, si verifica prima l'effettiva disponibilità di fondi da parte dell'utente, per poi finalizzare il pagamento.

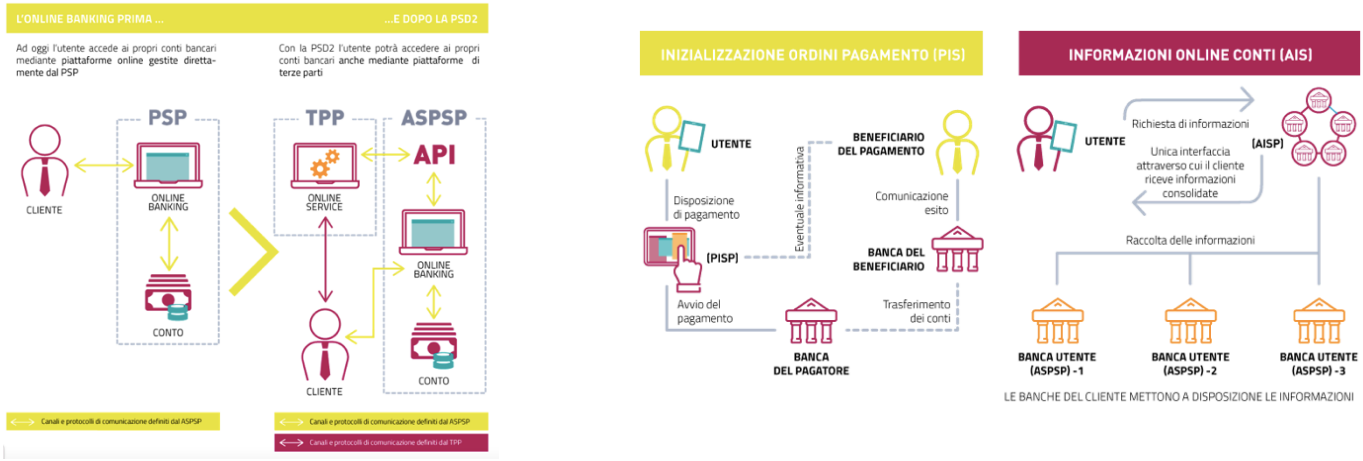


Figura 11: Evoluzione dell'online banking[22]

Le principali novità introdotte dalla PSD2 sono relative a:

- Responsabilità e protezione del consumatore: la PSD2 introduce regole più stringenti per proteggere i consumatori dalle frodi, limitare la loro responsabilità in caso di pagamenti non autorizzati e garantire il rimborso tempestivo in caso di transazioni errate o contestate.

[21] Per capire il perché dell'introduzione di questi strumenti, si deve entrare nell'ottica di una sempre più crescente economia digitale, la quale sta facendo molto affidamento sulle fintech, specialmente dopo l'era del COVID-19.

[22] *Fonte: Global Open Banking Ecosystem, "Nuova normativa PSD2"*

- Trasparenza e comunicazione: La direttiva richiede una maggiore trasparenza nella comunicazione delle tariffe, dei termini e delle condizioni relative ai servizi di pagamento. Ciò include l'obbligo per i fornitori di servizi di pagamento di fornire informazioni chiare e comprensibili su commissioni, diritti e responsabilità.
- Licenze e supervisione: la PSD2 stabilisce requisiti più rigidi per la licenza e la supervisione dei fornitori di servizi di pagamento, al fine di garantire la sicurezza e l'affidabilità del settore. Ciò include la necessità per i nuovi operatori di ottenere l'autorizzazione delle autorità competenti prima di iniziare a fornire servizi di pagamento.
- Autenticazione forte del cliente: la PSD2 richiede l'adozione di un tipo di un'autenticazione, definita forte o multi-fattore, del cliente, per migliorare la sicurezza dei pagamenti elettronici. Questa è stata pensata per permettere una corrispondenza univoca tra chi sta compiendo il pagamento e l'azione di pagamento stessa (principio del non ripudio) e, nel contempo, ridurre al minimo i casi di frode connessi agli attacchi degli hacker denominati Man-in-the-middle, ovvero attacchi in cui una persona terza si inserisce tra il soggetto e il sistema di pagamento dirottando le transazioni verso un altro conto diverso da quello del destinatario della transazione. Per tale ambito, è stato richiesto a EBA di produrre un Regulatory Technical Standard (RTS) specifico.
- Gestione dei gravi incidenti di sicurezza: la PSD2 richiede che gli incidenti che occorrono sui sistemi ICT a supporto dei servizi di pagamento siano classificati e notificati alle Autorità competenti (in Italia è Banca d'Italia). Anche in questo caso, è stato richiesto ad EBA di produrre delle opportune Linee Guida specifiche.
- Misure di Sicurezza: la PSD2 richiede che tutti i sistemi ICT di supporto ai servizi di pagamento adottino delle misure di sicurezza obbligatorie per garantire la loro sicurezza. Anche in questo caso, è stato richiesto ad EBA di produrre delle opportune Linee Guida Specifiche. Dopo una prima versione emessa nel gennaio 2018, EBA ha sostituito queste linee guida con un nuovo documento denominato "Linee Guida per la Gestione dei Rischi ICT e di Sicurezza" che lo ha sostituito a settembre 2019. Le nuove Linee Guida hanno un approccio più ampio in quanto si è passato da un mero elenco di misure di sicurezza da adottare, ad un documento che descrive come gestire i rischi ICT e Cyber connessi ai servizi di pagamento.

Da quanto esposto, si evince che la PSD2 è composta da una normativa principale rappresentata dalla Direttiva che è stata recepita nell'ordinamento legislativo italiano e una normativa secondaria composta dagli RTS e Linee Guida predisposte dall'EBA.

Le componenti della normativa secondaria predisposte da EBA sono:

- RTS sulle norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri: è sicuramente la componente della normativa secondaria PDS2 più importante e affronta sia il tema dell'autenticazione forte del cliente che gli standard tecnici che devono

essere adottati dalle banche per consentire alle terze parti (i cosiddetti TPP) di poter accedere ai conti dei clienti detenuti dalle banche.

Le principali novità introdotti dall'RTS sono:

- l'accesso ai conti e le transazioni di pagamento devono essere protetti dall'autenticazione forte del cliente che prevede l'utilizzo di almeno due fattori di autenticazione tra quelli contemplati nelle tre tipologie di conoscenza, possesso e inerenza. Almeno uno dei due elementi di autenticazione utilizzati deve essere non prevedibile né riproducibile;
- altro adempimento rilevante è l'introduzione, per l'accesso ai conti e per le transazioni di pagamento, del concetto di "dynamic linking", ovvero la comunicazione su canale alternativo a quello su cui si effettua la transazione delle principali informazioni (beneficiario e importo) che si sta autorizzando. Tale meccanismo, realizzato mediante invio di OTP sullo smartphone e/o autorizzazione tramite pop-up sull'APP del fornitore del servizio, consente di contrastare gli attacchi di man-in-the-middle che gli anni scorsi hanno prodotto un elevato numero di frodi con relative perdite per i clienti e per gli operatori di tali servizi.
- L'RTS prevede anche delle esenzioni alla SCA (es. pagamenti sono una certa cifra) che gli operatori dei servizi di pagamento possono adottare. Alcuni di questi sono agganciati al tasso di frodi che l'operatore registra nell'anno. Da questo sono derivate altre Linee Guida EBA[23] che impongono a tutti gli operatori di servizi di pagamento di comunicare annualmente alle Autorità competenti i tassi di frodi, calcolate secondo regole stabilite dalle Linee Guida EBA, che hanno registrato nell'anno.
- Predisposizione di interfacce dedicate sui sistemi di on-line banking di interfacce dedicate per l'accesso delle Terze Parti ai conti dei clienti. Oltre alle tematiche di sicurezza connesse (es. riconoscimento della terza parte che deve essere censita su un registro pubblico certificato), sono presenti anche tematiche di tipo "politico" perché gli operatori devono garantire l'accesso ai propri sistemi a terze parti che sono loro concorrenti sul mercato dei servizi di pagamento. Negli anni successivi all'emissione dell'RTS, ci sono state varie discussioni con emissione, da parte di EBA e della Autorità nazionali, di ulteriori adempimenti per garantire la disponibilità di queste interfacce garantendo nel contempo lo sviluppo del mercato dei sistemi di pagamento.

- le Linee Guida EBA in materia di segnalazione dei gravi incidenti: le Linee Guida, riprendendo quanto già normato nella Direttiva Network Information Security (NIS), stabiliscono dei criteri oggettivi per la classificazione degli incidenti che possono occorrere sui sistemi di pagamento[24] e tempi e modalità per la comunicazione di tali incidenti alle Autorità competenti (per l'Italia è Banca d'Italia). Come

[23] Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) – luglio 2020

[24] Gli incidenti che possono occorrere sui sistemi di pagamento si dividono tra "incidenti operativi" (incidenti dovuti a malfunzionamenti e anomalie) e "incidenti di sicurezza" 8incidenti dovuti ad eventi di sicurezza quale malware, attacchi cyber, etc)

detto in precedenza, Banca d'Italia ha esteso tali adempimenti a tutti gli incidenti ICT definendo delle istruzioni operative su come classificare e comunicare tali incidenti differenziandoli per banche Significant, banche Less Significant, Istituti di Pagamento (IP) e Istituti di Moneta Elettronica (IMEL);

- le Linee Guida sulla Gestione dei Rischi ICT e di Sicurezza: come accennato in precedenza, la prima versione di queste linee guida forniva un elenco delle misure si sicurezza che dovevano essere adottate sui sistemi di pagamento. In seguito, è stata prodotta da EBA un'altra versione che è improntata sulla gestione dei rischi connessi ai sistemi di pagamento e non fornendo solo una mera lista di misure di sicurezza.

  I principali ambiti coperti da tali linee guida sono:

  - Governance e Strategia: fornisce requisiti sulle responsabilità che devono essere assunte nelle banche per le tematiche inerente l'ICT, rischi e la Sicurezza ICT, nonché adempimenti sulla definizione e implementazione della strategia in tale ambito.
  - Quadro di riferimento per la gestione dei rischi ICT e di Sicurezza: in questa sezione vengono indicati gli adempimenti per la costruzione ed implementazione di un quadro di riferimento per la gestione dei rischi ICT e di Sicurezza inerenti i sistemi di pagamento considerando tutti gli aspetti quali la complessità, l'interconnessione e la dipendenza dalle infrastrutture esterne e garantendo che i rischi ICT e di Sicurezza siano adeguatamente identificati, valutati, monitorati e mitigati.
  - Sicurezza dell'informazione: descrive tutte le misure di sicurezza, logica e fisica, che devono essere adottate per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi ICT. Vengono forniti anche adempimenti relativamente al monitoraggio della sicurezza, all'analisi, valutazione e verifica della sicurezza e formazione e sensibilizzazione in tale ambito.
  - Gestione delle Operazioni ICT: in tale sezione vengono forniti gli adempimenti per mettere in sicurezza tutti i processi operativi di gestione del sistema informativo. Particolare enfasi è dedicata al processo di gestione degli incidenti dove vengono referenziate le Linee Guida di EBA specifiche.
  - Gestione dei progetti e dei cambiamenti ICT: in tale sezione vengono forniti dei requisiti su come effettuare in sicurezza i progetti ICT e i cambiamenti al sistema informativo aziendale. Particolare enfasi è riportata sulla identificazione, valutazione e mitigazione dei rischi connessi a tali cambiamenti, nonché delle modifiche che essi possono apportare al profilo di rischio degli asset ICT impattati.
  - Gestione della Continuità Operativa: la sezione contiene tutti gli adempimenti che devono essere adottati per garantire la continuità operativa dei sistemi di pagamento. Particolare enfasi

viene posta sull'Analisi di Impatto preliminare che deve identificare gli scenari di crisi applicabili, le persone e gli asset coinvolti.

- Gestione del rapporto con gli utenti dei servizi di pagamento: la consapevolezza da parte degli utilizzatori dei rischi connessi i servizi di pagamento è un aspetto cruciale in quanto, come noto, il fattore umano è l'anello debole per la gestione della sicurezza. In tale sezione, le Linee Guida EBA definiscono degli adempimenti che gli operatori devono adottare verso i propri clienti che sono per lo più inerenti a interventi formativi e comunicazioni continue che hanno la principale finalità di aumentare la loro consapevolezza verso i rischi che si corrono e, in generale, verso la sicurezza informatica.

La PSD2 è stata recepita nell'ordinamento nazionale con il D. lgs. n. 218 del 15 dicembre 2017 ed è entrato in vigore il 13 gennaio 2018.

Relativamente alla normativa secondaria, con l'esclusione dell'RTS sulla SCA che essendo un regolamento di fatto era applicabile a tutti gli stati dell'Unione Europea una volta approvato dal parlamento europeo, le altre Linee Guida EBA sono state recepite da Banca d'Italia nella Circolare 285 per quando riguarda le Banche e nel Provvedimento per la vigilanza degli IP e IMEL.

Come accennato in precedenza, nel recepimento delle Linee Guida EBA nella Circolare 285, Banda d'Italia a esteso tali adempimenti a tutto il sistema informativo e non solo ai sistemi di pagamento.

2.2.3 Il Regolamento Europeo Digital Operational Resilience Act (DORA)

Il regolamento connotato con l'acronimo DORA (Digital Operational Resilience Act) è una legislazione proposta dall'Unione Europea per rafforzare la resilienza operativa delle entità del settore finanziario e proteggere i consumatori e il sistema finanziario dagli attacchi informatici e dalle interruzioni dei servizi. Il regolamento è entrato in vigore il 17 gennaio 2023 e avrà completa attuazione il 17 gennaio 2025.

Un primo accenno del DORA compare nel settembre 2020, quando la Commissione europea ha pubblicato il pacchetto sulla finanza digitale. Esso comprendeva la strategia per la finanza digitale e la strategia per i pagamenti al dettaglio, oltre a due proposte legislative, i mercati dei cripto-asset (MiCA) e la legge sulla resilienza operativa digitale (DORA). La strategia per la finanza digitale si basa sulla costruzione di un piano d'azione per le Fin Tech e sostiene la transizione digitale del settore finanziario, abbracciando le innovazioni tecnologiche. Tuttavia, la trasformazione digitale del settore finanziario può avere successo solo con sistemi IT resilienti, di tutte le entità finanziarie europee, per questo motivo il Pacchetto Finanza Digitale include DORA.

La minaccia di attacchi informatici nel settore finanziario è aumentata drasticamente negli ultimi anni. Rispetto ad altri settori, quello finanziario rappresenta un obiettivo interessante per i criminali informatici. Gli attacchi informatici hanno anche il potenziale per disturbare o interrompere i servizi finanziari che sono importanti per il sistema finanziario globale. Si stima che nei soli primi sei mesi del 2021, gli attacchi di phishing nel settore

finanziario sono aumentati del 22% rispetto allo stesso periodo del 2020. Oltre a ciò, le aziende finanziarie stanno affrontando un aumento degli attacchi ransomware e DDoS (Distributed Denial of Service). Già in passato, alcune voci autorevoli nel mercato finanziario hanno previsto che la prossima crisi finanziaria potrebbe derivare da un attacco informatico sistemico. La Commissione europea ha prestato attenzione ai rischi informatici e li ha affrontati nella proposta DORA, in modo da rafforzare la sicurezza informatica delle imprese finanziarie nell'UE.

Il campo di applicazione del DORA è molto ampio e viene definito nell'articolo 2; esso comprende tutte le entità finanziarie controllate, non solo gli istituti finanziari tradizionali, come banche, assicurazioni e imprese di investimento. Il DORA si applica anche a entità finanziarie meno tradizionali, come le agenzie di rating del credito, i repertori di dati sulle negoziazioni, gli istituti di pagamento e di moneta elettronica e le sedi di negoziazione. La causa di questo ampio campo d'applicazione deriva dal fatto che la minaccia data dai numerosi rischi cyber è onnipresente nel settore finanziario. Le nuove entità finanziarie basate sulla tecnologia dovrebbero mantenere fin dall'inizio alcune regole di base per *l'igiene informatica*. E' da considerare che, anche se soprattutto le FinTech più giovani si troveranno per la prima volta ad affrontare la normativa DORA in materia di cyber, ciò non risulta eccessivo, dal momento che il DORA contiene un quadro semplificato di gestione del rischio ICT per queste microimprese, così come per le piccole e medie imprese. Il DORA non si applicherà alle società di revisione, perché l'obiettivo del regolamento è quello di rafforzare la resilienza informatica degli enti finanziari, e i revisori contabili non sono imprese finanziarie e non sono nemmeno controllati dalle autorità di vigilanza finanziaria.

Il DORA mira a stabilire un quadro completo sulla resilienza operativa digitale per le entità finanziarie dell'UE, per tale motivo i 5 pilastri su cui si fonda sono:

1. la gestione del rischio delle tecnologie dell'informazione e della comunicazione (ICT risk management)
2. la gestione, la classificazione e la segnalazione degli incidenti legati alle ICT (ICT-related incidents management)
3. la gestione del rischio ICT di terzi (ICT third-party risks management)
4. segnalazione di incidenti (information sharing)
5. i test di resilienza operativa digitale (digital operational resilience testing)

Per migliorare la loro resilienza informatica, le imprese finanziarie sono tenute, ai sensi dell'articolo 4 del regolamento, a istituire un quadro interno di governance e controllo per garantire una gestione efficace e prudente di tutti i rischi ICT. Ciò include l'istituzione di un organo di gestione per definire, approvare e supervisionare l'attuazione di tutte le disposizioni relative a un quadro di gestione del rischio ICT. Il quadro di gestione del rischio ICT deve includere strategie, politiche, procedure, protocolli e strumenti ICT necessari per proteggere adeguatamente tutte le informazioni e gli asset ICT e, ai sensi dell'articolo 7, identificare,

classificare e documentare adeguatamente tutte le funzioni aziendali supportate dalle ICT, i ruoli e le responsabilità, gli asset informativi e gli asset ICT che supportano tali funzioni, nonché i loro ruoli e le loro dipendenze dal rischio ICT.

L'articolo 9 del DORA obbliga le entità finanziarie a dotarsi di meccanismi per individuare tempestivamente le attività anomale. Al fine di garantire il ripristino dei sistemi e dei dati ICT con tempi di inattività minimi, interruzioni e perdite limitate, come parte del loro quadro di gestione del rischio TIC, le entità finanziarie devono sviluppare e documentare politiche di backup e metodi di ripristino, nonché una strategia di comunicazione. La gestione del rischio è un elemento importante, ma deve sempre essere attuata con misure adeguate al livello di rischio delle entità finanziarie. Una guida chiara da parte delle autorità di vigilanza europee su come mettere in pratica questi requisiti sarà sicuramente apprezzata dalle entità finanziarie interessate.

Negli ultimi anni, la portata e la natura delle entità finanziarie con fornitori di servizi terzi si sono evolute, in particolare nel campo della tecnologia. Il documento "G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector (2018)" afferma che gli organi direttivi delle entità sono responsabili e devono rispondere di un'efficace supervisione e dell'implementazione della gestione del rischio informatico di terzi. Sebbene in base alla DORA gli enti non possano esternalizzare le proprie responsabilità a terzi, il DORA prevede principi chiave per una sana gestione del rischio informatico di terzi e considera la complessità delle dipendenze legate all'ICT. Ciò potrebbe aiutare gli organi di governo a comprendere meglio i rischi di terzi.

