NTT DATA
Trusted Global Innovator

81 milioni di motivi per aderire al framework SWIFT:

il programma di sicurezza informatica volto a combattere gli attacchi cyber e difendere le transazioni finanziarie

WHITE PAPER / CYBERSECURITY

Indice

Introduzione

È il 4 febbraio 2016 e la Banca Centrale del Bangladesh, al termine della settimana lavorativa, saluta i dipendenti e chiude le sue porte dando inizio al weekend.

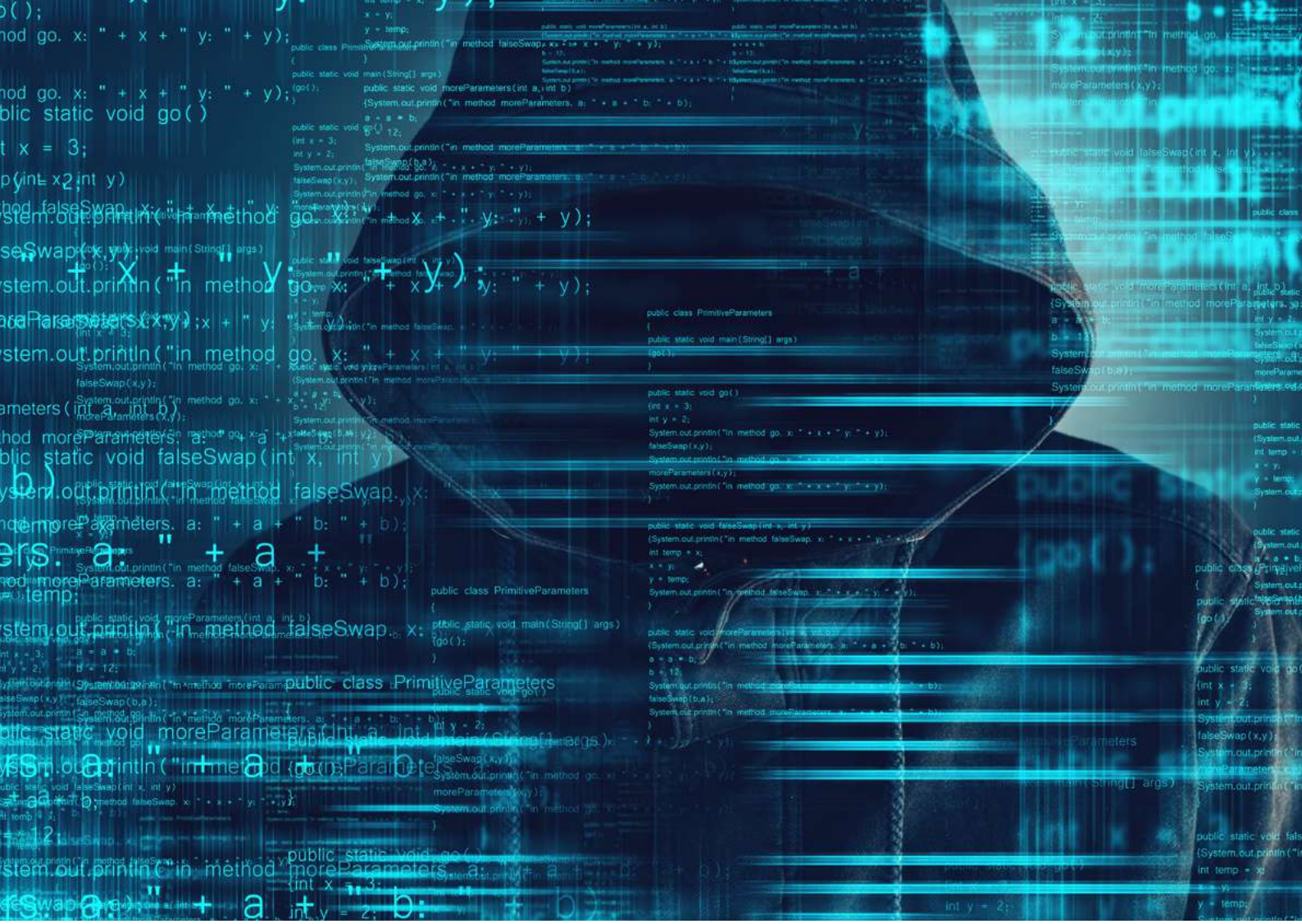
Il giorno successivo, la Federal Reserve di New York (banca con caveau a 20 metri sotto il livello del mare, telecamere, posti di blocco, tessere elettroniche, meccanismi sofisticati di sicurezza, pareti blindate spesse sei metri e duecentotrenta tonnellate di acciaio [1]) riceve una richiesta per conto della Banca Centrale del Bangladesh in seguito alla quale trasferisce più di 100 milioni di dollari.

