Roma, 27 maggio 2014

ABI Lab
Tecnologia utile

La Circolare 263: sintesi dei punti chiave e degli impatti sulla sicurezza informatica

Romano Stasi

Segretario Generale

Consorzio ABI Lab – Centro di Ricerca e Innovazione per la Banca

L'evoluzione del quadro normativo in tema di sicurezza informatica

Crescente **attenzione** da parte delle **istituzioni** di riferimento a livello **nazionale** ed **europeo** in merito ai **rischi informatici** e all'esigenza di garantire **elevati livelli di sicurezza** nella realizzazione di **pagamenti da remoto** e nella **gestione dei dati**, come testimoniato dal recente fermento normativo in materia.

- Le **principali evoluzioni normative** con impatti sulla **gestione della sicurezza e del rischio informatico** in banca investono principalmente gli ambiti di:
  - **Sicurezza degli accessi e dei servizi di pagamento**
    - *Payment Service Directive e recepimento a livello nazionale*
    - *Raccomandazioni BCE sulla sicurezza dei pagamenti internet + Assessment Guide BCE*
    - *Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento*
    - *Raccomandazioni BCE sulla sicurezza dei pagamenti Mobile*
  - **Sicurezza nel trattamento di dati e informazioni bancarie**
    - *Provvedimento Autorità Garante per la Privacy per la circolazione delle informazioni bancarie e il trattamento dei dati bancari*
  - **Valutazione del rischio informatico e correlazione con la gestione del rischio operativo**
    - *Disposizioni di vigilanza prudenziale di Banca d'Italia in materia di sistema dei controlli interni, sistema informativo e continuità operativa*

✓ emanato in corso di emanazione

Nuove disposizioni di Vigilanza Prudenziale – circolare 263

Aggiornamento Titolo V: principali evidenze

- **Principi di fondo della normativa:**
  - **coinvolgimento vertici** aziendali
  - **visione integrata** dei **rischi**
  - **efficienza ed efficacia dei controlli**
  - applicazione delle norme in **funzione** della **dimensione** e della **complessità operativa**

- **Principali elementi di novità – focus capitolo 8**
  - Definizione dei **compiti e delle responsabilità** degli **organi** aziendali con funzione di **supervisione strategica**, **gestione** e **controllo**.
  - Introduzione di una disciplina in materia di **esternalizzazione** delle **funzioni aziendali** e del **sistema informativo**
  - In materia di **sistemi informativi**, la disciplina è stata **integralmente rivista**, regolamentando:
    - **governance** e **organizzazione** del sistema informativo
    - **gestione del rischio informatico**
    - requisiti per assicurare la **sicurezza informatica** e il sistema di **gestione dei dati**.
    - presidi di sicurezza per l'**accesso** a sistemi e servizi critici tramite il canale **internet**, recependo le **raccomandazioni della BCE** in materia di sicurezza dei pagamenti in internet

Fonte: Fonte: Comunicato Stampa Banca d'Italia http://www.bancaditalia.it/media/comsta/2013/20130703_disp_vig.pdf

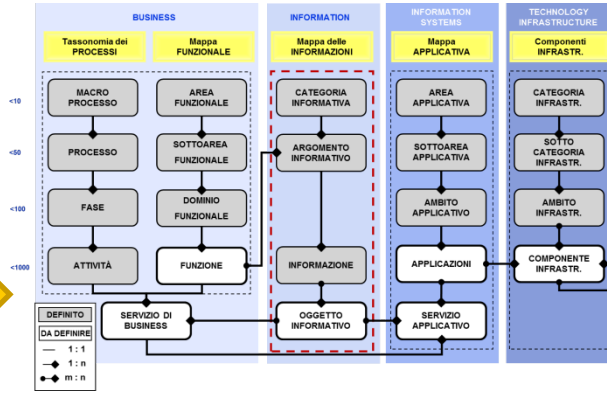
Nuove disposizioni di Vigilanza Prudenziale – circolare 263

Attività ABI Lab

APPROFONDIMENTI NEI TAVOLI DI LAVORO ABI LAB

- Osservatorio Sicurezza e Frodi Informatiche
- Osservatorio Business Continuity
- Osservatorio Architetture IT
- GdL Information Governance

- **Analisi** dei **capitoli 8 e 9** e della **check list**
- **Approfondimenti** in corso congiunti con i referenti DIPO sui temi di **analisi di rischio informatico** (RI) e correlazione con i rischi operativi
  - **Tassonomia delle minacce di RI e correlazione con gli Event Type di Basilea II**
  - **Analisi di possibili metriche di misura degli impatti di un evento di RI**
  - **Collegamento dell'elenco delle minacce agli asset/ risorse ICT impattate**



