



Impatti operativi del 40° aggiornamento della circolare 285/2013 della Banca d'Italia e regolamento DORA. Le regole per la resilienza operativa digitale nel settore finanziario

***Normativa Banca d'Italia – Circolare 285/2013
40° aggiornamento e Circolare 288***

Ing. Francesco Micillo
Presidente Commissione Informatica
Ordine degli Ingegneri della Provincia di Roma

Roma, 20 marzo 2024



Chi sono:

Ing. Francesco Micillo





Agenda:

- Trends regolamentari e normativi sul mercato finanziario
- Normativa Banca d'Italia – Circolare 285 e 288
- Normativa Banca d'Italia - 40° agg. Circolare 285
 - ❖ Quadro sinottico delle principali novità e loro portata innovativa
 - ❖ Il sistema dei controlli interni
 - ❖ Il sistema informativo
 - I compiti degli organi aziendali sui profili ICT
 - La funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza
 - La gestione della sicurezza dell'informazione, delle operazioni e dei progetti ICT
 - La gestione delle esternalizzazioni e delle terze parti
 - La sicurezza dei servizi di pagamento e la gestione del rapporto con gli utenti
 - ❖ La continuità operativa
- Focus su sicurezza e cyber security, rischi connessi e impatti Banca
 - ❖ Impatti e rischi IT e Cyber nel mondo bancario



Agenda:

- **Trends regolamentari e normativi sul mercato finanziario**

Trends regolamentari e normativi sul mercato finanziario

Regulatory Trends | E' in corso un processo articolato e pervasivo di evoluzione regolamentare che implica sfide da fronteggiare in ottica strategica e non di mero adeguamento regolamentare

CIRCOLARE 285

Il **40° Aggiornamento della Circolare 285** di Banca d'Italia entrato in vigore a partire dal 4 Novembre 2022 è stato prodotto al fine di integrare gli Orientamenti dell'EBA/GL/2019/04 in materia di **gestione dei rischi ICT e di sicurezza** attraverso importanti elementi di novità

OPERATIONAL RESILIENCE & CRITICAL THIRD PARTIES

Il nuovo **Regolamento DORA** (che fa parte della strategia per la finanza digitale della Commissione europea) metterà i player finanziari di fronte alla **necessità di rafforzare la loro resilienza informatica e operativa** attraverso nuovi e più stringenti requisiti

TRANSITION TO A SUSTAINABLE ECONOMY & CLIMATE RELATED RISK

Prosegue il percorso di attuazione progressiva della **roadmap ESG** per la **transizione verso un'economia sostenibile e green**, con riforme e misure che hanno un impatto su banche, compagnie assicurative e società di investimento

INNOVATION, PAYMENTS, DIGITAL ASSETS, DATA... and related RISKS

Per rispondere all'**evoluzione delle open/digital solutions** nei settori finanziari, sono in corso iniziative normative rilevanti per **regolamentare nuove aree di business** (es. MiCA for crypto-assets, new EU authority to fight ML/FT, PSD2 review ...) e garantire la **cybersecurity dei prodotti digitali**, nonché assicurare un quadro efficiente e sicuro per lo sharing dei dati

INTEGRATION OF CAPITAL MARKETS AND RETAIL CONDUCT

Nel 2023 sono previste alcune tappe fondamentali relative al **Piano d'azione 2020 Capital Markets Union (CMU)**, volto a promuovere la piena integrazione dei mercati finanziari, rafforzare l'accesso ai finanziamenti e facilitare le opportunità di investimento in tutta l'UE

Trends regolamentari e normativi

I player di sistema sono così posti di fronte ad una serie di sfide che impattano trasversalmente sulle strategie, sul business, sul modello organizzativo e operativo e sui presidi a fronte dei rischi attuali e prospettici. Emerge in modo netto l'esigenza di una visione globale e olistica dei rischi e di risposte di sistema in termini di prevenzione e gestione

Da un approccio tradizionale a silos...

Approccio reattivo tradizionale

Approccio basato sull'iniziativa dei singoli player spesso rivelatosi **inefficace** e non sufficiente a fronteggiare **scenari di rischio sempre più complessi e trasversali** che coinvolgono direttamente e/o indirettamente tutti gli attori della catena del valore aziendale (banca, terze e quarte parti, autorità di vigilanza, infrastrutture, istituzioni di settore, ...)

