



Sicurezza e rischio informatico: lo scenario normativo e gli impatti per le banche italiane

Monica Pellegrino, *Research Analyst*, **ABI Lab**

Roma, 5 Giugno 2013

Il contesto di riferimento

- Continua **evoluzione e sofisticazione delle minacce** e degli attacchi verso i servizi di **Internet e Mobile Banking, di pari passo con l'innovazione delle tecnologie** e delle modalità offerte alla clientela per accedere ai prodotti bancari, soprattutto da remoto.
- 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**
 - *Raccomandazioni BCE sulla sicurezza dei pagamenti internet*
 - *Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento*
- **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*

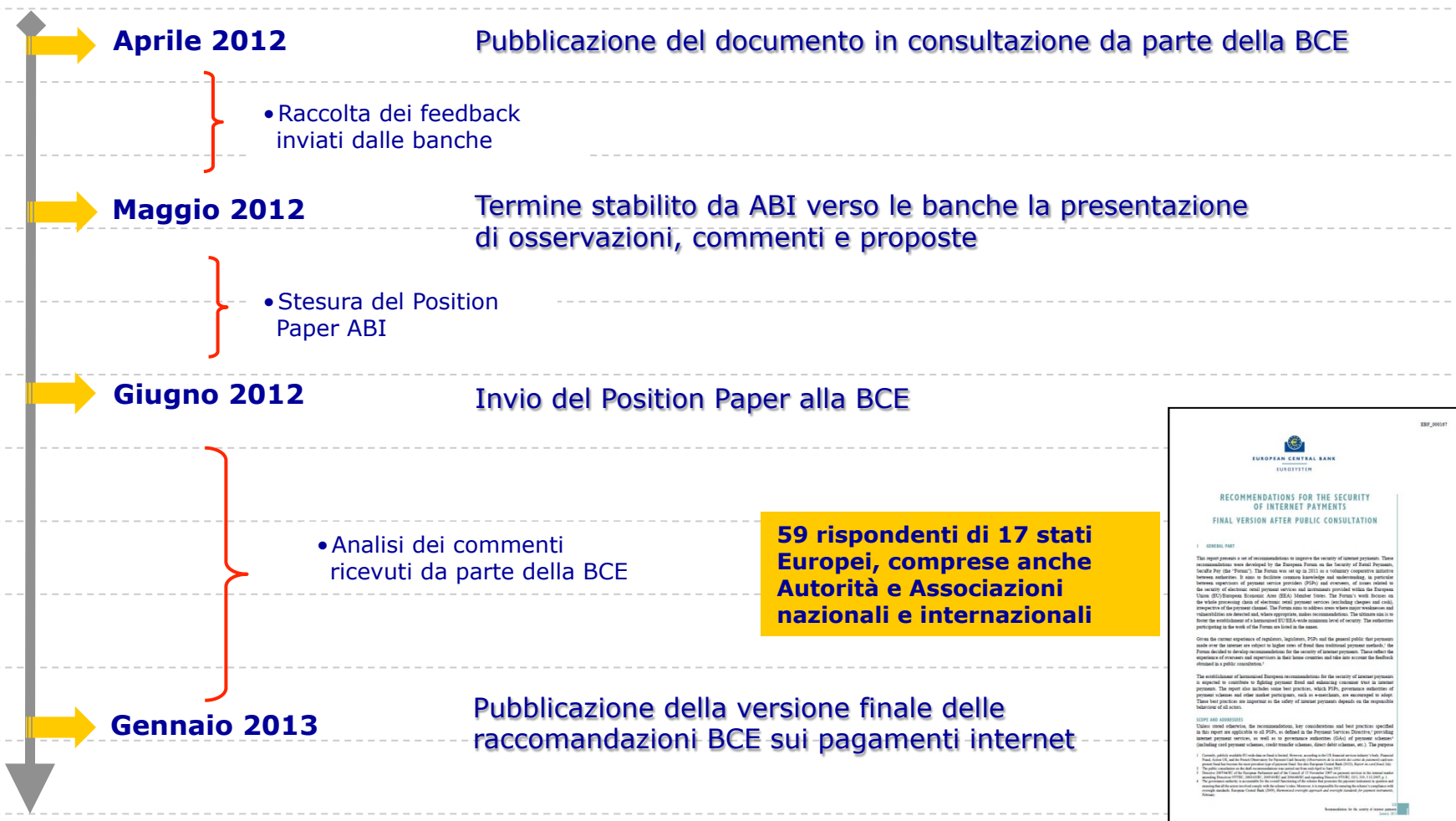
- Tali evoluzioni potranno integrarsi negli **obiettivi più ampi di protezione cibernetica e sicurezza informatica nazionale**, definiti a livello di Sistema Paese nell'ambito del **DPCM 23 gennaio 2013**