- Focus **gestione fornitori critici**
- Analisi dell'impatto sulla funzione **architetture**
- Focus su **metodologie e framework** per la **catalogazione** del **patrimonio ICT**
- Impatti sui **processi di Information Governance** e di **gestione** della **qualità di dati**

OUTPUT PRODOTTI e ATTIVITÀ DI COMUNICAZIONE

- Realizzazione di un **commentario** con osservazioni a supporto della lettura dei capitoli 8 e 9, per evidenziare i principali punti da considerare in fase di adeguamento e i relativi impatti
- Definizione di **percorsi di formazione con ABI dedicati alla 263**

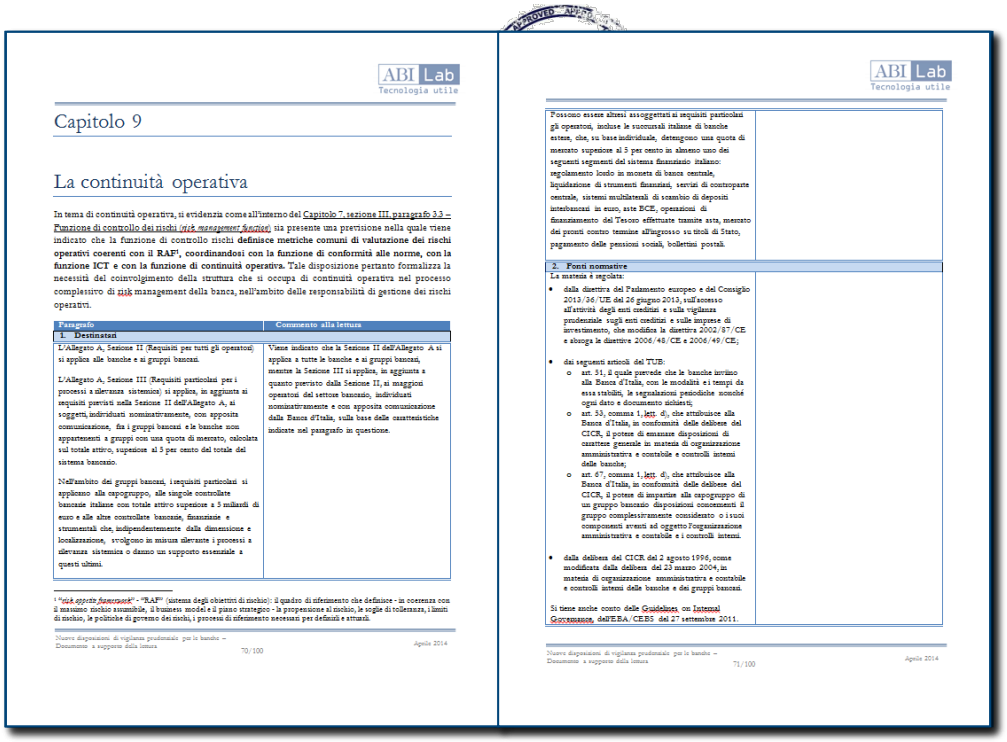
Attività ABI Lab a supporto dell'adeguamento

Lettura e interpretazione delle disposizioni

ABI Lab
Tecnologia utile

Materiale disponibile sul portale ABI Lab

1. Redazione di un COMMENTARIO



ABI Lab
Tecnologia utile

Capitolo 9

La continuità operativa

In tema di continuità operativa, si evidenzia come all'interno del Capitolo 7, sezione III, paragrafo 3.3 – Funzione di controllo dei rischi (*risk management function*) sia presente una previsione nella quale viene indicato che la funzione di controllo rischi **definisce metriche comuni di valutazione dei rischi operativi coerenti con il RAF[1], coordinandosi con la funzione di conformità alle norme, con la funzione ICT e con la funzione di continuità operativa.** Tale disposizione pertanto formalizza la necessità del coinvolgimento della struttura che si occupa di continuità operativa nel processo complessivo di risk management della banca, nell'ambito delle responsabilità di gestione dei rischi operativi.

Paragrafo	Commento alla lettura
1. Destinatari	
L'Allegato A, Sezione II (Requisiti per tutti gli operatori) si applica alle banche e ai gruppi bancari. L'Allegato A, Sezione III (Requisiti particolari per i processi a rilevanza sistemica) si applica, in aggiunta ai requisiti previsti nella Sezione II dell'Allegato A, ai soggetti, individuati nominativamente, con apposita comunicazione, fra i gruppi bancari e le banche non appartenenti a gruppi con una quota di mercato, calcolata sul totale attivo, superiore al 5 per cento del totale del sistema bancario. Nell'ambito dei gruppi bancari, i requisiti particolari si applicano alla capogruppo, alle singole controllate bancarie italiane con totale attivo superiore a 5 miliardi di euro e alle altre controllate bancarie, finanziarie e strumentali che, indipendentemente dalla dimensione e localizzazione, svolgono in misura rilevante i processi a rilevanza sistemica o danno un supporto essenziale a questi ultimi.	Viene indicato che la Sezione II dell'Allegato A si applica a tutte le banche e ai gruppi bancari, mentre la Sezione III si applica, in aggiunta a quanto previsto dalla Sezione II, ai maggiori operatori del settore bancario, individuati nominativamente e con apposita comunicazione dalla Banca d'Italia, sulla base delle caratteristiche indicate nel paragrafo in questione.