...ad una visione globale e olistica dei rischi

Approccio proattivo

Sulla scia dell'inaspettata **evoluzione dello scenario di mercato** e al sempre più **rapido processo di sviluppo della tecnologia** nel settore finanziario, è nata l'esigenza di un percorso **di rafforzamento del framework regolamentare** per renderlo funzionale a sollecitare un percorso, graduale ma rapido, di **raggiungimento di adeguati standard di resilienza operativa** del sistema finanziario

Implicazioni

Tali fattori e i rischi connessi hanno evidenziato l'importanza e la centralità della creazione di un **quadro normativo comunitario** che guidi verso **la gestione armonizzata del rischio informatico** e promuova **la resilienza operativa digitale** nel settore finanziario



Agenda:

- **Normativa Banca d'Italia – Circolare 285 e 288**

Normativa Banca d'Italia – Circolare 285

La Circolare n. 285 del 17 dicembre 2013, nell'ambito del *Titolo IV* «Governo societario, controlli interni e gestione dei rischi», all'interno del *Capitolo 5* in apposite sezioni, norma i **principi del sistema informativo**, strumento di primaria importanza per il **conseguimento degli obiettivi strategici e operativi delle Banche**.

Sezione II - Governo, organizzazione e controlli del sistema informativo

Le Banche attribuiscono agli organi e funzioni aziendali ruoli e responsabilità, relativi allo sviluppo e alla gestione del sistema informativo e dei rischi ICT e di sicurezza, nel rispetto del **principio della separazione** delle funzioni di controllo da quelle di supervisione e gestione.

Sezione III – La gestione del rischio ICT e di sicurezza

Il **processo di gestione dei rischi ICT e di sicurezza** è pienamente integrato e allineato con il **processo di gestione dei rischi della banca**. Le banche assicurano che **tutti i rischi ICT e di sicurezza assunti o assumibili** siano individuati, analizzati, misurati, monitorati, gestiti, comunicati e mantenuti entro i limiti della propensione al rischio ICT e di sicurezza della banca.

Sezione IV – La gestione della sicurezza dell'informazione e delle operazioni ICT

Sulla base della policy di sicurezza dell'informazione, devono essere stabilite e attuate misure di sicurezza per attenuare i rischi ICT e di sicurezza ai quali sono esposti. Inoltre, le operazioni ICT devono essere gestite sulla base di procedure e processi documentati¹. I gravi incidenti operativi o di sicurezza sono notificati tempestivamente alla Banca d'Italia, con l'invio di un **rapporto sintetico** recante una **descrizione** dell'incidente e dei **disservizi** provocati agli utenti interni e alla clientela, nonché degli **altri dati e informazioni** previsti dalle istruzioni emanate dalla Banca d'Italia.

Sezione IV BIS – La gestione dei progetti e dei cambiamenti ICT

Le Banche si dotano di **processi per la gestione dei progetti ICT nel corso del loro intero ciclo di vita**, l'acquisizione e lo sviluppo e la manutenzione di servizi e sistemi ICT, nonché per la gestione dei cambiamenti di tali servizi e sistemi².

Sezione V – Il sistema di gestione dei dati

Il sistema di registrazione e reporting dei dati è deputato a tracciare tempestivamente tutte le operazioni aziendali al fine di fornire informazioni complete e aggiornate sulle attività aziendali e sull'evoluzione dei rischi. Esso assicura nel continuo l'integrità, completezza e correttezza dei dati conservati e delle informazioni rappresentate; inoltre, garantisce l'**accountability** e l'**agevole verificabilità** (ad es. da parte delle funzioni di controllo) delle operazioni registrate.

Sezione VI – L'esternalizzazione del sistema informativo e il ricorso a soggetti terzi per la prestazione di servizi ICT

Devono essere attuate misure di governance interna, tra cui una **rigorosa gestione dei rischi**, in caso di **esternalizzazione** delle proprie funzioni, in particolare in caso di **esternalizzazione di funzioni essenziali o importanti**³.

Sezione VII – Disposizioni specifiche in materia di prestazione di servizi di pagamento

Le Banche che prestano servizi di pagamento applicano le disposizioni del Capitolo 4 e del Capitolo 5 anche con riferimento ai rischi operativi e di sicurezza dei servizi di pagamento⁴. Le Banche trasmettono a Banca d'Italia la relazione annuale dei rischi operativi e di sicurezza relativi ai servizi di pagamento e notificano senza indugio i gravi incidenti operativi o di sicurezza relativi ai servizi di pagamento.



Normativa Banca d'Italia – Circolare 285

La Circolare n. 285 del 17 dicembre 2013, nell'ambito del *Titolo IV* «Governance societaria, controlli interni e gestione dei rischi», all'interno del *Capitolo 5* norma i **principi della continuità operativa**. Le Banche adottano un **approccio esteso** che, partendo dalla **identificazione dei processi aziendali critici**, definisca per ciascuno di essi **presidi organizzativi** e **misure di continuità operativa commisurate ai livelli di rischio**.

Ambito del piano di continuità operativa

Le Banche **definiscono un piano di continuità operativa per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale**, aziendale ovvero a **catastrofi estese che colpiscono l'operatore o le sue controparti rilevanti** (altre società del gruppo; principali fornitori; clientela primaria; specifici mercati finanziari; sistemi di regolamento, compensazione e garanzia).

