CIPA | Convenzione Interbancaria per l'Automazione

ABI Associazione Bancaria Italiana

Rilevazione sull'IT nel settore bancario italiano

Profili tecnologici e di sicurezza

Cyber security nel settore bancario: rischi e nuove minacce

Questionario

2025

Sommario

Premessa

La “Rilevazione sull’IT nel settore bancario italiano”, curata annualmente da CIPA e ABI, ha l’obiettivo di fornire una visione d’insieme dell’utilizzo dell’Information and Communication Technology nelle banche, analizzandone i diversi aspetti organizzativi, economici, tecnologici e di sicurezza.

La Rilevazione si articola in due distinte indagini: la prima è dedicata all’esame dei profili economici e organizzativi dell’IT; la seconda, a cui si riferisce il presente questionario, è riservata ai profili tecnologici e di sicurezza ed è centrata di volta in volta su uno specifico argomento.

L’indagine, dedicata in questa edizione al tema **“Cyber security nel settore bancario: rischi e nuove minacce”**, approfondisce gli aspetti strategici, organizzativi e tecnologici connessi alla sicurezza informatica. In particolare, vengono esaminati i principali processi di sicurezza, le strategie adottate, le strutture organizzative e le tecnologie impiegate dalle banche italiane per fronteggiare i rischi cyber, in un contesto di minacce in continua evoluzione. L’indagine esplora inoltre l’adozione di strumenti innovativi quali l’intelligenza artificiale, la crittografia post-quantistica e l’utilizzo degli EUDI Wallet in tale ambito.

I risultati delle analisi sono illustrati in un rapporto pubblicato sul sito internet della CIPA (www.cipa.it).

Le informazioni, attuali e storiche, fornite da banche e gruppi su base volontaria, sono raccolte e utilizzate dalla Segreteria Tecnica della CIPA esclusivamente a fini statistici per attività di analisi e studio ai sensi dell'Art. 1 della Convenzione Interbancaria per l'Automazione e sono diffuse all'esterno soltanto in forma aggregata o anonima. Il trattamento dei dati si svolge, senza intervento di terze parti, con modalità atte a garantirne la sicurezza e la riservatezza.

Glossario

Asset

Qualsiasi bene che abbia valore per l'organizzazione e che richieda protezione. Include sistemi/piattaforme hardware e software, infrastrutture di rete, personale, sedi e struttura organizzativa.

Attestato elettronico di attributi (EAA - Electronic Attestation of Attributes)

Un attestato rilasciato in forma elettronica che consente l'autenticazione di attributi (cfr. *infra*) e che, ai sensi del regolamento eIDAS (cfr. *infra*), viene rilasciato da un prestatore di servizi fiduciari qualificato o da un organismo del settore pubblico responsabile di una fonte autentica (cfr. *infra*) o da un organismo del settore pubblico designato da uno Stato UE per rilasciare tali attestati per conto di organismi del settore pubblico responsabili di fonti autentiche. Esempi di attestazioni elettroniche di attributi potrebbero essere: il numero della patente di guida, titolarità dell'IBAN di un c/c, indicazione di persona politicamente esposta, titolo di studio.

Attori della minaccia

Individui, gruppi, organizzazioni o governi che conducono o hanno l'intenzione di condurre attacchi informatici a danno di sistemi, risorse, dati o infrastrutture, per finalità economiche, politiche, ideologiche o strategiche.

Attributo

Pezzo di informazione che caratterizza un individuo o un'entità: caratteristiche, qualità, diritti o autorizzazioni di una persona fisica o giuridica o di un oggetto ai sensi del Regolamento eIDAS (cfr. *infra*).

Attività di Awareness di sicurezza

Attività di sensibilizzazione del personale interno e gli altri portatori di interesse sui principali rischi alla sicurezza informatica e sulle condotte virtuose per prevenirli o mitigarli.

Blue team

Team di sicurezza informatica interno all'organizzazione, che ha il compito di proteggerla dagli attacchi informatici, inclusi quelli simulati nell'ambito delle attività di Red Teaming (cfr. *infra*).

Crittografia post quantistica

Crittografia progettata per resistere ad attacchi di computer quantistici su larga scala.

CERT/CSIRT

Computer Emergency Response Team/ Computer Security Incident Response Team: team di esperti che studia e monitora i profili evolutivi della minaccia cyber e offre servizi per la sicurezza reattiva, preventiva e proattiva.

Cyber resilience

Capacità di un'organizzazione di continuare a svolgere i propri compiti anticipando e adattandosi alle minacce cyber e ad altri cambiamenti rilevanti nell'ambiente, e di resistere, contenere e riprendersi rapidamente dagli incidenti informatici.

Cyber Threat Intelligence (CTI)

Processo di raccolta, aggregazione, trasformazione, analisi, interpretazione, arricchimento e condivisione di informazioni relative alle minacce informatiche (cfr. *infra*), finalizzato a fornire il contesto necessario a supporto delle decisioni operative, tattiche e strategiche.