[1] "*risk appetite framework*" - "RAF" (sistema degli obiettivi di rischio): il quadro di riferimento che definisce - in coerenza con il massimo rischio assumibile, il business model e il piano strategico - la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli.

Nuove disposizioni di vigilanza prudenziale per le banche – Documento a supporto della lettura — 70/100 — Aprile 2014

Possono essere altresì assoggettati ai requisiti particolari gli operatori, inclusi le succursali italiane di banche estere, che, su base individuale, detengono una quota di mercato superiore al 5 per cento in almeno uno dei seguenti segmenti del sistema finanziario italiano: regolamento lordo in moneta di banca centrale, liquidazione di strumenti finanziari, servizi di controparte centrale, sistemi multilaterali di scambio di depositi interbancari in euro, aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, mercato dei pronti contro termine all'ingrosso su titoli di Stato, pagamento delle pensioni sociali, bollettini postali.

2. Fonti normative

La materia è regolata:

- dalla direttiva del Parlamento europeo e del Consiglio 2013/36/UE del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE;
- dai seguenti articoli del TUB:
  - art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;
  - art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
  - art. 67, comma 1, lett. d), che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di impartire alla capogruppo di un gruppo bancario disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni.
- dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari.

Si tiene anche conto delle Guidelines on Internal Governance, dell'EBA/CEBS del 27 settembre 2011.

Nuove disposizioni di vigilanza prudenziale per le banche – Documento a supporto della lettura — 71/100 — Aprile 2014

Nel **documento** sono inserite tutte le disposizioni presenti nei capitoli 8 e 9 della Circolare 263: alla stesura del commentario hanno partecipato le **banche e i partner** dei tavoli di lavoro ABI Lab sulla **sicurezza informatica** e la **continuità operativa**.

Attività ABI Lab a supporto dell'adeguamento

Analisi dei contenuti e pianificazione attività

ABI Lab
Tecnologia utile

Materiale disponibile sul portale ABI Lab

2. Individuazione MACRO FILONI PROGETTUALI

- Architetture IT
- Organizzazione IT
- Tassonomia rischi
- Presidi e contromisure tecnologiche
- Gestione incidenti
- Policy
- Contratti e SLA
- Information Governance
- Analisi e monitoraggio

Governance e Organizzazione del Sistema Informativo	*Metodologie di analisi del rischio informatico e correlazione con RO*	*Gestione della Sicurezza Informatica*
Gestione operazioni critiche	*Governance e Gestione dei dati*	*Gestione esternalizzata del Sistema Informativo*

Capitolo 8

- I **Macro Progetti individuati** sono stati successivamente analizzati con l'obiettivo di avere una **visione di insieme di tutte le attività da porre in essere per l'adeguamento**, anche alla luce di quanto previso dalla Gap Analysis richiesta da Banca d'Italia.

3. Approfondimento degli aspetti legati alla GESTIONE DELLE INFORMAZIONI

Lo scenario e gli elementi di novità:

- L'**affidabilità e sicurezza delle informazioni aziendali** rientra tra le finalità del sistema dei controlli interni; **la gestione dei dati rientra nel più ampio processo di gestione dei rischi**.
- **La registrazione dei fatti aziendali è completa**, **corretta, tempestiva** e opportunamente **documentata**, al fine di consentire la ricostruzione dell'attività svolta, favorire l'assunzione di decisioni consapevoli e abilitare la corretta attuazione del processo di gestione dei rischi
- Le **procedure settoriali**, i meccanismi di **integrazione tra informazioni**, le attività di **data warehousing** e i processi di **acquisizione di dati** da information provider sono definiti in maniera attenta e sono dettagliatamente documentati, al fine di consentire la verifica sulla qualità dei dati
- È definito uno **standard aziendale di data governance**, che **individua ruoli e responsabilità** delle funzioni coinvolte nel trattamento dell'informazione. Tali standard sono approvati dall'OFG, estesi a livello aziendale.
- **Integrità** o **accuratezza**, **riservatezza**, **disponibilità**, l'**accountability** e **verificabilità** dei dati sono i principi che devono essere rispettati dal sistema di gestione dei dati relativi alle operazioni registrate.
- L'**Outsourcer partecipa al Sistema di Information Governance**: è tenuto a garantire la sicurezza delle informazioni relative all'attività della banca, sotto gli aspetti di **disponibilità**, **integrità** e **riservatezza**.