Analisi di impatto (*Business Impact Analysis, BIA*)

Preliminare alla stesura del piano di continuità operativa (periodicamente aggiornata), **individua il livello di rischio relativo ai singoli processi aziendali** sulla base di un **approccio quantitativo e qualitativo** e pone in **evidenza le conseguenze dell'interruzione del servizio**. I rischi residui, non gestiti dal piano di continuità operativa, sono **documentati ed esplicitamente** accettati dagli organi aziendali competenti.

Definizione del piano di continuità operativa e gestione delle crisi

- **Ruolo degli organi aziendali** - Il tema della continuità operativa è **adeguatamente valutato a tutti i livelli di responsabilità**.
- **Processi critici** – Si **identificano** in modo circostanziato i **processi relativi a funzioni aziendali di particolare rilevanza** che, per l'impatto dei danni conseguenti alla loro indisponibilità, **necessitano di elevati livelli di continuità operativa** da conseguire mediante **misure di prevenzione e con soluzioni di continuità operativa** da attivare in caso di incidente.
- **La responsabilità del piano di continuità operativa** - Il responsabile del piano di continuità operativa aziendale ha una **posizione gerarchico – funzionale adeguata**, **cura lo sviluppo del piano di continuità operativa, ne assicura l'aggiornamento nel continuo**, a fronte di cambiamenti organizzativi o tecnologici rilevanti, e ne verifica l'adeguatezza, con cadenza almeno annuale. Tale figura tiene inoltre i **contatti con la Banca d'Italia e con la Banca centrale europea in caso di crisi**.
- **Il contenuto del piano di continuità operativa** - Il piano operativo **documenta i presupposti e le modalità per la dichiarazione dello stato di crisi, l'organizzazione e le procedure da seguire** in situazione di crisi, **l'iter per la ripresa della normale operatività**.
- **Le verifiche** – Le Banche **sottopongono periodicamente a verifica i propri piani per la continuità operativa** delle funzioni, dei servizi, dei sistemi, delle transazioni e delle interdipendenze riferite ai processi critici.
- **Le risorse umane** - Il piano di continuità operativa **individua il personale essenziale per assicurare la continuità operativa dei processi critici e fornisce allo stesso indicazioni dettagliate sulle attività da porre in essere** in caso di crisi.
- **Ricorso a soggetti esterni per la prestazione di servizi ICT, esternalizzazione, infrastrutture e controparti rilevanti** - In caso di ricorso a soggetti esterni per la prestazione di servizi ICT e di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano di continuità operativa **prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore, sul soggetto terzo o sul fornitore di servizi esternalizzati**.
- **Controlli** - Il piano di continuità operativa e il relativo processo di aggiornamento sono **oggetto di regolare verifica da parte della funzione di revisione interna**. L'**internal audit** prende visione dei **programmi di verifica, assiste alle prove e ne controlla i risultati**, proponendo **modifiche al piano di continuità operativa sulla base delle mancanze riscontrate**.
- **Comunicazioni alla Banca d'Italia e alla Banca centrale europea** - In caso di crisi, **successivamente al ripristino dei processi critici**, l'operatore fornisce alla Banca d'Italia e alla Banca centrale europea **valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti**.



La Circolare n. 288 del 3 aprile 2015, nell'ambito del Titolo III «Organizzazione amministrativa e contabile e controlli interni», all'interno del Capitolo 1, Sezione IV, norma i principi generali del **sistema informativo contabile**, pre-requisito essenziale per il buon funzionamento dell'intermediario finanziario.



La disponibilità di **idonei strumenti informativi** permette agli **organi aziendali** di **monitorare regolarmente i rischi aziendali** e di **assumere decisioni consapevoli e coerenti con gli obiettivi aziendali**

- SIM;
- SGR;
- SICAV;
- SICAF;
- Etc...



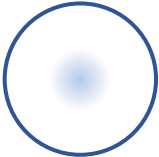
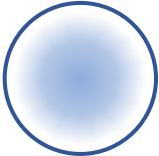
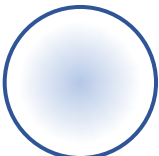
Agenda:

- **Normativa Banca d'Italia - 40° agg. Circolare 285**
 - ❖ **Quadro sinottico delle principali novità e loro portata innovativa**
 - ❖ **Il sistema dei controlli interni**



Quadro sinottico delle principali novità e portata innovativa

Il 40° aggiornamento introduce elementi innovativi funzionali a dare attuazione agli Orientamenti EBA sulla gestione dei rischi ICT e di sicurezza, oltre ad alcuni interventi di raccordo e aggiornamento dei riferimenti interni alla Sezione I del Capitolo 3 «Il sistema dei controlli interni»
Le banche dovevano adeguarsi entro il 30 giugno 2023 e trasmettere entro il 1° settembre 2023 alla Banca d’Italia una relazione che descriva gli interventi effettuati