Sicurezza degli accessi e dei servizi di pagamento

Raccomandazioni BCE in materia di sicurezza dei pagamenti Internet (1/2)

IL PROCESSO DI EMANAZIONE E LE ATTIVITÀ ABI e ABI Lab



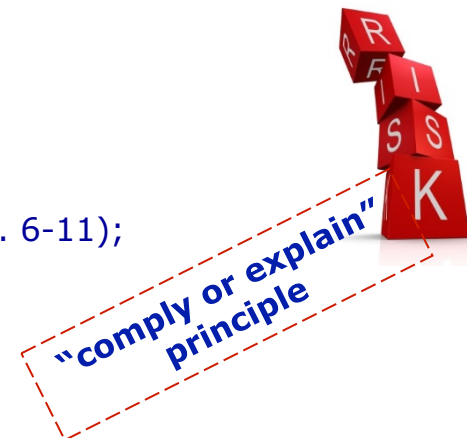
Raccomandazioni BCE in materia di sicurezza dei pagamenti Internet (2/2)

OBIETTIVO GENERALE

- Definire i **requisiti minimi** indirizzati a PSP*, **Autorità di governo** di schemi e sistemi di pagamento ed **e-merchant**, da applicare nell'erogazione di pagamenti tramite cards, credit transfers, e-mandate ed e-money

STRUTTURA del DOCUMENTO

- Le **14 Recommendations** rimangono **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);composte da *Key Considerations* e *Best Practices*.



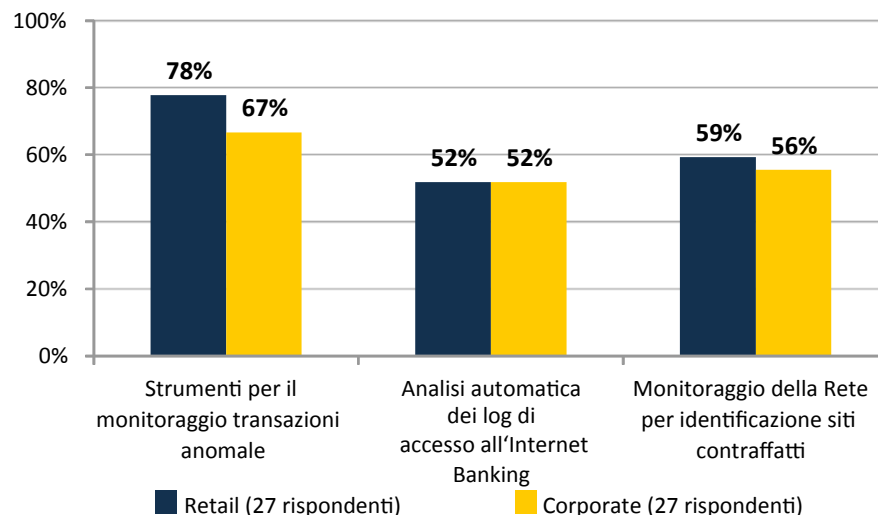
TEMPI DI IMPLEMENTAZIONE

- A livello nazionale, **le raccomandazioni saranno recepite da Banca d'Italia e inserite nelle Nuove Disposizioni di Vigilanza Prudenziale**.
- La scadenza per il recepimento è prevista per il **1 febbraio 2015**

IMPATTI PER LE BANCHE

- Secondo quanto previsto dai principi guida fondanti le raccomandazioni, sono previste le seguenti attività:
 - Realizzazione di un **assessment specifico** dei **rischi** connessi all'offerta dei servizi di pagamento online;
 - Introduzione di strumenti di **strong authentication** in fase di accesso ai servizi on line;
 - Implementazione di **procedure efficaci** in merito all'autorizzazione e monitoraggio delle transazioni per identificare comportamenti anomali e prevenire le frodi;
 - Promozione di **iniziative di sensibilizzazione** della **clientela**.