Attività ABI Lab a supporto dell'adeguamento

Focus architetture IT

ABI Lab
Tecnologia utile

4. Considerazioni su tematiche relative all'ARCHITETTURA S.I.

I PRINCIPALI ASPETTI, IN 5 PUNTI:

L'ARCHITETTURA PORTA VALORE AL BUSINESS

In linea con le best practice di settore, l'architettura è qualificata come **risultato di un processo** orientato a **supportare concretamente il business**.

L'ARCHITETTURA SUPPORTA IL DISEGNO DELLA STRATEGIA IT

L'architettura esce dalla pura dimensione tecnico/tecnicistica e viene portata **all'attenzione dei massimi livelli manageriali**: diventa base e **strumento di decisione**.

L'ARCHITETTURA È IMPORTANTE PER L'ORGANIZZAZIONE E LA GOVERNANCE DELL'IT

Il modello architetturale assume importanza quale **riferimento per la strutturazione organizzativa** della funzione ICT e per il disegno delle **politiche di IT Governance**.

L'ARCHITETTURA È UNO STRUMENTO PER GESTIRE I CAMBIAMENTI

L'architettura IT è importante ai fini di valutare le **opportunità di evoluzione** dei sistemi e gli **impatti dei cambiamenti** del contesto sull'infrastruttura ICT.

LA COERENZA DELL'ARCHITETTURA IT FAVORISCE LA SICUREZZA INFORMATICA

L'architettura si ritrova tra i principali fattori che definiscono e determinano le caratteristiche di **sicurezza e qualità del sistema informativo aziendale**.

Attività ABI Lab a supporto dell'adeguamento

Correlazione tra minacce – rischio informatico – rischio operativo (1/2)

ABI Lab Tecnologia utile

5. Analisi MINACCE di RISCHIO INFORMATICO e realizzazione TASSONOMIA

Documento in corso di revisione

L1	Livello 1	L1	L2	Livello 2	L3	Livello 3	Minaccia	COD	VULN
F	DISFUNZIONE DI BUSINESS O DI SISTEMA	ET6	1	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici	a	Hardware	PERDITA DI DATI DOVUTI A ERRORI HARDWARE(SUPPORTI DI MEMORIZZAZIONE)	F1a	
	DISFUNZIONE DI BUSINESS O DI SISTEMA	ET6	1	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici	b	Software	MANUTENZIONE DEL SOFTWARE INADEGUATA		X
		ET6	1	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici			INEFFICIENZA DOVUTA A SOFTWARE ERRATO O MANUTENZIONE SOFTWARE INADEGUATO	F1b	
		ET6	1	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici			GUASTI APPLICATIVI DOVUTI AD ACQUISIZIONE INCONTROLLATA DI SOFTWARE	F1b	
	DISFUNZIONE DI BUSINESS O DI SISTEMA	ET6	1	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici	c	comunicazioni	FERMO TECNICO PER GESTIONE DELLA RETE INSUFFICIENTE	F1c	
		ET6	1	Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici			LARGHEZZA DI BANDA INADEGUATA	F1c	
	DISFUNZIONE DI BUSINESS O DI SISTEMA	ET		Inadeguatezza/ inefficienza/ malfunzionamento o blocco dei sistemi tecnologici	d	Interruzione del servizio /avarie	DANNEGGIAMENTI DI LINEE	F1d	
G	GESTIONE DEI PROCESSI	ET7		Esecuzione e perfezionamento delle transazioni	a	Errori di comunicazione	DUPLICAZIONE DI MESSAGGI DI ERRORE UTILIZZO INCONTROLLATO DI STRUMENTI DI COMUNICAZIONE	G1a	
	GESTIONE DEI PROCESSI	ET7	1	Esecuzione e perfezionamento delle transazioni					
	GESTIONE DEI PROCESSI	ET7	1	Esecuzione e perfezionamento delle transazioni	b	Errori di inserimento dati/mantenimento/caricamento	PROCEDURE DI BACK UP INADEGUATE		X
	GESTIONE DEI PROCESSI	ET7	1	Esecuzione e perfezionamento delle transazioni			INSUFFICIENTE CAPACITA' DI RIPRISTINO DEI DATI CAUSATA DA PROCEDURE DI BACK UP INADEGUATE	G1b	
				Esecuzione e perfezionamento		Data di consegna o		G1c	

