CONVENZIONE INTERBANCARIA
PER I PROBLEMI DELL'AUTOMAZIONE

ASSOCIAZIONE BANCARIA
ITALIANA

Questionario per la

Rilevazione dello stato dell'automazione del sistema creditizio

Profili tecnologici e di sicurezza

Dicembre 2010

NOTA:

IL PRESENTE QUESTIONARIO NON PUÒ ESSERE UTILIZZATO O RIPRODOTTO, ANCHE PARZIALMENTE, PER ALTRI FINI SENZA UNA PREVENTIVA AUTORIZZAZIONE DA PARTE DELLA CIPA E DELL'ABI.

Dati identificativi

Codice ABI ¦__¦__¦__¦__¦__¦

Ragione sociale.....

.....

.....

Dati del referente per la compilazione del questionario

Cognome.....

Nome.....

Recapito aziendale:

Indirizzo.....

CAP.....***Città***..... ***Prov.*** .....

Telefono..... ***Fax***.....

E-mail.....@.....

Eventuale casella funzionale della struttura.....@.....

Avvertenza

Per la compilazione del questionario si raccomanda vivamente di consultare il Manuale allegato al Questionario, che contiene chiarimenti e informazioni sul contenuto di ciascuna domanda.

Il Questionario e il Manuale di compilazione sono anche disponibili sul sito internet della CIPA (www.cipa.it) sotto la voce:

- *Documenti*
  - *Rilevazione dello stato dell'automazione del sistema creditizio*

Assistenza alla compilazione

Coordinamento del gruppo interbancario:

Isabella VICARI: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6803

Romano STASI: Associazione Bancaria Italiana Tel. 06 / 6767.269

I chiarimenti per la compilazione del questionario possono essere richiesti a:

Paola MOSTACCI: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.7682

Pier Luigi POLENTINI: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6449

Alessandro PASCIUTO: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6660

Andrea GENTILI: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6517

Ernesto FERRARI: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6469

Daniela D'AMICIS: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6943

Francesco CAVALLO: Banca d'Italia (Segreteria CIPA) Tel. 06 / 4792.6101

Silvia ATTANASIO: Associazione Bancaria Italiana Tel. 06 / 6767.793

Hanno collaborato alla stesura del questionario:

Christian ALTOMARE: Deutsche Bank

Fabrizio BELLOLI: UBI Banca

Giovanni BONACCI: Banca Etruria

Marco BRUZZESI: Banca Sella

Stefano BUCCINO: Banca Popolare di Vicenza

Marco CODA: Banca Sella

Carlo COTRONEO: Banca Nazionale del Lavoro

Maria EVANGELISTA: Consorzio Operativo Gruppo MPS

Leonardo GIOSCIA: UGF Banca

Sara GIROLDI: Credito Emiliano

Agostino LUCONI: Banca delle Marche

Emilio SAGLIO: Credito Valtellinese

Francesca MASTELLA: Banco Popolare - SGS

Giampiero MELEGARI: Banca Popolare dell'Emilia Romagna

Antonio MELINA: IntesaSanpaolo

Claudio PAGLIA: IntesaSanpaolo

Lucia PASTORE: Veneto Banca

Massimo RIMINUCCI: Banca CARIGE

Patrizia ROSSI: Banca CARIGE

Filiberto Luigi ROSSI: Consorzio Operativo Gruppo MPS

Giovanni SCOSCINI: Banca Etruria

Marco TEMPRA: Banca Popolare di Sondrio

Sebastiano VITA: UniCredito Italiano - UGIS

Giorgio VIVORI: Banca Popolare di Milano

Paolo ZACCO: Cassa di Risparmio di Parma e Piacenza

Sabina Di GIULIOMARIA: Banca d'Italia (Unità di Supporto d'Area)

Premessa

La Rilevazione dello stato dell'automazione del sistema creditizio ha l'obiettivo di fornire una visione d'insieme dell'utilizzo dell'*Information and Communication Technology* nelle banche, analizzando, senza alcuna pretesa di esaustività, i diversi profili dell'ICT nelle aziende che aderiscono all'iniziativa: aspetti organizzativi, tecnologici, di accessibilità e di sicurezza.

Quest'anno la *Rilevazione dello stato dell'automazione del sistema creditizio* è stata strutturata in due sezioni distinte: nella prima sono stati esaminati i profili economici, organizzativi e di *governance* dell'IT; i risultati, riferiti all'esercizio 2009, sono stati pubblicati a luglio 2010. Nella seconda, cui si riferisce il presente questionario, vengono esaminati i profili tecnologici e di sicurezza, in particolare l'utilizzo delle tecnologie innovative - nel contatto con la clientela e nei processi amministrativi interni - e i presidi adottati per il contenimento e il controllo del rischio informatico. L'ambito di riferimento è la situazione a dicembre 2010.

Il questionario tecnologico viene rivolto, secondo una scelta ormai consolidata, a un duplice campione: uno "di gruppo", ampliato quest'anno a ventiquattro gruppi bancari tra i maggiori per totale attivo, e uno "individuale", costituito da banche singole, non aderenti a gruppi o aderenti a gruppi diversi da quelli partecipanti all'iniziativa.

I risultati dell'analisi vengono illustrati in un apposito documento che viene pubblicato sui siti internet della CIPA (www.cipa.it) e dell'ABI (www.abi.it).