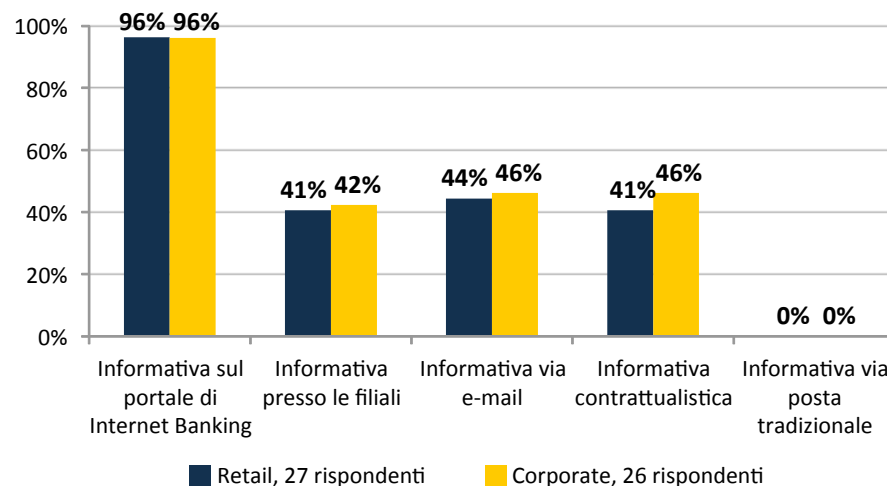
Attività di monitoraggio e dotazione tecnologica



- In linea con quanto già previsto dalle raccomandazioni, sono estremamente **diffuse** presso le banche **attività di carattere informativo** verso la clientela, comunicate principalmente sul **portale Internet Banking** della banca (**96%**) o, in alternativa, via e-mail o riportate nel contratto.
- Nelle **campagne** di informazione e sensibilizzazione sono di solito rappresentati i **rischi** e le **principali minacce** informatiche e viene data **evidenza** degli **strumenti** messi a **disposizione** dalle banche, insieme con una serie di regole e **comportamenti** per l'utente utili a **proteggere i dati** da eventuali attacchi.

- Un **numero sempre maggiore** di **banche** si sta dotando di **strumenti** in grado di **monitorare** costantemente gli accessi all'Internet Banking e di svolgere un **presidio** continuativo della **rete** e delle **operazioni** effettuate dalla clientela, sia **Retail** che **Corporate**.
- In deciso **aumento** anche le banche che partecipano direttamente a **community di information sharing** e a iniziative associative per la **collaborazione intersettoriale**, e che ricorrono a servizi di **segnalazione** ed **early warning** offerto da società esterne.