Crypto agility

Capacità di reagire velocemente alle minacce crittografiche, sostituendo, rapidamente e in modo controllato, gli algoritmi crittografici diventati vulnerabili.

Digital forensics

Processo di identificazione, acquisizione, conservazione, analisi e presentazione delle informazioni digitali aventi valore probatorio, nel rispetto dei principi di integrità, autenticità, ripetibilità e tracciabilità.

eIDAS

Regolamento UE/2014/910 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e sue modificazioni e integrazioni.

EUDI Wallet

Portafoglio dell'identità digitale europea e relativo quadro normativo ai sensi del Regolamento eIDAS (cfr. *infra*).

Fonte autentica

Archivio o sistema, tenuto sotto la responsabilità di un organismo del settore pubblico o del settore privato che contiene e fornisce gli attributi (cfr. *infra*) e che è considerato una fonte primaria di tali informazioni o la cui autenticità è riconosciuta conformemente al diritto dell'Unione o nazionale, inclusa la prassi amministrativa.

Identità digitale eIDAS

Regime di identificazione elettronica ai sensi del Regolamento eIDAS (cfr. *infra*). L'Italia ha notificato alla Commissione europea due schemi di identificazione elettronica: CIE ("CieID") e SPID. (cfr. anche "Livelli di garanzia delle identità digitali eIDAS").

Incident response

Processo di rilevazione, analisi e gestione degli incidenti di sicurezza informatica, con l'obiettivo di limitare i danni, ridurre i tempi e i costi di recupero e prevenire il ripetersi di eventi simili.

Indicatori di compromissione (IOC)

Artefatti o pattern specifici osservabili che caratterizzano una minaccia e il cui rilevamento all'interno del perimetro dell'organizzazione è indice di una possibile violazione, passata o in corso, della riservatezza, integrità o disponibilità delle informazioni.

Information sharing

Processo che definisce le modalità per lo scambio volontario di dati, informazioni e intelligence relativi a eventi o incidenti cyber tra differenti organizzazioni nell'ambito di un rapporto di fiducia.

Livello della minaccia cyber (CTL)

Scala di valori utile a qualificare lo stato corrente della minaccia cyber orientata contro l'organizzazione in funzione del quale l'organizzazione stessa potrà valutare il livello di "prontezza difensiva" più idoneo da adottare in termini di attivazione dei presidi di difesa, tecnici e organizzativi. Concorrono alla determinazione del livello della minaccia cyber fattori come: le informazioni sullo scenario della minaccia cyber relativo al settore finanziario desunte da autorità e organismi di settore, l'incremento delle capacità tecniche e finanziarie degli attori della minaccia (cfr. *infra*), eventi che potrebbero rappresentare una minaccia per l'organizzazione (es. diffusione nel deep/dark web di dati riconducibili all'organizzazione, registrazione di domini di phishing, presenza di vulnerabilità non sanate su asset esposti).

Livello di garanzia delle identità digitali eIDAS

Tre livelli di garanzia definiti negli atti di esecuzione previsti dal Regolamento eIDAS (cfr. *infra*) e denominati, per gli schemi di identificazione elettronica nazionali, "Livello 1", "Livello 2" e "Livello 3".

Malware

Software progettato con intenti malevoli che contiene funzionalità o capacità che possono potenzialmente causare danni, direttamente o indirettamente, a soggetti o ai loro sistemi informativi.

Minaccia informatica

Qualsiasi circostanza, evento o azione potenziale che possa danneggiare, perturbare o avere un impatto negativo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi o su altri portatori di interesse.

Network Operation Center (NOC)

Funzione o servizio formalmente riconosciuto che si occupa di monitorare lo stato di operatività delle componenti di rete, garantendo i livelli di servizio concordati e gestendo eventi e incidenti con procedure definite per gli interventi, l'escalation, la risoluzione, il feedback e il miglioramento continuo della qualità dei servizi offerti.

Penetration Test (PT)

Una metodologia di test in cui i valutatori, utilizzando tutta la documentazione disponibile (ad esempio, progetto di sistema, codice sorgente, manuali) e lavorando sotto vincoli specifici, tentano di aggirare i presidi di sicurezza di un sistema informativo.

Red Teaming

Attività di verifiche di sicurezza in cui operatori umani tentano di raggiungere obiettivi prefissati agendo come un attore della minaccia, senza, o con limitati, vincoli e senza alcuna notifica o avviso preventivo ai team di difesa, o blue team (cfr. *infra*) dell'organizzazione sottoposta al test.

Risk Assessment IT

Processo di identificazione, analisi e valutazione dei rischi legati a sistemi informatici, reti, applicazioni e dati.

Security Assessment e Testing

Processo strutturato di test che rivela se un sistema presenta punti deboli che possono essere sfruttati per causare effetti indesiderati (es. manipolazione di dati, denial of service).

Security Operation Center (SOC)

Funzione o servizio formalmente riconosciuto responsabile della protezione dei sistemi informatici. Include il monitoraggio, il rilevamento, la valutazione e la correzione di minacce e incidenti informatici.