Le informazioni fornite su base volontaria e raccolte da CIPA e ABI vengono utilizzate esclusivamente ai fini dell'indagine e sono diffuse all'esterno soltanto in forma aggregata. Il trattamento dei dati si svolge, senza intervento di terze parti, con modalità atte a garantirne la sicurezza e la riservatezza.

Tecnologie innovative, canali distributivi e misure di sicurezza

1 - Utilizzo di tecnologie innovative nel sistema bancario

1.1 – Per quali delle seguenti tecnologie sono stati sostenuti o si prevede di sostenere costi?

1 = Già sostenuti o previsti entro il 2011;

2 = Non ancora sostenuti, ma previsti nel successivo biennio (2012-2013);

3 = Non sostenuti e non previsti.

Tecnologie		*Campi di applicazione*	
		Funzioni interne	*Funzioni di business*
1.	Contactless	|__|	|__|
2.	Sistemi di riconoscimento biometrico	|__|	|__|
3.	Applicazioni Mobile	|__|	|__|
4.	Applicazioni Web 2.0 (social networking, ecc.)	|__|	|__|
5.	Business Intelligence	|__|	|__|
6.	Cloud computing	|__|	|__|
7.	VoIP	|__|	
8.	Web Conferencing	|__|	
9.	Applicazioni in logica Service Oriented (SOA)	|__|	
10.	Green IT	|__|	

1.1 bis – Per chi ha risposto "1" o "2" ai punti 1, 3, 4 della domanda 1.1, specificare gli ambiti applicativi interessati.

1 = Applicazione già realizzata o prevista entro il 2011;

2 = Applicazione prevista nel successivo biennio (2012-2013);

3 = Non realizzata, né prevista.

Contactless		
1.	Riconoscimento (esclusivamente)	¦__¦
2.	Applicazioni di pagamento	¦__¦
3.	Altro, specificare _____	¦__¦

Applicazioni Mobile		
4.	Riconoscimento con uso congiunto contactless e mobile	¦__¦
5.	Pagamento contactless su rete locale	¦__¦
6.	Pagamento via gestore telefonico	¦__¦
7.	Remote banking	¦__¦
8.	Altro, specificare _____	¦__¦

Applicazioni Web 2.0		
9.	Supporto all'operatività corrente	¦__¦
10.	Applicazioni per ATM	¦__¦
11.	Social networking, blog, forum, ecc.	¦__¦
12.	Altro, specificare _____	¦__¦

1.2 – Qual è l'andamento previsto nell'impiego delle seguenti tecnologie nei servizi bancari per il prossimo biennio (2012-2013)?

1 = In aumento;
2 = Stabile;
3 = In diminuzione;
4 = Non applicabile / non previsto.

Tecnologie		
1.	Contactless	¦__¦
2.	Sistemi di riconoscimento biometrico	¦__¦
3.	Applicazioni Mobile	¦__¦
4.	Applicazioni Web 2.0 (social networking, ecc.)	¦__¦
5.	Business Intelligence	¦__¦
6.	Cloud computing	¦__¦
7.	VoIP	¦__¦
8.	Web Conferencing	¦__¦
9.	Applicazioni in logica Service Oriented (SOA)	¦__¦
10.	Green IT	¦__¦

1.3 – Per chi ha risposto "1" o "2" ai rispettivi punti della domanda 1.1, indicare se per l'utilizzo di quelle tecnologie si ritiene necessario disporre prevalentemente di specifiche competenze professionali e con quali modalità.

1 = Competenze professionali già presenti *in House* (incluse le Società strumentali);
2 = Competenze professionali di cui si prevede di dotarsi *in House* (incluse le Società strumentali);
3 = Competenze professionali presso fornitore esterno.

Tecnologie		*Competenze operative*	*Competenze di coordinamento e di management*
1.	Contactless	¦__¦	¦__¦
2.	Sistemi di riconoscimento biometrico	¦__¦	¦__¦
3.	Applicazioni Mobile	¦__¦	¦__¦
4.	Applicazioni Web 2.0 (social networking, ecc.)	¦__¦	¦__¦
5.	Business Intelligence	¦__¦	¦__¦
6.	Cloud computing	¦__¦	¦__¦
7.	VoIP	¦__¦	¦__¦
8.	Web Conferencing	¦__¦	¦__¦
9.	Applicazioni in logica Service Oriented (SOA)	¦__¦	¦__¦
10.	Green IT	¦__¦	¦__¦

1.4 – Facendo riferimento ai canali di contatto con la clientela (diversi dallo sportello), indicare quali delle tecnologie elencate vengono attualmente utilizzate e con quali modalità vengono realizzate applicazioni/interventi.

1 = Sì, *in House* (incluse le Società strumentali);
2 = Sì, in *outsourcing* presso fornitore esterno;
3 = No.

Tecnologie		***Canali***				
		ATM	Call Center / Phone banking	Internet banking	Mobile banking	Promotore finanziario
1.	Contactless	|__|	|__|	|__|	|__|	|__|
2.	Sistemi di riconoscimento biometrico	|__|	|__|	|__|	|__|	|__|
3.	Applicazioni Mobile	|__|	|__|	|__|	|__|	|__|
4.	Applicazioni Web 2.0 (social networking, ecc.)	|__|	|__|	|__|	|__|	|__|
5.	Business Intelligence	|__|	|__|	|__|	|__|	|__|
6.	Cloud computing	|__|	|__|	|__|	|__|	|__|
7.	VoIP	|__|	|__|	|__|	|__|	|__|
8.	Web Conferencing	|__|	|__|	|__|	|__|	|__|
9.	Applicazioni in logica Service Oriented (SOA)	|__|	|__|	|__|	|__|	|__|
10.	Green IT	|__|	|__|	|__|	|__|	|__|

1.5 – Indicare, per tipologia di servizio bancario e per ciascun canale di contatto messo a disposizione della clientela, il trend di utilizzo previsto nel breve periodo (12 mesi).