Vulnerabilità

Minaccia generata

ESEMPLIFICATIVO – VISTA PARZIALE

L3 correlati

Attività ABI Lab a supporto dell'adeguamento

Correlazione tra minacce – rischio informatico – rischio operativo (2/2)

ABI Lab Tecnologia utile

6. Impostazione di una metodologia di GESTIONE DEL RISCHIO INFORMATICO

1. **Raccolta**
   - •eventi
   - •accadimenti
   - •attacchi

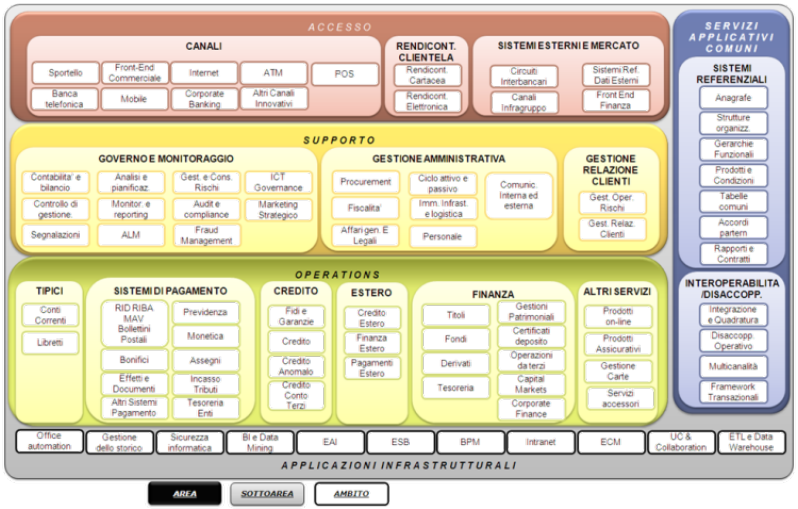
2. **Mappatura** eventi su Tassonomia Minacce