Si tratta in realtà di un attacco hacker che puntava ad un bottino di 100 milioni di dollari, dei quali solamente 20 verranno effettivamente recuperati dalle forze dell'ordine tramite le attività di indagine [2].

Come è potuto succedere tutto questo?

L'attacco hacker ha colpito il sistema di servizi e messaggistica interbancari fornito a 11mila istituti di credito in tutto il mondo dalla Society for Worldwide Interbank Financial Telecommunication, nota come SWIFT,e attraverso una campagna di phishing che ha infettato la rete bancaria del Bangladesh senza che nessuno se ne accorgesse, hanno inviato 35 richieste di trasferimento di denaro attraverso un falso ordine di pagamento SWIFT.

1 - https://ricerca.repubblica.it/repubblica/archivio/repubblica/1991/09/06/il-cuore-oro-della-fed.html
2 - https://st.ilsole24ore.com/art/mondo/2016-03-15/chi-ha-rubato-100-milioni-conto-banca-centrale-bangladesh-fed-new-york-164850.shtml?uuid=ACWmmaoC



Per fortuna anche gli hacker commettonoerrori, come quelli di ortografia in questo caso. Sono bastati infatti qualche nome sgrammaticato e nomi di società fittizie sospette a ridurre drasticamente i loro guadagni.

Avanti veloce di un anno, è il 2017 quando SWIFT mette a punto un nuovo programma di sicurezza informatica vincolante per tutti gli Istituti Bancari appartenenti alla propria rete, noto come Customer Security Programme (CSP), con l'obiettivo di aiutare "le istituzioni finanziarie a garantire che le loro difese contro gli attacchi informatici siano aggiornate ed efficaci, per proteggere l'integrità della più ampia rete finanziaria" [3].

3 - https://www.swift.com/myswift/customer-security-programme-csp

Agli utenti della rete SWIFT, identificati con un codice numerico di 8 cifre noto come Bank Identifier Code (BIC), è richiesto di adeguare le proprie misure di sicurezza a quanto stabilito nel Customer Security Controls Framework (CSCF), il quadro di requisiti di sicurezza elaborati da SWIFT suddivisi in controlli obbligatori e facoltativi sulla base della tipologia di architettura tecnologica di cui l'istituto bancario dispone, e al suo grado di outsourcing.

La mancata conformità al CSP comporta il richiamo da parte di SWIFT al regolatore nazionale, all' esecuzione di un Independent Assessment di terza parte per ordine di SWIFT (Mandated Assessment) e, se protratta, all'allontanamento dalla rete con conseguenti risvolti economico-finanziari. L'ultimo caso documentato si riferisce all'esclusione dalla retedi alcune banche russe, a causa del conflitto in Ucraina scoppiato a febbraio 2022. Questa particolare situazione ha disconnesso tali banche dal sistema finanziario internazionale e creato ostacoli alla capacità di operare a livello globale. Allo stesso modo i titoli quotati connessi a società di origine russa saranno impattati e probabilmente verranno sospesi dalle transazioni sui mercati regolamentati [4].

4 - https://www.altalex.com/documents/2022/03/09/l-esclusione-di-alcune-banche-russe-dal-sistema-swift-e-le-sue-conseguenze

Come diventare compliant e quali sono i benefici

Ogni anno SWIFT pubblica sul proprio portale la nuova versione del CSCF, obbligatoria a partire dall'anno successivo, seguendo una logica che si potrebbe definire di "aggiornamento progressivo":

- da un lato introduce i nuovi controlli sotto forma di requisiti facoltativi in prospettiva di promuoverli ad obbligatori nelle successive versioni del CSCF;
- dall'altro attua una graduale e sempre più puntuale estensione del perimetro tecnologico oggetto dei requisiti di sicurezza.