1 = In aumento;
2 = Stabile;
3 = In diminuzione;
4 = Non applicabile / Canale non disponibile.

		Canali offerti					
		ATM	Call Center / Phone Banking	Internet Banking	Mobile Banking	Promotore finanziario	Sportello
Servizi		*Trend*					
1.	Bancari informativi (es. saldo e movimenti c/c, situazione assegni)	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦
2.	Bancari dispositivi (es. bonifici)	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦
3.	D'investimento informativi (es. quotazioni)	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦
4.	D'investimento dispositivi (es. trading)	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦
5.	Servizi commerciali (es. info sui prodotti)	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦
6.	Accessori non bancari (es. ricariche prepagate)	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦
7.	Customer Care e Help desk	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦	¦__¦

1.6 – Quali delle seguenti funzioni sono rese disponibili alla clientela attraverso specifiche applicazioni Internet *o su piattaforma* Mobile*?*

1 = Funzione disponibile;
2 = Funzione prevista;
3 = Funzione non disponibile.

Funzioni		*Internet*		*Mobile banking*	
		senza password	*con password*	*nativo*	*navigazione ottimizzata*
1.	Localizzazione Filiale/ATM	¦__¦	¦__¦	¦__¦	¦__¦
2.	Iniziative di *education*	¦__¦	¦__¦	¦__¦	¦__¦
3.	Area FAQ per le offerte alla clientela	¦__¦	¦__¦	¦__¦	¦__¦
4.	*Social media (PodCast*, *Community*, ecc.)	¦__¦	¦__¦	¦__¦	¦__¦
5.	*Live chat* con operatori o promotori	¦__¦	¦__¦	¦__¦	¦__¦
6.	Calendario eventi	¦__¦	¦__¦	¦__¦	¦__¦

1.7 – Nello sviluppare applicazioni per offrire servizi su Internet o piattaforma Mobile *all'utenza esterna, indicare quali criteri di accessibilità si applicano.*

1 = Criterio applicato sempre;
2 = Criterio applicato a seconda del contesto;
3 = Criterio non applicato

	Criteri	*Internet*	*Mobile banking*
1.	Utilizzo di tecnologie compatibili con l'accessibilità	|__|	|__|
2.	Utilizzo di tecnologie assistive, con contenuti consistenti su diversi canali sensoriali	|__|	|__|
3.	Facilità di utilizzo dell'applicazione	|__|	|__|
4.	Facilità di individuazione delle azioni necessarie per ottenere servizi	|__|	|__|

1.8 – Sono state attuate o sono in programma iniziative per:

1 = Iniziativa già attuata;
2 = Iniziativa in programma nel breve periodo;
3 = Iniziativa non attuata e non in programma.

1.	Utilizzare il *social networking* come strategia di canale interna ed esterna	|__|
2.	Sperimentare l'utilizzo del *social networking* nell'ambiente di lavoro per migliorare la comunicazione e la collaborazione	|__|
3.	Sperimentare l'utilizzo del *social networking* con la clientela esterna a fini di ampliamento del target, fidelizzazione e rafforzamento del marchio	|__|
4.	Sperimentare forme di *social networking* in situazioni *business-to-business* per migliorare la comunicazione, la collaborazione e l'accesso alle informazioni	|__|

2 – Le misure di sicurezza

2.1 – Sono stati adottati standard riconosciuti (ovvero sono in corso iniziative per la loro adozione) o si fa riferimento a* best practices *per la gestione della sicurezza informatica?

1 = Sì, adottati;
2 = Sì, iniziative in corso;
3 = No.

Riferimenti		
1.	Norma ISO 27001, per la sicurezza	
2.	Norma ISO 27002, per l'*auditing*	
3.	Service Organization Control (SOC) Report (ex SAS70 Report)	
4.	PCI / DSS (per le transazioni finanziarie)	
5.	Best practices (es.: NIST, SANS, ….)	
6.	Standard OWASP per lo sviluppo sicuro delle applicazioni	
7.	Altro, specificare _____	

2.2 – Oltre a produttori di antivirus e/o di firewall, da quali fonti vengono assunte informazioni rispetto ad attacchi, virus e malfunzionamenti dei sistemi e del software?

1 = Sì;
2 = No.

Fonti		
1.	Centri di assistenza e di supporto presso i *Technology providers*	
2.	Siti governativi	
3.	Centri di ricerca, Centri specializzati in sicurezza di servizi finanziari, Osservatori di organizzazioni e associazioni no profit	
4.	Altro, specificare _____	

2.3 – Oltre che per gli adempimenti rivenienti dalla normativa sulla privacy, è stato adottato un sistema di classificazione delle informazioni aziendali?

1 = Sì, per tutto il patrimonio informativo aziendale di alto livello;
2 = Sì, per la parte prevalente del patrimonio informativo aziendale;
3 = Sì, per una parte ancora marginale del patrimonio informativo aziendale;
4 = No.

|__|

2.4 – Classificare, per ordine crescente di spesa, da "1" a "6", i seguenti scenari di rischio, sulla base degli investimenti sostenuti o previsti in budget.