Strategia di sicurezza informatica

Approccio sistemico alla gestione del rischio informatico, finalizzato a definire gli obiettivi di sicurezza in coerenza con il profilo di rischio dell'organizzazione.

Terze parti

Entità esterne all'organizzazione che forniscono ad essa beni e/o servizi IT, direttamente o per il tramite di subfornitori.

Third-Party Risk Management (TPRM)

Insieme di processi, politiche e controlli che un'organizzazione adotta per identificare, monitorare e mitigare i rischi indotti da terze parti (cfr. *infra*) in relazione agli asset, alle persone e ai processi dell'organizzazione con cui entrano in contatto.

Threat-Led Penetration Test (TLPT)

Tipologia di test Red teaming (cfr. *infra*) che consiste in un tentativo controllato di compromettere la cyber resilience (cfr. *infra*) di un'organizzazione emulando le tattiche, le tecniche e le procedure d'attacco avanzate adottate da reali attori della minaccia nei confronti di persone, processi e tecnologie. I TLPT sono inoltre: condotti sulla base di analisi CTI (cfr. *infra*); riducendo al minimo il numero di persone a conoscenza del test; pianificati e condotti con un approccio risk-based allo scopo di minimizzarne gli impatti sull'operatività dell'organizzazione sotto test.

TTP

Tattiche, tecniche e procedure utilizzate dall'attaccante e che ne caratterizzano il *modus operandi.*

Vulnerabilità

Debolezza, suscettibilità o falla in un asset (cfr. *infra*) o nei relativi controlli di sicurezza che può essere sfruttata da una o più minacce per compromettere la riservatezza, l'integrità o la disponibilità delle informazioni.

Vulnerability and Patch Management (VPM)

Processo continuo volto all'identificazione, valutazione, prioritizzazione e successiva risoluzione o mitigazione delle vulnerabilità presenti in sistemi, reti, applicazioni e dispositivi IT, attraverso interventi correttivi tempestivi, inclusi l'applicazione di patch di sicurezza, aggiornamenti software e adozione di altre contromisure tecniche o organizzative proporzionate al livello di rischio.

Vulnerability Assessment (VA)

Valutazione sistematica di un sistema informativo, dei suoi controlli e dei suoi processi, per determinare l'adeguatezza delle misure di sicurezza, identificare le carenze, fornire dati per prevedere l'efficacia delle misure di sicurezza proposte e confermare l'adeguatezza di tali misure dopo l'implementazione.

Fonti:

Le definizioni sono state adattate ai fini del seguente questionario a partire da quelle proposte da organismi di standardizzazione internazionali e fonti normative tra cui FSB Cyber Lexicon, ISACA Cybersecurity Fundamentals Glossary, CPMI-IOSCO, ISO/IEC 27000, ISO/IEC 27005, NIST Glossary, Regolamento (UE)2014/910, Regolamento (UE) 2019/881, Regolamento (UE) 2022/2554.

Dati del compilatore e della struttura

Dati identificativi della Banca

Codice ABI	☐☐☐☐☐
Ragione sociale	

Struttura organizzativa che cura la compilazione del questionario

Denominazione[1]			
Indirizzo[2]			
Città		CAP	☐☐☐☐☐
Provincia			
E-mail[3]			

Dati del compilatore[4] del questionario

Cognome	
Nome	
Telefono	
E-mail	

[1] Denominazione aziendale della struttura.
[2] Inserire il recapito aziendale con tutti i dati richiesti, al fine di poter recapitare lettere o plichi.
[3] Casella email funzionale (cioè non legata a una persona fisica) della struttura o, in sua mancanza, indirizzo email di un referente della struttura.
[4] Recapiti aziendali del compilatore, compreso l'indirizzo email, per la richiesta di eventuali informazioni e chiarimenti o per la segnalazione di anomalie nella compilazione.

1 Aspetti strategici

1.1 **Indicare se è stata definita e approvata una strategia aziendale per la sicurezza informatica e se viene aggiornata periodicamente.**

	Risposta
1=Sì, esiste e l'aggiornamento è previsto almeno ogni cinque anni	
2=Sì, esiste e l'aggiornamento è previsto almeno ogni tre anni	
3=Sì, esiste e l'aggiornamento avviene principalmente in seguito a incidenti gravi e/o nuove minacce rilevanti	
4=Sì, esiste ma non è previsto il suo aggiornamento	☐
5=No, non esiste una strategia ma sono trattati specifici aspetti della sicurezza informatica	
6=No	
7=Altro, specificare:	

1.2 **Indicare quali delle seguenti tematiche sono attualmente indirizzate all'interno della strategia per la sicurezza informatica della banca/gruppo bancario. (Risposta multipla)**

Indirizzi	Risposta
Cyber security (contrasto di attori della minaccia esterni ed eventi malevoli)	☐
Cyber resilience	☐
Identità digitale	☐
Sicurezza fisica e ambientale	☐
Formazione e awareness	☐
Collaborazioni con altre organizzazioni e attività di infosharing	☐
Gestione dei rischi legati alle terze parti	☐
Transizione alla crittografia post-quantistica	☐
Intelligenza Artificiale (IA)	☐
Distributed Ledger Technology (DLT)	☐
Altro, specificare:	☐