Le entità finanziarie devono essere consapevoli della natura, della complessità e dell'importanza delle dipendenze legate all'ICT. Per questo motivo, le entità finanziarie devono mantenere un registro di informazioni in relazione a tutti gli accordi contrattuali sull'uso dei servizi ICT forniti da fornitori terzi. Il registro deve distinguere tra i servizi che coprono funzioni critiche o importanti e quelli che non lo sono. Il registro è un elemento chiave per la corretta gestione dei rischi legati a terzi. L'articolo 27 del DORA prevede disposizioni contrattuali fondamentali per garantire condizioni più equilibrate tra l'entità finanziaria e il fornitore di servizi di terzi. L'accordo contrattuale deve includere almeno disposizioni sull'accessibilità, la disponibilità e l'integrità, nonché disposizioni per garantire l'accesso, il recupero, le descrizioni dei livelli di servizio e il diritto di recesso, nonché l'obbligo del servizio di terze parti ICT di prestare assistenza in caso di incidente legato alle ICT. Le clausole contrattuali dovrebbero rafforzare soprattutto le entità finanziarie più piccole durante la negoziazione dei contratti con le aziende tecnologiche più prospere e dominanti, le cosiddette BigTech.

La segnalazione di incidenti legati all’ICT all'autorità di vigilanza è un elemento chiave della sicurezza informatica. La notifica offre una maggiore possibilità di comprendere e identificare meglio la fonte dell'incidente, di analizzare le potenziali ripercussioni e di richiedere assistenza. Una rapida notifica di un incidente potrebbe anche aiutare altri istituti a prepararsi meglio ad attacchi simili. Le autorità informate sono in grado di mettere in guardia e prevenire pubblicamente altri attacchi.

Purtroppo, le regole di segnalazione sono frammentate, esiste una frammentazione tra i settori e le giurisdizioni per quanto riguarda la portata di ciò che dovrebbe essere segnalato per un incidente informatico. Inoltre, le tempistiche per la segnalazione degli incidenti informatici e le modalità di utilizzo delle informazioni sugli incidenti informatici sono diverse nella maggior parte delle giurisdizioni. Questa è una sfida soprattutto per le istituzioni finanziarie che operano in più Paesi. Queste imprese si trovano ad affrontare diversi requisiti di segnalazione per un singolo incidente informatico. Inoltre, anche le autorità di vigilanza finanziaria ricevono informazioni eterogenee sugli incidenti.

Il DORA armonizza gli obblighi di segnalazione per tutti gli istituti finanziari con sede nell'UE. Le entità finanziarie devono stabilire e implementare un processo di gestione degli incidenti legati all'ICT per rilevare, gestire e notificare gli incidenti legati all'ICT. Mentre tutti gli incidenti devono essere registrati, le entità finanziarie devono riferire solo gli incidenti gravi all'autorità di vigilanza finanziaria. I criteri rilevanti per determinare un incidente grave sono, tra gli altri, la rilevanza dell'incidente sulla criticità dei servizi interessati, la durata dell'incidente e l'impatto economico. Le autorità di vigilanza europee sono incaricate di sviluppare standard tecnici di regolamentazione per stabilire il contenuto della notifica di minacce informatiche significative e modelli uniformi. La condivisione delle informazioni è fondamentale per raggiungere la resilienza informatica di cui il DORA tanto parla, per prevenire ulteriori danni da attacchi informatici. Pertanto, sarà importante che l'autorità di vigilanza finanziaria condivida le informazioni pertinenti con l'autorità NIS (Network Information Security). Le due autorità hanno ruoli diversi: l'autorità di vigilanza finanziaria si concentra sui potenziali impatti di un incidente sul sistema finanziario, mentre l'autorità per la sicurezza delle reti e dell'informazione deve analizzare i potenziali impatti sui fornitori di infrastrutture critiche di tutti i settori che sono essenziali per il funzionamento di una società e di un'economia.

Una volta che un'entità finanziaria ha raggiunto la maturità informatica, in quanto ha sviluppato e implementato un piano efficace e attuabile e un'infrastruttura per mantenere la sua attività resiliente, dovrebbe essere testata.

Il DORA obbliga le entità finanziarie a testare regolarmente la propria resilienza operativa e definisce standard comuni per i programmi di test. Essi dovrebbero includere anche valutazioni di vulnerabilità, analisi open-source e revisioni del codice sorgente. Il DORA impone alle entità finanziarie più grandi di effettuare almeno ogni tre anni un test di penetrazione guidato dalle minacce ("TLPT: threat led penetration test"). Il TLPT può essere effettuato in modo proporzionato alle dimensioni, alla scala, all'attività e al rischio complessivo dell'entità finanziaria. Il testo "G-7 Fundamental Elements for Threat-Led Penetration Testing" definisce il TLPT come: "un tentativo controllato di compromettere la resilienza informatica di un'entità simulando le tattiche, le tecniche e le procedure degli attori delle minacce reali. Si basa su informazioni mirate sulle minacce e si concentra sulle persone, i processi e la tecnologia di un'entità, con una conoscenza preliminare minima e un impatto sulle operazioni. Lo scopo della TLPT è valutare e fornire indicazioni sulle capacità di resilienza delle entità contro un incidente informatico simulato nel mondo reale. Il TLPT deve essere condotto entro un

ambito prestabilito e incorporare un processo di gestione del rischio per garantire un test controllato che riduca al minimo i rischi per le entità".

Il DORA risulta essere un regolamento innovativo per diversi motivi:

1. Armonizzazione delle regole: il DORA propone un quadro normativo comune per tutti gli Stati membri dell'UE, armonizzando le regole e riducendo le discrepanze tra le diverse giurisdizioni. In questo modo, le entità finanziarie saranno in grado di adottare un approccio coerente e standardizzato per affrontare i rischi informatici.
2. Supervisione delle ICT: il DORA prevede un approccio di supervisione basato sul rischio per valutare e monitorare la resilienza operativa delle entità finanziarie. Ciò include l'identificazione e la mitigazione dei rischi cyber, il monitoraggio delle risorse ICT e la pianificazione di strategie di ripristino in caso di incidenti.
3. Requisiti per i fornitori di servizi ICT: I fornitori di servizi ICT che forniscono servizi critici alle entità finanziarie saranno soggetti a requisiti specifici, inclusa la necessità di essere registrati presso un'autorità competente e di adottare misure appropriate per garantire la resilienza operativa.
4. Test di resilienza: Le entità finanziarie saranno tenute a condurre regolari test di resilienza ICT per valutare la loro capacità di resistere e riprendersi da incidenti informatici. Questi test devono essere basati su scenari realistici e tenere conto delle minacce emergenti.
5. Incident reporting: DORA stabilisce requisiti dettagliati per la segnalazione degli incidenti informatici alle autorità competenti, consentendo una rapida identificazione e risposta agli incidenti che potrebbero avere un impatto significativo sul sistema finanziario. Tale requisito deriva dalle Direttive NIS e PSD2 dove era già stato adottato in precedenza, ma il DORA lo rafforza.
6. Coordinamento e cooperazione: La direttiva prevede una stretta cooperazione tra le autorità nazionali e l'Unione Europea per garantire un efficace scambio di informazioni e coordinamento nella supervisione delle entità finanziarie e dei fornitori di servizi ICT.

In sintesi, il DORA è innovativo poiché affronta in modo proattivo i crescenti rischi informatici nel settore finanziario, promuovendo la resilienza operativa digitale di tutto il settore. In aggiunta, il tempismo del DORA non potrebbe essere migliore. La situazione delle minacce informatiche è allarmante, non solo per il settore finanziario. L'obiettivo principale del DORA è prevenire o almeno mitigare meglio le crescenti minacce informatiche nel settore finanziario. Per raggiungere questo obiettivo, il quadro DORA stabilisce le giuste priorità in materia di governance ICT, reporting e test. Sebbene alcune parti del DORA siano piuttosto prescrittive, l'approccio basato sul rischio del DORA porterà a un'applicazione equilibrata dei requisiti.

2.3 Metodologie di identificazione e valutazione di rischi cyber

L'identificazione e la valutazione dei rischi cyber sono un processo fondamentale per proteggere le attività e le risorse di un'organizzazione dalle minacce informatiche. Ci sono diverse metodologie che possono essere utilizzate per identificare e valutare i rischi cyber.

Tendenzialmente si fa una distinzione tra metodologie quantitative e qualitative; le prime rappresentano il calcolo della probabilità che l'evento dannoso accada e stimano l'impatto e la quantità della perdita, mentre le seconde fanno una classificazione qualitative (es. in "alto", "medio", "basso") in base all'impatto delle minacce e solitamente fanno uso di policy aziendali per seguire uno schema di controlli, classificazioni e così via.

Le principali tecniche che queste metodologie utilizzano sono:

1. Analisi dei requisiti di sicurezza: questa tecnica prevede la valutazione dei requisiti di sicurezza e delle policy adottate dall'organizzazione, per individuare le vulnerabilità e le minacce. Ciò include la valutazione delle attività aziendali, dei processi e delle tecnologie utilizzate, nonché degli obiettivi aziendali e delle normative applicabili.
2. Analisi dei punti deboli: questa tecnica prevede l'identificazione dei punti deboli del sistema informatico dell'organizzazione, tra cui le vulnerabilità, le lacune di sicurezza e gli errori umani. Ciò include anche la valutazione dei sistemi di sicurezza esistenti per garantire che siano adeguati per proteggere contro le minacce cyber.
3. Analisi delle minacce: questa tecnica prevede l'identificazione delle minacce cyber attuali e potenziali, tra cui malware, phishing, attacchi DDoS e vulnerabilità zero-day. Ciò include anche la valutazione della gravità di tali minacce e delle loro probabilità di verificarsi.
4. Analisi degli impatti: questa tecnica prevede la valutazione degli impatti che potrebbero derivare da una violazione della sicurezza informatica, come ad esempio la perdita di dati, la violazione della privacy, la perdita finanziaria e la compromissione della reputazione dell'organizzazione.
5. Test di penetrazione: questa tecnica prevede la simulazione di un attacco informatico per valutare la capacità del sistema di resistere alle minacce. Ciò include la verifica della robustezza della sicurezza informatica e la valutazione delle vulnerabilità e dei punti deboli.

In sintesi, queste sono solo alcune delle tecniche che possono essere utilizzate per identificare e valutare i rischi cyber. La scelta di quale usare dipende dalle specifiche esigenze e obiettivi dell'organizzazione e dovrebbe essere effettuata da professionisti esperti in sicurezza informatica.

Le varie metodologie di analisi e valutazione dei rischi cyber adottano una o più delle tecniche indicate sopra sulla base di valutazioni quali la disponibilità dei dati a corredo, la criticità delle risorse ICT da valutare, tempi, costi e così via.

2.3.1 Metodologie di valutazione degli impatti e delle perdite

Le metodologie di valutazione degli impatti e delle perdite nei rischi cyber sono strumenti utilizzati per valutare gli effetti di potenziali incidenti informatici sulle attività aziendali e sui beni informativi dell'organizzazione. Queste metodologie possono essere utilizzate per valutare i rischi ICT e Cyber, valutare le minacce e le vulnerabilità, assegnare priorità ai rischi, pianificare le misure di mitigazione e valutare l'efficacia delle misure di sicurezza informatica adottate. Le metodologie usate per valutare gli impatti e le perdite nei rischi cyber sono diverse e variano a seconda dell'organizzazione, delle esigenze specifiche e del contesto in cui sono utilizzate. Tuttavia, alcune delle metodologie più comuni includono:

1. Business Impact Analysis (BIA): questa metodologia si concentra sull'analisi degli impatti degli incidenti informatici sulle attività aziendali, in particolare sulla continuità operativa dell'organizzazione. La BIA valuta l'impatto di potenziali interruzioni dei servizi, dei sistemi o delle applicazioni sull'operatività aziendale e sulle attività quotidiane dell'organizzazione e sulle attività di ripristino. Essa comprende una componente esplorativa per rivelare eventuali minacce e vulnerabilità e una componente di pianificazione per sviluppare strategie di minimizzazione del rischio. Il risultato è un rapporto di analisi dell'impatto sul business, che descrive i rischi potenziali specifici dell'organizzazione studiata. Uno degli assunti di base di una BIA è che ogni componente dell'organizzazione si basa sul funzionamento continuo di tutti gli altri. Tuttavia, alcuni sono più cruciali di altri e richiedono una maggiore allocazione di fondi e risorse operative in caso di disastro. Ad esempio, un'azienda può essere in grado di continuare più o meno normalmente se la mensa deve chiudere, ma si fermerebbe completamente se i sistemi informativi e l'infrastruttura IT si bloccassero

	Fire in data center	Loss of specialized staff	Vehicle crash in front entrance of office building	Vandalism to primary product assembly line	Loss of staff due to COVID-19 illness
BUSINESS ACTIVITY AFFECTED	All activities in data center	Activities that require specialized staff	All activities at that location unless an alternate access option is available	Loss of primary production line	Loss of possibly key employees needed to run the business
POTENTIAL OPERATIONAL LOSS	Inability to function normally	Reduced ability to function normally	Nominal disruption based on how quickly the vehicle can be removed and the front entrance reopened	Inability to produce the company's primary product	May be nominal to significant depending on who is affected
POTENTIAL FINANCIAL LOSS	$3,000 to $4,000 revenue loss per hour	None, assuming backup staff is available	None, assuming alternate entrance is available and access to building facilities is available	$25,000 to $40,000 per hour in lost revenue	Could be minimal assuming employees can work remotely
MINIMUM TIME NEEDED TO RECOVER OPERATIONS	Three to four hours	One to two hours	Depending on the damage from the crash, up to one day	Days if a workaround can be built; weeks if an alternate production facility must be found and launched	24-48 hours depending on health status and if employees can work remotely

Figura 12: Gli elementi di una Business Impact Analysis[25]

Le BIA hanno molti obiettivi. Vengono utilizzate per determinare le funzioni aziendali più cruciali, i sistemi, il personale e le risorse tecnologiche necessarie per un funzionamento ottimale. Vengono inoltre utilizzate per valutare il periodo di tempo entro il quale le funzioni devono essere recuperate per riportare l'organizzazione a uno stato di funzionamento normale. L'analisi può essere manuale o assistita da computer. Le sfide includono la determinazione dell'impatto sui ricavi di una funzione aziendale e la quantificazione dell'impatto a lungo termine della perdita di quote di mercato, reputazione aziendale o clienti. Gli impatti da considerare sono innumerevoli, come ad esempio i ritardi nelle vendite o nel reddito, l'aumento delle spese di manodopera, le multe normative, le sanzioni contrattuali, l'insoddisfazione dei clienti, ecc. In questo caso la BIA non deve essere confusa con la Risk Assessment in quanto esse sono due processi distinti ma complementari che sono utilizzati per gestire i rischi aziendali. Una risk assessment è incentrata sulla valutazione dei potenziali rischi associati a una determinata attività, processo o situazione, mentre la BIA si concentra sulla valutazione degli impatti che possono derivare da un'interruzione del business. La differenza principale tra una risk assessment e una BIA è che la prima si concentra sulla valutazione dei rischi potenziali, mentre la seconda si concentra sugli impatti finanziari e operativi dell'interruzione delle attività aziendali. Entrambi i processi sono importanti per gestire i rischi aziendali e possono essere utilizzati in combinazione per creare una strategia completa di gestione del rischio

Figura 13: Come la BIA e la Risk Assessment interagiscono[26]

2. Economic Loss Quantification (ELQ): questa metodologia si concentra sull'analisi delle perdite economiche che possono derivare da incidenti informatici. L'ELQ valuta i costi diretti e indiretti associati agli incidenti informatici, come ad esempio i costi di riparazione, i costi di interruzione dell'attività e i costi di reputazione.

[25] Fonte: Paul Kirvan, Carlos Sliwa, "Business Impact Analysis", Maggio 2022.
[26] Fonte: Paul Kirvan, Carlos Sliwa, "Business Impact Analysis", Maggio 2022

3. Risk Assessment Methodology for Information Systems (RAMIS): questa metodologia è stata sviluppata dal National Institute of Standards and Technology (NIST) degli Stati Uniti e si concentra sulla valutazione dei rischi informatici per i sistemi informativi. La RAMIS valuta gli impatti di potenziali incidenti informatici sui sistemi informativi, sui dati e sui processi aziendali. La peculiarità di questa metodologia è quella di eseguire l'analisi del rischio di sicurezza delle informazioni utilizzando l'opinione pubblica, la quale si ottiene conducendo un sondaggio. Il RAMIS è fondamentalmente un processo di preparazione e conduzione di un sondaggio per valutare i rischi per la sicurezza in un'organizzazione. Il sondaggio è composto da domande e risposte relative al problema della sicurezza informatica. Manager, direttori, personale tecnico e personale abituale sono i candidati a rispondere alle domande del sondaggio. L'obiettivo del sondaggio è capire l'effetto del problema della sicurezza delle informazioni sul sistema o sull'organizzazione. In altre parole, condurre un'indagine è un po' come fare un'analisi as-is[27]. La RAMIS effettua un'analisi strutturata dell'as-is per valutare il rischio causato dal problema di sicurezza delle informazioni. La preparazione e la conduzione dell'indagine e l'ottenimento di un risultato sul rischio dall'indagine sono definite in base a fasi ben definite. Il modello di rischio sottostante al RAMIS si basa su una formula di rischio fondamentale e semplice dove il Risk rappresenta la probabilità che si verifichi una violazione della sicurezza e l'incognita X le conseguenze della violazione della sicurezza.

$$Risk = \left(\frac{\sum_m [\tau_1(\sum_i w_i * p_i)]}{m}\right) * \left(\frac{\sum_n [\tau_2(\sum_j w_j * p_j)]}{n}\right)$$

In RAMIS vengono condotti due processi di indagine separati e indipendenti per i due parametri di rischio, ovvero la probabilità che si verifichi una violazione della sicurezza e le conseguenze di tale violazione. I parametri contenuti nel modello di rischio RAMIS sono:

- i: Il numero di domande per l'indagine volta a stimare il parametro della probabilità che si verifichi una violazione della sicurezza
- j: il numero di domande per l'indagine volta a stimare le conseguenze del verificarsi di una violazione della sicurezza,
- m: Il numero di partecipanti al sondaggio per stimare la probabilità di occorrenza della violazione della sicurezza
- n: Il numero di partecipanti al sondaggio per stimare le conseguenze del verificarsi di una violazione della sicurezza
- w: Peso della domanda
- p: Valore dell'opzione di risposta
- τ_1: Tabella di rischio per analizzare il risultato della probabilità di

[27] L'analisi "as-is" è una metodologia utilizzata per comprendere e documentare la situazione corrente di un'organizzazione, un processo o un sistema. È un passo fondamentale nella gestione del cambiamento e nello sviluppo di soluzioni migliorate o nuovi processi

- di violazione della sicurezza
- τ_2: tabella dei rischi per analizzare il risultato delle conseguenze del
- di una violazione della sicurezza
- Risk: Singolo valore numerico per rappresentare il rischio

La metodologia RAMIS si compone di sette fasi principali. Nella prima fase, si verifica la consapevolezza del problema della sicurezza delle informazioni. Successivamente, il processo RAMIS si divide in due sottoprocessi paralleli. Uno di questi sottoprocessi riguarda la probabilità che si verifichi una violazione della sicurezza e l'altro le conseguenze di tale violazione. Ci si concentrerà però solo sul sottoprocesso relativo alla probabilità di occorrenza della violazione della sicurezza. Il lavoro svolto sarà lo stesso per gli altri parametri di rischio. Nella seconda fase di RAMIS, si elencano tutti i fattori che possono influenzare la probabilità che si verifichi una violazione della sicurezza. Questa è una parte fondamentale perché fa si che si ottengano risultati realistici e oggettivi. Tutte le persone coinvolte in questo passaggio devono avere una prospettiva generale di sicurezza e provenire dall'azienda stessa, dato che, affinché questo processo abbia successo, almeno tre persone devono partecipare all'elenco dei fattori. Queste persone devono avere una conoscenza sufficiente del problema della sicurezza delle informazioni, dei suoi effetti e delle sue probabili cause. Dopo aver elencato tutti i possibili fattori per il parametro di rischio di base, si assegnano valori numerici ai fattori per ponderare ciascun fattore. Il fattore di ponderazione viene utilizzato perché i fattori elencati non influenzano la probabilità in modo uguale; infatti, un fattore può avere un effetto maggiore sulla probabilità di accadimento rispetto all'altro. Successivamente nella terza fase di RAMIS, i fattori vengono convertiti in domande del sondaggio e vengono determinate le opzioni di risposta per ogni domanda. Tutte le domande devono avere lo stesso numero di opzioni per un'analisi coerente dei risultati. Di norma, per un'analisi efficace si suggeriscono almeno quattro opzioni di risposta. Come già visto con i fattori, anche le opzioni di risposta alle domande devono essere selezionate con cura, infatti le risposte selezionate dai partecipanti al sondaggio saranno i principali elementi di valutazione del rischio. Pertanto, è necessario fornire alcune differenziazioni tra le risposte di una domanda. Le scelte devono essere selezionate in modo che ogni scelta rappresenti un diverso livello di rischio. Le scelte delle domande devono essere disposte in modo tale che la prima scelta sia quella che influisce maggiormente sulla probabilità che si verifichi una violazione della sicurezza, mentre l'opzione di risposta che influisce meno dovrebbe essere l'ultima. Nel caso di un'analisi quantitativa, le opzioni di risposta saranno convertite in numeri. Nella quarta fase vengono preparate le tabelle dei rischi. Queste tabelle scalano i parametri di rischio fondamentali sia dal punto di vista quantitativo che qualitativo sulla base dei risultati dell'indagine. Queste tabelle sono i principali punti di riferimento per la valutazione dei risultati dell'indagine, in quanto scalano i possibili risultati dell'indagine per due parametri di rischio fondamentali. Le tabelle di rischio sono tabelle dinamiche, ovvero il loro contenuto cambia in base alle

diverse indagini condotte. Una tabella di rischio costituisce un collegamento tra il risultato dell'indagine e i valori quantitativi e qualitativi del parametro di rischio considerato.