Scenari di rischio		*Spesa sostenuta*	*Spesa prevista*
1.	Furto o compromissione di credenziali per clienti *retail*	|__|	|__|
2.	Furto o compromissione di credenziali per clienti *corporate*	|__|	|__|
3.	Attacco informatico (*Virus*, *Denial of service*, ecc.)	|__|	|__|
4.	Dati compromessi da parte di un fornitore *outsourcer*	|__|	|__|
5.	Violazioni interne ad opera di dipendenti	|__|	|__|
6.	Attacco da *malware* su client	|__|	|__|

2.5 – Quali modalità e livelli di autenticazione vengono adoperati e in quali tipologie di conto?

1 = Sì;
2 = No.

Modalità e livelli di autenticazione			
1° livello – informativo		*Retail*	*Corporate*
1.	Autenticazione statica	¦__¦	¦__¦
2.	Autenticazione dinamica	¦__¦	¦__¦
3.	Altro, specificare _____	¦__¦	¦__¦

2° livello – dispositivo		*Retail*	*Corporate*
4.	Autenticazione statica	¦__¦	¦__¦
5.	Autenticazione dinamica	¦__¦	¦__¦
6.	Altro, specificare _____	¦__¦	¦__¦

2.6 – Nel caso sia stato adottato il doppio fattore di autenticazione, quali tecnologie vengono utilizzate a supporto?

1 = Sì;
2 = No.

Tecnologie di autenticazione			
1. TOKEN		*Retail*	*Corporate*
1.1	OTP via hardware connesso	|__|	|__|
1.2	OTP via hardware disconnesso	|__|	|__|
1.3	Certificato digitale su token	|__|	|__|
1.4	Altro, specificare_____	|__|	|__|

2. MOBILE		*Retail*	*Corporate*
2.1	OTP su SIM	|__|	|__|
2.2	OTP via SMS	|__|	|__|
2.3	OTP via numero verde	|__|	|__|
2.4	Certificato digitale su SIM	|__|	|__|
2.5	Firma digitale su SIM	|__|	|__|
2.6	Mobile strong authentication	|__|	|__|
2.7	Altro, specificare_____	|__|	|__|

3. BIOMETRIA		*Retail*	*Corporate*
3.1	Supporto hardware	|__|	|__|
3.2	Supporto software	|__|	|__|
3.3	Altro, specificare_____	|__|	|__|

4. CARTE		*Retail*	*Corporate*
4.1	Tessera a combinazione	|__|	|__|
4.2	Software su smart card	|__|	|__|
4.3	Certificato digitale su smart card	|__|	|__|
4.4	OTP su smart card	|__|	|__|
4.5	OTP via lettore EMV	|__|	|__|
4.6	Token card	|__|	|__|
4.7	Altro, specificare_____	|__|	|__|

5. SISTEMI SOFTWARE		*Retail*	*Corporate*
5.1	OTP generata da software	¦__¦	¦__¦
5.2	Firma digitale	¦__¦	¦__¦
5.3	Certificato digitale	¦__¦	¦__¦
5.4	Software adattativi di profilazione utenti	¦__¦	¦__¦
5.5	Altri sistemi software evoluti	¦__¦	¦__¦
5.6	Altro, specificare_____	¦__¦	¦__¦

2.7 – In caso di adozione di un secondo canale, per quali funzioni è stato previsto?

1 = Sì;
2 = No.

Funzioni		*Secondo canale*		
		SMS	*E-mail*	*Telefono*
1	Autenticazione al servizio	¦__¦	¦__¦	¦__¦
2.	Autorizzazione dell'operazione	¦__¦	¦__¦	¦__¦
3.	Notifica	¦__¦	¦__¦	¦__¦

2.8 – Quali iniziative di carattere organizzativo vengono adottate per mitigare i rischi di frode interna/esterna?

1 = Sì;
2 = No.

Iniziative		Frode interna	Frode esterna
1.	*Assessment* di sicurezza e sensibilizzazione del personale interno	¦__¦	¦__¦
2.	Previsione di policy specifiche	¦__¦	¦__¦
3.	Applicazione del principio del *four eyes* nelle transazioni critiche	¦__¦	¦__¦
4.	Applicazione di una metodologia di sviluppo secondo le *best practices* di sicurezza	¦__¦	¦__¦
5.	Tracciamento dell'operatività	¦__¦	¦__¦
6.	Applicazione del principio del minimo privilegio (utente, software e *hardening* dei sistemi)	¦__¦	¦__¦
7.	Servizio di alert per attacco in corso	¦__¦	¦__¦

2.9 – Quali iniziative verso l'utenza sono state adottate, o si ha intenzione di adottare, per mitigare i rischi di frode nell'offerta di servizi telematici?