Circolare 285	Principali elementi di novità	Portata innovativa
Capitolo 3 Il sistema dei controlli interni	Integrazione dei rischi ambientali, sociali e di governance (ESG) all’interno del processo di gestione del rischio	 <u>BASSA</u>
Capitolo 4 Il sistema informativo	- Nuovi compiti per gli Organi aziendali nella gestione del rischio ICT - Istituzione di una funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza - Nuovi processi, procedure e policy per la gestione della sicurezza dell’informazione e dei progetti ICT - Elementi integrativi da prevedere negli accordi tra banca e fornitori di sistemi e servizi ICT - Nuove disposizioni ed obblighi segnalativi nei confronti dei prestatori di servizi di pagamenti	 <u>ALTA</u>
Capitolo 5 La continuità operativa	- Integrazione di alcune specifiche componenti del contenuto del piano di continuità operativa - Condivisione del piano con le unità operative e di supporto e aggiornamento con cadenza almeno annuale - Integrazione misure da attuare in caso di crisi con impatto rilevante sul fornitore di servizi esternalizzati	 <u>MEDIA</u>



Il sistema dei controlli interni

Focus sugli elementi di novità

Topic	Elementi di novità
Processo di gestione dei rischi: integrazione dei rischi di sostenibilità	Nella definizione di «processo di gestione dei rischi»... <i>«l'insieme delle regole, delle procedure, delle risorse (umane, tecnologiche e organizzative) e delle attività di controllo volte a identificare, misurare o valutare, monitorare, prevenire o attenuare nonché comunicare ai livelli gerarchici appropriati tutti i rischi assunti o assumibili (8) nei diversi segmenti, a livello di portafoglio di impresa e di gruppo, relativi ad attività in bilancio e fuori bilancio, cogliendone, in una logica integrata e sulla base di valutazioni di tipo top-down e bottom-up, anche le interrelazioni reciproche e con l'evoluzione del contesto esterno;»</i> ...viene inserito un rimando esplicito ai rischi di sostenibilità come si evince dalla nota (8): <i>«(8) Devono essere considerati, a titolo esemplificativo e non esaustivo, il rischio strategico, il rischio di credito, il rischio di controparte, il rischio di concentrazione, il rischio di mercato, il rischio di tasso di interesse, il rischio operativo, il rischio di liquidità, il rischio connesso alla quota di attività vincolate (asset encumbrance), il rischio di reputazione, il rischio di modello, i rischi derivanti da prestiti in valuta estera, il rischio paese, il rischio di trasferimento nonché i rischi derivanti dall'ambiente macroeconomico in cui la banca opera anche con riferimento all'andamento del ciclo economico e i rischi di sostenibilità (ambientali, sociali o di governance, ESG). Si riportano, nell'Allegato A, le linee guida riferite a specifiche categorie di rischio, fermo restando quanto previsto nelle specifiche discipline relative alle singole tipologie di rischio.»</i>



Agenda:

➤ **Normativa Banca d'Italia - 40° agg. Circolare 285**

❖ Il sistema informativo

- I compiti degli organi aziendali sui profili ICT
- La funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza
- La gestione della sicurezza dell'informazione, delle operazioni e dei progetti ICT
- La gestione delle esternalizzazioni e delle terze parti
- La sicurezza dei servizi di pagamento e la gestione del rapporto con gli utenti



Il sistema informativo

I compiti degli organi aziendali sui profili ICT

Nell'ambito della generale disciplina dell'organizzazione e dei controlli interni, **sono attribuiti agli organi e funzioni aziendali ruoli e responsabilità, relativi allo sviluppo e alla gestione del sistema informativo e dei rischi ICT e di sicurezza**, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione

Organo aziendale	Elementi di novità
Organo con funzione di supervisione strategica	- Definisce e approva la strategia ICT, in considerazione dell'evoluzione del settore di riferimento e in coerenza con gli indirizzi strategici della banca. Il documento di indirizzo strategico comprende, oltre al «modello di riferimento architetturale» e alle «strategie di sourcing» già previste, propensione al rischio ICT e di sicurezza – prima trattato come «rischio informatico» linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi ICT - Approva l'assetto organizzativo e di governo della banca con riferimento al sistema informativo, alla gestione del rischio ICT e di sicurezza e alla continuità operativa, garantendo la chiara distinzione dei compiti e delle responsabilità degli organi e delle funzioni aziendali - Approva i piani d'azione per l'attuazione della strategia ICT e la policy di sicurezza dell'informazione È, inoltre, informato: Periodicamente, circa l'applicazione e l'adeguatezza dei piani d'azione per l'attuazione della strategia ICT Tempestivamente, in caso di gravi problemi derivanti da incidenti e malfunzionamenti del sistema informativo
Organo con funzione di gestione	- Definisce i piani di azione sulla strategia ICT, ne monitora e misura l'efficacia, ne cura il riesame periodico - Definisce i ruoli e le responsabilità per la funzione ICT e per la gestione del rischio ICT e di sicurezza, nonché per le relative attività di continuità operativa - Definisce l'assetto organizzativo, metodologico e procedurale per il processo di gestione del rischio ICT e di sicurezza - Assicura che tutto il personale riceva una formazione adeguata in materia di rischi ICT e di sicurezza, nonché di sicurezza dell'informazione, almeno una volta all'anno o con maggiore frequenza se necessario