Una volta terminata la preparazione delle tabelle di rischio, si procede all'indagine, la quale è la quinta fase di RAMIS. Questa fase è la parte più particolare del RAMIS, in cui i normali utenti del sistema informativo partecipano attivamente al processo di analisi del rischio. Le risposte alle domande del sondaggio sono già informazioni preziose per l'intero processo di analisi del rischio. Tuttavia, lo scopo principale di RAMIS è quello di convertire queste risposte in valori numerici e calcolare un singolo valore di rischio. Nella sesta fase di RAMIS, viene applicata la formula scritta precedentemente, per ottenere i risultati quantitativi dalle risposte ai sondaggi. Durante questo processo quantitativo, vengono utilizzate le tabelle di rischio per ottenere risultati quantitativi oggettivi. Infine, l'ultima fase del RAMIS è la fase di valutazione. Nella fase di valutazione, non vengono valutati solo i risultati numerici del sondaggio, ottenuti nella fase precedente, ma vengono esaminate anche le singole scelte di risposta dei partecipanti al sondaggio.

Tutte queste fasi consentono la partecipazione attiva dei manager e del personale al processo di analisi del rischio. In tutte queste fasi non vengono utilizzati complicati strumenti matematici. Il numero di domande del sondaggio, i tipi di domande e le strutture delle tabelle dei rischi possono essere modificati in base al problema della sicurezza delle informazioni. La flessibilità del metodo consente a RAMIS di essere applicato efficacemente a diversi problemi di sicurezza informatica.

4. Failure Modes and Effects Analysis (FMEA): questa metodologia si concentra sull'analisi delle modalità di guasto e degli effetti degli incidenti informatici sui sistemi informativi. La FMEA valuta gli impatti di potenziali guasti dei sistemi informativi e delle applicazioni sull'operatività aziendale e sulle attività quotidiane dell'organizzazione. I guasti vengono classificati in base alla gravità delle loro conseguenze, alla frequenza con cui si verificano e alla facilità con cui possono essere rilevati. Lo scopo dell'FMEA è quello di intraprendere azioni per eliminare o ridurre i guasti, iniziando da quelli a più alta priorità. Questa metodologia si articola in 5 fasi normalmente: una fase preliminare dove si decidono gli obbiettivi da raggiungere, il perimetro di analisi, la raccolta di dati e si costituisce il gruppo di lavoro, dopodiché vi è una fase qualitativa dove si analizzano i modi di guasto, le cause e gli effetti, poi vi è la fase quantitativa dove si decidono gli indici di rischio e le priorità di intervento, infine ci sono la fase correttiva e di valutazione che sviluppano le azioni per ridurre il rischio e ne definiscono altrettante per valutare l’efficienza del modello.

Function	Potential Failure Mode	Potential Effects(s) of Failure	S	Potential Cause(s) of Failure	O	Current Process Controls	D	RPN	CRIT	Recommended Action(s)	Responsibility and Target Completion Date	Action Results					
												Action Taken	S	O	D	RPN	CRIT
Dispense amount of cash requested by customer	Does not dispense cash	Customer very dissatisfied Incorrect entry to demand deposit system Discrepancy in cash balancing	8	Out of cash Machine jams Power failure during transaction	5 3 2	Internal low-cash alert Internal jam alert None	5 10 10	200 240 160	45 24 16								
	Dispenses too much cash	Bank loses money Discrepancy in cash balancing	6	Bills stuck together Denominations in wrong trays	2 3	Loading procedure (riffle ends of stack) Two-person visual verification	7 4	84 72	12 18								
	Takes too long to dispense cash	Customer somewhat annoyed	3	Heavy computer network traffic Power interruption during transaction	7 2	None None	10 10	210 60	21 6								

Figura 14: Esempio di metodologia FMEA[28]

In sintesi, le metodologie di valutazione degli impatti e delle perdite nei rischi cyber sono utili strumenti per valutare gli effetti di potenziali incidenti informatici sulle attività aziendali e sui beni informativi dell'organizzazione. Tuttavia, è importante scegliere la metodologia più adatta alle esigenze specifiche dell'organizzazione e di adattarla al contesto in cui viene utilizzata.

2.3.2 Metodologie di valutazione della probabilità di accadimento delle minacce cyber

La valutazione della probabilità di accadimento delle minacce cyber è un processo cruciale per identificare e gestire i rischi informatici. Le principali metodologie di valutazione della probabilità di accadimento delle minacce cyber sono:

1. Analisi qualitativa del rischio: Questa metodologia si basa sull'esperienza, l'intuizione e il giudizio degli esperti per determinare la probabilità di accadimento di una minaccia cyber. Si utilizzano scale qualitative, come ad esempio bassa, media o alta, per esprimere la probabilità.
2. Analisi quantitativa del rischio: L'analisi quantitativa cerca di assegnare valori numerici alla probabilità di accadimento delle minacce cyber, utilizzando modelli matematici e statistiche. In questo modo, è possibile ottenere una stima più precisa e basata sui dati.
3. Framework OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): OCTAVE è un framework di valutazione del rischio informatico che include l'identificazione delle minacce,

[28] Fonte: Nancy R. Tague, "The Quality Toolbox, second edition", 2005

l'analisi delle vulnerabilità e la determinazione degli impatti. Il processo OCTAVE combina sia elementi qualitativi che quantitativi per determinare la probabilità di accadimento delle minacce cyber. A differenza della maggior parte degli altri metodi di valutazione del rischio, l'approccio OCTAVE è guidato dal rischio operativo e dalle pratiche di sicurezza e non dalla tecnologia. È stato progettato per consentire a un'organizzazione di:

- dirigere e gestire autonomamente le valutazioni del rischio per la sicurezza delle informazioni
- Prendere le decisioni migliori in base ai propri rischi specifici
- Concentrarsi sulla protezione delle risorse informative chiave
- Comunicare efficacemente le informazioni chiave sulla sicurezza

La metodologia OCTAVE è organizzata intorno a tre aspetti fondamentali che consentono al personale dell'organizzazione di ottenere un quadro completo delle esigenze di sicurezza delle informazioni dell'organizzazione. Le fasi sono:

- Build Asset-Based Threat Profiles: Si tratta di una valutazione organizzativa in cui si determina cosa è importante per l'organizzazione (risorse informatiche) e cosa viene fatto attualmente per proteggere tali risorse. Vengono selezionati quindi gli asset più importanti per l'organizzazione (asset critici) e vengono descritti i requisiti di sicurezza per ciascun asset critico. Infine, si identificano le minacce per ogni asset critico, creando un profilo di minaccia per quell'asset.
- Identify Infrastructure Vulnerabilities: Si tratta di una valutazione dell'infrastruttura informatica in cui si esaminano i percorsi di accesso alla rete, identificando le classi di componenti informatici relativi a ciascun asset critico e viene successivamente determinato il grado di resistenza di ciascuna classe di componenti agli attacchi di rete.
- Develop Security Strategy and Plans: Durante questa parte della valutazione si identificano i rischi per gli asset critici dell'organizzazione e si decide cosa fare al riguardo. Viene creata una strategia di protezione per l'organizzazione e piani di mitigazione per affrontare i rischi per gli asset critici, sulla base di un'analisi delle informazioni raccolte.

4. Metodo FAIR (Factor Analysis of Information Risk): FAIR è un modello di valutazione del rischio basato su fattori che quantifica il rischio informatico in termini di probabilità e impatto finanziario. Si basa sull'analisi di diversi fattori, come la frequenza delle minacce, la vulnerabilità delle risorse e l'impatto potenziale.
5. CVSS (Common Vulnerability Scoring System): Il CVSS è uno standard di settore per valutare la gravità delle vulnerabilità informatiche. Sebbene non sia specificamente focalizzato sulla probabilità di accadimento delle minacce cyber, il CVSS può essere utilizzato per stimare la probabilità basandosi sul punteggio di gravità assegnato a una vulnerabilità. Questa metodologia offre i seguenti servizi:
    - Punteggi di vulnerabilità standardizzati: Quando un'organizzazione normalizza i punteggi di vulnerabilità su tutte le sue piattaforme software e hardware, può sfruttare un'unica politica di

gestione delle vulnerabilità. Questa politica può essere simile a un accordo sui livelli di servizio che stabilisce la velocità con cui una particolare vulnerabilità deve essere convalidata e risolta.

- Struttura aperta: Gli utenti possono essere confusi quando a una vulnerabilità viene assegnato un punteggio arbitrario. "Quali proprietà gli hanno assegnato quel punteggio? In cosa differisce da quella rilasciata ieri?". Con CVSS, chiunque può vedere le singole caratteristiche utilizzate per ottenere un punteggio.
- Rischio prioritario: quando viene calcolato il punteggio ambientale, la vulnerabilità diventa contestuale. In altre parole, i punteggi di vulnerabilità sono ora rappresentativi del rischio effettivo per un'organizzazione. Gli utenti sanno quanto è importante una determinata vulnerabilità in relazione ad altre vulnerabilità.

Per spiegare brevemente il funzionamento della metodologia, essa si basa su tre gruppi di metriche: Base, Temporale ed Ambientale; quella Base rappresenta le caratteristiche intrinseche e fondamentali di una vulnerabilità che sono costanti nel tempo e negli ambienti di utilizzo, quella Temporale rappresenta le caratteristiche di una vulnerabilità che cambiano nel tempo, ma non tra gli ambienti di utilizzo, mentre quella Ambientale rappresenta le caratteristiche di una vulnerabilità che sono rilevanti e uniche per l'ambiente di un particolare utente. Lo scopo del gruppo di base è quello di definire e comunicare le caratteristiche fondamentali di una vulnerabilità. In questa maniera la metodologia utilizza un approccio oggettivo alla caratterizzazione delle vulnerabilità fornisce agli utenti una rappresentazione chiara e intuitiva di una vulnerabilità e una tassonomia comune per la descrizione. Gli utenti possono quindi invocare i gruppi temporali e ambientali per fornire informazioni contestuali che riflettono più accuratamente il rischio per il loro ambiente specifico. Ciò consente di prendere decisioni più informate quando si cerca di mitigare i rischi posti dalle vulnerabilità. La metodologia implica che alle metriche di base vengono assegnati dei valori, l'equazione di base calcola un punteggio che va da 0 a 10 e crea un vettore. Il vettore, che è una stringa di testo che contiene i valori assegnati a ciascuna metrica, facilita la natura "aperta" del framework. Esso viene utilizzato per comunicare esattamente come è stato ricavato il punteggio di ogni vulnerabilità, in modo che chiunque possa capire il meccanismo e, se lo desidera, confermare la validità di ogni metrica. Pertanto, il vettore dovrebbe sempre essere visualizzato insieme al punteggio della vulnerabilità.

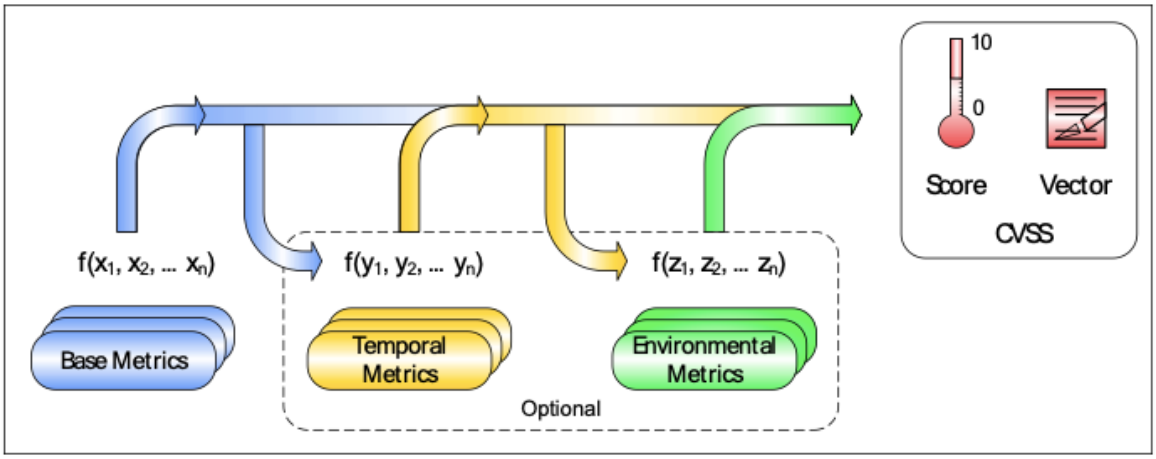


Figura 15: Metodologia CVSS[29]

6. Tecniche di simulazione: Metodi come il Monte Carlo o la Simulazione di Eventi Discreti possono essere utilizzati per stimare la probabilità di accadimento delle minacce cyber. Questi metodi si basano sull'esecuzione di numerosi scenari ipotetici e sull'analisi delle loro conseguenze per determinare la probabilità di accadimento delle minacce. È importante notare che nessuna metodologia è perfetta e che spesso è consigliabile combinare più approcci per ottenere una valutazione della probabilità di accadimento delle minacce cyber più accurata e completa

2.3.3 Metodologie di valutazione degli scenari di rischio cyber

Le metodologie di valutazione degli scenari di rischio cyber sono processi sistematici utilizzati per identificare, analizzare e quantificare le vulnerabilità e le minacce informatiche che potrebbero compromettere la sicurezza delle informazioni e delle infrastrutture IT. Queste metodologie consentono alle organizzazioni di prendere decisioni informate e di implementare contromisure appropriate per ridurre i rischi.

Esistono diverse metodologie di valutazione del rischio cyber, tra cui:

1. Framework NIST (National Institute of Standards and Technology): Il framework NIST è uno standard ampiamente adottato che fornisce linee guida per la gestione del rischio informatico. Il NIST SP 800-30, o "Guide for Conducting Risk Assessments", è una pubblicazione del National Institute of Standards and Technology (NIST) che fornisce un approccio strutturato alla valutazione del rischio nel contesto della sicurezza informatica. La guida fa parte della più ampia serie Special Publication 800 del NIST, che si concentra su vari aspetti della sicurezza informatica e delle informazioni. La pubblicazione NIST SP 800-30 viene utilizzata per tradurre il rischio informatico in un modo comprensibile per il consiglio di amministrazione e l'amministratore delegato. Esso ha l'obiettivo di aiutare le organizzazioni a comprendere e implementare un processo di valutazione del rischio

[29] Fonte: Peter Mell, Karen Scarfone, Sasha Romanosky, "The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems", Agosto 2007, NIST Interagency Report 7435.

completo, in grado di identificare le minacce, le vulnerabilità e i rischi potenziali per i sistemi e le risorse informatiche. I componenti principali di questo processo sono:

- Preparazione della valutazione del rischio: questa fase prevede la definizione dell'ambito, degli obiettivi e dei confini della valutazione del rischio, nonché l'identificazione delle parti interessate e delle risorse necessarie per il processo.
- Conduzione della valutazione del rischio: essa avviene attraverso l'identificazione delle minacce (le potenziali fonti di danno ai sistemi informativi e agli asset dell'organizzazione, come disastri naturali, attacchi informatici o minacce interne), l'identificazione delle vulnerabilità (analizzare i sistemi informativi e gli asset dell'organizzazione per determinare i potenziali punti deboli che potrebbero essere sfruttati dalle fonti di minaccia), la valutazione dell'impatto (stimare il danno potenziale per l'organizzazione se una minaccia dovesse sfruttare una vulnerabilità, considerando fattori quali la perdita finanziaria, l'interruzione operativa e il danno alla reputazione), la valutazione il rischio (determinare il livello di rischio complessivo considerando la probabilità che una minaccia sfrutti una vulnerabilità e il conseguente impatto sull'organizzazione) e la priorità del rischio (dare una priorità ai rischi in base al loro livello di rischio complessivo, per aiutare le organizzazioni a concentrarsi prima sui rischi più significativi)
- Comunicazione e condivisione delle informazioni sulla valutazione del rischio: questa fase prevede la condivisione dei risultati della valutazione del rischio con le parti interessate, come i responsabili delle decisioni, i gestori del rischio e il personale addetto alla sicurezza, per consentire un processo decisionale informato e la pianificazione della riduzione del rischio.
- Mantenimento e aggiornamento della valutazione del rischio: le valutazioni del rischio devono essere continuamente aggiornate e mantenute per garantire che il profilo di rischio dell'organizzazione rimanga accurato e aggiornato. Ciò comporta la revisione e il riesame periodico delle valutazioni del rischio in base ai cambiamenti dell'ambiente, della tecnologia o del panorama delle minacce dell'organizzazione.

Seguendo le linee guida del NIST SP 800-30, le organizzazioni possono stabilire un solido processo di valutazione del rischio che le aiuti a identificare e gestire i rischi per i loro sistemi informativi e le loro risorse, migliorando in ultima analisi la loro posizione complessiva di cybersecurity.

2. ISO/IEC 27005: Lo standard ISO/IEC 27005 fornisce linee guida per la gestione del rischio informatico, in linea con i principi del sistema di gestione della sicurezza delle informazioni stabilito dall'ISO/IEC 27001. Questo standard copre l'intero ciclo di vita della gestione del rischio, dalla valutazione alla mitigazione e alla revisione. L'innovazione più importante in merito alla seguente normativa è che l'identificazione del rischio non si baserà più su degli asset ma su degli eventi.

Attraverso questo approccio si creano degli scenari strategici basati sull'accadimento di determinate minacce e la maniera con cui esse impattano il rischio.