1 = Sì, sono effettuate periodicamente una o più volte l'anno
2 = Sì, periodicamente con intervalli superiori all'anno
3 = No

	Iniziative	*Internet*	*Mobile banking*
1.	Iniziative mirate ad elevare la consapevolezza del cliente sui rischi dell'operatività *online*	|__|	|__|
2.	Iniziative volte ad illustrare i comportamenti che gli utenti devono adottare per mitigare i rischi	|__|	|__|
3.	Iniziative volte ad illustrare gli accorgimenti tecnici che gli utenti possono adottare per mitigare i rischi	|__|	|__|
4.	Iniziative volte ad illustrare le principali misure poste in atto per elevare la sicurezza dei servizi offerti	|__|	|__|

Manuale per la compilazione
del Questionario per la

Rilevazione
dello stato dell'automazione
del sistema creditizio

Profili tecnologici e di sicurezza

Dicembre 2010

Avvertenze generali

⇒ *Per ciascun capitolo del questionario sono indicati gli obiettivi conoscitivi perseguiti;*

⇒ *per ciascuna domanda vengono fornite indicazioni per la corretta compilazione delle risposte;*

⇒ *una mancata risposta esclude la banca o il gruppo dall'elaborazione delle risposte concernenti la specifica domanda;*

⇒ *i singoli campi vanno riempiti selezionando la risposta tra quelle disponibili nel menù a tendina ovvero digitando il valore nella rispettiva cella senza eseguire operazioni di copia e incolla;*

⇒ *il* ***questionario*** *integra una logica di controllo automatico di coerenza delle risposte fornite; in caso di errore, vengono visualizzati messaggi di* warning.

Dati identificativi del Gruppo o della Banca

- In caso di gruppo bancario, indicare il codice ABI della banca capogruppo (cinque cifre senza cin di controllo); in caso di banca, indicare il codice ABI della banca stessa.
- Inserire la ragione sociale del gruppo bancario o della banca.

Dati del referente per la compilazione del questionario

- Inserire il cognome e nome del referente per la compilazione del questionario.
- Inserire il recapito aziendale, con tutti i dati richiesti, al quale sia possibile far riferimento per eventuali informazioni o chiarimenti.

NOTE: è consigliabile indicare il nominativo di una persona a cui, all'occorrenza, possa essere segnalata la presenza di anomalie o comunque possano essere richieste informazioni.

TECNOLOGIE INNOVATIVE, CANALI DISTRIBUTIVI E MISURE DI SICUREZZA

1. Utilizzo di tecnologie innovative nel sistema bancario

Obiettivi conoscitivi:

- ✓ individuare l'utilizzo corrente di tecnologie innovative, le modalità di realizzazione delle iniziative a loro collegate e le previsioni di sviluppo;
- ✓ individuare l'esigenza di specifiche competenze professionali e l'eventuale modalità di approvvigionamento;
- ✓ rilevare quali canali di contatto vengono messi a disposizione della clientela per i vari servizi bancari;
- ✓ individuare quali funzioni sono disponibili - ovvero saranno presto disponibili - su internet e su piattaforma *mobile*.

1.1 – Per quali delle seguenti tecnologie sono stati sostenuti o si prevede di sostenere costi?

Per le tecnologie elencate nella prima parte della tabella (punti 1-6) si vuole conoscere il campo di applicazione, ossia l'utilizzo della tecnologia nell'attività operativa della banca ("funzioni interne") o nei rapporti con il cliente ("funzioni di *business*").
Ad esempio, per la tecnologia "*contactless*", la timbratura *contactless* dei dipendenti della banca è una "funzione interna" mentre il pagamento *contactless* con carte di credito abilitate è una "funzione di *business*".
Nella seconda parte della tabella (punti 7-10) sono indicate le tecnologie c.d. *orizzontali*, ossia presenti nel tessuto organizzativo della banca e difficilmente restringibili a funzioni specifiche.
Vanno riempite tutte le caselle.

Si riporta di seguito una descrizione di massima delle tecnologie cui si fa riferimento nella domanda.

Contactless

Con il termine *contactless* ci si riferisce a tecnologie che permettono l'interazione di due o più entità senza contatto fisico, per esempio per applicazioni di riconoscimento. Tipicamente per *contactless* si intende la tecnologia RFID (*Radio Frequency IDentification*) o la più recente NFC (*Near Field Communication*).
La risposta a questa domanda va valutata indipendentemente dal fatto che questa tecnologia sia integrata o meno in dispositivi *mobile* (ad esempio: *smart card* NFC integrata in uno *smartphone*). Un maggiore dettaglio in tal senso verrà richiesto nelle successive domande.

Sistemi di riconoscimento biometrico

Si fa riferimento a quei sistemi in grado di identificare una persona tramite il riconoscimento di una o più caratteristiche biologiche e comportamentali (ad esempio, le impronte digitali, il colore e la dimensione dell'iride, la fisionomia del volto, l'impronta vocale, la firma, ecc.).

Applicazioni Mobile

Per *mobile* si intende l'insieme di quei dispositivi definiti come *handheld*, ossia terminali mobili di dimensioni ridotte dai quali l'utente è in grado di effettuare operazioni originariamente effettuabili esclusivamente da PC.
Esempi di dispositivi *mobile* cui ci si riferisce sono: i cellulari, gli *smartphone*, i palmari e i PDA (*Personal Digital Assistant*). In questo contesto, un *PC portatile* non è un dispositivo *mobile*.
Le applicazioni *mobile* possono essere utilizzate indifferentemente dall'interno o dall'esterno dell'azienda e indirizzate sia alla clientela sia al personale dell'azienda stessa.

Applicazioni Web 2.0

Il termine Web 2.0 indica il recente sviluppo di strumenti *software* in grado rendere più interattiva la fruizione del web e la comunicazione fra fornitori di servizi e utenti.
Il Web 2.0 identifica qui un approccio interattivo per usare la connessione con la banca a fini operativi o informativi.