3. **Articolazione** su Mappa
   - •Infrastrutturale
   - •Applicativa

4. **Valutazione** rischio e **quantificazione** impatto

5. **Individuazione** contromisure

6. **Aggiornamento** contromisure

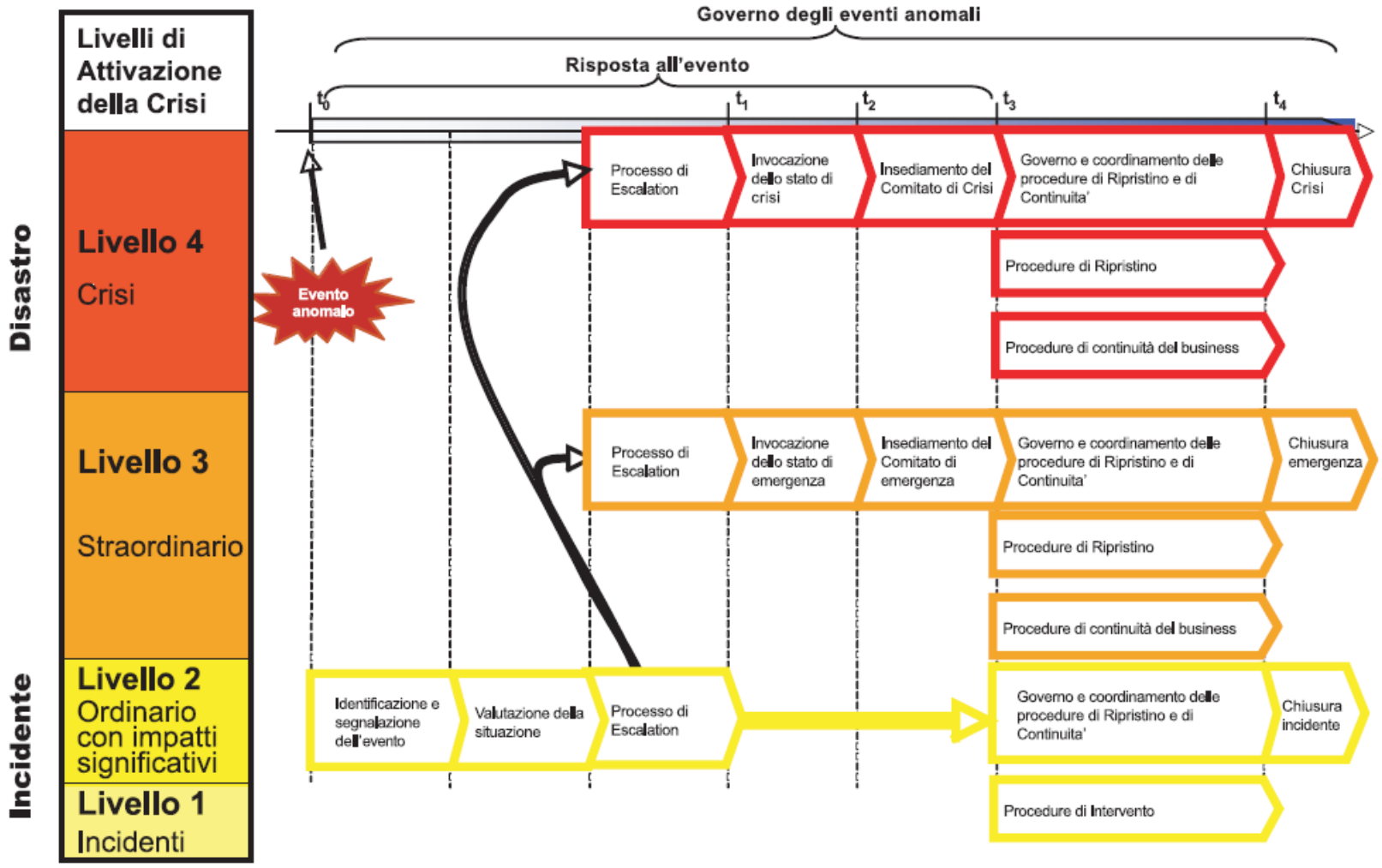


Attività ABI Lab a supporto dell'adeguamento

Incident management

ABI Lab
Tecnologia utile

7. Richiamo al processo di GESTIONE DEGLI INCIDENTI



Fonte: ABI Lab - Struttura di massima dei Processi di governo di eventi/ situazioni anomale – Linee Guida per il Crisis Management - 2008

Focus sicurezza informatica

- RECEPIMENTO RACCOMANDAZIONI BCE
  - **14 Recommendations** organizzate in **3 categorie**
    - Controlli generali (Racc. 1-5);
    - Controlli specifici e misure di sicurezza per i pagamenti internet (Racc. 6-11);
    - Comunicazione con la clientela e customer awareness (Racc. 12-14);

    e composte da *Key Considerations* e *Best Practices.*

- FOCUS STRONG AUTHENTICATION
  - L'adozione di strumenti di **strong authentication** segue il **principio del *comply or explain***.

    ↳ **Bisognerà giustificare la scelta** dello strumento adottato attraverso un'adeguata **analisi del rischio** che tiene in considerazione **dati pregressi** e **prospettive future**.
  - Per l'**autenticazione forte** nella fase di **accesso ai dati sensibili di pagamento** occorre ragionare sulla **definizione di *sensitive payment data***.

    ↳ **Sarà necessario individuare i dati** interessati dalle previsioni e sviluppare **eventuali ulteriori approfondimenti**.
  - L'analisi del documento «**Assessment Guide**», pubblicato dalla **BCE** e collegato alle raccomandazioni per la sicurezza dei pagamenti internet, potrebbe essere di **supporto all'adeguamento alle previsioni normative**.

    ↳ Il documento, **indirizzato alle Autorità locali di vigilanza e di sorveglianza** e di supporto nel valutare la compliance alle raccomandazioni, è molto **utile** anche alle banche **per comprendere le richieste dei supervisori**.

"The initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication".

STRONG AUTHENTICATION

Strong customer authentication *is a* ***procedure based on the use of two or more of the following elements*** *– categorised as knowledge, ownership and inherence:*

i. ***something only the user knows****, e.g. static password, code, personal identification number****;***

ii. ***something only the user possesses****, e.g. token, smart card, mobile phone;*

iii. ***something the user is****, e.g. biometric characteristic, such as a fingerprint. In addition,* ***the elements selected must be mutually independent****, i.e. the breach of one does not compromise the other(s).*

At least one of the elements should be non-reusable and non-replicable *(except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data"*

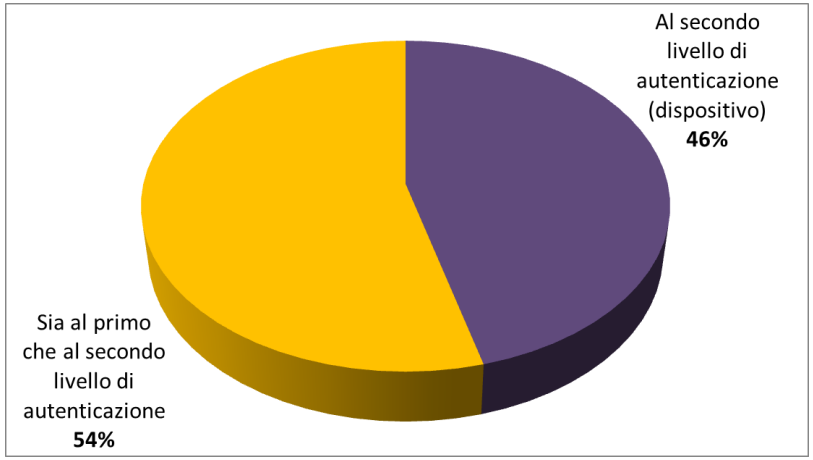
Le informazioni di dettaglio sulle soluzioni di strong authentication vengono fornite nella Raccomandazione 7.