Il sistema informativo

La funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza

Controlli di II livello: Opzioni regolamentari

Nell'istituzione della Funzione di controllo dei rischi ICT e di sicurezza prevista dalla Circolare 285 le banche possono:

1 «...attribuire i compiti della funzione di controllo dei rischi ICT e di sicurezza a una **funzione di secondo livello appositamente istituita** alla funzione si applicano le disposizioni previste dal Capitolo 3, Sezione III, par. 1. Tra la funzione di controllo ICT e le altre funzioni aziendali di controllo sono assicurati opportuni livelli di raccordo e adeguate forme di coordinamento, conformemente a quanto previsto nel Capitolo 3, Sezione III, par. 3.5»

2 «In alternativa, assegnare tali compiti alle **funzioni aziendali di controllo dei rischi e di compliance**, in relazione ai ruoli, alle responsabilità e alle competenze proprie di ciascuna delle due funzioni, a condizione che siano assicurati il **corretto svolgimento dei compiti**, l'**efficacia dei controlli** e le **necessarie competenze tecniche**»

Ref: Parte Prima, Titolo IV, Capitolo 4, Sezione II, Par. 4 La funzione di controllo dei rischi ICT e di sicurezza

Soluzioni percorribili e Implicazioni organizzative/operative

A Attribuzione compiti ad una FAC già esistente – (Es. Controllo rischi)

- Assicurare un **adeguato bilanciamento** dei compiti tra i diversi livelli di controllo, in primis con le funzioni di primo livello finora detentrici quasi esclusive di competenze in ambito
- Possibilità di sfruttare le **competenze della funzione** che ha già svolto in questi anni attività di IT Risk Management
- Possibilità di sfruttare la **conoscenza storica** della funzione già esistente sulle tematiche relative alla gestione dei rischi ICT e Sicurezza
- Possibilità di sfruttare le **interazioni e le sinergie già consolidate** fra la funzione che già svolge l'attività e le UO di supporto

B Istituzione nuova FAC

- Verificare che la scelta di istituire un nuova funzione sia **coerente con il principio di proporzionalità e con le caratteristiche organizzative ed operative della Società**
- **Verificare la sostenibilità** di tale scelta organizzativa in relazione ai profili e alle competenze disponibili.
- Definire un **modello operativo integrato** nell'ambito del complessivo sistema dei controlli interni (approccio metodologico, strumenti, meccanismi di integrazione e coordinamento con gli altri attori del sistema di controllo interno, etc.)
- Assicurare che la **complessiva filiera dei controlli** non preveda duplicazioni di attività/competenze

NOTA: Le banche che ricorrono all'esternalizzazione di funzioni aziendali all'interno o all'esterno del gruppo applicano i Titoli I, II, III e IV degli Orientamenti in materia di outsourcing dell'EBA.

In generale, attraverso il ricorso all'esternalizzazione, la Banca non può: delegare le proprie responsabilità, né la responsabilità degli organi aziendali, alterare il rapporto e gli obblighi nei confronti dei suoi clienti, mettere a repentaglio la propria capacità di rispettare gli obblighi previsti dalla disciplina di vigilanza né mettersi in condizione di violare le riserve di attività previste dalla legge, pregiudicare la qualità del sistema dei controlli interni e ostacolare la vigilanza.

Il sistema informativo

La funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza

In linea con il 40° Aggiornamento, la **funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza è responsabile** di quanto segue:



! Gli istituti finanziari dovrebbero garantire l'indipendenza e l'obiettività di tale funzione di controllo, separandola adeguatamente dai processi operativi dell'ICT (rif. Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza, Sezione 1.3.1)

Il sistema informativo

La gestione della sicurezza dell'informazione, delle operazioni e dei progetti ICT