3. La Metodologia IRAM2: tale metodologia è stata sviluppata dall'Information Security Forum (ISF), la quale è una organizzazione globale indipendente che fornisce informazioni e supporto per la gestione della sicurezza informatica alle aziende e alle organizzazioni di tutti i settori e dimensioni. La metodologia di identificazione e misurazione dei rischi cyber proposta dall'ISF viene identificata con l'acronimo IRAM2, che sta per Information Risk Assesment 2 ed è una metodologia prettamente pratica che ha come obbiettivo aiutare le aziende contro i rischi cyber e tutte le minacce da loro comportati. La IRAM2 prevede diversi passaggi, tra cui:
   - Identificazione dei beni informativi critici: in questa fase, vengono identificati i beni informativi critici dell'organizzazione, come ad esempio dati personali dei clienti, proprietà intellettuale, informazioni finanziarie, ecc. Questi beni informativi sono i punti focali dell'analisi dei rischi cyber.
   - Identificazione delle minacce: in questa fase, vengono identificate le minacce che possono compromettere i beni informativi critici dell'organizzazione. Queste minacce possono includere attacchi informatici esterni, errori umani, malintenzionati interni, disastri naturali, ecc.
   - Identificazione delle vulnerabilità: in questa fase, vengono identificate le vulnerabilità dei sistemi informatici e delle applicazioni utilizzate dall'organizzazione. Queste vulnerabilità possono essere utilizzate dai malintenzionati per compromettere i beni informativi critici.
   - Valutazione della probabilità e dell'impatto: in questa fase, vengono valutate la probabilità che le minacce sfruttino le vulnerabilità e l'impatto che queste minacce potrebbero avere sui beni informativi critici. Questa valutazione si basa sull'analisi dei dati storici e sulle conoscenze degli esperti.
   - Prioritizzazione dei rischi: in questa fase, vengono assegnate priorità ai rischi identificati in base alla probabilità e all'impatto. Questa priorizzazione consente all'organizzazione di concentrarsi sui rischi più critici per i beni informativi.
   - Pianificazione delle misure di mitigazione: in questa fase, vengono pianificate le misure di mitigazione dei rischi. Queste misure possono includere la riduzione della probabilità delle minacce, la riduzione dell'impatto dei rischi, la prevenzione delle minacce, la rilevazione e risposta alle minacce, la resilienza e il ripristino dei servizi.
   - Monitoraggio e valutazione continua: in questa fase, vengono monitorati i rischi e le misure di mitigazione adottate e viene effettuata una valutazione continua della loro efficacia. Questo processo consente all'organizzazione di adattarsi ai cambiamenti dell'ambiente informatico e di garantire che la sicurezza informatica sia allineata con gli obiettivi aziendali.

4. Metodo CORAS (A Model-driven Method for Security Risk Analysis): CORAS è una metodologia di analisi dei rischi basata su modelli che integra tecniche qualitative e quantitative. L'obiettivo principale di CORAS è di fornire una valutazione del rischio accurata e affidabile che supporti la presa di decisioni e la pianificazione della sicurezza.

Indipendentemente dalla metodologia scelta, la valutazione degli scenari di rischio cyber dovrebbe essere un processo continuo e iterativo, in quanto le minacce e le vulnerabilità possono evolversi rapidamente. La valutazione del rischio consente alle organizzazioni di essere proattive nella protezione delle loro risorse e nella mitigazione delle potenziali minacce.

2.4 Processo di analisi dei rischi cyber

Il processo di analisi dei rischi cyber è una procedura strutturata che aiuta le organizzazioni a identificare, valutare e affrontare i rischi legati alla sicurezza informatica. L'obiettivo principale dell'analisi dei rischi cyber è proteggere le informazioni e gli asset digitali di un'organizzazione da minacce potenziali e vulnerabilità. Il processo di analisi dei rischi cyber può essere suddiviso in diverse fasi, tra cui:

1. Creare un risk management team specializzato sui rischi cyber
2. Identificazione degli asset: individuare e catalogare gli asset digitali dell'organizzazione, come server, reti, dispositivi, dati e software. Questo permette di avere un quadro completo delle risorse che necessitano di protezione. In aggiunta si dovrebbe catalogate il software-as-a-service, la piattaforma-as-a-service e l'infrastruttura-as-a-service utilizzati da ogni reparto, specificando quali reparti e fornitori hanno accesso a questi servizi. I tipi di dati dovrebbero essere classificati, specialmente in base alla loro sensibilità, in questo modo si riesce a tracciare le informazioni che viaggiano attraverso la rete e tra gli stakeholder.
3. Valutazione delle minacce: Questa fase comporta l'identificazione delle minacce potenziali che potrebbero compromettere la sicurezza degli asset digitali. Le minacce possono includere attacchi informatici, malware, errori umani, disastri naturali e interruzioni del servizio.
4. Identificazione delle vulnerabilità: Il team di gestione del rischio deve identificare le minacce e le vulnerabilità da tutte le parti dell'organizzazione, ovvero si identificano le vulnerabilità presenti nei sistemi e nelle infrastrutture IT dell'organizzazione. Questo può essere fatto attraverso l'uso di strumenti di scansione delle vulnerabilità, test di penetrazione, revisioni della configurazione e analisi del codice sorgente.
5. Valutazione dei rischi: Una volta identificate le minacce e le vulnerabilità, si procede alla valutazione dei rischi associati. Si stima la probabilità che una minaccia sfrutti una vulnerabilità e l'impatto che ciò avrebbe sull'organizzazione. In base a queste informazioni, si può assegnare un livello di rischio a ciascuna combinazione di minaccia e vulnerabilità.

6. Trattamento dei rischi: Dopo aver valutato i rischi, si devono sviluppare e implementare strategie per il loro trattamento. Questo può includere l'identificazione di misure di sicurezza che lo mitigano quando il rischio è superiore alla soglia di accettazione del rischio definita dalla banca, l'accettazione è inferiore alla soglia di accettazione del rischio definita dalla banca, il trasferimento del rischio sottoscrivendo, ad esempio, un'assicurazione e l'eliminazione quando il rischio non può essere mitigato, accettato o trasferito.
7. Monitoraggio e revisione: Infine, è fondamentale monitorare e rivedere regolarmente il processo di analisi dei rischi cyber. Ciò aiuta a garantire che le misure di sicurezza siano efficaci e che i nuovi rischi vengano identificati e affrontati tempestivamente.

L'analisi dei rischi cyber è un processo continuo che richiede un impegno costante da parte dell'organizzazione. Mantenere una buona comprensione delle minacce emergenti e delle vulnerabilità del sistema è fondamentale per garantire la protezione delle informazioni e degli asset digitali. In generale, l'analisi del rischio in tema di cybersecurity è un requisito richiesto da molti enti normativi e framework di cybersecurity. Essa offre diversi vantaggi alle organizzazioni che eseguono regolarmente le analisi come parte della loro strategia di sicurezza informatica: riduzione dei costi a lungo termine, un modello per le valutazioni future, consapevolezza organizzativa, prevenire la perdita dei dati ed eventuali multe regolamentari.

L'identificazione e la prevenzione tempestive dei rischi nell'organizzazione possono ridurre i costi operativi. Ad esempio, ripristinare o ristrutturare l'infrastruttura IT è molto più costoso che sviluppare misure preventive contro le minacce informatiche e le interruzioni. Inoltre, controlli rigorosi favoriscono processi più coerenti e una qualità più elevata. L'implementazione di una valutazione e di un'analisi formale del rischio informatico in un'organizzazione rende più facile ripetere questi processi. Non solo si avrà un personale con una conoscenza diretta dei concetti, ma anche gli strumenti e i modelli giusti per semplificare le attività di gestione dei rischi. In generale, un'analisi del rischio di cybersecurity porta a una gestione del rischio più forte, che aiuta a prevenire le minacce. Questo, a sua volta, si traduce in una minore possibilità di perdita di dati a causa di violazioni e in una minore possibilità di azioni normative conseguenti, comprese le sanzioni pecuniarie.

3 Case Study: integrazione di rischi cyber nei rischi operativi delle banche

L'accelerazione digitale del settore bancario ha portato con sé una miriade di opportunità, ma anche una serie di rischi emergenti, tra cui in particolare quelli cyber. Questi rischi, che possono variare da violazioni di dati a interruzioni operative, rappresentano una minaccia significativa per la stabilità finanziaria e l'integrità delle informazioni. L'incorporazione dei rischi cyber nei rischi operativi delle banche è quindi diventata una necessità imperativa per garantire la resilienza di questi istituti nell'era digitale.

La creazione di un modello di integrazione dei rischi cyber nei rischi operativi richiede un approccio olistico, che tenga conto di molteplici aspetti. Questo include l'identificazione e la valutazione dei potenziali rischi

cyber, l'integrazione di tali rischi nei modelli di rischio operativo esistenti, la creazione di processi di risposta efficaci, e il costante monitoraggio e aggiornamento del modello per rispecchiare le mutevoli dinamiche del panorama cyber.

Tuttavia, la sfida non è solo tecnica, ma anche culturale. Le banche devono riconoscere i rischi cyber come una componente intrinseca della loro operatività e non come un'area separata di preoccupazione. Questa trasformazione richiede un cambiamento di mentalità a tutti i livelli dell'organizzazione, dalla direzione ai dipendenti di base.

Nel contesto di questa discussione, esploreremo come si può realizzare un modello di integrazione efficace, gli ostacoli potenziali che possono sorgere e le migliori pratiche che possono guidare le banche in questo percorso essenziale verso la sicurezza informatica

3.1 Tassonomia di rischi cyber e mappatura sugli event-type di Basilea (Operational Cyber Risks)

Tassonomia dei Rischi ICT e Cyber

La tassonomia dei rischi ICT e Cyber è un sistema di classificazione utilizzato per identificare, organizzare e gestire tali tipi di rischi. Tale sistema può essere utilizzato per comprendere meglio i rischi, per facilitare la comunicazione e la collaborazione tra le parti interessate, e per sviluppare strategie di mitigazione più efficaci. I rischi cyber però coinvolgono un'ampia varietà di fattori di rischio e tocca quasi tutti i settori del pubblico e del privato, presentando molte sfaccettature, che combinano conoscenze tecniche e aspetti comportamentali e culturali. Questa eterogeneità multidimensionale rende la definizione e la classificazione degli eventi correlati all'ICT e al cyber un compito non univoco, al punto che non è ancora stata raggiunta una classificazione del rischio ICT e Cyber universalmente accettata e standardizzata in tutti i settori industriali e della società. Esistono classificazioni e tassonomie sviluppate da diverse prospettive industriali. Inoltre, molte istituzioni pubbliche e private hanno cercato di produrre classificazioni che affrontassero gli aspetti più importanti dei rischi ICT e Cyber rilevanti per i propri operatori.

Tra queste si evidenzia la classificazione data da EBA nelle Linee Guida sulla valutazione dei Rischi ICT a norma del processo di revisione e valutazione prudenziale (SREP) che suddivide i rischi ICT in 5 categorie:

Categoria di Rischio ICT	Descrizione
Rischio di disponibilità e continuità ICT	Il rischio che le prestazioni e la disponibilità dei sistemi e dei dati ICT siano influenzati negativamente, incluso il rischio di incapacità di ripristinare tempestivamente i servizi dell'ente a causa di un guasto delle componenti ICT hardware o software; debolezze nella gestione dei sistemi ICT; o qualsiasi altro evento, come ulteriormente esposto nell'allegato
Rischio di sicurezza ICT	Il rischio di accesso non autorizzato ai sistemi e ai dati dei sistemi ICT dell'ente, dall'interno o dall'esterno (ad esempio nel caso di attacchi informatici), come ulteriormente esposto nell'allegato.

Categoria di Rischio ICT	Descrizione
Rischio relativo ai cambiamenti ICT	Il rischio derivante dall'incapacità dell'ente di gestire i cambiamenti dei sistemi ICT in modo tempestivo e controllato, in particolare per quanto concerne programmi di modifica complessi e di grandi dimensioni, come ulteriormente esposto nell'allegato.
Rischio di integrità dei dati ICT	Il rischio che i dati archiviati ed elaborati dai sistemi ICT siano incompleti, inesatti o incoerenti nei vari sistemi, in seguito, ad esempio, a controlli ICT carenti o assenti durante le varie fasi del ciclo di vita dei dati ICT (vale a dire, progettazione dell'architettura dei dati, costruzione del modello e/o dei dizionari di dati, verifica degli inserimenti dei dati, controllo delle estrazioni, dei trasferimenti e delle elaborazioni dei dati, inclusi i risultati forniti), tali da compromettere la capacità di un ente di fornire servizi e di produrre le informazioni finanziarie e relative alla gestione (del rischio) in modo corretto e tempestivo come ulteriormente esposto nell'allegato.
Rischio di esternalizzazione ICT	Il rischio che il ricorso a una terza parte o a un'altra entità del gruppo (esternalizzazione intra-gruppo), per la fornitura di sistemi ICT o servizi connessi incida negativamente sulle prestazioni e sulla gestione del rischio dell'ente, come ulteriormente esposto nell'allegato.

Figura 16: Categorie di rischio ICT – Linee Guida EBA ICT Risk SREP

Nelle Linee Guida EBA sono anche indicati i vari rischi ICT e Cyber afferenti ad ognuna delle categorie sopra riportate. Per ognuno di essi, EBA fornisce un nome, una descrizione e alcuni esempi di cause che ne possono determinare l'occorrenza.

Nella figura riportata qui di seguito sono contenuti i rischi ICT e Cyber identificati da EBA e riportati nell'allegato nelle Linee Guida citate sopra.

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[30])	Descrizione del rischio	Esempi
Rischi di disponibilità e continuità ICT	Inadeguata gestione della capacità	La mancanza di risorse (ad es. hardware, software, personale, fornitori di servizi) può comportare un'incapacità di offrire un servizio che soddisfi esigenze aziendali, interruzioni di sistema, degrado di servizio e/o errori operativi.	La mancanza di capacità può influenzare la velocità di trasmissione e la disponibilità della rete (Internet) per servizi come l'Internet banking. La mancanza di personale (interno o esterno) può comportare interruzioni di sistema e/o errori operativi
	Guasti dei sistemi ICT	Perdita di disponibilità a causa di guasti hardware.	Guasti/malfunzionamento di dispositivi di archiviazione (hard disk), server o altre apparecchiature ICT, causati, ad esempio, da mancanza di manutenzione
		Perdita di disponibilità a causa di malfunzionamenti software e bug.	Loop infinito nel software applicativo che impedisce l'esecuzione delle operazioni. Interruzioni dovute all'uso continuo di sistemi e soluzioni ICT obsoleti che non soddisfano più i requisiti attuali di disponibilità e resilienza e/o che non sono più supportati dai loro fornitori.

[30] I rischi ICT sono elencati nella categoria di rischio sulla quale hanno un impatto maggiore, ma potrebbero influenzare anche altre categorie di rischio

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[30])	Descrizione del rischio	Esempi
	Inadeguatezza dei piani di ripristino in caso di disastro e della continuità dei sistemi ICT	Inefficienza delle soluzioni pianificate per la disponibilità e/o di continuità ICT e/o del piano di ripristino in caso di disastro (ad es. centri dati di ripristino alternativi) quando attivato per intervenire in caso di incidente	Le differenze di configurazione tra il centro dati primario e quello secondario possono causare l'incapacità del centro dati alternativo di fornire la continuità di servizio prevista.
	Attacchi informatici dirompenti e distruttivi	Attacchi per scopi diversi (ad es. movimenti militanti, ricatto) che comportano un sovraccarico dei sistemi e della rete, impedendo agli utenti legittimi di accedere ai servizi informatici online.	Gli attacchi di tipo DDOS (Distributed Denial of Service) hanno l'intento di interrompere il servizio e vengono eseguiti tramite una moltitudine di sistemi informatici su Internet controllati da un hacker, che invia a servizi Internet una grande quantità di richieste di servizio apparentemente legittime (ad es. servizi di e-banking).
Rischi di sicurezza ICT	Attacchi informatici e altri attacchi esterni ICT	Attacchi eseguiti attraverso Internet o da reti esterne per scopi diversi (ad es. frode, spionaggio, movimenti militanti /sabotaggio, terrorismo informatico) utilizzando una gamma di tecniche (ad es. social engineering, tentativi di intrusione attraverso lo sfruttamento delle vulnerabilità, utilizzo di software malevoli) per ottenere il controllo dei sistemi ICT interni.	Diversi tipi di attacchi: Attacchi mirati e persistenti (APT, Advanced Persistent Threat) per ottenere il controllo dei sistemi interni o rubare informazioni (ad es. informazioni relative all'identità, informazioni su carte di credito). Software malevolo (ad es. ransomware) che crittografa i dati allo scopo di ricatto. Contagio dei sistemi ICT interni mediante software trojan per commettere azioni malevole sui sistemi in modo celato. Sfruttamento delle vulnerabilità di sistemi ICT e/o applicazioni (web), come SQL injection, per accedere al sistema ICT interno.
		Esecuzione di operazioni di pagamento fraudolente da parte di hacker attraverso l'accesso non autorizzato o l'elusione della sicurezza dei servizi di e-banking e di pagamento e/o attaccando e sfruttando le vulnerabilità di sicurezza dei sistemi di pagamento interni dell'ente.	Attacchi a servizi di e-banking o di pagamento, con l'obiettivo di effettuare operazioni non autorizzate. Creazione e invio di transazioni di pagamento fraudolente da parte dei sistemi di pagamento interni dell'ente (ad es. messaggi SWIFT fraudolenti).
		Esecuzione di operazioni in titoli fraudolente da parte di hacker attraverso l'accesso non autorizzato o l'elusione della sicurezza dei servizi di e-banking che forniscono anche l'accesso ai conti dei titoli dei clienti.	Attacchi pump & dump tramite cui gli hacker ottengono l'accesso ai conti titoli e-banking dei clienti ed effettuano acquisti o vendite fraudolenti per influenzare il prezzo di mercato e/o ottenere guadagni in base a posizioni e titoli prcedentemente stabilite.
		Attacchi su connessioni di comunicazione e conversazioni di tutti i tipi o sistemi ICT con l'obiettivo di raccogliere informazioni e/o commettere frodi.	Intercettazione della trasmissione non protetta dei dati di autenticazione codificati in testo non crittografato
	Insufficiente sicurezza interna delle ICT	Accesso non autorizzato dall'interno dell'ente a sistemi ICT critici per scopi diversi (ad es. frode, esecuzione e occultamento di attività commerciali illecite, furto di dati, attivismo/sabotaggio) mediante una varietà di tecniche (ad es. abusi e/o sfruttamento di privilegi, furto d'identità, ingegneria sociale, sfruttamento delle vulnerabilità dei sistemi ICT, utilizzo di software malevoli).	Installazione di keylogger per rubare ID utente e password e ottenere l'accesso non autorizzato a dati riservati e/o commettere frodi. Decifrare/indovinare password deboli per ottenere diritti di accesso illegittimi o elevati. L'amministratore di sistema utilizza sistemi operativi o servizi di database (per modifiche dirette del database) per commettere frodi.