Attività informativa verso la clientela

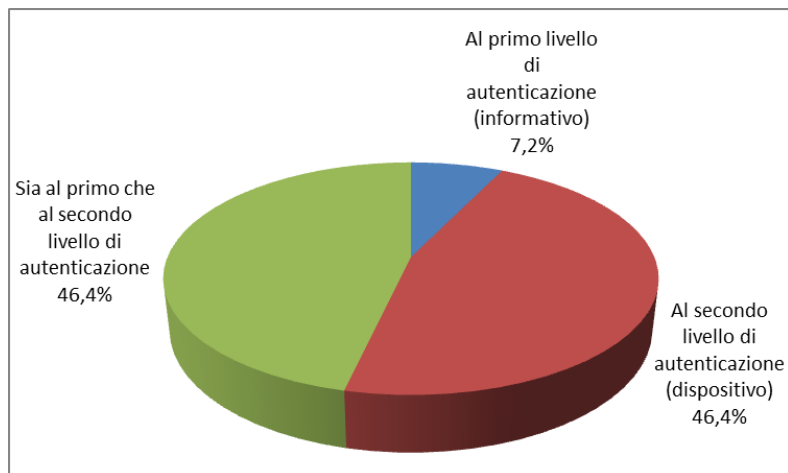


Lo scenario italiano

Contromisure tecnologiche

Segmento Retail

II fattore di autenticazione*

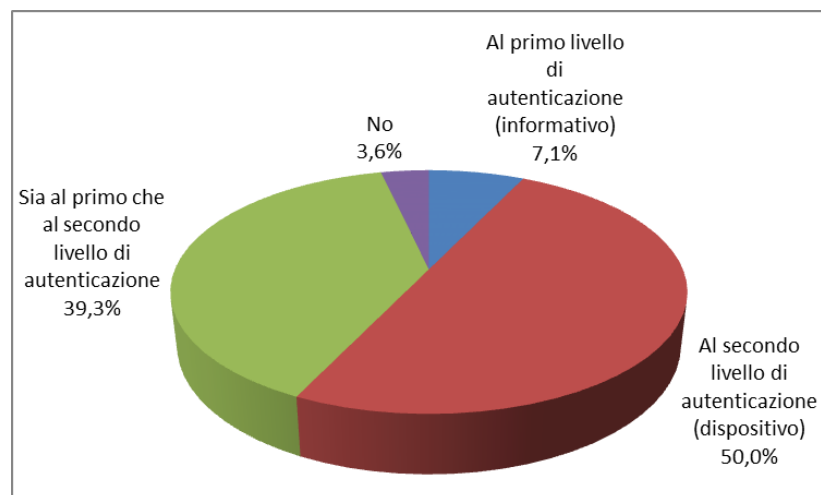


- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- **Tutte** le banche mettono a disposizione **almeno una tecnologia di II fattore**:
 - l'uso è **obbligatorio per tutti i clienti** nel **67,9%** delle banche
 - Tra le tecnologie più diffuse, vi sono l'**OTP via hardware disconnesso (57,1%)**, la **tessera a combinazione (35,7%)** e l'**OTP via SMS (28,6%)**
- Il **64,3%** delle banche ha messo a disposizione della clientela un **II canale di comunicazione** per **notificare** le operazioni disposte via Internet Banking

Segmento Corporate

- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- Il **96,4%** delle banche mette a disposizione **almeno una tecnologia di II fattore**:
 - l'uso è **obbligatorio per tutti i clienti** nel **59,3%** delle banche
 - Tra le tecnologie più diffuse, vi sono l'**OTP via hardware disconnesso (55,6%)**, il **certificato digitale (33,3%)** e la **tessera a combinazione (29,6%)**
- Il **50%** delle banche ha messo a disposizione della clientela un **II canale di comunicazione** per **notificare** le operazioni disposte via Internet Banking

II fattore di autenticazione*





- ❖ Tra le nuove opportunità di **identificazione** si inseriscono le potenzialità di innovazione che emergeranno dal **Progetto Europeo STORK 2.0**, cui partecipa anche **ABI Lab**, finalizzato a:
 - garantire l'**interoperabilità** a livello EU dei sistemi d'identità elettronica nazionali
 - permettere a imprese e cittadini di utilizzare la propria **eID nazionale** in qualsiasi Stato membro e in diversi contesti, tra cui l'ambito **bancario**.

PILOT BANCARIO



Use case 1: Apertura da remoto e cross-border di un nuovo conto corrente

- Obiettivo: consentire a **cittadini/imprese di una Nazione A** di **aprire da remoto online** un **conto corrente bancario** in una **Nazione B** differente.



Use case 2: Accesso da remoto e cross-border all'Internet Banking

- Obiettivo: consentire a **cittadini/imprese dei MS** partecipanti di utilizzare la propria identità elettronica per accedere alla piattaforma di **Internet Banking** di una **banca di un altro Paese**, a fini **informativi** e **dispositivi**. Tra le attività in programma nel pilota, è prevista la sperimentazione dell'autorizzazione del **pagamento delle fatture (e-invoicing)**.

Si ritiene che gli **esiti dei pilota** definiti nel progetto **STORK 2.0** possano ulteriormente **sensibilizzare** le **Istituzioni** dei singoli stati membri nei riguardi dell'**uso integrato e cross settoriale dell'identità elettronica**

Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento (1/2)

La Banca Centrale Europea ha pubblicato il 31 gennaio u.s. in **consultazione** un documento di **raccomandazioni** relativo ai **servizi di accesso ai conti di pagamento**

OBIETTIVO GENERALE

- Definire i **requisiti minimi** principali che **soggetti terzi** (TP) **non regolamentati** devono rispettare quando utilizzano **servizi di accesso all'informazione sui conti di pagamento**, nell'ottica di contrastare e prevenire le frodi e aumentare la fiducia dei consumatori nell'utilizzo di tali servizi