1.3 **Specificare per <u>tutte</u> le figure di seguito elencate il coinvolgimento nella definizione della strategia della sicurezza informatica della banca/gruppo.**

<u>Risposta</u>**:**
1=Figura non presente nella banca/gruppo
2=Sì, è coinvolta
3=No, è presente ma non coinvolta

Ambito	Risposta
CEO - Chief Executive Officer	☐
CSO - Chief Security Officer	☐
Capo funzione Organizzazione	☐
Capi unità di business	☐
Capo del CERT/CSIRT	☐
Figura CISO formalizzata	☐
Unità specialistiche (es. SOC, NOC, Red Team)	☐
CIO - Chief Information Officer	☐
Organo appositamente costituito (es. Comitato sicurezza e/o Comitato dei rischi)	☐
Altro, specificare:	☐

1.4 **In considerazione dei principali processi di sicurezza elencati, specificare il relativo livello di maturità e indicare se la banca/gruppo ha avviato iniziative di tipo progettuale.**

Livello di maturità:
0=Non presente
1=Presente ma non definito e formalizzato
2=Definito ma non formalizzato
3=Formalizzato ma non aggiornato sistematicamente
4=Formalizzato e aggiornato sistematicamente

Iniziative:
1=Sì, sono rilevanti
2=Sì ma non sono rilevanti
3=No

Processi di sicurezza	Livello di maturità	Iniziative
1.GOVERNO DELLA SICUREZZA IT (definizione di ruoli/responsabilità, strategia e piano attuativo)	☐	☐
2.DEFINIZIONE DELLA NORMATIVA DI SICUREZZA INTERNA (es. policy, manuali, prassi operative)	☐	☐
3.CYBER THREAT INTELLIGENCE (CTI)	☐	☐
4.RISK ASSESSMENT IT	☐	☐
5.PROGETTAZIONE E IMPLEMENTAZIONE MISURE DI SICUREZZA (progetti, infrastrutture, dati)	☐	☐
6.SECURITY ASSESSMENT e TESTING [5]	☐	☐
7.VULNERABILITY AND PATCH MANAGEMENT	☐	☐

[5] Vulnerability Assessment/Penetration Testing, Pre Production Security Assessment/Production Security Assessment e TLPT e/o Red Teaming.

8.GESTIONE IDENTITA' E CONTROLLO DEGLI ACCESSI	☐	☐
9.FORMAZIONE E AWARENESS DI SICUREZZA	☐	☐
10.INFORMATION SHARING	☐	☐
11.MONITORAGGIO E ALERTING	☐	☐
12.GESTIONE DEGLI INCIDENTI DI SICUREZZA	☐	☐
13.DIGITAL FORENSICS	☐	☐
14.GESTIONE DEL RISCHIO DELLE TERZE PARTI	☐	☐
15.SICUREZZA FISICA E AMBIENTALE	☐	☐
16.BUSINESS CONTINUITY e DISASTER RECOVERY	☐	☐
17.AUDIT	☐	☐

1.5 **Indicare se negli ambiti elencati la banca/gruppo ha avviato iniziative di miglioramento della sicurezza informatica o intende avviarle nel biennio 2026-2027, specificandone in prevalenza lo stato.**

Stato:
1=Prototipi/Sperimentazioni
2=Iniziative in corso
3=Iniziative implementate
4=Nessuna iniziativa

Ambiti	**2025**	**2026-2027**
Introduzione di nuovi servizi/infrastrutture di sicurezza	☐	☐
Acquisizione di tool e strumenti	☐	☐
Revisione di metodologie	☐	☐
Revisione e rafforzamento della sicurezza per sistemi/infrastrutture	☐	☐
Revisione della mappa dei rischi e dei controlli	☐	☐
Revisione dei processi di sicurezza	☐	☐
Revisione dell'architettura di sicurezza	☐	☐

1.6 **Con riferimento al processo "4.Risk Assessment IT" della domanda 1.4, indicare quali delle seguenti minacce - che caratterizzano anche il rischio cyber in chiave geopolitica - sono esplicitamente considerate. (Risposta multipla)**

Minacce	**Risposta**
Attacchi da attori statuali o sponsorizzati da Stati	☐
Aumento delle campagne di disinformazione digitale	☐
Uso di malware avanzati e ransomware anche in chiave geopolitica	☐
Attacchi finalizzati all'interruzione dei servizi bancari e compromissione delle infrastrutture critiche	☐

Furto di dati sensibili e informazioni finanziarie	☐
Problematiche nella catena di fornitura software	☐
Problematiche nella catena di fornitura tecnologica (escluso il software)	☐
Impatti legati a nuove tecnologie (es. IA, tecnologie quantistiche)	☐
Nessuna delle precedenti	☐
Altro, specificare:	☐