Secondo l'approccio del Forum, i PSP senza o con procedure di autenticazione semplice non potranno, in caso di disputa, provare che il cliente abbia effettivamente autorizzato l'operazione.

Lo scenario italiano
Soluzioni di secondo fattore

Segmento Retail

Secondo fattore di autenticazione*



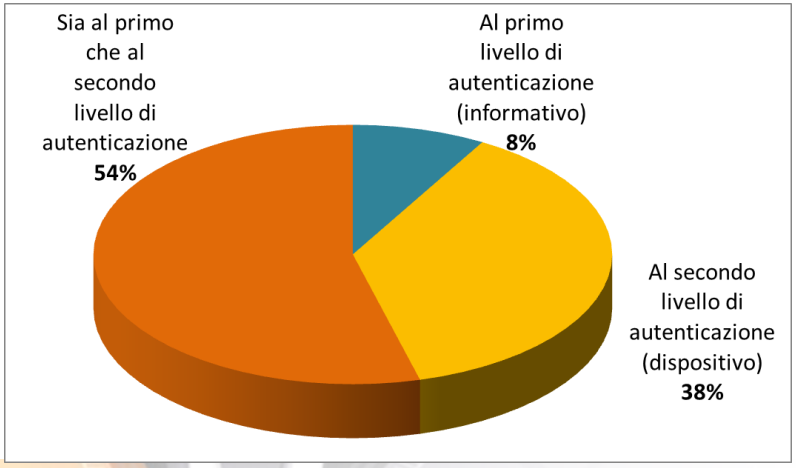
* 24 rispondenti

- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- **Tutte** le banche mettono a disposizione **almeno una tecnologia di secondo fattore**. In particolare:
  - Il **91,8%** delle banche **obbliga tutti i propri clienti** all'**utilizzo di strumenti di II fattore** (o di almeno uno, a scelta del cliente, se ne vengono forniti diversi).
  - Tra le tecnologie più diffuse, si riportano l'**OTP via hardware disconnesso** (**70,8%**), **l'OTP via SMS** (**37,5%**) e la **tessera a combinazione** (**25%**).

Segmento Corporate

- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- **Tutte** le banche mettono a disposizione **almeno una tecnologia di secondo fattore**. In particolare:
  - Le **banche che obbligano tutti i propri clienti** all'utilizzo di almeno uno strumento di secondo fattore rappresentano l'**83,4%** del campione.
  - Oltre all'**OTP via hardware disconnesso** (**58,3%**), alla clientela Corporate viene messo a disposizione il certificato di firma digitale (**29,2%**) e l'OTP via SMS (**20,8%**).