FINALITÀ

- Far adottare a **TP misure di sicurezza** e di **controllo** simili a quelle richieste ai PSP nelle raccomandazioni sulla sicurezza dei pagamenti internet
- Aumentare la **trasparenza** e la **consapevolezza** dell'**utente** in fase di accesso ai servizi forniti da TP
- Assicurare la **tracciabilità** mediante opportuna **autenticazione** in tutte le comunicazioni tra le diverse entità coinvolte (TP, PSP, e-merchant e proprietario del conto)
- Favorire lo **scambio di informazioni** in caso di ripudio, incidenti di sicurezza e casi di frode
- Assicurare la **gestione** del **numero minimo di dati necessario** per l'erogazione del servizio
- Promuovere la **contrattualizzazione** dei rapporti tra TP ed e-merchants

TEMPI di IMPLEMENTAZIONE

- I tempi previsti per l'adeguamento **non** sono stati **ancora stabiliti** ma dipenderanno dalle problematiche e dalle esigenze emerse in fase di consultazione

PRINCIPI GUIDA

- I 4 principi fondamentali delle raccomandazioni cui devono attenersi i destinatari prevedono:
 - Realizzazione di un **assessment** specifico dei **rischi**
 - Ricorso a strumenti di **strong authentication in fase di accesso** ai servizi
 - Implementazione di procedure efficaci in merito all'**autorizzazione e monitoraggio delle transazioni** per identificare comportamenti anomali e prevenire le frodi
 - Promozione di **iniziative di sensibilizzazione** della clientela

Si applica il **principio di "comply or explain"**

STRUTTURA DEL DOCUMENTO

- Il documento contiene **14 raccomandazioni**, distinte in 3 categorie
 - **General Control and Security Environment**
 - **Specific Control and Security Measures for Payment Account Access Services**
 - **Customer Awareness, Education and Communication**
- Ogni raccomandazione è specificata nel dettaglio attraverso Key Consideration (**KC**) e Best Practice (**BP**)
- La **struttura** e il **contenuto** delle raccomandazioni è simile al **documento di raccomandazioni** sulla sicurezza dei pagamenti internet

PRINCIPALI ELEMENTI DI ATTENZIONE EVIDENZIATI DAL POSITION PAPER ABI IN RISPOSTA ALLA CONSULTAZIONE

- Equiparare i fornitori di servizi di accesso ai conti – come status e responsabilità – **a tutti gli altri PSP**, in modo che siano **governati da norme vincolanti**
- Definire **accordi contrattuali** tra PSP e TP e tra queste e l'utente
- Introdurre **regole** per la **condivisione** delle **credenziali di sicurezza degli utenti con le TP**

Sicurezza nel trattamento di dati e informazioni bancarie

MISURE NECESSARIE (sanzionabili):

- Designazione dell'**outsourcer** come **responsabile del trattamento** quando il trattamento dei dati personali dei clienti da parte dell'outsourcer è svolto restando alle banche i poteri riconosciuti dal Codice privacy solo al titolare del trattamento (e dunque quando **in concreto** tali poteri non sono in capo all'outsourcer)
- **Tracciamento delle operazioni**, attraverso l'adozione di idonee soluzioni informatiche
- **Conservazione dei log** di tracciamento delle operazioni
- Implementazione di **alert** che individuino comportamenti anomali/a rischio per operazioni di inquiry
- **Audit interno** di controllo e la redazione obbligatoria di rapporti periodici.

Le misure necessarie dovranno essere implementate entro 30 mesi dalla pubblicazione del provvedimento in GU e quindi entro il 3 dicembre 2013.

MISURE OPPORTUNE

- Resa dell'**informativa all'interessato** circa la **circolazione dati** tra agenzie e filiali della stessa banca
- **Comunicazione all'interessato** delle operazioni di **trattamento illecito** (c.d. "data breach notification")
- **Comunicazione al Garante** in caso di accertata **violazione** accidentale o illecita di particolare rilevanza.



Da valutare anche gli **impatti** anche derivanti dalle nuove **evoluzioni** in materia di **data privacy**

ATTIVITÀ OPERATIVE

- **Definizione**, nell'ambito dell'Osservatorio Sicurezza e Frodi Informatiche di ABI Lab, di un **sottogruppo di lavoro ad hoc** costituito da **banche e partner ICT** con l'obiettivo di realizzare **approfondimenti**, in particolare di tipo **tecnologico e operativo**
- Sviluppo di una **metodologia di analisi del Provvedimento** a supporto delle banche così definita:



- Realizzazione di un documento di **linee guida** di carattere tecnologico e operativo a supporto delle banche in fase di adeguamento