Ad esempio, rientrano nel concetto di Web 2.0:

- lo sviluppo di un'applicazione web di "Assistente digitale" che informa il cliente rispondendo a domande come un assistente umano;
- un sistema di *social networking* sviluppato per i dipendenti della banca.

Non rientrano nel concetto di Web 2.0:

- una pagina di FAQ (Frequently Asked Questions);
- una pagina di un *social network* esterno dedicata alla banca.

Business Intelligence

Insieme di processi aziendali e tecnologie per raccogliere e analizzare informazioni strategiche, trasformando dati e informazioni in "conoscenza". Generalmente le informazioni vengono raccolte e analizzate per indirizzare le decisioni direzionali (*Decision support systems*) nelle aree di *business* e per il controllo di gestione.
Esempi di *business intelligence* sono i processi di *benchmarking* dell'operatività interna, applicazioni di presentazione di dati nell'interfaccia con il cliente, *dashboard* di supporto al *management*.

Cloud computing

Con il termine *Cloud computing* si intende un insieme di tecnologie informatiche che permettono l'utilizzo di risorse *hardware* (*storage*, CPU, ecc.) o *software* distribuite in remoto.
Una caratteristica del *Cloud computing* è di rendere disponibili all'utilizzatore le risorse come se fossero implementate da sistemi (*server* o periferiche personali) "standard". L'allocazione effettiva delle risorse non è definita in modo dettagliato; anzi l'idea è proprio che l'implementazione sia un insieme eterogeneo e distribuito – *the cloud*, in inglese nuvola – di risorse le cui caratteristiche non sono note all'utilizzatore.

Il termine "*Cloud computing*" si differenzia dal "*Grid computing*" che è un paradigma orientato al calcolo distribuito e in generale, richiede che le applicazioni siano progettate in modo specifico. Tipologie di Cloud computing sono:

- SaaS (Software as a Service) - Consiste nell'utilizzo di programmi in remoto, spesso attraverso un *server web*.
- PaaS (Platform as a Service) - È simile al SaaS, ma prevede l'utilizzo in remoto non di un singolo programma, ma di una piattaforma software che può essere costituita da diversi servizi, programmi, librerie, etc.
- IaaS (Infrastructure as a Service) – Consiste nell'utilizzo di risorse hardware in remoto (le risorse vengono utilizzate su richiesta, al momento in cui un utente ne ha bisogno).

VoIP

Voice over IP protocols; tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o un'altra rete dedicata che utilizza il protocollo IP. Le conversazioni VoIP non devono necessariamente viaggiare su Internet, ma possono anche usare come mezzo trasmissivo una qualsiasi rete privata basata sul protocollo IP, per esempio una LAN all'interno di un edificio o di un gruppo di edifici.
Sono esempi di utilizzo di VoIP: la telefonia VoIP per il personale, l'installazione di software VoIP sui PC dei dipendenti (in sostituzione della tradizionale comunicazione telefonica), il servizio clienti interattivo tramite VoIP.

Web Conferencing

Si intende un sistema di videoconferenza veicolato su rete Internet tramite software installato sul terminale dei partecipanti ovvero tramite un'applicazione *web*. Rispetto alla videoconferenza, il *web conferencing* offre funzioni aggiuntive caratteristiche, come ad esempio la possibilità di gestire: presentazioni di *slides*, proiezioni di video, votazioni (anche anonime) tra i partecipanti, *web tours*, ecc. La presenza di questa tecnologia va segnalata solo quando prevista come strumento organizzativo.

Applicazioni in logica Service Oriented (SOA)

Le tecnologie *Service Oriented* enfatizzano l'esposizione di specifiche funzionalità tramite interfacce standardizzate, così da consentire l'utilizzo delle singole applicazioni come *componenti* dei processi interni o di *business* e soddisfare le richieste degli utenti in modo integrato e trasparente. Ad esempio, è un'applicazione *service oriented* un portale *home banking* collegato a un servizio di "acquisizione clienti" e/o a un servizio di "acquisizione ordini", a prescindere dalle modalità di realizzazione (linguaggi, *vendor*, standard, ecc.).

Green IT

Termine che identifica l'utilizzo di criteri ambientali per la valutazione e la selezione di apparecchiature e di servizi IT; i criteri ambientali prendono in esame l'impatto delle apparecchiature e dei servizi IT sull'ambiente durante tutto il loro ciclo di vita, includendo tra i parametri valutativi anche il consumo energetico diretto e indiretto (energia primaria e necessità di condizionamento) e la riciclabilità dei componenti. Esempi di Green IT sono l'investimento in *hardware energy-efficient* o la virtualizzazione di *server* o *storage*.

1.1 bis – Per chi ha risposto "1" o "2" ai punti 1, 3, 4 della domanda 1.1, specificare gli ambiti applicativi interessati.

Questa domanda è rivolta a chi ha indicato l'utilizzo di tecnologie *Contactless*, Applicazioni *Mobile* e Applicazioni *Web 2.0* rispondendo "1" o "2" alla domanda 1.1.
Se si valorizza con "1" o "2" la voce "Altro, specificare", occorre indicare nell'apposito spazio l'applicazione realizzata.
Vanno riempite tutte le caselle.

1.2 – Qual è l'andamento previsto nell'impiego delle seguenti tecnologie nei servizi bancari, per il prossimo biennio (2012-2013)?