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[30])	Descrizione del rischio	Esempi
		Utilizzi non autorizzati dell'ICT dovuti a procedure e pratiche di gestione degli accessi inadeguate.	Mancata disattivazione o eliminazione di account non necessari, ad esempio di membri del personale che hanno cambiato funzione e/o hanno lasciato l'ente, inclusi ospiti o fornitori che non hanno più bisogno di accesso, che dà luogo all'accesso non autorizzato ai sistemi ICT. Concessione di diritti e privilegi di accesso eccessivi, consentendo accessi non autorizzati e/o di celare attività illecite
		Minacce alla sicurezza dovute alla mancanza di responsabilizzazione in materia di sicurezza per cui i dipendenti non comprendono, trascurano o non rispettano le politiche e le procedure di sicurezza ICT.	Dipendenti raggirati e portati a fornire assistenza per un attacco (ad es. ingegneria sociale). Cattive pratiche relative alle credenziali: condivisione di password, utilizzo di password "facili" da indovinare, stessa password per diversi scopi, ecc. Archiviazione di dati riservati non crittografati su computer portatili (laptop) e dispositivi portatili di archiviazione dati (ad es. chiavette USB) che possono essere persi o rubati.
		Archiviazione o trasferimento non autorizzato di informazioni riservate all'esterno dell'ente.	Persone che ottengono indebitamente, comunicano deliberatamente o forniscono illegalmente informazioni riservate a persone non autorizzate o al pubblico
	Insufficiente sicurezza fisica ICT	Uso improprio o furto di componenti ICT tramite accesso fisico che provochi danni, perdita di beni o dati o altre possibili minacce.	Irruzione fisica in uffici e/o centri dati per appropriarsi indebitamente delle apparecchiature ICT (ad es. computer, computer portatili, soluzioni di archiviazione) e/o per copiare dati accedendo fisicamente ai sistemi ICT
		Eventuali danni materiali alle componenti ICT, accidentali o volontari, causati da terrorismo, incidenti o manomissioni fatali/erronee da parte del personale dell'ente e/o di terzi (fornitori, personale della manutenzione	Terrorismo (ad es. bombe terroristiche) o sabotaggio di beni ICT. Distruzione del centro dati in seguito a incendi, perdite d'acqua o altri fattori.
		Protezione fisica insufficiente contro le catastrofi naturali risultante nella distruzione parziale o totale di sistemi ICT /centri dati a seguito di catastrofi naturali.	Terremoti, calore estremo, tempeste di vento, forti tempeste di neve, inondazioni, incendi, fulmini.
Rischi relativi ai cambiamenti ICT	Controlli inadeguati rispetto a cambiamenti dei sistemi ICT e sviluppo di ICT	Incidenti causati da errori o vulnerabilità non rilevati a seguito di un cambiamento di, ad esempio, software, sistemi e dati ICT (ad es. effetti imprevisti di un cambiamento o di un cambiamento gestito in modo errato a causa di mancanza di test o di pratiche di gestione del cambiamento improprie).	Messa in produzione di software insufficientemente testati o modifiche di configurazione con effetti negativi imprevisti sui dati (ad es. corruzione, cancellazione) e/o sulle prestazioni del sistema ICT (ad es. guasto, degrado delle prestazioni). Cambiamenti incontrollati dei sistemi ICT o dei dati nell'ambiente di produzione. Messa in produzione di sistemi informatici e applicazioni Internet non sicuri, che creano opportunità per gli hacker di attaccare i servizi Internet forniti e/o di violare i sistemi ICT interni.

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[30])	Descrizione del rischio	Esempi
			Cambiamenti incontrollati del codice sorgente del software sviluppato internamente. Test insufficienti a causa dell'assenza di ambienti di prova adeguati
	Architettura ICT inadeguata	Una debole gestione delle architetture ICT in fase di progettazione, costruzione e manutenzione dei sistemi ICT (ad es. software, hardware, dati) può portare, nel tempo, a sistemi ICT poco flessibili e complessi, difficili e costosi in termini di gestione, che non sono più sufficientemente allineati alle esigenze aziendali e ai requisiti di gestione dei rischi in vigore.	Modifiche a sistemi, software e/o dati ICT gestite in modo inadeguato per un lungo periodo di tempo, che portano a sistemi e architetture ICT poco flessibili e complessi, eterogenei e difficili da gestire, causando impatti negativi sulle attività aziendali e sulla gestione del rischio (ad es. mancanza di flessibilità e agilità, incidenti e guasti ICT, costi operativi elevati, indebolimento di sicurezza e resilienza ICT, riduzione della qualità dei dati e capacità di segnalazione). Eccessiva personalizzazione ed estensione dei pacchetti software commerciali con software sviluppato internamente, che impedisce di utilizzare versioni successive e aggiornamenti del software commerciale, generando il rischio di non essere più supportati dal fornitore.
	Gestione inadeguata del ciclo di vita e delle patch	Mancanza di un adeguato inventario di tutti i beni ICT a supporto di (e unitamente alle) pratiche di gestione del ciclo di vita e della corretta gestione delle patch. Ciò porta a sistemi ICT con patch insufficienti (e quindi più vulnerabili) e obsoleti che potrebbero non supportare le esigenze aziendali e di gestione dei rischi.	Sistemi informatici non aggiornati e obsoleti che possono causare impatti negativi sulle attività aziendali e sulla gestione del rischio (ad es. mancanza di flessibilità e agilità, interruzioni ICT, indebolimento di sicurezza e resilienza ICT).
Rischi di integrità dei dati ICT	Trattamento o gestione inadeguati dei dati ICT	A causa di errori o guasti di sistema, di comunicazione e/o di applicazione o errori di estrazione, trasferimento e caricamento (ETL) di dati, questi potrebbero essere danneggiati o persi.	Errore del sistema IT nel trattamento dei batch, che genera saldi non corretti nei conti bancari dei clienti. Query eseguite in modo errato. Perdita di dati dovuta all'errore di replica (backup) dei dati.
	Controlli di validazione dei dati progettati in modo inadeguato per i sistemi ICT	Errori causati da mancanti o inefficaci controlli automatizzati di alimentazione e di accettazione dei dati (ad es. dati utilizzati da terze parti), di trasferimento, di elaborazione e output di dati nei sistemi ICT (ad es. controlli di validità degli input, riconciliazione dei dati).	Formattazione/convalida insufficiente o invalida degli input dei dati nelle applicazioni e/o nelle interfacce utente. Assenza di controlli di riconciliazione dei dati sugli output Assenza di controlli sui processi di estrazione dei dati eseguiti (ad es. query di database) che generano dati errati. Utilizzo di dati esterni difettosi.
	Modifiche dei dati non adeguatamente controllate nei sistemi ICT in Produzione	Errori sui dati causati dalla mancanza di controlli sulla correttezza e sulla legittimità delle manipolazioni dei dati in produzione nei sistemi ICT.	Sviluppatori o amministratori di database che accedono e modificano i dati direttamente nei sistemi ICT di produzione in modo non controllato, ad esempio nel caso di un incidente ICT.
	Architettura di dati, flussi di dati, modelli di dati o dizionari di dati	Le architetture, i modelli, i flussi o i dizionari di dati gestiti in modo inadeguato possono creare più versioni degli stessi dati nei sistemi ICT che non sono più coerenti a causa	Esistenza di diversi database clienti per ogni prodotto o unità di business con diverse definizioni e campi di dati, che genera dati dei clienti inadeguati e difficili da

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[30])	Descrizione del rischio	Esempi
	progettati e/o gestiti in modo inadeguato	di modelli di dati o definizioni dei dati applicati in modo diverso e/o delle differenze nel processo di generazione e modifica dei dati sottostanti.	confrontare e integrare a livello globale dell'ente o del gruppo finanziario.
Rischi di esternalizzazione ICT	Resilienza insufficiente di servizi di terzi o di altri enti del gruppo	La mancata disponibilità di servizi ICT critici esternalizzati, servizi di telecomunicazione e utenze. Perdita o corruzione di dati fondamentali/sensibili affidati al fornitore di servizi	Mancata disponibilità dei servizi di base a causa di errori in sistemi o applicazioni ICT (esternalizzati) dei fornitori. Interruzione dei collegamenti di telecomunicazione. Interruzione dell'alimentazione elettrica.
	Organizzazione inadeguata dell'esternalizzazione	Grave degrado o interruzione dei servizi dovuti a processi di preparazione o di controllo inefficienti da parte del fornitore dei servizi esternalizzati.	Procedure inadeguate di gestione degli incidenti, meccanismi di controllo contrattuali e garanzie integrate nell'accordo per la fornitura dei servizi che aumentano la dipendenza da terzi e fornitori.
		Un'inefficace organizzazione dell'esternalizzazione può provocare una mancanza di adeguate competenze e capacità per identificare, valutare, mitigare e	Controlli di gestione del cambiamento inadeguati relativi all'ambiente ICT del fornitore di servizi possono causare un degrado o un'interruzione del servizio
	Insufficiente sicurezza di terzi o altri enti del gruppo	L'attacco informatico ai sistemi ICT dei fornitori di servizi, con un impatto diretto sui servizi esternalizzati o sui dati fondamentali/riservati archiviati presso il fornitore del servizio. Personale del fornitore di servizi che ha ottenuto l'accesso non autorizzato a dati fondamentali/sensibili memorizzati presso il fornitore di servizi.	L'attacco informatico ai fornitori di servizi da parte di criminali o terroristi, come punto di accesso ai sistemi ICT degli enti o per accedere/distruggere i dati fondamentali o sensibili archiviati presso il fornitore dei servizi. Soggetti malintenzionati, operanti presso il fornitore di servizi, tentano di appropriarsi indebitamente e vendere dati sensibili

Figura 17: Classificazione dei rischi ICT – Allegato Linee Guida EBA ICT Risk SREP

La classificazione dei rischi ICT e Cyber proposta da EBA Linee Guida sulla valutazione dei Rischi ICT a norma del processo di revisione e valutazione prudenziale (SREP) riveste una particolare utilità e importanza per le banche nella gestione di tali rischi per i seguenti motivi:

- anche se i rischi indicati non possono essere considerati esaustivi, così come indicato da EBA, essi comunque rappresentano un ottimo punto di partenza per le banche per identificare e gestire tali rischi;
- le Linee Guida EBA forniscono per ogni tipologia dei rischi ICT i controlli che devono essere implementati per la loro mitigazione e questo fornisce alle banche delle ottime indicazioni su quali sono le aree in cui devono investire;
- nella descrizione dei rischi e negli esempi riportati sono indicati anche i fattori di rischio e le possibili conseguenze ad essi connessi. Queste indicazioni sono utili per poter determinare i fattori di rischio, gli eventi e gli effetti connessi ai rischi ICT e Cyber per poter effettuare una mappatura sugli Event

Type di Basilea e procedere alla integrazione di tali rischi nel modello di gestione dei rischi operativi adottato.

Va infine osservato che, anche se tali Linee Guida sono dirette alle Autorità Europee e Nazionali (vedi Banca d'Italia) per garantire la convergenza delle pratiche di vigilanza per la valutazione dei rischi ICT a norma del processo di revisione e valutazione prudenziale (SREP), esse sono state adottate come riferimento dai principali gruppi bancari europei.

Mappatura dei rischi ICT e Cyber sugli Event-type di Basilea

Per la creazione di un modello efficace di integrazione dei rischi ICT e Cyber all'interno dei rischi operativi, si seguirà un ordine in sequenza composto da una relazione di causa-effetto tale per cui, a fronte di uno o più fattori scatenanti, si genera l'evento pregiudizievole. Per tale ragione, per poter spiegare nella sua interezza l'evento pregiudizievole accaduto, è necessario specificarlo secondo tre componenti

- Causa: rappresenta il fattore di rischi
- Evento: Loss Event type
- Effetto: Loss Effect type

Questa sequenza sarà associata a sua volta, in relazione ai rischi ICT e Cyber a:

- Vulnerabilità (Causa): debolezza del sistema dovuto alla mancata implementazione di uno o più controlli IT
- Minaccia (Loss Event Type): evento che sfruttando una vulnerabilità produce un impatto
- Impatto (Loss Effect Type): conseguenza legata al verificarsi di una minaccia

Come detto in precedenza quando si è illustrata la classificazione dei rischi ICT e Cyber proposta da EBA, i fattori di rischio connessi ai rischi ICT e Cyber sono stati mappati nella categoria in cui hanno il maggior impatto, ma essi possono avere impatti anche in altre categorie.

Viceversa, fattori di rischio che apparentemente non sono direttamente connessi con i rischi cyber, possono comunque avere una rilevanza negli incidenti connessi a tali rischi (cd Incidenti Cyber) e diventarne la causa. A titolo esemplificativo, quasi tutti i fattori di rischio previsti per le Risorse Umane (es Inadeguato sistema di selezione del personale, Inadeguato know-how delle risorse, Inadeguati programmi e piani di formazione, Inadeguata assegnazione delle responsabilità (in relazione alla professionalità e alle competenze della risorsa), Turn-over elevato di personale chiave, hanno una rilevanza per i rischi ICT e Cyber quando essi si applicano al personale delle funzioni aziendali deputate alla gestione del sistema informativo e a tutti i processi di monitoraggio e gestione della sicurezza ICT.

Per tale ragione, una volta mappati i rischi ICT e Cyber sul modello di gestione dei rischi operativi adottato dalla banca, è buona prassi comunque valutare sempre anche l'impatto che gli altri fattori di rischio possono avere sui rischi cyber.

A titolo esemplificativo e non esaustivo, nella tabella riportata di seguito sono indicati i fattori di rischio specifici per i rischi ICT e Cyber mappati sui fattori di rischio di Basilea e organizzati una classica struttura a 3 livelli. I fattori di rischio sono stati derivati dalla classificazione dei rischi ICT e Cyber proposta da EBA.

Fattore di rischio di Basilea	Fattore di rischio di 1° livello	Fattore di rischio di 2° livello	Fattore di rischio di 3° livello
Sistema Informativo	Rischi di sicurezza ICT	Amministrazione della sicurezza	• Inadeguatezza del piano di Security Awareness per cui i dipendenti non comprendono, trascurano o non rispettano le politiche e le procedure di sicurezza ICT (ex: condivisione di password, utilizzo di password facili da indovinare, utilizzo di stessa password per diversi scopi)
			• Archiviazione di dati riservati non crittografati su computer portatili (laptop) e dispositivi portatili di archiviazione dati (e.s: chiavette USB) che possono essere persi o rubati
		Gestione degli accessi	• Assenza di un processo strutturato per la creazione/modifica/cancellazione di una utenza di accesso
			• Mancata previsione di un accesso differenziato a sistemi sulla base del principio 'need to know - need to do' (profili di accesso)
			• Inadeguata gestione dei profili utente (ex: attribuzione dei privilegi, revisione periodica dei diritti di accesso degli utenti, controllo sull'utilizzo di passepartout da parte di personale IT)
			• Inadeguati presidi per il controllo e la tracciatura degli accessi logici e delle attività svolte (autore, data e ora)
			• Assenza di strumenti per la registrazione delle violazioni e dei tentativi di violazione
			• Mancata definizione delle azioni da intraprendere a fronte di violazioni/tentativi di violazione riscontrati
			• Separazione tra gli ambienti di sviluppo, collaudo e produzione
			• Password associate alle utenze di accesso visibili in chiaro durante la digitazione • Mancata disabilitazione di una utenza dopo N tentativi di accesso con password errata
			• Mancata disconnessione di una sessione di collegamento dopo N minuti di inattività del terminale
			• Mancata definizione di un periodo di validità delle password
		Controllo degli accessi fisici ai locali IT	• Mancata predisposizione di strumenti per l'identificazione del personale autorizzato alla sala dove risiedono application e data server (e.g. lettori di badge, porte apribili dall'interno)
			• Assenza di una policy che regola gli accessi dei consulenti e dei tecnici esterni
			• Mancata definizione delle azioni da intraprendere a fronte di violazioni di accesso
		Politiche di network security	• Assenza di un Tool di Intrusion Detection
			• Assenza di un sistema di cifratura delle informazioni scambiate sulla rete e di autenticazione dei soggetti
			• Inadeguata gestione del servizio di accesso da remoto (e.g. Token, One Time Password)
			• Errata configurazione dei firewall (anche con riferimento alla segmentazione logica della rete)

Fattore di rischio di Basilea	Fattore di rischio di 1° livello	Fattore di rischio di 2° livello	Fattore di rischio di 3° livello
			• Password per l'autenticazione degli utenti senza i requisiti minimi di network security
			• Inadeguata gestione dei software antivirus
			• Assenza di una policy sull'accesso fisico alle apparecchiature di commutazione di rete (router, switch) al solo personale autorizzato
			• Assenza di un tool contro attacchi DDoS (Distributed Denial of Service)
		Attacchi informatici e altri attacchi esterni ICT	• Attacchi mirati e persistenti (APT, Advanced Persistent Threat) • Malware • Ransomware • Attacchi a servizi di e-banking o di pagamento • Intercettazione della trasmissione
	Rischi di disponibilità e continuità ICT	Gestione dell'indisponibilità di dati e/o applicazioni	• Inadeguata/mancata definizione e/o attuazione delle procedure di backup periodico degli archivi e del software
			• Mancata/inadeguata definizione di un Business Continuity Plan (incluso il Disaster Recovery Plan)
		Gestione infrastrutture IT	• Obsolescenza dell'infrastruttura IT (e.g. Hardware, Software, Applicazioni, DBMS, Networking)
			• Incompleta integrazione e interoperabilità tra i sistemi
			• Inadeguatezza delle applicazioni rispetto alle esigenze operative
			• Limitata capacità dell'infrastruttura tecnologica (e.g. capacità elaborativa, capacità trasmissiva, capacità immagazzinamento dati, tempi di accesso e di risposta delle applicazioni) rispetto alle esigenze operative
		Procedure di risoluzione delle criticità lato utente	• Tempi eccessivi per la risoluzione di malfunzionamenti riscontrati nei sistemi
			• Tempi eccessivi per l'esecuzione di modifiche agli applicativi
			• Tempi eccessivi di ripristino degli archivi oggetto di backup
			• Inadeguato servizio di supporto agli utenti (help desk)
		Attacchi informatici dirompenti e distruttivi	• Attacchi DDoS
	Rischi relativi ai cambiamenti ICT	Sviluppo e manutenzione dei sistemi	• Inadeguato disegno dei processi per la gestione dei progetti di sviluppo e manutenzione dei software
			• Inadeguato processo di IT Demand Management
			• Inadeguato piano di testing
			• Inadeguato processo di aggiornamento del software e hardware in relazione alle mutate necessità operative
		Processo di acquisizione Hardware e software	• Inadeguato processo di acquisizione Hardware, Software, altre risorse IT
			• Mancata inventariazione di tutte le risorse tecnologiche (hardware, software, dati, procedure)
	Rischi di integrità dei dati ICT	Trattamento o gestione inadeguati dei dati ICT	• A causa di errori o guasti di sistema, di comunicazione e/o di applicazione o errori di estrazione, trasferimento e caricamento (ETL) di dati, questi potrebbero essere danneggiati o persi.
		Controlli di validazione dei dati progettati in modo inadeguato per i sistemi ICT	• Errori causati da mancanti o inefficaci controlli automatizzati di alimentazione e di accettazione dei dati.

Fattore di rischio di Basilea	Fattore di rischio di 1° livello	Fattore di rischio di 2° livello	Fattore di rischio di 3° livello
		Modifiche dei dati non adeguatamente controllate nei sistemi ICT in Produzione	• Errori sui dati causati dalla mancanza di controlli sulla correttezza e sulla legittimità delle manipolazioni dei dati in produzione nei sistemi ICT.
		Architettura di dati, flussi di dati, modelli di dati o dizionari di dati progettati e/o gestiti in modo inadeguato	• Le architetture, i modelli, i flussi o i dizionari di dati gestiti in modo inadeguato
	Rischi di esternalizzazione ICT	Resilienza insufficiente di servizi di terzi o di altri enti del gruppo	• La mancata disponibilità di servizi ICT critici esternalizzati, servizi di telecomunicazione e utenze. Perdita o corruzione di dati fondamentali/sensibili affidati al fornitore di servizi
		Organizzazione inadeguata dell'esternalizzazione	• Grave degrado o interruzione dei servizi dovuti a processi di preparazione o di controllo inefficienti da parte del fornitore dei servizi esternalizzati.
		Insufficiente sicurezza di terzi o altri enti del gruppo	• L'attacco informatico ai sistemi ICT dei fornitori di servizi, con un impatto diretto sui servizi esternalizzati o sui dati fondamentali/riservati archiviati presso il fornitore del servizio. • Personale del fornitore di servizi che ha ottenuto l'accesso non autorizzato a dati fondamentali/sensibili memorizzati presso il fornitore di servizi.