1.7 **Più in generale, indicare se i processi di sicurezza elencati nella domanda 1.4 tengono esplicitamente conto dei rischi connessi all'attuale contesto geopolitico[6].**

	Risposta
1=Sì, tutti i processi	
2=Sì, la maggior parte dei processi	
3=Sì, solo alcuni processi	☐
4=No, ma è in previsione	

1.8 **Con riferimento al processo "3.Cyber Threat Intelligence" della domanda 1.4, indicare se viene valutato, e con quale modalità, il livello della minaccia cyber[7]. (Risposta multipla)**

	Risposta
No, non viene valutato	☐
Sì, viene valutato solo nella produzione di report strategici periodici	☐
Sì, viene valutato, qualificato e considerato nell'analisi dei rischi	☐
Sì, viene valutato e quantificato tramite indicatori di rischio e il suo valore viene considerato nei piani di continuità operativa e di gestione della crisi	☐
Altro, specificare:	☐

1.9 **Con riferimento al processo di "10.Information Sharing" della domanda 1.4, indicare se la banca/gruppo bancario partecipa a una 'trusted community' per lo scambio di informazioni su minacce informatiche specificando la tipologia di iniziativa.**

Tipologia di iniziativa	**Risposta**
1=Sì, nazionale (es. CERT-Fin, ABI Lab, iniziative promosse da autorità o associazioni italiane)	
2=Sì, internazionale (es. FS-ISAC, reti europee o globali)	
3=Sì, nazionale e internazionale	☐
4=No	

[6] cfr. minacce di cui alla domanda precedente.
[7] cfr. Glossario.

2 Aspetti economici e organizzativi

2.1 **Indicare se la banca/gruppo si avvale di una metodologia per la rilevazione dei costi legati alla sicurezza informatica.**

	Risposta
1=Sì, a livello IT	
2=Sì, a livello aziendale	
3=Sì, sia a livello IT sia a livello aziendale	
4=No, ma è prevista nel biennio 2026-2027	☐
5=No	
6=Altro, specificare:	

2.2 **Con riferimento al Budget IT 2026, specificare se per la sicurezza informatica[8] è previsto uno stanziamento dedicato e indicare il trend rispetto all'anno precedente, distinguendo tra investimenti e spesa corrente.**

Stanziamento dedicato:
1=Sì
2=No

Trend 2026 rispetto al 2025:
1=In aumento
2=Stabile
3=In diminuzione

Budget IT Sicurezza Informatica	Stanziamento dedicato	Trend 2026
Investimenti	☐	☐
Spesa corrente	☐	☐

2.3 **Con riferimento alle attività elencate nel seguito, indicare il livello di copertura delle competenze presenti nella banca/gruppo (AS IS), quello da raggiungere nel biennio 2026-2027 (TO BE) e la modalità prevalente di reperimento delle competenze IT.**

Livello di copertura AS IS e TO BE: punteggio da 0 (nullo) a 5 (max)

Modalità prevalente di reperimento competenze IT:
1=Assunzione di personale IT all'interno della banca/gruppo
2=Formazione del personale IT all'interno della banca/gruppo
3=Ricorso a risorse esterne

Attività	AS IS	TO BE	Modalità
Funzioni di Risk assessment	☐	☐	☐
Funzioni di Cyber Threat Intelligence	☐	☐	☐
Attività di Security Awareness	☐	☐	☐

[8]Considerare la componente IT dei processi elencati nella domanda 1.4.

Funzioni di Security Operation Center	☐	☐	☐
Funzioni di Network Operation Center	☐	☐	☐
Funzioni di Vulnerability Assessment/Penetration Test	☐	☐	☐
Attività di Red Teaming	☐	☐	☐
Funzioni di Incident Response	☐	☐	☐
Funzioni di Digital forensics	☐	☐	☐
Analisi dei malware	☐	☐	☐

2.4 Indicare la collocazione organizzativa delle seguenti funzioni di sicurezza.

Collocazione:

1=Nel settore IT della banca/gruppo
2=Fuori dal settore IT della banca/gruppo
3=Distribuita in settori IT e non IT della banca/gruppo
4=Esternalizzata
5=Funzione non presente

Funzioni di sicurezza	Assetto
Governo della sicurezza	☐
Funzioni di Cyber Threat Intelligence	☐
Attività di Security Awareness verso i dipendenti	☐
Attività di Security Awareness verso la clientela	☐
Funzioni di Monitoraggio e alerting	☐
Funzioni di Vulnerability Assessment/Penetration Test	☐
Funzioni di valutazione della vulnerabilità	☐
Attività di testing di Red Teaming	☐
Funzioni di Incident Response	☐
Funzioni di Digital forensics	☐

2.5 Con riferimento all'assunzione di personale, indicare quali requisiti vengono considerati nella valutazione di un candidato esperto in sicurezza informatica. (Risposta multipla)

Requisiti	Risposta
Certificazioni possedute	☐
Esperienza pregressa in specifici ambiti di sicurezza	☐
Esperienza in ambito bancario	☐
Conoscenza di normative e standard	☐
Attività di vetting	☐
Altro, specificare:	☐