A prescindere dai costi sostenuti o già previsti, si chiede di indicare il *trend* di utilizzo stimato delle tecnologie elencate.
Nel caso in cui una tecnologia non venga utilizzata, né se ne preveda l'uso, indicare "4".
Vanno riempite tutte le caselle.

1.3 – Per chi ha risposto "1" o "2" ai rispettivi punti della domanda 1.1, indicare se per l'utilizzo di quelle tecnologie si ritiene necessario disporre prevalentemente di specifiche competenze professionali e con quali modalità.

Con riferimento alle tecnologie citate, indicare le esigenze in termini di competenze professionali per il loro utilizzo.

1.4 – Facendo riferimento ai canali di contatto con la clientela (diversi dallo sportello) indicare quali delle tecnologie elencate vengono attualmente utilizzate e con quali modalità vengono realizzate applicazioni/interventi.

La domanda è indirizzata solamente a chi ha segnalato l'effettivo utilizzo della tecnologia (cioè coloro che hanno risposto "1" alla corrispondente riga della domanda 1.1).
Vanno riempite tutte le caselle.

1.5 – Indicare, per tipologia di servizio bancario e per ciascun canale di contatto messo a disposizione della clientela, il trend di utilizzo previsto nel breve periodo (12 mesi).

L'obiettivo della matrice è rilevare quali servizi vengono offerti su quali canali e il trend di utilizzo per ciascuno di essi.
Vanno riempite tutte le caselle.

1.6 – Quali delle seguenti funzioni sono rese disponibili alla clientela attraverso specifiche applicazioni Internet o su piattaforma Mobile?

La domanda fa esclusivamente riferimento alle funzioni offerte sui canali *Internet* e *Mobile*. Per applicazione su piattaforma *Mobile*, s'intende una serie di funzioni espressamente disegnate per essere utilizzate tramite telefono cellulare o computer palmare (non ci si riferisce qui al fatto che si possa accedere tramite cellulare alle analoghe funzioni messe a disposizione sul *web*).

Quando, nello sviluppo o nella progettazione di una funzione su piattaforma *Mobile*, si è anche previsto il riconoscimento della casa produttrice e/o del modello del dispositivo, ottimizzando così l'interfaccia e la comunicazione a seconda dei casi, si utilizzerà per la risposta la colonna *Navigazione ottimizzata.*
Vanno riempite tutte le caselle.

1.7 – Nello sviluppare applicazioni per offrire servizi su Internet o piattaforma Mobile all'utenza esterna, indicare quali criteri di accessibilità si applicano.

Lo domanda è volta a conoscere l'attenzione dedicata ai criteri di accessibilità, nello sviluppo di applicazioni *web*.
La Legge n.4 del 9 gennaio 2004 definisce:

> ***accessibilità:*** la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari;
> ***tecnologie assistive:*** gli strumenti e le soluzioni tecniche, hardware e software, che permettono alla persona disabile, superando o riducendo le condizioni di svantaggio, di accedere alle informazioni e ai servizi erogati dai sistemi informatici.

Per eventuali approfondimenti, si rimanda ai *"Criteri e metodi per la verifica tecnica e requisiti tecnici di accessibilità per i contenuti e i servizi forniti per mezzo di applicazioni basate su tecnologie Web",* allegato A del DM 8 luglio 2005 - versione 26-4-2010.
Vanno riempite tutte le caselle.

1.8 – Sono state attuate o sono in programma iniziative per:

La domanda approfondisce il settore del *Social networking* con l'obiettivo di raccogliere dati sull'utilizzo attuale e nel medio termine della tecnologia, per fini organizzativi e/o di *business*. Non vanno qui segnalate le iniziative che si limitano alla semplice definizione di una utenza o di una pagina su *social network* esterni.
Vanno riempite tutte le caselle.

2. Le misure di sicurezza

Obiettivi conoscitivi:

√ rilevare l'utilizzo di standard riconosciuti e di *best practices* in materia di sicurezza informatica;

√ rilevare le modalità e i livelli di autenticazione per gli accessi *on-line*;

√ individuare le principali modalità usate per raccogliere informazioni sulla vulnerabilità dei sistemi;

√ rilevare l'esistenza di una classificazione sistematica dei dati aziendali di alto livello;

√ rilevare le iniziative verso l'utenza, i processi organizzativi e i presidi tecnici predisposti allo scopo di mitigare i rischi informatici.

2.1 – Sono stati adottati standard riconosciuti (ovvero sono in corso iniziative per la loro adozione) o si fa riferimento a best practices *per la gestione della sicurezza informatica?*

Indicare anche eventuali altri standard adottati non compresi nell'elenco, indicandoli alla voce "Altro, specificare".
Vanno riempite tutte le caselle.

2.2 – Oltre a produttori di antivirus e/o di firewall, da quali fonti vengono assunte informazioni rispetto ad attacchi, virus e malfunzionamenti dei sistemi e del software?

Indicare anche eventuali altre fonti non comprese nell'elenco, indicandole alla voce "Altro, specificare".
Vanno riempite tutte le caselle.

2.3 – Oltre che per gli adempimenti rivenienti dalla normativa sulla privacy, è stato adottato un sistema di classificazione delle informazioni aziendali?

Specificare il valore appropriato nella casella.

2.4 – Classificare, per ordine crescente di spesa, da "1" a "6", i seguenti scenari di rischio, sulla base degli investimenti sostenuti o previsti in budget.

Ordinare per valore crescente di spesa (attribuendo il valore "1" allo scenario con la spesa minore e "6" a quello con la spesa maggiore) gli scenari di rischio proposti.
Vanno riempite tutte le caselle.