ATTIVITÀ ISTITUZIONALI

- Collaborazione con l'**Ufficio Affari Legali ABI** sui punti di più complessa interpretazione → **FAQ (in attesa di risposta formale)**
- Partecipazione a **incontri con gli Uffici dell'Autorità Garante** per l'analisi del Provvedimento e la rappresentazione dei principali impatti sulle banche
- **Richiesta** formale da parte di ABI e Poste di **posticipare la scadenza al 3 dicembre 2014** → **in attesa di risposta formale**

INDICE dei CONTENUTI

Introduzione e Obiettivi del documento

Parte I – I contenuti del Provvedimento

1. Profili generali

- 1.1 Scopo del Provvedimento
- 1.2 Ambito soggettivo di applicazione
- 1.3 Attività svolta

2. Circolazione delle informazioni tra banche del gruppo

- 2.1 Aspetti organizzativi emersi
- 2.2 Profili di protezione

3. Circolazione delle informazioni tra banche del gruppo e gestori SI

- 3.1 Aspetti organizzativi emersi
- 3.2 Profili di protezione

4. Il tracciamento delle operazioni e gli strumenti di audit

- 4.1 Aspetti organizzativi emersi
- 4.2 Tracciamento degli accessi e i tempi di conservazione dei file di log
- 4.3 Implementazione di alert e le attività di controllo

5. Informazioni e comunicazioni in caso di accessi non autorizzati

- 5.1 Informazioni all'interessato
- 5.2 Comunicazioni al Garante

6. Sintesi conclusiva

Parte II – Le azioni delle banche ai fini dell'adeguamento

7. Il contesto di applicazione del Provvedimento

- 7.1 Definizione del perimetro di intervento – approccio metodologico
- 7.2 Contestualizzazione del Provvedimento
- 7.3 Analisi dei processi e dei servizi bancari in perimetro
- 7.4 Analisi delle applicazioni in perimetro
- 7.5 Applicabilità del Provvedimento
- 7.6 Specificità ed esclusioni

8. Aspetti operativi e tecnologici

- 8.1 Requisiti delle soluzioni tecnologiche (Raccolta, Gestione e Analisi delle informazioni)
- 8.2 Soluzioni tecnologiche (Identificazione e criteri di scelta)

9. Policy interne e verifiche

- 9.1 Ambito di intervento
- 9.2 Policy interne
- 9.3 Processi di verifica e di gestione delle segnalazioni

10. Aspetti organizzativi

- 10.1 Funzioni di controllo
- 10.2 Considerazioni sulla circolazione delle informazioni tra le banche del gruppo e i soggetti che gestiscono i SI

APPENDICE

I. Il testo integrale del Provvedimento

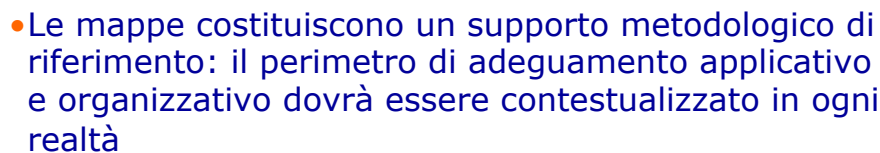
II. Le FAQ presentate all'Autorità Garante (in attesa di risposta, da inserire)

ABI Lab
Tecnologia utile

- I. Mappa funzionale** → per identificazione di **processi/attività** in perimetro