Così facendo SWIFT assicura ai propri utenti il tempo necessario per adeguarsi alle evoluzioni normative e programmare le necessarie attività di aggiornamento.
L'obbligo di compliance deve essere annualmente assolto entro il 31 dicembre tramite:

- La compilazione di una Self Attestation (SA), da pubblicare sul portale dedicato Know Your Customer-Self Attestation (KYC-SA) e dal 2020 accessibile a controparti per principio di trasparenza.
- L'esecuzione di un Independent Assessment (IA).

Il costante aggiornamento condotto da SWIFT in ambito Security, per rispondere alle continue minacce cyber, rappresenta anche per i BIC una sfida continua al fine di conseguire, ad ogni rinnovo, la compliance entro il termine perentorio del 31 dicembre.

Ciò presuppone una serie di attività in capo al BIC, quali un'attenta analisi degli aggiornamenti normativi contenuti nella nuova versione del CSCF, la verifica dello status quo in cui versa il BIC, l'individuazione degli interventi necessari da portare a termine e la previsione di budget e tempistiche per concludere il programma di adeguamento entro la scadenza.

In particolare, l'independet assessment può essere svolto in due modalità:

- Internal , ovvero quando l'assessment è condotto da una linea di controllo (es. Internal Audit, Risk) interna all'organizzazione, indipendente da chi effettua la self attestation ;
- External, ovvero quando l'assesment è condotto da assessor appartenenti ad un'organizzazione esterna e indipendente.

I benefici derivanti dalla certificazione SWIFT possono riscontrarsi non solo nell'effettivo aumento di sicurezza e nella riduzione dei rischi derivanti dal supporto specialistico, che aziende come NTT DATA assicurano per indirizzare correttamente le esigenze di compliance, ma anche la possibilità di dimostrare all'intero ecosistema finanziario il commitment sulla sicurezza, con conseguenti benefici d'immagine e per il business.

Non tutte le banche sono uguali

Ogni istituzione possedente un BIC deve dimostrare la propria compliance agli attuali 32 requisiti (23 mandatory e 9 advisory) specificati nel CSCF.

I controlli mandatory devono essere obbligatoriamente implementati ogni anno entro la scadenza del 31 dicembre, secondo quanto stabilito nella versione del CSCF pubblicata nell'anno precedente. La nuova versione del CSCF viene pubblicata da SWIFT a cadenza annuale, in genere i primi giorni del mese di luglio, ed entra in vigore solo a partire dall'anno successivo.

In questo modo gli utenti hanno a disposizione un arco temporale di 18 mesi per attivarsi e prevedere le necessarie attività di adeguamento rispetto alle novità di volta in volta introdotte.

I controlli non sono applicabili indifferentemente a tutti i BIC: un controllo che per un BIC è classificato come mandatory, potrebbe infatti non essere implementabile o risultare advisory per un altro. La differenza dipende dall'architettura stessa dell'ente, ovvero dalla modalità con cui quest'ultimo si collega alla rete SWIFT e da quali e quanti sistemi informatici sono o meno delegati a terzi. A seconda, dunque, di che cosa viene delegato a terzi, aumenta o diminuisce il numero dei controlli di sicurezza del framework SWIFT a cui essere conformi. Sebbene l'implementazione dei controlli advisory sia solamente consigliata, è da evidenziare che essi rappresentano di fatto la best practice raccomandata da SWIFT per i propri clienti.