Figura 17: Fattori di rischio ICT e Cyber

Attraverso questa figura si sono andati a specificare i singoli eventi, connessi ai fattori di rischio di Basilea, che creano delle vulnerabilità all'interno dell'operatività dell'intermediario finanziario.

Il passo successivo è l'analisi dei cosiddetti Loss Even Type, ovvero le minacce, legate alle infrastrutture ICT che, attraverso le vulnerabilità, potrebbero produrre un impatto.

Anche in questo caso, la base di partenza è la classificazione dei rischi ICT e Cyber definita da EBA identificando tutti quei potenziali eventi (i cosiddetti incidenti cyber) che possono provocare un effetto, ovvero una perdita per la banca.

A titolo esemplificativo e non esaustivo, nella figura riportata qui di seguito sono indicati i Loss Event Type connessi ai rischi ICT e Cyber mappati sui Loss Event Type di Basilea. Anche in questo caso, i Loss Event Type sono stati derivati dalla classificazione dei rischi ICT e Cyber proposta da EBA e sono organizzati su una struttura a 3 livelli.

Anche in questo caso la figura vuole essere esemplificativa e non esaustiva sia perché l'obiettivo è illustrare un metodo, sia perché i possibili Loss Event Type applicabili ad una banca sono molteplici e diversi e dipendono dai processi, dai servizi e dalle caratteristiche del sistema informativo della banca.

Va infine osservato che i fattori di rischio che possono provocare un Loss Event Type sono molteplici e, molto spesso, concatenati tra di loro.

A titolo esemplificativo, una frode esterna verso un cliente dalla banca sui sistemi di pagamento della stessa può essere perpetrata in diversi modi (es. phishing, sottrazione di dati, social engneering,..) e l'attacco può prevedere diverse fasi concatenate tra di loro e svolte con tecniche diverse.
Risulta perché essenziale per una banca poter identificare nella maniera più precisa i possibili Loss Event Type collegandoli a tutti i fattori di rischio che li possono provocare.

Loss Even Type di 1° livello	Loss Even Type di 2° livello	Loss Even Type di 3° livello
Frode interna	Attività non autorizzata	• Accessi logici e/o fisici non autorizzati a sistemi informatici o a dati da personale interno
		• Manipolazione di file, programmi e hardware
Frode esterna	Sicurezza dei sistemi	• Pirateria informatica
		• Utilizzo non autorizzato di risorse ICT
Interruzioni dell'operatività e disfunzione dei sistemi informatici	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici	• Guasti ai sistemi ICT
		• Inadeguatezza dei piani di ripristino in caso di disastro e della continuità dei sistemi ICT
		• Interruzione nella fornitura di servizi da parte di Information Providers
		• Interruzioni/guasti nell'erogazione di servizi di utilities
		• Interruzione di servizio di sistemi di pagamento esterni
		• Inadeguata gestione dei dati che può pregiudicarne l'integrità, la disponibilità e la riservatezza
		• Fallimenti dei Change
		• Inadeguata progettazione e/o gestione dell'architettura dei sistemi ICT
Esecuzione, consegna e gestione dei processi	Esecuzione e perfezionamento delle transazioni	• Mancata/non adeguata/tardiva manutenzione delle basi dati
		• Errori nell'invio di comunicazioni a Banche Dati / Data Base esterni
		• Errori nell'inserimento dei dati a sistema
		• Mancata/non adeguata/tardiva manutenzione delle basi dati
		• Errori nello sviluppo/implementazione degli applicativi/sistemi •
		• Assente e/o inadeguata inventariazione degli asset ICT
	Produttori e fornitori	• Insufficiente sicurezza ICT del fornitore

Figura 18: Loss Event Type ICT e Cyber

Infine, si hanno i Loss Effect Type, ovvero le conseguenze che risultano dall'eventuale accadimento dell'evento dannoso.

Va osservato che gli attacchi cyber possono avere un impatto sulle banche attraverso i tre aspetti principali connessi alla sicurezza delle informazioni: riservatezza, integrità e disponibilità:

- i problemi di riservatezza sorgono quando le informazioni private di una banca vengono divulgate a terzi, come nel caso delle violazioni dei dati;
- i problemi di integrità riguardano l'uso improprio dei sistemi, come nel caso delle frodi;
- infine, i problemi di disponibilità sono legati alle interruzioni dell'attività.

I tre tipi di attacchi cyber hanno impatti diretti diversi sugli obiettivi:

- le interruzioni dell'attività impediscono alle banche di operare, con conseguente perdita di ricavi;
- le frodi portano a perdite finanziarie dirette;
- gli effetti delle violazioni dei dati richiedono più tempo per concretizzarsi, attraverso effetti sulla reputazione e costi di contenzioso.

Più in generale, il rischio di una perdita di fiducia a seguito di attacchi cyber potrebbe essere elevato per il settore finanziario, dato che le istituzioni finanziarie fanno affidamento sulla fiducia dei loro clienti. Inoltre, per quanto riguarda il sistema finanziario, è più probabile che le interruzioni dell'attività abbiano effetti diretti di contagio a breve termine rispetto alle frodi o alle violazioni di dati, che tendono a colpire principalmente l'impresa bersaglio nel breve periodo.

Da quanto esposto, si evince che gli effetti connessi ai Loss Event Type connessi ai rischi ICT e Cyber ricadono prevalentemente nelle seguenti tipologie di perdite già presenti nei rischi operativi delle banche:

- **Responsabilità legale**: sentenze, sanzioni, compromessi/risarcimenti e altri costi legali;
- **Azione dell'Autorità di Regolamentazione**: ammende e pagamenti diretti per altre sanzioni (es. sanzioni connessi ai Data Breach di dati personali, sanzioni per non adeguamento alle normative obbligatorie, ecc)
- **Perdite e danni a beni**: riduzione diretta del valore di beni fisici dovuta a qualche incidente (es. negligenza, incidente, incendio, terremoto, ecc.);
- **Risarcimenti**: pagamenti a terzi a seguito di perdite operative di cui l'azienda è legalmente responsabile;
- **Perdite per errore non recuperate**: perdite subite quando una terza parte non rispetta le sue obbligazioni verso l'azienda e che sono attribuibili ad un errore o evento operativo dell'azienda stessa (tali perdite si sarebbero potute evitare anche se la controparte non volesse o non potesse pagare);
- **Svalutazioni**: riduzione diretta del valore dell'attivo dovuto a furto, frode, attività non autorizzata, errata operatività, o perdite di mercato o di credito risultanti da eventi operativi;
- **Altro**: voci che non ricadono in una categoria specifica (es. danno Reputazionale).

3.2 Metodi di valutazione quali-quantitativa degli Operational Cyber Risks (perdite, dati esterni e valutazioni prospettiche)

Come si evince dal Capitolo 2, tutte le metodologie di analisi e valutazione di rischi ICT e Cyber ruotano intorno a 3 elementi fondamentali:

- gli asset ICT;
- le misure di sicurezza (detti anche controlli ICT) su di essi applicate;
- le minacce che ad essi afferiscono.

L'asset ICT è l'elemento centrale delle analisi dei rischi ICT e Cyber in quanto rappresenta "l'oggetto" sul quale valutare i rischi. Essi sono generalmente degli aggregati di elementi ICT hardware e software e sono mappati sui processi di business che supportano e sui dati che gestiscono.

Sugli asset ICT viene valutato il rischio inerente (ovvero il massimo impatto che una minaccia può provocare) e il rischio residuo che è valutato come funzione della probabilità che una minaccia occorra sull'asset e provochi un impatto e il valore dell'impatto provocato.

Il rischio residuo, così come quello inerente, viene valutato rispetto ai tre scenari di rischio connessi alle caratteristiche dei dati gestiti, ovvero:

- violazione della riservatezza dei dati;
- violazione della integrità dei dati;
- indisponibilità dell'asset.

Il rischio residuo degli asset ICT, qualora superiore alla soglia di accettazione stabilita dalla banca, viene trattato con le classiche modalità di:

- mitigazione del rischio attraverso la revisione delle misure di sicurezza applicate e/o implementazione di nuove misure di sicurezza;
- trasferimento del rischio ad altra entità (sottoscrizione di un'assicurazione cyber che copre l'impatto quando si verifica);
- eliminazione del rischio o mediante tecniche di ristrutturazione dell'asset (es. suddivisione dell'asset in più asset meno critici) o modificando il processo/servizio di business che supporta.

Le misure di sicurezza hanno la principale finalità di mitigare i rischi ICT e Cyber su un asset ICT o contrastando l'accadimento della minaccia (es. controllo accessi logici) o mitigando gli impatti che la minaccia può provocare (es. backup dei dati da utilizzare quando si verifica una perdita degli stessi).

Il livello di implementazione delle misure di sicurezza su un asset ICT rispetto all'insieme delle misure di sicurezza che dovrebbero essere implementate per ridurre i rischi al minimo (il cosiddetto profilo ottimale di sicurezza) è un ottimo indicatore oggettivo che fornisce il livello di vulnerabilità[31] dell'asset ICT e può essere

[31] Le vulnerabilità di un asset ICT possono essere definite come l'assenza di un controllo ICT o come la mancata efficacia di un controllo ICT

quindi utilizzato per valutare la probabilità che una minaccia applicabile all'asset possa accadere provocando un impatto.

Infine, le minacce sono quelli eventi che possono provocare un impatto sugli asset ICT provocando quello che viene chiamato incidente ICT o incidente Cyber sulla base della causa (ovvero la minaccia) che lo ha provocato.

Come è noto, le minacce possono essere interne o esterne e possono essere provocati da agenti interni o esterni e possono essere intenzionali o accidentali.

La valutazione dei rischi ICT e Cyber sono di solito integrate con altre le informazioni disponibili internamente alla banca (Fonti Interne) o esternamente (Fonti Esterne).

A titolo esemplificativo, ma non esaustivo, alcune informazioni utili per la valutazione dei rischi ICT e cyber sono:

- gli incidenti occorsi per meglio quantificare sia la probabilità di accadimento delle minacce che la quantificazione degli impatti;
- le vulnerabilità riscontrate dalle verifiche di sicurezza periodiche la banca esegue (es. Vulnerability Assessment, Penetration test, assessment di sicurezza, livello di patching degli asset ICT,..) per una migliore valutazione del livello di vulnerabilità degli asset ICT utile a valutare la probabilità di accadimento delle minacce;
- informazioni da fonti esterne (es. ENISA, Clusit, ORX[32],..) per capire quali sono le principali minacce nel settore di business in cui si opera e i relativi trend in termini di probabilità di occorrenza e severità (ovvero gli impatti) che esse provocano.

A seguito dell'esecuzione dell'analisi e valutazione dei rischi ICT e Cyber deve essere aggiornata la tassonomia di tali rischi introducendo i nuovi rischi riscontrati durante l'analisi (es. presenza di nuove minacce) ed eliminando quei rischi non più applicabili e/o obsoleti.

Tale valutazione dei rischi ICT e Cyber è funzionale alla sua gestione, ma per poter procedere ad una integrazione nei rischi operativi della banca bisogna identificare gli eventi ICT/Cyber che possono provocare un impatto (di seguito indicati come Loss Event Type ICT/Cyber) connessi agli asset ICT e procedere alla loro valorizzazione per una successiva integrazione nei rischi operativi dalla banca.

Un semplice processo per poter identificare e valorizzare i Loss Event Type ICT/Cyber è quello descritto nel seguito che è composto da 5 fasi:

- Identificazione dei loss event type ICT/Cyber
- Analisi qualitativa dei loss event type ICT/Cyber
- Quantificazione dei loss event type ICT/Cyber
- Revisione della quantificazione dei loss event type ICT/Cyber
- Quantificazione perdita annuale pesata per singolo loss event type ICT/Cyber

[32] Operational Risk eXchange association

Identificazione dei loss event type ICT/Cyber

Partendo dalla tassonomia dei loss event type definita, vengono analizzati tutti gli asset ICT che durante l'analisi dei rischi hanno registrato un valore di rischio residuo superiore alla soglia definita dalla banca e si verifica quali siano i Loss Event Type ICT/Cyber applicabili agli asset ICT in esame.

I driver che si possono utilizzare per identificare i loss event type ICT/Cyber applicabili ad un asset ICT sono:

- le minacce afferenti agli agli asset ICT e l'impatto che queste provocano sugli scenari di riservatezza, integrità e disponibilità analizzati;
- gli incidenti occorsi, con relative e/o mancati guadagni, i tentativi di frode o dati posseduti dai responsabili dei processi che gli asset supportano (es. reclami dei clienti);
- i dati connessi alle vulnerabilità presenti sull'asset ICT (assenza o implementazione parziali di controlli ICT, report dei Vulnerabilty assessment, Penetration test, verifiche di sicurezza e così via);
- i dati esterni provenienti da fonti esterne accreditate (es. ENISA, Clusit, ORX,..) e afferenti all'ambito in cui la banca opera.

Tutti i dati sopra elencati sono disponibili dall'analisi e valutazione dei rischi ICT effettuata in quanto sono stati utilizzati per valutare la probabilità di accadimento delle minacce e l'impatto che queste provocano sugli asset ICT.

Come detto prima, il punto di partenza è la tassonomia dei loss event type ICT/Cyber definita dalla banca, ma la fase di identificazione è utile perché permette di effettuare una verifica di tale tassonomia, ovvero permette di identificare nuovi loss event type ICT/Cyber di nuova introduzione e, nel contempo, di eliminare dei loss event type ICT/Cyber non più applicabili o obsoleti.

Nella fase di identificazione dei loss event type ICT/Cyber vengono anche acquisite le informazioni utili per la loro successiva quantificazione.

Tra questi si evidenziano:

- tutti i dati storici correlati agli asset ICT i quali giocano un ruolo fondamentale nella costruzione di un Loss Event Type ICT/Cyber perché forniscono esempi reali di incidenti occorsi, sui quali costruire la simulazione che configura quello che potenzialmente potrebbe succedere;
- i dati connessi alle vulnerabilità presenti sull'asset ICT (es. risultati di VA, PenTest, verifiche di sicurezza, ecc);
- informazioni sulle evoluzioni dell'asset ICT (es. cambi di tecnologia, inserimento/modifica di dati, aggiunta/modifica delle funzionalità implementate, ecc), dei controlli ICT su di esso implementati e tutte le informazioni di contesto associate all'asset (es. numero di clienti, numero di transazioni, numero di utenti e così) che sono utili per valutare in prospettiva come i rischi ICT e Cyber dell'asset possono evolvere in prospettiva;

- i processi che gli asset ICT supportano e quindi le funzioni aziendali coinvolte. Questa mappatura non è molto semplice perché non è quasi mai univoca perché molti degli asset ICT di una banca supportano più di un processo se non tutta l'operatività della banca (vedi ad esempio l'infrastruttura di rete, le infrastrutture elettriche, ecc);

Un altro aspetto rilevante che va considerato quando si identificano gli eventi ICT e Cyber e la correlazione che esiste tra questi che, in quest'ambito, può rilevarsi significativa.

Un attacco cyber può essere molto articolato e prevedere fasi e tecniche diverse per essere perpetrato.

A titolo esemplificativo, un evento connesso ad un accesso non autorizzato ai sistemi ICT aziendali con furto dei dati (cd data breach) potrebbe essere il preludio per altri eventi con finalità diverse.

A titolo esemplificativo:

- una frode esterna in quanto i dati rubati erano le credenziali di accesso ai conti on line dei clienti;
- la richiesta di un riscatto legata alla minaccia di pubblicare i dati on line;
- l'utilizzo dei dati rubati per proprie finalità di business (es. azienda concorrente che vuole rubare i clienti offrendo servizi più vantaggiosi).
- Pubblicazione dei dati per danneggiare la reputazione della banca.

Per tale ragione, bisogna analizzare gli eventi ICT e Cyber e identificare sia loss event type ICT/Cyber generici che loss event type ICT/Cyber specifici che correlano insieme i diversi eventi cercando di rappresentare delle situazioni che realisticamente possono capitare.

Questo approccio permette di mantenere i loss event type ICT/Cyber indipendenti che, come noto, è una delle ipotesi dei modelli di valutazione dei rischi operativi basati sulle metodologie AMA.

Analisi qualitativa dei loss event type ICT/Cyber

L'analisi che precede la quantificazione dei loss event type ICT/Cyber e consta di:

- descrizione del loss event type ICT/Cyber: descrizione dell'evento, il perimetro di copertura in termini di asset ICT coinvolti, processi aziendali supportati, elementi generali di contesto compresa l'eventuale evoluzione prevista per gli asset ICT e per i processi, il riferimento ad altri documenti significativi ai fini della misurazione della rischiosità associata all'evento.
- Descrizione delle Cause: per ogni loss event type ICT/Cyber devono essere identificate e descritte le possibili cause, ovvero le minacce che possono provocare l'impatto (effetto) connesso al verificarsi dell'evento. A tal fine può essere utilizzata la tassonomia di rischi ICT/Cyber definita aggiornata a seguito della fase di identificazione dei loss event type ICT/Cyber. Ad ogni possibile causa/minaccia devono essere associati una descrizione, un commento, l'indicazione della funzione aziendale che ha subito l'impatto ed il relativo processo.

  Non è necessario che tutte le cause si verifichino simultaneamente perché il loss event type ICT/Cyber accada. Le cause possono essere:

- esterne: a titolo esemplificativo un atto deliberato esterno (frode esterna), una calamità naturale/incidente, una inadempienza di una controparte esterna e così via;
- interne: a titolo esemplificativo un atto deliberato interno (frode interna), un errore umano, un guasto informatico (interno), un malfunzionamento dell'infrastruttura, un malfunzionamento di una procedura o di un processo interno e così via.

- Descrizione dei controlli ICT: il controllo ICT è un mezzo per impedire il verificarsi del loss event type ICT/Cyber o per limitarne gli effetti. I controlli sono qui intesi in senso ampio come tutto ciò che possa mitigare i rischi. In particolare, i controlli ICT possono essere:
  - controlli diretti alla prevenzione del rischio che il loss event type ICT/Cyber si verifichi. Questi controlli sono utilizzati a valutarne la frequenza;
  - controlli diretti al contenimento degli impatti che il loss event type ICT/Cyber può causare. Questi controlli sono utilizzati per valutarne la gravità.

  Devono essere menzionati i controlli ICT mancanti e/o inefficaci in quanto sono d'ausilio nella valutazione delle frequenze e degli impatti. Tali informazioni sono acquisibili dall'analisi dei rischi ICT e Cyber effettuata che ha utilizzato tali informazioni per valutare la probabilità di accadimento di una minaccia connesso all'effetto che essa può provocare.
- Descrizione degli effetti: gli effetti sono le conseguenze economiche connesse ad un loss event type ICT/Cyber e possono essere descritti in maniera descrittiva per facilitare la comprensione della situazione conseguente all'evento. Per la descrizione degli effetti, far riferimento alla tassonomia degli effetti di cui al paragrafo 3.1.

Quantificazione dei loss event type ICT/Cyber

La quantificazione dei loss event type ICT/Cyber prende in considerazione gli stessi elementi utilizzati in ambito analisi dei rischi ICT e Cyber, ma approfondisce l'analisi in un'ottica più quantitativa che qualitativa. I fattori che devono essere considerati sono:

- gli incidenti storici registrati all'interno (frequenza e severità), il cui impatto è una perdita, un guadagno o mancato guadagno, o anche una perdita condizionata;
- gli incidenti storici subiti da istituti di natura comparabile a quella della banca (frequenza e severità), nella misura in cui questa informazione sia disponibile nelle basi dati esterne a disposizione.