2.5 – Quali modalità e livelli di autenticazione vengono adoperati e in quali tipologie di conto?

Per *autenticazione statica* s'intende l'utilizzo di una credenziale che non cambia tra utilizzi successivi, tipicamente una *password*. L'autenticazione viene definita *statica*, perché la *password* è modificata in genere solo in caso di scadenza o dimenticanza.
Per *autenticazione dinamica* s'intende invece un qualsiasi sistema di autenticazione che preveda la modifica della credenziale a ogni accesso.
Indicare eventuali altre modalità di autenticazione non comprese nell'elenco alla voce "Altro, specificare".
Vanno riempite tutte le caselle.

2.6 – Nel caso sia stato adottato il doppio fattore di autenticazione, quali tecnologie vengono utilizzate a supporto?

Indicare le tecnologie di autenticazione utilizzate a supporto del doppio fattore di autenticazione. L'elenco proposto dal questionario è quello elaborato dal Consorzio Patti Chiari in collaborazione con ABI Lab in occasione della definizione dell'*Impegno per la Qualità* per garantire un sempre più elevato livello di protezione del servizio di *home banking*.

TOKEN

OTP via hardware connesso: prevede che, al momento dell'accesso, il *token* in possesso dell'utente (tipicamente un dispositivo USB) venga connesso al PC per la generazione di una password utilizzabile una sola volta (One Time Password - OTP);

OTP via hardware disconnesso: la generazione della password avviene sul *token*, indipendentemente dalla sua connessione ad altri dispositivi;

Certificato digitale su Token: si tratta di un documento elettronico che attesta, per mezzo di una firma digitale, l'associazione tra una chiave pubblica e l'identità del soggetto (una persona, una società, un computer) che la rivendica come propria.

MOBILE

OTP su SIM: OTP associata a una specifica SIM e generata tramite apposita applicazione presente sul cellulare del cliente;

OTP via SMS: la OTP è generata remotamente e inviata al cliente tramite SMS;

OTP via numero verde: numero verde dinamico comunicato al cliente al momento dell'accesso;

Certificato digitale su SIM: analogo a quello su *Token* descritto sopra, ma memorizzato nella SIM;

Firma digitale su SIM: in questo caso viene utilizzato il certificato di firma delle disposizioni di *home banking* fornito tramite cellulare e associato alla SIM del cliente;

Mobile strong authentication: l'autenticazione delle credenziali è realizzata attraverso procedure basate sull'utilizzo del cellulare del cliente.

BIOMETRIA

Supporto hardware: richiesto per particolari caratteristiche biometriche, dove la rilevazione non è effettuabile tramite dispositivi di largo consumo (es. verifica della firma come velocità, pressione e angolo della penna);

Supporto software: richiesto per le caratteristiche biometriche rilevabili tramite dispositivi di largo consumo quali *webcam* e microfoni.

CARTE

Tessera a combinazione: è una carta a combinazione in cui sono riportati schemi numerici attraverso i quali vengono identificate le credenziali di accesso all'*home banking*;

Software su smart card: la *smart card* produce una password valida per l'identificazione;

Certificato digitale su smart card: analogo a quello su *Token* descritto sopra, ma memorizzato nella *smart card*;

OTP su smart card: OTP generata tramite apposita logica implementata/programmata nella *smart card*;

OTP via lettore EMV: è la password OTP generata da apposito lettore di carte con tecnologia EMV;

Token card: si tratta di carte con display per la generazione di OTP.

SISTEMI SOFTWARE

OTP generata da software: OTP generata tramite apposita logica programmata da un applicativo sviluppato per questo scopo;

Firma digitale: in questo caso viene utilizzata una firma elettronica qualificata, basata sull'utilizzo della tecnologia di autenticazione a chiavi asimmetriche;

Certificato digitale: analogo a quello su *Token* descritto sopra, ma memorizzato nel PC utilizzato per l'accesso;

Software adattativi di profilazione utenti: applicativi software in grado di identificare un utente in base all'utilizzo che fa delle risorse (es. navigazione di pagine web, numero di tentativi di accesso con password diverse, modifica dei dati personali di un account, ecc.);

Altri sistemi software evoluti: si tratta di altre tipologie di software installato sul PC del cliente che costituiscono un fattore supplementare senza il quale non si è abilitati ad accedere al servizio di *home banking* (ad esempio, l'identificazione del DNA dell'hardware del cliente, tipicamente il MAC address della scheda di rete).

Vanno riempite tutte le caselle.

2.7 – In caso di adozione di un secondo canale, per quali funzioni è stato previsto?

Per *secondo canale* va inteso un ulteriore canale di comunicazione, diverso da quello su cui si svolge la transazione, sul quale vengono fatti viaggiare dati che l'utente dovrà confermare di aver ricevuto.
Vanno riempite tutte le caselle.

2.8 – Quali iniziative di carattere organizzativo vengono adottate per mitigare i rischi di frode interna/esterna?

La domanda ha l'obiettivo di identificare quali iniziative di carattere organizzativo o tecnico-organizzativo sono adottate per mitigare fenomeni di frode.
Vanno riempite tutte le caselle.

2.9 – Quali iniziative verso l'utenza sono state adottate, o si ha intenzione di adottare, per mitigare i rischi di frode nell'offerta di servizi telematici?

Vanno riempite tutte le caselle.

Fine del documento