Topic	Elementi di novità
 Sicurezza dell'informazione e gestione operazioni ICT	Sicurezza dell'informazione: • Estensione dei programmi di formazione annuale anche ai fornitori, oltre che ai dipendenti • Inclusione di misure di sicurezza fisica per garantire la protezione da «rischi ambientali» dei locali, data center e aree sensibili • Protezione degli endpoint e realizzazione di configurazione di sicurezza di base per tutti i componenti di rete • Integrazione di misure sicurezza dell'informazione come: pratiche di Red Team, revisioni del codice sorgente e cifratura dei dati Gestione delle operazioni ICT: • Registrazione e monitoraggio delle attività operative dell'ICT critiche • Definizione di processi adeguati di gestione degli incidenti e dei problemi, criteri e soglie per la classificazione di degli incidenti
 Gestione dei progetti ICT	Le banche si dotano di un piano e/o un processo per il governo dei progetti, in aggiunta: • Un processo che disciplini l'acquisizione, lo sviluppo e la manutenzione dei sistemi ICT • Requisiti di sicurezza chiaramente definiti e approvati, oltre che misure per proteggere l'integrità dei codici sorgente dei sistemi ICT sviluppati internamente
 Gestione delle esternalizzazioni e delle terze parti	A riguardo, nell'accordo scritto tra banca e fornitori di sistemi e servizi ICT, sono state previste ulteriori integrazioni, con riferimento a: • Misure e obiettivi in materia di sicurezza dell'informazione • Specifiche relative al ciclo di vita dei dati della banca ed eventuali requisiti relativi alla cifratura dei dati, alla sicurezza di rete e ai processi di monitoraggio della sicurezza, e l'ubicazione dei centri dati • Procedure di gestione degli incidenti operativi e di sicurezza
 Gestione del rapporto con gli utenti dei servizi di pagamento	• Definire e attuare processi per accrescere le conoscenze degli utenti sui rischi per la sicurezza, oltre che assistenza ed orientamento • Consentire agli utenti di disattivare specifiche funzionalità di pagamento • Concedere la possibilità di modificare i limiti di spesa di specifici strumenti di pagamento (entro il limite massimo concordato) • Offrire agli utenti la possibilità di ricevere avvisi in caso di tentativi, iniziati e/o falliti, di effettuare operazioni di pagamento, consentendo così rilevare un uso fraudolento o dannoso



Agenda:

- **Normativa Banca d'Italia - 40° agg. Circolare 285**
 - ❖ **La continuità operativa**



La continuità operativa

Focus sugli elementi di novità

Topic	Elementi di novità
 Aggiornamenti al contenuto del piano di continuità operativa	• Oltre ai tempi di ripristino, con questo aggiornamento il piano dovrà espressamente contenere anche gli «obiettivi di punto di ripristino» dei processi critici. Il nuovo concetto di «obiettivo di punto di ripristino» è definito come «il periodo massimo durante il quale è accettabile che i dati vadano persi in caso di incidente» • Il piano dovrà inoltre considerare anche opzioni alternative nel caso in cui il ripristino non sia attuabile nel breve periodo a causa di costi, rischi, fattori logistici o circostanze impreviste
 Documentazione, condivisione e aggiornamento del piano di continuità operativa	• Piano documentato e messo a disposizione delle unità operative (<i>business unit</i>) e di supporto e immediatamente accessibile in caso di emergenza • Piano aggiornato sulla base dei risultati delle verifiche, delle informazioni sulle minacce esistenti e dell'esperienza maturata in occasione di eventi precedenti, considerando anche le modifiche delle funzioni aziendali, dei processi e delle risorse informatiche di supporto nonché dei tempi di ripristino e degli obiettivi di punto di ripristino
 Esternalizzazione, infrastrutture e controparti rilevanti	• In caso di ricorso a soggetti esterni per la prestazione di servizi ICT e di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano dovrà prevedere misure da attuare in caso di crisi con impatto rilevante sull'operatore, sul soggetto terzo o sul fornitore di servizi esternalizzati



Agenda:

- **Focus su sicurezza e cyber security, rischi connessi e impatti Banca**
 - ❖ **Impatti e rischi IT e Cyber nel mondo bancario**

Focus su sicurezza e cyber security, rischi connessi e impatti Banca

Impatti e rischi ICT e Cyber nel mondo bancario

Per il settore dei servizi finanziari ha sempre più peso la capacità di adeguarsi al contesto tecnologico circostante.

La digitalizzazione svolge un ruolo sempre più strategico nel raggiungimento dei risultati aziendali e con esso anche il rischio ICT e Cyber ha assunto un ruolo di primo piano nell'agenda aziendale.

Rischio ICT e Cyber

Rischio di incorrere in perdite a causa di 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.



Cyber security

La **cybersecurity** comprende tutte le attività necessarie per **proteggere i sistemi critici e le informazioni sensibili dalle minacce informatiche**, sia che tali minacce **provengano dall'interno che dall'esterno di un'organizzazione.**



Cyber security breaches come rischio di primaria importanza

Nelle aziende, la **portata delle potenziali perdite fisiche e finanziarie** derivanti da un incidente informatico è **ampia**, a causa della **natura pervasiva dei rischi associati**

Oltre la perdita/corruzione dei dati: danni a proprietà, alla reputazione e all'interruzione dell'attività

I **danni ed i costi** di un attacco informatico o di sicurezza non si limitano alla perdita, sottrazione o danneggiamento del dato, ma **includono**:

- potenziali **danni alla reputazione** di un'azienda
- **danni associati all'interruzione dell'operatività bancaria o gravi interruzioni delle infrastrutture critiche**

Le perdite possono derivare da un **attacco doloso proveniente dall'interno o dall'esterno** dell'organizzazione.