	23 MANDATORY CONTROLS	Architecture Types	9 ADVISORY CONTROLS	Architecture Types
SECURE YOUR ENVIRONMENT	1.1 SWIFT Environment Protection	A1 A2 A3	1.2 Operating System Privileged Account Control	B
	1.2 Operating System Privileged Account Control	A1 A2 A3 A4	1.5A Customer Environment Protection	A4
	1.3 Virtualization Platform Protection	A1 A2 A3 A4	2.4A Back-Office Data Flow Security	A1 A2 A3 A4 B
	1.4 Restriction of internet access	A1 A2 A3 A4 B	2.5A External Transmission Data Protection	A1 A2 A3 A4
	2.1 Internal Data Flow Security	A1 A2 A3	2.7 Vulnerability Scanning	B
	2.2 Security Updates	A1 A2 A3 A4 B	2.8A Critical Activity Outsourcing	A1 A2 A3 A4 B
	2.3 System Hardening	A1 A2 A3 A4 B	2.11A RMA Business Controls	A1 A2 A3 A4 B
	2.6 Operator Session Confidentiality and Integrity	A1 A2 A3 A4 B		
	2.7 Vulnerability Scanning	A1 A2 A3 A4		
	2.9 Transaction Business Controls	A1 A2 A3 A4 B		
	2.10 Application Hardening	A1 A2 A3		
	3.1 Physical Security	A1 A2 A3 A4 B		
KNOW AND LIMIT ACCESS	4.1 Password Policy	A1 A2 A3 A4 B	5.3A Personnel Vetting Process	A1 A2 A3 A4 B
	4.2 Multi-Factor Authentication	A1 A2 A3 A4 B		
	5.1 Logical Access Control	A1 A2 A3 A4 B		
	5.2 Token Management	A1 A2 A3 A4 B		
	5.4 Physical and Logical Password Storage	A1 A2 A3 A4 B		
DETECT AND RESPOND	6.1 Malware Protection	A1 A2 A3 A4 B	6.2 Software Integrity	A4
	6.2 Software Integrity	A1 A2 A3	6.5A Intrusion Detection	A1 A2 A3 A4
	6.3 Database Integrity	A1 A2 A4	7.3A Penetration Testing	A1 A2 A3 A4 B
	6.4 Logging and Monitoring	A1 A2 A3 A4 B	7.4A Scenario Risk Assessment	A1 A2 A3 A4 B
	7.1 Cyber Incident Response Planning	A1 A2 A3 A4 B		
	7.2 Security Training and Awareness	A1 A2 A3 A4 B		

Quadro dei controlli CSCF v2022

SWIFT identifica 5 differenti architetture per i suoi clienti, che in ordine decrescente di controlli applicabili sono:

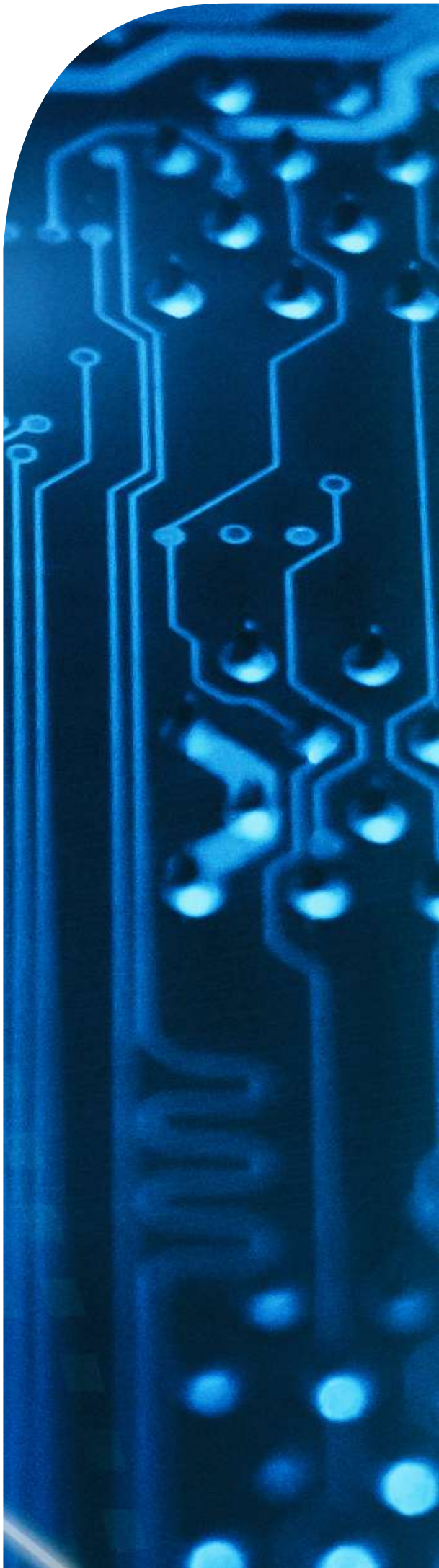
- Architettura di tipo A1: definita FULL STACK, in cui l'interfaccia di comunicazione con SWIFT è di proprietà e dell'utente. Si parla di architettura di tipo A1 anche quando la banca possiede la licenza per l'interfaccia di comunicazione che, o gestisce per altri utenti, o viene gestita in sua vece da terzi.