2.6 **Con riferimento alla formazione e all'assunzione del personale tecnico specializzato in sicurezza informatica, indicare, tra i seguenti istituti di formazione, quelli a cui la banca/gruppo ricorre prevalentemente. (Risposta multipla)**

Istituti di formazione	Risposta
SANS / GIAC	☐
ISC2	☐
ISACA	☐
EC Council	☐
Offensive Security	☐
Altro, specificare:	☐
Specificare le prime tre certificazioni di riferimento:	☐

2.7 **Con riferimento al processo "9.Formazione e Awareness di sicurezza" della domanda 1.4, indicare se la banca/gruppo svolge iniziative formative in tema di sicurezza informatica, per i destinatari di seguito elencati, e specificarne la periodicità. (Risposta multipla)**

Periodicità:
1=Sì, regolarmente,
2=Sì, occasionalmente,
3=No

Destinatari	Risposta
Personale tecnico specialistico nella sicurezza informatica	☐
Personale tecnico	☐
Personale amministrativo/business	☐
Alta dirigenza	☐
Clientela	☐
Fornitori	☐
Altro, specificare:	☐

2.8 **Con riferimento a standard, linee guida e framework in materia di sicurezza informatica, indicare quali organismi vengono maggiormente considerati dalla banca/gruppo. (Risposta multipla)**

Organismi	Risposta
ISO/IEC	☐
NIST	☐
ACN	☐
CPMI/IOSCO	☐
CINI	☐
Autorità di supervisione/vigilanza	☐
CERTFin	☐
Altro, specificare:	☐

3 Aspetti tecnologici ed evolutivi

3.1 Indicare quali tra i seguenti strumenti sono in uso nella banca/gruppo. (Risposta multipla)

Strumenti	Risposta
Catalogo degli assets (CMDB - Configuration Management Database)	☐
Catalogo dei dati e metadati; dizionario dei dati	☐
SIEM (Security Information and Event Management)	☐
TIP (Threat Intelligence Platform)	☐
VAP (Vulnerability Assessment Platform)	☐
SOAR (Security Orchestration, Automation and Response)	☐
Sistemi per la detection e response per eventi su sistemi e reti	☐
Nessuno dei precedenti	☐

3.2 Indicare la modalità di autenticazione adottata dalla banca/gruppo per l'accesso ai dispositivi aziendali (PC/PC portatili) connessi alla rete da parte dei dipendenti e delle terze parti (es. fornitori, consulenti, collaboratori esterni).

Modalità di autenticazione	Dipendenti	Terze parti
Password	☐	☐
Smart card con PIN	☐	☐
Password e smart card con PIN	☐	☐
Password e token fisico	☐	☐
Password e fattore biometrico	☐	☐
Fattore biometrico	☐	☐
Password e OTP via SMS/email/telefonata (*non offline*)	☐	☐
Password e OTP tramite app/authenticator non basato su SMS (*non offline*)	☐	☐
Altro (altra combinazione di password, fattore biometrico e token/smartcard/app/SMS/email/telefonata)	☐	☐

3.3 Indicare se la banca/gruppo bancario si è dotato di strumenti di monitoraggio automatizzati per valutare il rischio di terze parti (TPRM).

Tipologia di iniziativa	Risposta
1=Sì, sono applicati a tutti i fornitori	
2=Sì, sono applicati solo ai fornitori critici	
3=Sì, sono applicati alla maggior parte dei fornitori	☐

4=No, ma è in previsione
5=No

3.4 **Oltre ai test previsti dalla normativa DORA, indicare se sono state eseguiti e/o previsti esercizi di tipo Red Teaming (ad es. TLPT e test TIBER-EU/IT).**

	Risposta
1=Sì, sono stati già eseguiti ma non sono previsti in modo sistematico	
2=Sì, sono stati già eseguiti e sono regolarmente previsti almeno ogni tre anni	
3=Sì, sono stati già eseguiti e sono regolarmente previsti almeno ogni anno	
4=No, non sono stati ancora eseguiti ma sono regolarmente previsti almeno ogni tre anni	☐
5=No, non sono stati ancora eseguiti ma sono regolarmente previsti almeno ogni anno	
6=No, non sono stati né eseguiti e né sono previsti	
7=Altro, specificare:	

3.5 **Indicare l'assetto prevalente della banca/gruppo in relazione all'integrazione del monitoraggio della sicurezza logica (dispositivi ICT), dei dispositivi IOT e fisico-ambientale, anche in previsione nel biennio 2026-2027.**

Assetto	2025	2026-2027
1=Non viene effettuato un monitoraggio integrato dei dispositivi ICT, IOT e di sicurezza fisica e ambientale		
2=Un numero limitato di dispositivi ICT, IOT e di sicurezza fisica e ambientale sono integrati		
3=Un numero consistente di dispositivi ICT, IOT e di sicurezza fisica e ambientale sono integrati	☐	☐
4=La maggior parte dei dispositivi ICT, IOT e di sicurezza fisica e ambientale sono integrati		
5=Piena integrazione dei dispositivi ICT, IOT e di sicurezza fisica e ambientale		
6=Altro, specificare:		