III. Mappa applicativa →

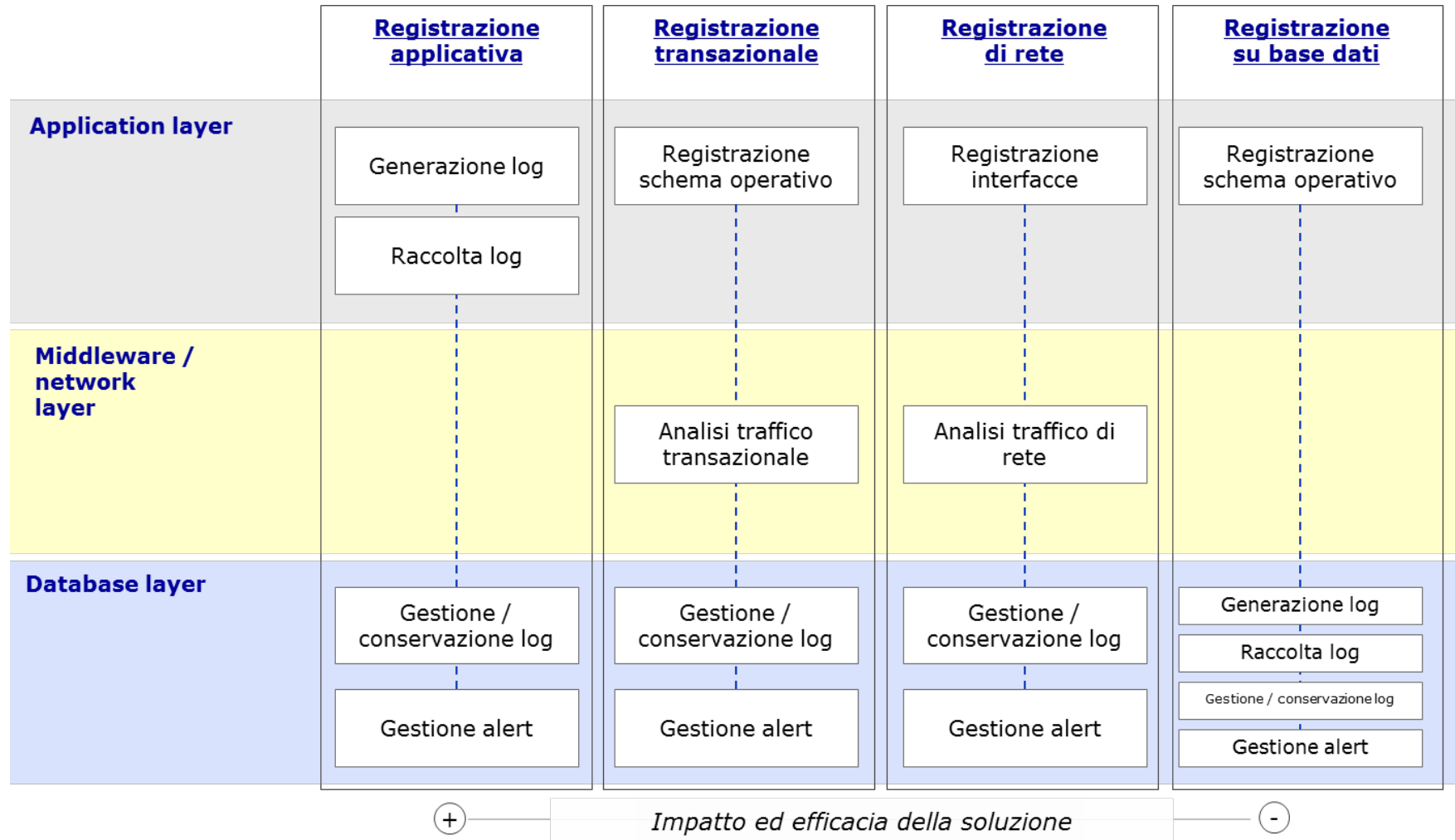
per identificazione di
componenti applicative
in perimetro



- 15 -

Focus – Aspetti operativi e tecnologici

Identificazione delle soluzioni IT di riferimento



Ciascuna famiglia di soluzioni presenta **pro** e **contro** che ogni banca dovrà valutare rispetto alle specifiche del sistema informativo esistente

Valutazione del rischio informatico e correlazione con i rischi operativi

STRUTTURA DEL DOCUMENTO IN CONSULTAZIONE

Capitolo 7: Il sistema dei controlli interni

- Sezione I: Disposizioni preliminari e principi di carattere generale
- Sezione II: Il ruolo degli organi aziendali
- Sezione III: Funzioni aziendali di controllo
- Sezione IV: Esternalizzazione di funzioni aziendali (Outsourcing)
- Sezione V: Il sistema dei controlli interni nei gruppi bancari
- Sezione VI: Imprese di riferimento
- Sezione VII: Procedure di allerta interna
- Sezione VIII: Succursali di banche comunitarie e di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci o in quelli inclusi in un elenco pubblicato dalla Banca d'Italia

5 BOX con quesiti posti da Banca d'Italia su temi specifici

Capitolo 8: Sistema informativo

- Sezione I: Disposizioni di carattere generale
- Sezione II: Governo e organizzazione dell'ICT
- Sezione III: La gestione del rischio informatico
- Sezione IV: Il sistema di gestione della sicurezza informatica
- Sezione V: Il sistema di gestione dei dati
- Sezione VI: L'esternalizzazione di sistemi e servizi ICT