L'analisi quantitativa dei loss event type ICT/Cyber è basata sulla valutazione dei due scenari o casi, il caso verosimile (likely case) ed il peggiore dei casi (worst case):

- il caso verosimile (likely case) rappresenta il caso più frequente dell'event type ICT/Cyber, ovvero la situazione che ha maggior probabilità di occorrenza nel caso in cui si verifichi. In termini tecnici, il caso verosimile è quello nel quale l'importo di perdita è uguale alla moda della distribuzione degli importi di perdita (distribuzione di severità) dell'event type ICT/Cyber. La scelta del caso verosimile

deriva dall'analisi della serie storica degli incidenti o in alternativa dall'analisi delle cause/minacce e dei controlli ICT.

- Il peggiore dei casi (worst case) rappresenta il peggiore dei casi e quindi la situazione più avversa che può ragionevolmente presentarsi nel quadro del verificarsi del loss event type ICT/Cyber. Il peggiore dei casi deve descrivere una situazione sfavorevole in termini di cause, controlli ed effetti, ma deve mantenersi nell'ambito di uno scenario ipotetico, raro, ma plausibile. Esso rappresenta dunque la combinazione di tutte le circostanze sfavorevoli che possono ragionevolmente essere ipotizzate.

In casi eccezionali è possibile costruire un solo caso (i Loss event type ICT/Cyber con un solo caso (single case)) che sono loss event type estremamente rari (ad esempio le catastrofi naturali) per i quali è inopportuno distinguere i due casi (likely e worst) perché la situazione che genera l'incidente è già di per sé talmente grave da rendere inutile la valutazione del peggiore dei casi. I single case di norma devono avere una frequenza debole dell'ordine di 1/100 per anno e non si giustificano per frequenze dell'ordine di 1 per anno.

Ad ognuno dei casi descritti prima, deve essere valutata la frequenza (frequency) di accadimento, ovvero il numero di volte in cui un loss event type ICT/Cyber è suscettibile di verificarsi in un determinato periodo (es. 1 anno). La frequenza del caso verosimile di un evento è in genere simile alla frequenza media degli eventi, mentre la frequenza del peggiore dei casi è spesso molto più bassa.

Generalmente si stima la frequenza del likely case a partire dai dati storici, mentre la frequenza del worst case sarà determinata analizzando differenti parametri, come le cause/minacce, i controlli e i dati esterni. La frequenza del peggiore dei casi non deve essere inferiore a 0,001 (ossia un caso ogni 1000 anni) e deve essere rara rispetto al caso verosimile, senza per questo che la differenza sia troppo grande. Un buon rapporto tra frequenza del likely case e del worst case è inferiore a 100.

Identificata la frequenza, viene quantificato l'impatto economico (severity) pe rognuno dei casi indicati prima che è la somma di tutti gli impatti finanziari netti di perdita, guadagno o mancato guadagno relativi a tutte le attività collegate al loss event type ICT/Cyber. La severity rappresenta di fatto la gravità del danno. Il risultato della quantificazione deve essere coerente con i dati storici interni ed esterni disponibili e con le valutazioni di rischio inerente effettuati sugli asset ICT in ambito analisi e valutazione dei rischi ICT e Cyber.

Può capitare che alcuni loss event type ICT/Cyber non hanno dati di perdita perché mai accaduti. In questo caso, i dati possono essere stimati attraverso un assessment quantitativo effettuato con i Process Owner delle diverse funzioni di Business che hanno processi supportati dall'asset ICT cui il loss event type afferisce.

Il giudizio dei Process Owner è utilizzato anche quando le osservazioni nella serie storica non sono sufficienti. Il giudizio dei Process Owner è anche utilizzato per quantificare l'esposizione rischiosa nei confronti di eventi rari e ad alto impatto. Le stime, soprattutto in assenza totale di dati storici, possono sfociare in margini di soggettività ed eventuali distorsioni e devono perciò essere rilevate nella fase di revisione della quantificazione

dei loss event type ICT/Cyber utilizzando i risultati dell'analisi dei rischi ICT/Cyber e/o dati andamentali di gestione.

Nella quantificazione dei loss event type ICT/Cyber devono essere considerati anche dei fattori aggravanti o d'attenuazione nella misura della frequenza o della severity.

In pratica, bisogna analizzare:

- le cause/minacce che hanno un'influenza diretta sulla frequenza degli eventi attraverso la loro probabilità di accadimento (informazione ricavabile dall'analisi dei rischi ICT). La gravità può essere influenzata da alcune cause/minacce che possono determinare il verificarsi del worst case;
- i fattori di contesto che possono determinare la generazione di casi e influenzare per definizione la gravità e la stima della frequenza. I fattori di contesto operativo sono principalmente finalizzati ad incorporare nella stima del requisito patrimoniale una componente prospettica che rifletta l'evoluzione del profilo di rischio ICT/Cyber a seguito delle variazioni intervenute sugli asset ICT, sui processi operativi, sulle risorse umane, tecnologiche ed organizzative. La scelta di ciascun fattore deve essere giustificata dalla sua capacità predittiva dell'esposizione ai rischi operativi. L'analisi del contesto di business e operativo, ovvero dei fattori di contesto in ottica evolutiva, è fondamentale nella valutazione dell'impatto di un loss event type ICT/Cyber. Una mutazione di contesto può infatti determinare una differenza sostanziale nel livello del rischio associato ad loss event type ICT/Cyber e quindi della frequenza e della gravità dello stesso.
- i controlli ICT implementati sull'asset. Come detto in precedenza, vengono censiti i controlli implementati, ma anche quelli mancanti che quelli inefficaci. Qualora la valutazione dell'implementazione dei controlli e della loro efficace non sia soddisfacente, si devono apportare dei correttivi sia alla frequenza (incremento percentuale del valore stimato) e/o alla severity stimata per il loss event type ICT/Cyber per compensare l'inadeguatezza dei controlli ICT sugli asset. Tali correttivi possono essere derivati dai risultati dell'analisi dei rischi ICT/Cyber effettuata sugli asset ICT.

Revisione della quantificazione dei loss event type ICT/Cyber

Una volta completata l'analisi quantitativa dei loss event type ICT/Cyber, è utile effettuare una revisione della quantificazione effettuata al fine di affinare l'analisi ed evitare potenziali sovrastime/sottostime dei rischi e quindi delle frequenze e delle severity ottenute per i likey case e i worst case degli loss event type ICT/Cyber analizzati.

Un primo criterio per revisionare la quantificazione dei loss event type ICT/Cyber è l'analisi dello scarto tra le frequenze.

Il caso verosimile (likely case) può essere in genere determinato in maniera univoca, anche sulla base degli incidenti occorsi, se la serie dei dati è esaustiva. Esiste per contro spesso un certo margine di discrezionalità per posizionare il peggiore dei casi (worst case).

Per stabilire in modo appropriato l'impatto e la frequenza del peggiore dei casi si possono seguire i seguenti criteri:

- la frequenza del peggiore dei casi deve essere bassa in confronto a quella del caso verosimile. In questo modo, il peggiore dei casi è davvero rappresentativo del livello di rischio estremo associato al loss event type ICT/Cyber considerato;
- non è corretto basare il peggiore dei casi su una situazione troppo improbabile per la quale la frequenza annua risulti molto bassa in quanto un simile approccio non è utile per la sua quantificazione.

La quantificazione del peggiore dei casi risulta tanto più imprecisa quanto più il peggiore dei casi si allontana dal caso verosimile. Generalmente non è utile prevedere un caso peggiore che risulti essere oltre 1000 volte più raro del caso verosimile. Nel caso in cui un loss event type ICT/Cyber presenta delle manifestazioni molto frequenti ma di impatto modesto e anche manifestazione molto più rara ma significativamente più grave, è preferibile sviluppare due loss event type ICT/Cyber distinti, uno con riferimento alle perdite correnti e l'altro con riferimento alle perdite estreme, ciascuno dei quali quantificato con un proprio caso verosimile ed un proprio caso peggiore.

A titolo indicativo, si possono utilizzar i seguenti parametri:

- un rapporto tra le frequenze di 100 sia adeguato a un loss event type ICT/Cyber che si verifica una volta l'anno o più;
- per un loss event type ICT/Cyber che si verifica una volta ogni 10 anni, un rapporto tra le frequenze compreso tra 5 e 10 è più appropriato;
- per loss event type ICT/Cyber molto rari (frequenza annua dell'ordine di 1/100 o meno) è sufficiente un rapporto tra le frequenze di 2 o 3.

Queste indicazioni non costituiscono, tuttavia, una regola assoluta e quindi il metodo migliore consiste nel determinare il valore dei fattori di quantificazione in modo che il rapporto tra le frequenze del caso verosimile e del caso peggiore rientri in una forbice accettabile.

Se ciò non è vero, si possono considerare una delle seguenti alternative:

- rivedere la modellizzazione in modo da ricondurre i valori entro i limiti di tolleranza se ciò non pregiudica la rappresentabilità del loss event type ICT/Cyber;
- dividere il loss event type ICT/Cyber in due eventi diversi;
- trattarlo come single case (ciò è ammesso solo nei casi in cui l'impatto è fisso e non è possibile ipotizzare un impatto diverso).

I risultati della quantificazione del likely case e del worst case devono comunque rispettare i seguenti principi:

- il likely case (LC) rappresenta le situazioni più frequenti;
- il worst case (WC) rappresenta le situazioni più gravi;
- la frequenza LC (FLC) deve essere superiore a quella WC (FWC);
- l'impatto unitario LC (SLC) deve essere inferiore a quello WC (SWC);

Quanto esposto si esplicita nel rispetto di alcuni criteri che portano ad escludere il loss event type ICT/Cyber dal calcolo del capitale se si verificano una o più delle seguenti condizioni:

FLC=0 FWC=0; SLC = 0 SWC = 0;

FLC <= FWC SLC >= SWC.

Infine, deve essere rivista anche la stima dell'impatto o "severity" associato ai loss event type ICT/Cyber.
Tale valore è misurato come la somma di tutti gli effetti generati dal loss event type ICT/Cyber. Nei casi in cui la serie storica delle perdite presenti caratteristiche tali da fornire una base solida per la valorizzazione della severity di un loss event type ICT/Cyber, i dati devono essere utilizzati per quantificare likely case e worst case.
Un metodo è quello di simulare le occorrenze del loss event type ICT/Cyber tra il caso verosimile ed il peggiore dei casi. Tale simulazione si effettua supponendo continue le distribuzioni di frequenza ed impatto, ciò significa che le situazioni intermedie tra i due casi devono essere possibili. Se tale ipotesi non è verificata, sarà necessario generare due loss event type ICT/Cyber distinti.
Una regola semplice comunque consiste nell'elaborare il peggiore dei casi estrapolandolo dal caso verosimile ed immaginando valori avversi dei fattori di quantificazione. Nel caso di presenza di dati storici la perdita più elevata non deve superare il valore del worst case.

Quantificazione perdita annuale pesata per singolo loss event type ICT/Cyber

Una volta identificati, quantificati e rivisti tutti i loss event type ICT/Cyber, si può calcolare la perdita annuale pesata (Weighted Annual Loss – WAL) che è basata sui valori di impatto e frequenza dei casi likely e worst associati al loss event type ICT/Cyber.
La formula da utilizzare è la seguente:

$$WAL = (F_l * S_l) + (F_w * S_w)$$

dove:

F_l è la frequenza del likely case

S_l è la severity del likely case

F_w è la frequenza del worst case

S_w è la severity del wort case

La quantificazione della Perdita annuale pesata per ogni loss event type ICT/Cyber ha la principale finalità di effettuare una classificazione dei loss event type ICT/Cyber per ipotizzare processi di gestione e monitoraggio differenziati.

In pratica, per i loss event type ICT/Cyber che registrano i valori maggiori di perdita si definiscono e implementano in priorità dei piani di remediation finalizzati alla risoluzione delle cause/minacce che possono provocarli.

Analogamente, si implementa per questi un processo di monitoraggio che cerca di anticipare il verificarsi dell'evento sia rivedendo le stime della frequenza e della severity di tali loss event type in periodi più brevi (es. ogni 3 – 6 mesi) sia definendo delle soglie di alerting che servono per attivare delle azioni di contrasto immediate finalizzate a impedire che le perdite si verifichino o comunque limitarle.

Ovviamente l'approccio dipende dal tipo di evento e può essere reattivo o proattivo o un mix di entrambi.

A titolo esemplificativo, eventi naturali catastrofici richiedono sia un approccio proattivo (predisposizione di un sito alternativo di Disaster recovery del sistema informativo allineato al sito principale) sia reattivo (attivazione del sito alternativo al verificarsi dell'evento).

Analogamente, un attacco di tipo ransomware che punta a cifrare i dati della banca per creare indisponibilità del sistema informativo, richiede un approccio prevalentemente reattivo basato su un sistema di monitoraggio tecnico che rilevi l'attacco nella maniera più tempestiva e consenta di attivare delle azioni di contrasto immediate che ne impediscano la diffusione. Anche in questo caso, si possono ipotizzare delle soluzioni di tipo proattivo (ad esempio la implementazione dei cosiddetti "backup off line" o "backup nascosti") che possono essere attivati nel momento in cui il sistema di monitoraggio implementato non ha funzionato e l'attacco ha avuto successo. In tale caso si limita la perdita totale dei dati o il pagamento del riscatto richiesto in quanto si possono recuperare i dati anche se ad un intervallo di tempo antecedente (es. 1-2 giorni).

3.4 Integrazione degli Operational Cyber Risk nei rischi operativi delle banche che hanno adottato il modello AMA

Una volta identificati i loss event type ICT/Cyber, si procede alla loro integrazione nei rischi operativi della banca in accordo al modello utilizzato dalla stessa. Uno degli approcci più utilizzati per la gestione dei rischi operativi è il modello AMA proposto dagli accordi di Basilea 2 che stabilisce dei requisiti minimi di ammissibilità; viene però lasciato a discrezione delle singole banche la facoltà di utilizzare il proprio modello interno utilizzato per la misurazione del rischio operativo, il quale viene verificato prima da parte delle autorità di vigilanza nazionali in merito alla presenza di determinate condizioni. Tra queste condizioni vi sono:

- L'abilità della banca di correlare i dati interni sulle perdite a specifiche linee di business e/o categorie di eventi;
- La competenza nel dimostrare che la misura del rischio generata dal modello sia calcolata su un arco di tempo di un anno e con un livello di fiducia estremamente elevato (99.9%);
- L'esistenza di un'unità autonoma dedicata al monitoraggio e alla gestione del rischio;
- Il coinvolgimento attivo del Consiglio di Amministrazione e dei vertici aziendali nella supervisione del processo di gestione del rischio operativo.

Tra le metodologie AMA, l'approccio LDA (Loss Distribution Approach), derivata dalle scienze attuariali, è l'approccio che nel tempo si è affermato come lo standard di riferimento nell'ambito della modellizzazione del rischio operativo. Come già precedentemente illustrato (vedi par. 1.1.5.3), l'approccio LSA si basa principalmente sull'utilizzo dei dati di perdita interna per creare una distribuzione associata alla perdita. L'efficacia di questa tecnica risiede nell'uso di dati interni, che sono specifici e rilevanti per la banca in questione. Per quanto riguarda il funzionamento effettivo, LDA impiega un metodo statistico in cui la banca determina, per ogni linea di attività e tipo di rischio, le funzioni di distribuzione di probabilità dell'effetto di un singolo evento e la frequenza dell'evento per il seguente (un) anno utilizzando i suoi dati interni, e successivamente calcola la funzione di distribuzione di probabilità della perdita operativa totale.

In questo paragrafo non si descriverà il funzionamento del modello LSA in quanto già ampiamente descritto nel par. 1.1.5.3, ma si analizzeranno gli aspetti peculiari dei rischi ICT e Cyber che devono essere considerati e trattati per poter procedere nella integrazione di tali rischi nel modello di gestione dei rischi operativi della banca.

Ripartizione dei rischi ICT e Cyber sui processi aziendali e sulle funzioni aziendali/Linee di business che li gestiscono.

Come illustrato nel paragrafo precedente, i loss event type ICT/Cyber sono abbinati agli asset ICT che nell'analisi e valutazione dei rischi ICT hanno registrato un valore del rischio residuo superiore alla soglia di accettazione di tali rischi stabilita dalla banca. Per gli altri asset ICT si assume che le perdite sono tollerabili e quindi non vengono considerati.

Va comunque osservato che lo stesso loss event type ICT/Cyber può essere abbinato a più asset ICT quando la causa che lo può provocare è la stessa. Ovviamente la severity (ovvero l'impatto) può essere diverso e, in tali casi, si procede alla duplicazione del loss event type in due eventi distinti. A titolo esemplificativo, un loss event type ICT/Cyber che ha come effetto un data breach ha un valore d'impatto diverso se applicato ad un asset ICT che ha dati personali e uno che non ne ha.

Gli asset ICT sono mappati sui processi aziendali che supportano, ma tale mappatura non è univoca in quanto l'asset ICT generalmente è utilizzato da più processi. Nei casi più estremi, l'asset ICT è trasversale a tutta la banca (vedi ad esempio gli asset ICT della rete di telecomunicazioni della banca) e quindi un evento su di esso ha un impatto su tutti i processi della banca.

Per tale ragione, prima di procedere alla integrazione dei rischi ICT e Cyber nei rischi operativi, bisogna ripartire i loss event type ICT/Cyber identificati sui processi della banca rivendendo la stima della severity sulla base delle caratteristiche dei processi.

Tale attività può essere effettuata con i process owner dei processi impattati attraverso un assessment attraverso i quali essi stabiliscono quale è la perdita imputabile ai processi di pertinenza, fermo restando le frequenze stabilite. Va considerato che tale analisi viene già effettuata nell'ambito del processo di analisi e valutazione dei rischi ICT e Cyber dove i process owner hanno indicato l'impatto sui loro processi

relativamente agli scenari di riservatezza, integrità e disponibilità degli asset ICT che li supportano[33]. Per tale ragione, è buona prassi arricchire il processo di valutazione e analisi dei rischi ICT e Cyber in modo da avere a disposizione questi dati di dettaglio che possono essere utilizzati già nella fase di identificazione e quantificazione dei loss event type ICT/Cyber soprattutto per quanto riguarda il worst case.

Analogamente, una volta valutato il rischio residuo sugli asset ICT, si può ribaltare tale rischio sui processi che supportano usando la stessa ripartizione utilizzata per ripartire il rischio inerente. Il valore di impatto del rischio residuo può essere utilizzato per valutare la severity del likely case.

Altra informazione utile per avere la ripartizione della severity sui processi supportati dagli asset ICT è l'analisi sugli incidenti occorsi e sulle perdite registrate. Tale valore può essere utilizzato come confronto per verificare che la severity stimata è realistica o meno.

Infine, per gli asset ICT trasversali a tutti i processi aziendali, i loss event type ICT/Cyber che vi afferiscono dovrebbero essere classificati come single case che hanno, come detto prima, solo il worst case.

In questo caso, l'impatto su ogni processo aziendale è valutato processo per processo considerando gli effetti che il loss event type ICT/Cyber ha su ognuno di essi.

A titolo esemplificativo, un attacco ransomware che cifra tutti i dati della banca di fatto blocca la completa operatività della stessa. La stima della severity deve essere fatta considerando il tempo che la banca impiega per il recupero dei dati (es. 1-2 giorni) e ripartire tale severity sui vari processi valutando quali sono gli impatti sul processo (es. mancati ricavi, costi operativi, ecc) se esso non può operare per 1-2 giorni.