3.6 **Con riferimento al processo "3.Cyber Threat Intelligence" della domanda 1.4, qualora presente, indicare quali dei seguenti sotto-processi viene messo in atto per rispondere a livello tattico-operativo alla minaccia cyber. (Risposta multipla)**

Sotto-processo	Risposta
Raccolta, analisi e condivisione di indicatori di compromissione (IOC)	☐
Aggiornamento automatico dei sistemi di sicurezza in base agli IOC	☐
Correlazione di tattiche, tecniche e procedure (TTP) con dati interni	☐
Ricerca proattiva di minacce all'interno del perimetro, a partire da IOC e TTP	☐

Adattamento dinamico dei presidi di difesa (es. prioritizzazione delle vulnerabilità, azioni di mitigazione)	☐
Altro, specificare:	☐

3.7 **Con riferimento alla Cybersecurity e al processo "7.Vulnerability e Patch Management" della domanda 1.4, indicare se le vulnerabilità di tipo infrastrutturale e/o applicativo prevedono la valutazione della prioritizzazione degli interventi.**

Sotto-processo	Risposta
1=No	
2=Sì, ma si tiene conto unicamente della criticità della vulnerabilità	
3=Sì, si tiene conto solo della criticità e della sfruttabilità della vulnerabilità	☐
4=Sì, si tiene conto della criticità, della sfruttabilità e dell'esposizione della vulnerabilità	
5=Altro, specificare:	

3.8 **Indicare per <u>tutti</u> gli strumenti o soluzioni tecniche adottati per la protezione, il monitoraggio e la gestione della sicurezza dei servizi ICT nel public cloud, di seguito elencati, l'assetto prevalente.**

<u>Assetto prevalente:</u>
1=Interno alla banca/gruppo
2=Presso il cloud provider
3=Strumento o soluzione non presente

Strumenti o soluzioni	Assetto prevalente
Gestione della postura di sicurezza (CSPM – Cloud Security Posture Management)	☐
Protezione dei workload (CWPP – Cloud Workload Protection Platform)	☐
Gestione delle identità e degli accessi (IAM/CIEM)	☐
Monitoraggio e rilevamento delle minacce (SIEM/SOAR)	☐
Gestione delle configurazioni e dell'infrastruttura (IaC Security)	☐
Crittografia e gestione delle chiavi (KMS, BYOK, HSM)	☐
Altro, specificare:	☐

3.9 **In relazione al processo "13.Digital forensics" della domanda 1.4, indicare se l'organizzazione ha definito una policy di 'forensic readiness', selezionando una delle opzioni elencate.**

	Risposta
1=No	
2=No, ma è in previsione	
3=Sì, le procedure sono state definite	☐

4=Sì, le procedure sono state definite ed è stato anche aggiornato il processo di gestione degli incidenti di sicurezza

5=Altro, specificare:

3.10 **Indicare quali delle seguenti iniziative in tema di post quantum cryptography sono state avviate, o si intende avviare nel biennio 2026-2027, per fronteggiare i rischi derivanti dall'uso di algoritmi crittografici (es. RSA, ECDSA) dichiarati vulnerabili ad attacchi condotti con sistemi dotati di capacità di computazione quantistica. (Risposta multipla)**

Iniziativa	2025	2026-2027
Analisi del proprio parco applicativo	☐	☐
Iniziative di crypto agility (es. disaccoppiamento tra applicazioni e algoritmi crittografici)	☐	☐
Adozione di algoritmi di crittografia quantum safe	☐	☐

3.11 **Con riferimento alla domanda precedente, in caso si siano intraprese iniziative di analisi del proprio parco applicativo, indicare se per tale attività ci si è dotati, o si intende farlo nel biennio 2026-2027, di uno o più dei seguenti strumenti. (Risposta multipla)**

Iniziativa	2025	2026-2027
Strumenti automatici (discovery and asset management tools)	☐	☐
Strumenti automatici integrati con i processi di continuous integration e di qualità del software	☐	☐
Standard per la descrizione degli asset crittografici (es. CBOM - Cryptographic Bill of Materials)	☐	☐

3.12 **Indicare in quali dei processi di sicurezza sono utilizzate tecnologie di Intelligenza Artificiale (IA) o ne è previsto l'utilizzo.**

Risposta:
1=Sì
2=È in previsione nel 2026-27
3=No

Processo	Risposta
1.GOVERNO DELLA SICUREZZA IT (definizione di ruoli/responsabilità, strategia e piano attuativo)	☐
2.DEFINIZIONE DELLA NORMATIVA DI SICUREZZA INTERNA (es. policy, manuali, prassi operative)	☐
3.CYBER THREAT INTELLIGENCE (CTI)	☐
4.RISK ASSESSMENT IT	☐
5.PROGETTAZIONE E IMPLEMENTAZIONE MISURE DI SICUREZZA (progetti, infrastrutture, dati)	☐
6.SECURITY ASSESSMENT e TESTING [5]	☐
7.VULNERABILITY AND PATCH MANAGEMENT	☐
8.GESTIONE IDENTITA' E CONTROLLO DEGLI ACCESSI	☐
9.FORMAZIONE E AWARENESS DI SICUREZZA	☐