Allo stesso modo, possono essere **legate** ad un **errore accidentale dell'uomo**.

I costi economici derivanti da una violazione informatica possono essere significativi

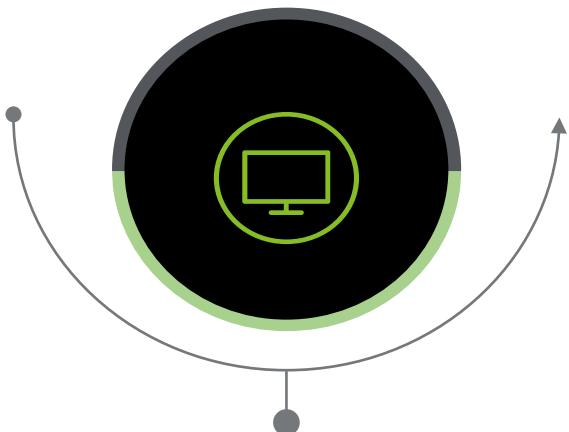
Al fine di **calcolare le perdite** derivanti da alcuni incidenti si dovrà tenere conto dell'**impatto economico più ampio degli incidenti cyber**, quali:

- costi derivanti dall'**interruzione dell'operatività bancaria (Business Interruption - BI)**
- **danni alla reputazione e perdita di clientela**
- **costi dei danni fisici**
- ecc...

Focus su sicurezza e cyber security, rischi connessi e impatti Banca

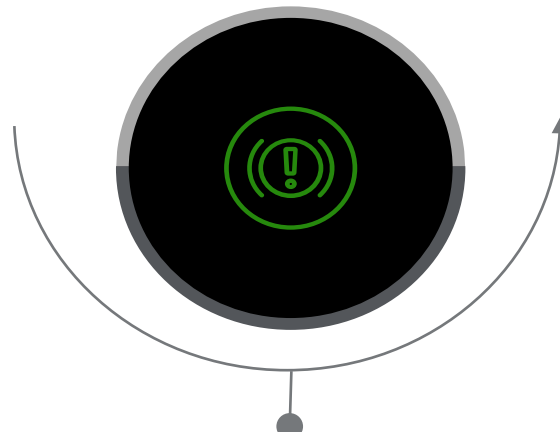
Impatti e rischi ICT e Cyber nel mondo bancario

I rischi informatici sono in continua evoluzione. Tre caratteristiche principali sottolineano la natura dinamica del rischio informatico.



Incremento della trasformazione digitale

- La **tecnologia digitale** ha sempre **più impatto** nei processi interni aziendali e nelle interazioni con i clienti, **creando nuovi modelli di business**
- I **protocolli di sicurezza tradizionali** spesso diventano **inadeguati** ad affrontare le continue **novità tecnologiche**
- Il ricorso crescente alla digitalizzazione e all'innovazione può portare a **sottovalutare i rischi operativi e di sicurezza emergenti**



Aumento delle fonti di vulnerabilità

- Sono sempre **più diffuse le tecnologie digitali nelle società finanziarie**, in termini di utilizzo di **strumenti elettronici, transazioni contactless e bonifici online** (via Internet o tramite collegamenti telematici)
- **Aumento dell'interconnessione** derivante dal **ricorso a terze parti e complesse catene di subfornitura**