Frequenza dei loss event type ICT/Cyber

Considerando la tipologia di tali eventi e la loro continua evoluzione no predicibile a priori, esiste per questi eventi la concreta probabilità di avere eventi sempre nuovi con effetti molto elevati se non distruttivi. Per tale ragione, un'analisi dei rischi operativi connessi agli eventi ICT e Cyber deve essere preferibilmente basata sulla coppia caso verosimile e caso estremo per aumentare in maniera significativa la componente prospettica della quantificazione di tali rischi. Tra l'altro, in tale configurazione, anche la modellizzazione della severity può utilizzare una distribuzione giunta (spliced distribution) ove il "corpo" della distribuzione, relativo alle perdite dei casi verosimili, è modellato secondo una distribuzione comune (ad esempio la Weibull, la Log-Normale o anche la distribuzione empirica), mentre la coda della distribuzione, relativa alle perdite più rare ma di maggior impatto è tipicamente caratterizzata attraverso tecniche della Extreme Value Theory.

A titolo esemplificativo, gli attacchi ransomware sono diventati sempre più diffusi negli ultimi anni diventando di fatto l'attacco più diffuso e temuto. Negli ultimi tempi, si sono diffusi gli attacchi detti "double extortion" dove gli attaccanti rubano i dati, poi li cifrano e ricattano l'azienda minacciandola di pubblicare on line i dati. Di fatto questo è un nuovo scenario che estende la finalità classica del ransomware (cifrare i dati per creare

[33] Il rischio inerente su un asset ICT è valutato come il massimo degli impatti sull'asset relativamente agli scenari di riservatezza, integrità e disponibilità

indisponibilità degli asset ICT e chiedere un riscatto per decifrarli) ad un data breach dei dati finalizzata anch'essa alla richiesta di un riscatto.
Altro esempio eclatante successo negli ultimi mesi, lo scoppio della guerra in Ucraina ha aumentato in maniera considerevole la possibilità di "attacchi distruttivi" da parte di hacker russi mirati alla distruzione totale, e non recuperabile, di tutti i dati dell'azienda. Questo ha spinto tutte le Autorità nazionali ed europee a sollecitare le aziende critiche, incluse le banche, del proprio Paese ad adottare nella maniera più tempestiva soluzioni tecniche per proteggersi da tali attacchi (es. effettuare il backup di tutti i dati aziendali su supporti rimovibili da portare in un sito remoto non connesso alla rete). Quindi uno scenario che caso mai non era stato considerato perché molto poco probabile, adesso diventa un caso con una concreta probabilità di accadere.
Da quanto detto si evince che i casi estremi in ambito rischi ICT e Cyber assumono una estrema rilevanza e quindi devono essere accuratamente identificati e quantificati perché forniscono quella visione prospettica che in ambito rischi Cyber è essenziale. Non è un caso che uno dei limiti che si è riscontrato nel modello LSA applicato ai rischi ICT e Cyber nelle banche è proprio connesso alla gestione dei casi peggiori perché generalmente le banche, per ovvi motivi, tendono a sottostimare tali casi sottostimando di fatto i rischi connessi.

3.4 Evoluzioni future

Come indicato nella introduzione della tesi, l'evoluzione della tecnologia ha spinto le banche ad innovare le loro modalità di svolgimento di determinate attività, iniziando a fare sempre più affidamento su sistemi di information e communication technology (ICT). Se da una parte l'utilizzo della tecnologia consente alle banche di ottimizzare i processi operativi e di offrire servizi sempre più innovativi (vedi ad esempio i pagamenti on line e il mobile payment), dall'altra espone le banche a dei rischi nuovi non sempre conosciuti e completamente compresi: i rischi Cyber.
Inoltre, il sempre maggiore utilizzo di terze parti da parte delle banche per acquisire competenze e tecnologie non presenti internamente e per ottimizzare i costi, rende le banche molto vulnerabili rispetto ai rischi ICT e Cyber in quanto possono provenire dalle infrastrutture tecniche di tali soggetti che non sono sotto il loro diretto controllo. I rischi diventano ancora più gravi quando i dati della banca sono gestiti sulle piattaforme tecnologiche delle sue terza parti.
In questo scenario molto complesso dove stanno comparendo anche nuovi attori (le cosiddette FinTech) che basano i loro business sull'utilizzo della tecnologia, le principali Autorità nazionali ed europee hanno compreso che devono intervenire in maniera tempestiva per evitare impatti significativi su tutto il settore finanziario considerando anche la sua estrema interconnessione.
Le principali iniziative di tali autorità, descritte al par. 2.2, mirano a superare, almeno dal punto di vista regolamentare, i limiti e le difficoltà che oggi sono presenti sulla gestione dei rischi ICT e Cyber:

- la continua e veloce evoluzione di tali rischi connessa alla evoluzione tecnologia che, se da un lato offre sicuramente nuove opportunità di business per gli operatori del settore, dall'altro rende gli attacchi cyber sempre più innovativi, impattanti e difficilmente predicibili;
- la scarsità delle informazioni connesse a tali rischi dovuta sia all'evoluzione della tecnologia, ma soprattutto alla resistenza degli operatori del settore a condividere le informazioni legate agli incidenti cyber occorsi visto il loro elevato impatto reputazionale. Come detto in precedenza, il successo dei servizi finanziari si basa molto sulla fiducia dei clienti verso il fornitore di tali servizi e un incidente cyber, soprattutto quando è molto impattante, può ledere in maniera significativa tale fiducia.

In tale contesto è emblematico il Regolamento europeo DORA (vedi par. 2.2.3) che indica chiaramente le direzioni in cui le autorità vogliono agire:

- gestione dei rischi ICT e Cyber, sia interni che delle terze parti, efficace attraverso l'obbligo di adempimenti stringenti sulla governance interna, sulle metodologie di analisi e valutazione dei rischi e sulle misure di sicurezza;
- comunicazione tempestiva degli incidenti cyber in modo da anticipare ed evitare la sua propagazione e il "contagio" tra i vari operatori;
- monitoraggio delle minacce e delle vulnerabilità più efficiente anche attraverso la simulazione di attacchi utilizzando le stesse tecniche degli hackers;
- creazione di una base dati condivisa tra gli operatori si tutte le informazioni correlate ai rischi ICT e Cyber al fine di utilizzarle in maniera proficua per la loro gestione.

In sintesi, l'obiettivo delle autorità è quello di ottenere una "compliance normativa" per gestire e difendersi da tali rischi e, nel contempo, forzare la sua implementazione presso tutti gli operatori del settore anche attraverso la commisurazione di sanzioni elevate.

Anche nell'ambito della quantificazione dei rischi operativi ci sono delle iniziative in corso che cercano di superare i limiti ad oggi esistenti. Non è un caso alcune delle iniziative in corso nell'ambito della revisione degli accordi di Basilea 3 (il cosiddetto Basilea 4) stanno puntando a rivedere le metodologie di quantificazione dei rischi operativi per aumentare in maniera significativa la parte prospettica e la gestione dei casi estremi al fine di superare il limite delle attuali metodologie che si basano prevalentemente sui dati di perdita storici.

4 Bibliografia

- *Maike Sundmacher, "THE BASIC INDICATOR APPROACH AND THE STANDARDISED APPROACH TO OPERATIONAL RISK: AN EXAMPLE- AND CASE STUDY- BASED ANALYSIS"* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=988282
- *Ewa Dziwok, "Methods of measuring operational risk and their influence on the level of bank's capital adequacy"* file:///Users/lavinia/Downloads/Methods_of_measuring_operational_ri.pdf
- *Davide Bazzarello, Bert Crielaard, Fabio Piacenza, Aldo Soprano, "Modeling insurance mitigation on operational risk capital"* https://web.archive.org/web/20061105041515id_/http://www.journalofoperationalrisk.com/data/jop/pdf/jop_v1n1a4.pdf
- *Chiara Cornanlba, Paolo Giudici, 2004, "Statistical models for operational risk management"* https://reader.elsevier.com/reader/sd/pii/S0378437104002341?token=DF191E8AC98F0086E204ABA2BC5BC56E51E6C93CB58BF980E3B43309F5068E31F1C8717E12597A5EEE51806F479D4F63&originRegion=eu-west-1&originCreation=20230228101950
- *Marcelo Cruz, Rodney Coleman, and Gerry Salkin, "Modeling and measuring operational risk"* https://www.researchgate.net/profile/Rodney-Coleman/publication/264847105_Modeling_and_measuring_operational_risk/links/5457b47c0cf2bccc49111464/Modeling-and-measuring-operational-risk.pdf
- *Bente Corneliu, "The management of operational risk in banks"* https://www.proquest.com/docview/1032810798/fulltextPDF/1388920296B84E12PQ/1?accountid=16503
- *Black Sea Trade & Development Bank, "Operational risk management policy"* https://www.bstdb.org/Operational_Risk_Management_policy.pdf
- *Akkizidis I. S., Bouchereau V. (2005) – "Guide to Optimal Operational Risk and BASEL II"* https://www.taylorfrancis.com/books/mono/10.1201/9781420031140/guide-optimal-operational-risk-basel-ii-ioannis-akkizidis-vivianne-bouchereau
- *Banca d'Italia, Novembre 2006, RECEPIMENTO DELLA NUOVA REGOLAMENTAZIONE PRUDENZIALE INTERNAZIONALE, PROCESSO DI CONTROLLO PRUDENZIALE AI SENSI DEL SECONDO PILASTRO: DETERMINAZIONE DEL CAPITALE INTERNO ADEGUATO.* https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/secondo_pilastro_icaap.pdf

- *R. Locatelli, E. Magistretti, P. Scaleandri, G. Carosio, 9 Novembre 2001, "IL RISCHIO OPERATIVO", Roma.*
  https://www.assbb.it/wp-content/uploads/2014/10/QR_193.pdf
- *Marco Ferfoglia, 15 Luglio 2019, "Basilea IV: il framework normativo".*
  https://www.borsaitaliana.it/notizie/sotto-la-lente/approfondimenti/basilea-3.htm
- *Borsa Italiana, 21 Settembre 2022, "Basilea 3: cosa prevede".*
  https://www.borsaitaliana.it/notizie/sotto-la-lente/approfondimenti/basilea-3.htm
- *Andrea Vivoli, 3 Febbraio 2020, "Il rischio operativo nel nuovo framework di Basilea IV", Risk and Compliance Platform Europe.*
  https://www.riskcompliance.it/news/il-rischio-operativo-nel-nuovo-framework-di-basilea-iv/
- *Andrea Giacchero, Giugno 2010, "Rischi operativi: definizione, contesto normativo e classificazione dei rischi operativi", Università Tor Vergata, Roma.*
  https://didattica-2000.archived.uniroma2.it//ASF_II/deposito/Rischi_operativi.pdf
- *Francesco Rossi, 28 Giugno 2018, "Gli accordi di Basilea", Starting Finance*
  https://startingfinance.com/approfondimenti/accordi-di-basilea/
- *Associazione Nazionale per lo Studio dei Problemi del Credito, Roma, 4 novembre 2021, "Le banche e gli anni di Basilea III"*
  https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2021/Signorini-4-novembre-2021.pdf
- *A. Frachot, P. Georges & T. Roncalli, Groupe de Recherche Op´erationnelle, Cr´edit Lyonnais, France, 25 Aprile 2001, "Loss Distribution Approach for operational risk"*
  https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1032523
- *Toshihiko Mori, Senior Manager Eiji Harada, Financial Analyst, Bank of Japan, 14 Marzo 2001, "Internal Measurement Approach to Operational Risk Capital Charge"*
  https://www.boj.or.jp/en/research/wps_rev/wps_2001/data/fwp01e02.pdf
- *Paolo Giudici, Università di Pavia, Novembre 2015, "Scorecard models for operations management"*
  https://www.academia.edu/2715963/Scorecard_Models_for_Operational_Risk_Management
- *Massimo Livatino, Paola Tagliavini, "I sistemi per la gestione del rischio, Modelli operativi, ruoli e responsabilità"*
  https://www2.deloitte.com/content/dam/Deloitte/it/Documents/risk/Board%20Academy%20Corso%20C6%2020%20dic%202012%20SDA%20Bocconi.pdf
- *Comitato di Basilea per la vigilanza bancaria, Gennaio 2001, "Presentazione del Nuovo Accordo di Basilea sui requisiti patrimoniali".*
  https://www.bis.org/publ/bcbsca02_i.pdf

- *Comitato di Basilea per la vigilanza bancaria, Giugno 2006, "Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali".*
  https://www.bis.org/publ/bcbs128ita.pdf
- *Comitato di Basilea per la vigilanza bancaria, Dicembre 2010, "Basilea 3- Schema di regolamentazione internazionale per il rafforzamento delle banche e dei sistemi bancari."*
  https://www.bis.org/publ/bcbs189_it.pdf
- *Banca d'Italia, Marzo 2006, "RECEPIMENTO DELLA NUOVA REGOLAMENTAZIONE PRUDENZIALE INTERNAZIONALE (NUOVO ACCORDO SUL CAPITALE DI BASILEA E NUOVA DIRETTIVA C.E. SUI REQUISITI DI CAPITALE DELLE BANCHE E DELLE IMPRESE DI INVESTIMENTO), RISCHI OPERATIVI (Metodi Base e Standardizzato) "*
  https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Doc_Cons_Rischi_operativi.pdf
- *Gazzetta ufficiale dell'Unione europea, 28 settembre 2005, "RISCHIO OPERATIVO"*
  https://eur-lex.europa.eu/resource.html?uri=cellar:d7660f93-1ff2-4c80-a0d4-98f1f4b35194.0011.02/DOC_63&format=PDF
- *Banca d'Italia, Luglio 2006, "RECEPIMENTO DELLA NUOVA REGOLAMENTAZIONE PRUDENZIALE INTERNAZIONALE, RISCHI OPERATIVI (Metodi Avanzati - AMA)"*
  https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Rischi_operativi_metodi_avanzati_AMA.pdf
- *Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici and Thomas Leach – "Operational and cyber risks in the financial sector" - BIS Working Papers No 840, February 2020*
  https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549526
- *Grzegorz Strupczewski, 2021, "Defining cyber risk", Department of Risk Management and Insourance, The Cracow University of Economics*
  https://reader.elsevier.com/reader/sd/pii/S092575352030539 7?token=D5793B92313EA508EE7CF765DC91FA1A00E87A002464D65DFF9DBC076BB3CBDA9FA75C2C3D8C37668BFF5EBE1532EFB8&originRegion=eu-west-1&originCreation=20230228112349
- *R. Egan*, S. Cartagena, R. Mohamed, V. Gosrani, J. Grewal, M. Acharyya, A. Dee, R. Bajaj, V.-J. Jaeger, D. Katz, P. Meghen, M. Silley, S. Nasser-Probert, J. Pikinska, R. Rubin and K. Ang, Ottobre 2017, "Cyber operational risk scenarios for insurance companies"*
  https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C90FF5F4EC6682A01E91F4E63A05F961/S1357321718000284a.pdf/cyber-operational-risk-scenarios-for-insurance-companies.pdf
- *James J. Cebula, Lisa R. Young – "A Taxonomy of Operational Cyber Security Risks" - Carnegie Mellon University Software Engineering, Dicembre 2010*

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395

- *Martin Eling, Settembre 2017, "What are the actual costs of cyber risk events", Insitute of Insourance Economics, University of St. Gallen*
  https://reader.elsevier.com/reader/sd/pii/S037722171830626X?token=762DB3774026902FDEE4CBCE840C225AA158AAC1D97ABA72CF2591992038E920D73D07CADE42B0FB3391540441BADE36&originRegion=eu-west-1&originCreation=20230228092101
- *Banca d'Italia, "Disposizioni di vigilanza per le banche, Circolare n. 285 del 17 dicembre 2013"*
  https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Circ_285_20_Aggto_Testo_integrale_ec-firmato.pdf
- *David Cecchi, "Direttiva PSD2 e sicurezza dei pagamenti online: nuovi strumenti e problematiche d'uso", 20 Novembre 2019*
  https://www.cybersecurity360.it/soluzioni-aziendali/direttiva-psd2-e-sicurezza-dei-pagamenti-online-nuovi-strumenti-e-problematiche-duso/
- *Domenico Gammaldi, 14 Novembre 2017, "PSD2 e cybersecurity, Banca d'Italia: queste le regole che proteggono la nuova fase die pagamenti"*
  https://www.agendadigitale.eu/cittadinanza-digitale/psd2-banca-ditalia-queste-le-regole-che-proteggeranno-la-nuova-fase-dei-pagamenti/
- website: "Pagamenti digitali.it", 17 Giugno 2022, "Strong Customer Authentication (SCA): cos'è, come funziona, obblighi per ecommerce e negozianti online"
  https://www.pagamentidigitali.it/payment-regulation/psd2/strong-customer-authentication-sca-cose-come-funziona-obblighi-per-ecommerce-e-negozianti-online/
- *Global Open Banking Ecosystem, "Nuova normativa PSD2"*
  https://www.cbiglobe.com/Il-servizio/PSD2?gclid=CjwKCAjwov6hBhBsEiwAvrvN6OULO-Rcj44WZUWppDm02kW5oaqfTmFN-Alf4p3HGYpoeOv1EQNMmRoCHlUQAvD_BwE
- *Ivano Asaro, Valeria Portale, Matteo Risi, Matteo Ruggieri, 24 Giugno 2022, "PSD2: cos'è, obblighi e funzionamento della direttiva europea"*
  https://www.pagamentidigitali.it/payment-regulation/psd2/psd2-cose-obblighi-e-funzionamento-della-direttiva-europea/
- *EBA, 28 Novembre 2019, "Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza"*
  https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880818/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_IT.pdf

- *Gazzetta Ufficiale dell'Unione Europea, "REGOLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022"*
  https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2554
- *Hal S. Scott, Settembre 2021, "The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies"*
  https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904113
- *Dirk Clausmeier, 16 Dicembre 2022, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)"*
  https://link.springer.com/article/10.1365/s43439-022-00076-5
- *Laura Friio, Arianna Martella, 22 Novembre 2022, "DORA – Digital Operational Resilience Act, cos'è, quando entrerà in vigore"*
  https://www.pagamentidigitali.it/esperti-e-analisti/dora-digital-operational-resilience-act-cose-quando-entrera-in-vigore/
- *Alberto Stefani, 27 Agosto 2020, "Cos'è la metodologia IRAM2 per la gestione dei rischi aziendali"*
  https://www.riskmanagement360.it/risk-assessment/cose-la-metodologia-iram2-per-la-gestione-dei-rischi-aziendali/
- *"The Quality Toolbox", "FAILURE MODE AND EFFECTS ANALYSIS (FMEA)"*
  https://asq.org/quality-resources/fmea
- Pa*ul Kirvan, Carol Sliwa, "business impact analysis (BIA)"*
  https://www.techtarget.com/searchstorage/definition/business-impact-analysis
- *Bilge Karabacak, Ibrahim Sogukpinar, 2004 "A Novel Approach to Information Security Risk Analysis"*
  https://fuse.franklin.edu/cgi/viewcontent.cgi?article=1038&context=facstaff-pub
- *Bilge Karabacak, İbrahim Soğukpınar, 2004 "A Novel Approach to Information Security Risk Analysis"*
  https://academic.oup.com/cybersecurity/article/9/1/tyac016/7000422
- *Pavel V Shevchenko, Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, Stefan Trück, 2023 "The nature of losses from cyber-related events: risk categories and business sectors"*
  https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1954038/45cae55c-7985-43bc-8d41-486cf320acd6/Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29_IT.pdf?retry=1
- *EBA, 11 settembre 2017, "Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP)"*