10.INFORMATION SHARING	☐
11.MONITORAGGIO E ALERTING	☐
12.GESTIONE DEGLI INCIDENTI DI SICUREZZA	☐
13.DIGITAL FORENSICS	☐
14.GESTIONE DEL RISCHIO DELLE TERZE PARTI	☐
15.SICUREZZA FISICA E AMBIENTALE	☐
16.BUSINESS CONTINUITY e DISASTER RECOVERY	☐
17.AUDIT	☐

4 Identità digitale

4.1 **Indicare se è definita una roadmap nella banca/gruppo per l'utilizzo degli EUDI Wallet come regime di autenticazione nei seguenti casi. (Risposta multipla)**

	Risposta
Sì, per l'accesso dei dipendenti	☐
Sì, verso la clientela per l'autenticazione forte nelle transazioni	☐
Sì, verso la clientela per l'onboarding (all'atto della stipula del contratto)	☐
Sì, verso la clientela in altri ambiti	☐
Sì, nei confronti delle terze parti	☐
Sì, nel contesto B2B (c.d. organisational wallet)	☐
Altro, specificare:	☐

4.2 **Con riferimento alla mappa applicativa ABILab, indicare quali ambiti sono o saranno interessati dagli EUDI Wallet e, qualora si esercitasse anche il ruolo di fonte autentica, dall'emissione di "attestazioni elettroniche di attributi" (EAA) nei confronti di terzi[9].**

Ambito	EUDI Wallet	EAA
Conti correnti	☐	☐
SDD	☐	☐
Bonifici	☐	☐
Tesoreria Enti	☐	☐
Monetica	☐	☐
Assegni	☐	☐
Incasso tributi	☐	☐
Credito	☐	☐
Finanza	☐	☐
Estero (credito, finanza, pagamenti)	☐	☐
Prodotti assicurativi	☐	☐
Gestione carte	☐	☐
Altro, specificare:	☐	☐

[9] es. clientela privata, clientela business, fornitori di terze parti, altre entità finanziarie – quindi sia in contesti B2C che in contesti B2B.

4.3 **Nel caso in cui la banca/gruppo decidesse di accettare "attestazioni elettroniche di attributi" (EAA) da soggetti terzi, indicare quali settori di provenienza sarebbero interessati.**

Settori	Risposta
Anagrafe	☐
Istruzione	☐
Fisco/Tributi	☐
Altre autorità di settore (es. Anticorruzione)	☐
Giustizia	☐
Motorizzazione (e trasporti in generale)	☐
Energia	☐
Entità finanziarie	☐
Altro, specificare:	☐

4.4 **Indicare le modalità di sviluppo a cui la banca/gruppo ricorre nel caso di soluzioni legate all'uso di EUDI Wallet e/o "attestazioni elettroniche di attributi" (EAA).**

Modalità di sviluppo:
1. Ricorso a Fintech/Startup
2. Ricorso ad altri fornitori esterni
3. Sviluppo in house
4. Modalità di sviluppo in house ed esterna

Ambito	Risposta
EUDI Wallet	☐
Attestazioni elettroniche di attributi (EAA)	☐

4.5 **Indicare se è previsto l'utilizzo di DLT per lo sviluppo di EUDI Wallet e/o di "attestazioni elettroniche di attributi" (EAA).**

	Risposta
Sì, per gli EUDI Wallet	☐
Sì, per le EAA	☐

4.6 **Indicare se la banca/gruppo aderisce a iniziative a livello europeo per lo sviluppo dell'ecosistema degli EUDI Wallet (es. progetti pilota su vasta scala).**

	Risposta
Sì, specificare:	☐
No	☐

4.7 **Con riferimento ai servizi forniti alla clientela e alle tipologie di operazioni di seguito specificate, indicare le modalità di autenticazione adottate anche in prospettiva con l'utilizzo di EUDI Wallet.**

Risposta:
1=Al 2025
2=Nel biennio 2026-2027

Modalità di autenticazione	**Onboarding**	**Dispositive**	**Potenzialmente critiche (es. Aumento massimali)**
Password e token fisico	☐	☐	☐
Password e fattore biometrico	☐	☐	☐
Fattore biometrico	☐	☐	☐
Password e OTP via SMS/email/telefonata (o app basata su SMS)	☐	☐	☐
Password e OTP via app/authenticator non basato su SMS	☐	☐	☐
Altro (altra combinazione di password, fattore biometrico e token/smartcard/app/SMS/email)	☐	☐	☐
Identità digitale eIDAS di livello 2 (es. SPID o CIE)	☐	☐	☐
Identità digitale eIDAS di livello 3 (con lettura tramite NFC)	☐	☐	☐
EUDI Wallet	☐	☐	☐