Evoluzione dei profili hacker

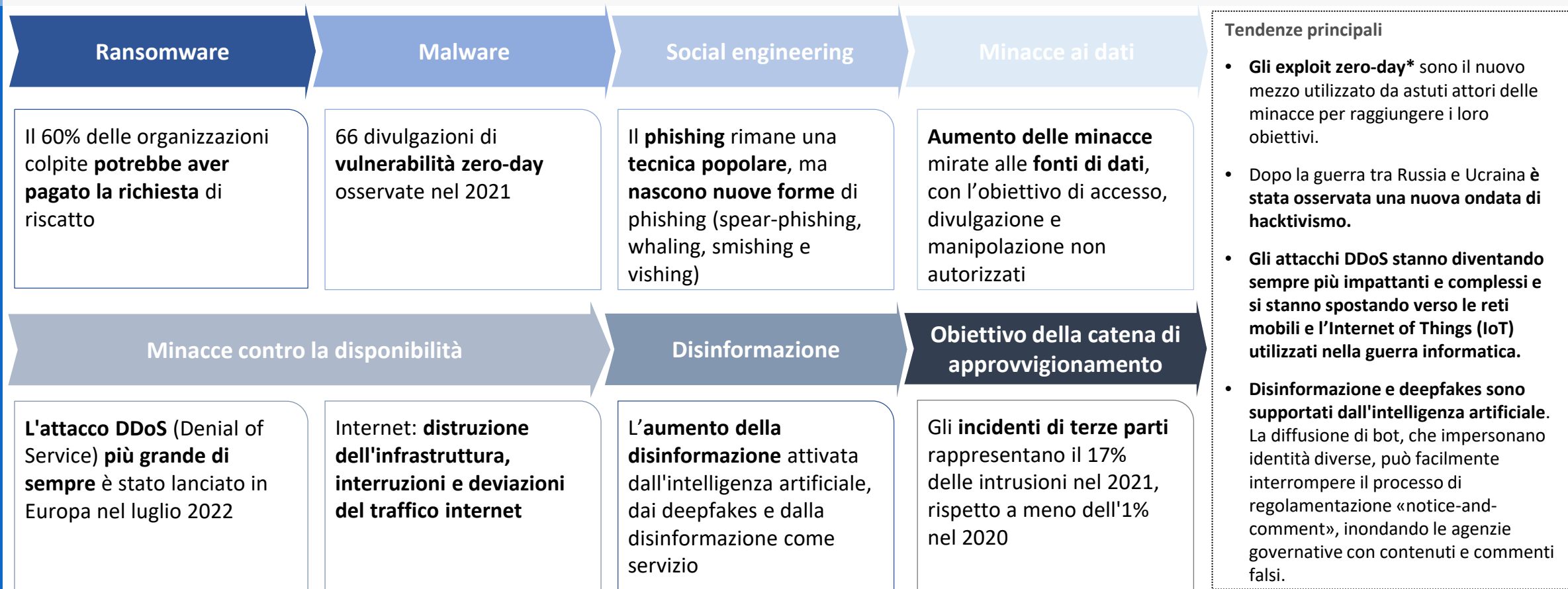
- Gli **hacker** diventano sempre **più sofisticati**:
 - I **dipendenti** sono spesso **strumentali** alla **propagazione degli attacchi**
 - Le **tecniche di phishing e social engineering** sono tra i metodi di attacco di **maggior successo** per sfruttare le **reti aziendali**

Focus su sicurezza e cyber security, rischi connessi e impatti Banca

Impatti e rischi ICT e Cyber nel mondo bancario

Il rapporto ENISA Threat Landscape (ETL) è il rapporto annuale dell'Agenzia dell'Unione Europea per la Cybersecurity, ENISA, sullo stato del panorama delle minacce alla cybersecurity. La decima e ultima edizione del rapporto copre un periodo di rendicontazione che va da aprile 2021 a luglio 2022.

L'ENISA ha suddiviso le minacce in 8 gruppi. La frequenza e l'impatto determinano la rilevanza di tutte queste minacce.



***exploit zero-day**: sfruttamento di una vulnerabilità informatica perché sono passati zero giorni da quando la vulnerabilità è stata conosciuta e riparata dallo sviluppatore prima che qualcuno possa scrivere un exploit per essa.

Focus su sicurezza e cyber security, rischi connessi e impatti Banca

Impatti e rischi ICT e Cyber nel mondo bancario

La sempre più crescente digitalizzazione ha causato l'emergere di nuove potenziali vulnerabilità, l'evoluzione dei vettori di attacco ed un cambiamento del profilo di rischio delle società. Si riportano a titolo esemplificativo alcune aree d'attenzione:



Controllo dell'accesso remoto degli utenti

Aumento della superficie di attacco con un maggior numero di utenti che si affidano a **soluzioni di accesso remoto** (ad esempio, Virtual Private Network o Remote Desktop Control).



Sicurezza di rete

I rischi per la sicurezza informatica aumentano con l'aumento degli utenti che utilizzano le **reti Wi-Fi domestiche**, che potrebbero **non essere sicure**.



Sicurezza degli endpoint

Ritardi nei processi di sicurezza (ad esempio, patch) dovuti alla concentrazione sulle attività operative chiave legate all'accesso remoto.



Accesso al cloud

Aumento dell'utilizzo di soluzioni basate su cloud per la collaborazione remota, la condivisione di file e le videoconferenze.



Sensibilizzazione degli utenti alla sicurezza

Aumentano le campagne di social engineering che sfruttano l'ingenuità delle vittime per gli attacchi.



Sicurezza delle e-mail

Aumento dei livelli di rischio informatico a causa degli **attacchi di phishing e malware**.



Rilevamento e risposta alle minacce

È necessario mettere a punto **nuovi set di regole di monitoraggio, soglie e percorsi di escalation, rivedere i modelli di traffico/comportamento** e rafforzare le capacità di risposta.



Backup delle informazioni

È necessario fornire ai dipendenti un **software per garantire il backup di documenti e informazioni critiche**.



GRAZIE PER L'ATTENZIONE

Ing. Francesco Micillo
francescomicillo@libero.it