Capitolo 9: Disposizioni in materia di continuità operativa

ATTIVITÀ ABI e ABI Lab IN FASE DI CONSULTAZIONE

- Redazione di un **Position Paper** grazie al coinvolgimento **gruppi di lavoro interbancari** ABI e ABI Lab
- Predisposizione **incontri** con **referenti Banca d'Italia** per rappresentare i principali **commenti** e **punti di attenzione** legati al documento in consultazione



Valutazione del rischio informatico e correlazione con rischio operativo

- **Coordinamento dei diversi attori coinvolti** – Risk Management, Sicurezza Informatica, IT e Utente
 - Importanza di una **stretta collaborazione tra le funzioni** preposte al governo della variabile informatica e la funzione di risk management/ORM
 - **Gestione del rischio informatico in coerenza** con il più ampio processo di **gestione e analisi del rischio operativo**
- **Indipendenza e flessibilità** dell'adeguamento alle disposizioni rispetto alla **struttura organizzativa**
- **Ruolo dell'utente responsabile**, tale da garantire un giusto equilibrio tra il business e le figure con competenze tecniche nella valutazione del rischio e delle relative soluzioni di mitigazione



Governo e organizzazione dell'ICT

- **Visibilità agli organi con funzioni di supervisione strategica e con funzione di gestione dei processi di gestione dell'ICT e della gestione dei sistemi informativi**
- **Indipendenza di giudizio della funzione di sicurezza informatica** nell'analisi delle variabili che concorrono alla determinazione del rischio informatico, affinché il dialogo fra la sicurezza informatica e la funzione IT favorisca la sinergia delle rispettive competenze, mantenendo al contempo l'indipendenza



Esternalizzazione di sistemi e servizi ICT

- **Distinzione tra outsourcing infragruppo presso società strumentale e outsourcing esterno alla banca/gruppo**: alcune previsioni in materia di esternalizzazione dovrebbero applicarsi solo al caso di affidamento di attività all'esterno del gruppo (es. vendor lock-in, previsione di exit strategies, etc.)

Strategia nazionale di sicurezza

Decreto del 23 Gennaio 2013 in materia di sicurezza informatica del Sistema Paese

- È stato pubblicato in GU il **19 marzo 2013** il **DPCM** recante «**indirizzi per la protezione cibernetica e la sicurezza informatica nazionale**».
- Il Decreto prevede lo **sviluppo delle iniziative di sicurezza nazionali** lungo **tre** linee di intervento:
 - strategico: confermato e consolidato il ruolo del **Comitato interministeriale per la sicurezza della Repubblica (CISR)**;
 - operativo: da istituire, con carattere permanente, **il Nucleo per la Sicurezza Cibernetica**;
 - presidio, contrasto e repressione: sarà costituito un **Tavolo interministeriale di crisi cibernetica**
- Tra gli obiettivi del **Decreto** vi è anche **favorire la cooperazione pubblico-privato** sui temi di sicurezza informatica



Opportunità di **definire** adeguate **procedure di cooperazione e information sharing**

In questo scenario, ABI Lab potrà farsi promotore di sinergie tra banche e soggetti pubblici

Sicurezza e Rischio Informatico – Agenda

- Nuove disposizioni di vigilanza di Banca d'Italia su controlli interni, sistema informativo e continuità operativa: focus su governance dei sistemi informativi, gestione e valutazione del rischio informatico
 - Pietro **Franchini**, *Direttore Vigilanza Bancaria e Finanziaria* **Banca d'Italia**
- Governance, rischi e compliance: una visione della sicurezza di tipo convergente
 - Fabio **Rovati**, *Security Practitioner* **KBE**
- Big data e sicurezza nelle banche: l'estensione delle regole di governance a tutte le informazioni sensibili
 - Sergio **Mucciarelli**, *Data Security Leader* **IBM Italia**
- Nuovi scenari di attacco multidimensionale: oltre Eurograbber
 - Giacomo **Paoni**, *Security Practice Manager* **Techub**
- Cyber Security nel contesto bancario
 - Tommaso **Stranieri**, *Partner* **Deloitte**
 - Luca **Lumini**, *Manager* **Deloitte**
- Sicurezza informatica delle pubbliche amministrazioni: il ruolo dell'Agenzia per l'Italia Digitale
 - Giovanni **Rellini Lerz**, *Responsabile della continuità operativa delle PA* **Agenzia per l'Italia Digitale**