Secondo fattore di autenticazione*

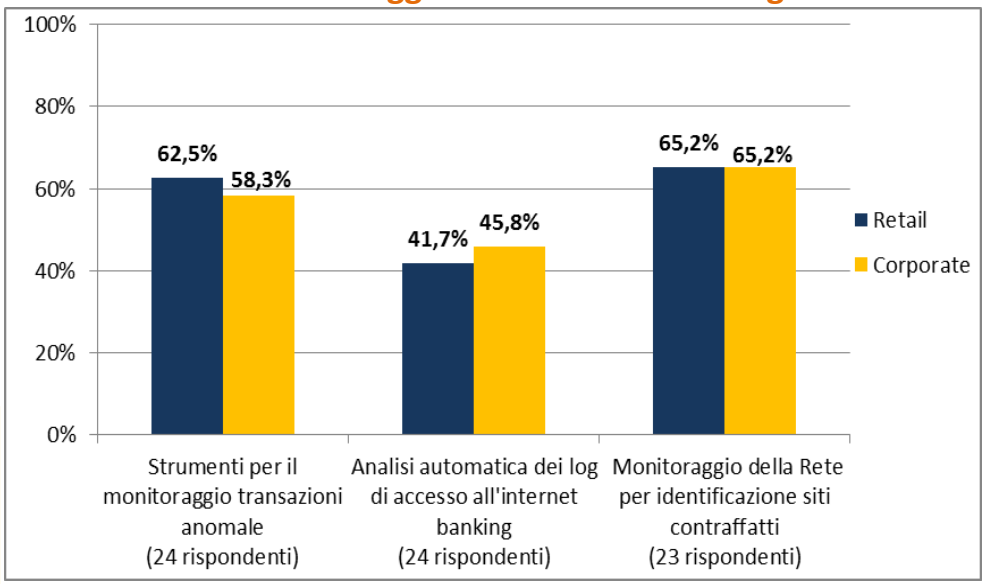


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Lo scenario italiano

Strumenti di monitoraggio e comunicazione con la clientela

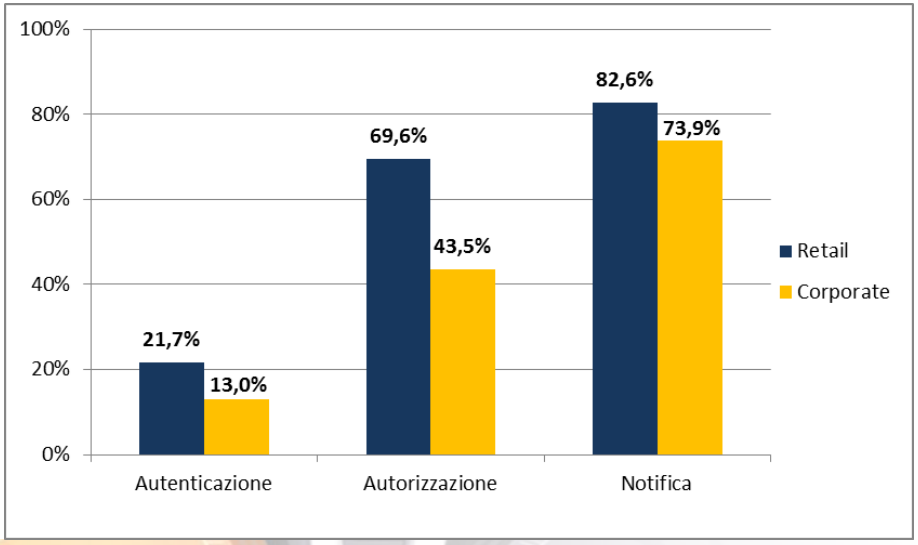
Attività di monitoraggio e dotazione tecnologica



- Sempre più banche si stanno dotando di **strumenti in grado di monitorare** la **rete**, le **transazioni anomale** effettuate e gli **accessi** al portale di Internet Banking da parte della propria clientela, sia **Retail** che **Corporate**.
- È evidente quindi come si mantenga **costante l'attenzione del settore bancario sul contrasto al fenomeno delle frodi informatiche**, anche attraverso l'utilizzo di **strumenti tecnologici** sempre più **evoluti e aggiornati**, in linea con le previsioni normative a livello europeo (Raccomandazioni BCE).

- Tra le **misure di sicurezza** per ridurre l'impatto di eventuali attacchi fraudolenti, particolare **importanza** viene riconosciuta al **canale alternativo di comunicazione** verso la clientela.
- A livello generale, qualche **margine di miglioramento** potrebbe esserci in relazione alla **clientela Corporate**, per la quale il **canale alternativo** di comunicazione **viene messo a disposizione in misura inferiore** rispetto al segmento **Retail**, specialmente in fase di **autorizzazione** delle disposizioni (particolarmente diffusi sono l'invio di SMS o di e-mail).

Utilizzo di un canale alternativo di comunicazione



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Sicurezza e rischio informatico – Agenda (1/2)

- **Vigilanza sostenibile: una visione olistica della Circolare 263**
  - Marco **Vismara,** *Partner, Responsabile Consulenza Organizzativa* **PRB**

- **Un Framework di riferimento per la gestione della sicurezza e del rischio informatico nelle banche**
  - Andrea **Agosti**, *Responsabile Servizio Security* **OASI**

- **From OTP to IT. Dalle password alla Identità Digitale**
  - Luca **Scotto D'Antuono**, *Product Manager* **Bit4id**

- **La normativa 263 e gli impatti sulla sicurezza ICT: un case study**
  - Marco **Deidda**, *Head of Data Access Management* **UniCredit Business Integrated Solutions**
  - Alessandro **Ronchi**, *Senior Security Project Manager* **Exprivia**

Sicurezza e rischio informatico – Agenda (2/2)

Tavola Rotonda di confronto su temi di Sicurezza e Analisi di Rischio Informatico, interverranno:

- John **Ramaioli,** *Responsabile Sicurezza e Business Continuity* **Banca Popolare di Milano**
- Enrico **Toso,** *IT Business Solution – ICT Regulatory, Risk and Control Specialist* **Deutsche Bank**
- Roberto **Lazzari,** *Head of Group ICT Risk and Regulation* **Gruppo UniCredit**
  Francesca **Bonora**, *Head of ICT Security* **Gruppo UniCredit**