- Architettura di tipo A2: definita PARTIAL STACK, in cui l'utente possiede l'interfaccia di messaggistica, ma non l'interfaccia di comunicazione. Un service provider possiede la licenza dell'interfaccia di comunicazione e fa da tramite. Si parla di architettura di tipo A2 anche quando la banca possiede la licenza per l'interfaccia di messaggistica, ma questa viene delegata a terze parti.

- Architettura di tipo A3: l 'utente comunica con SWIFT per mezzo di un service provider a cui si collega tramite una soluzione SWIFT connector.

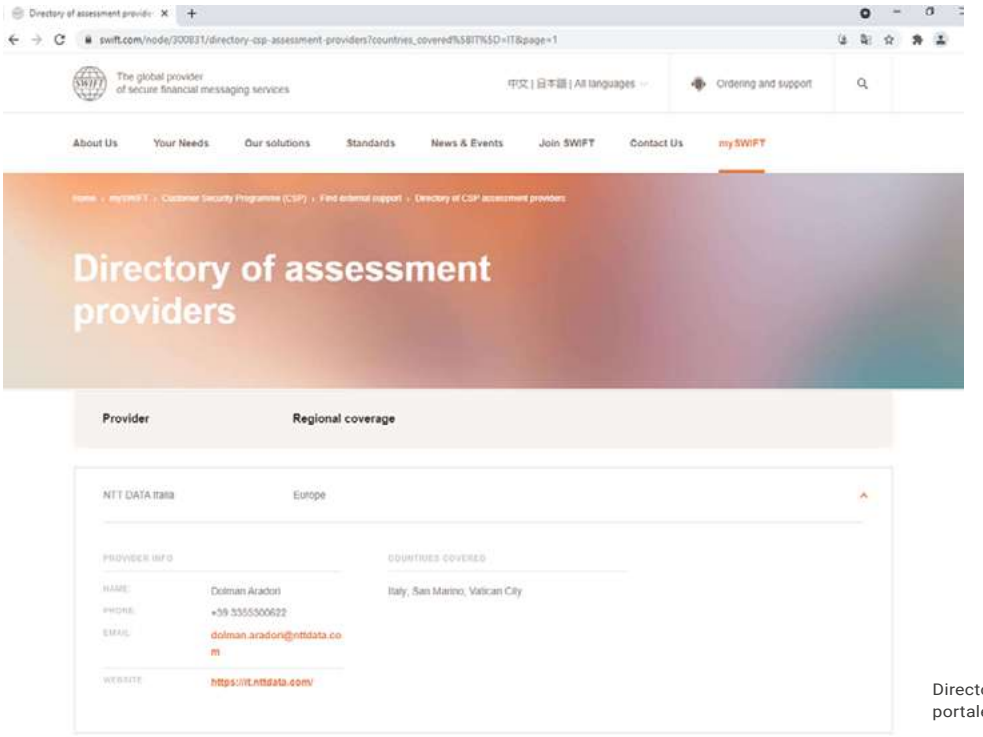
- Architettura di tipo A4: l'utente comunica con SWIFT per mezzo di un service provider a cui si collega tramite una soluzione proprietaria.

- Architettura di tipo B: l'utente comunica con SWIFT per mezzo di un service provider a cui si collega via GUI/APIs, senza quindi alcuna componente specifica.



L’approccio di NTT DATA

NTT DATA Italia si occupa continuativamente della tematica SWIFT già dal 2017 ed è censita nell’elenco ufficiale di Assessor SWIFT come Independent Assessor.



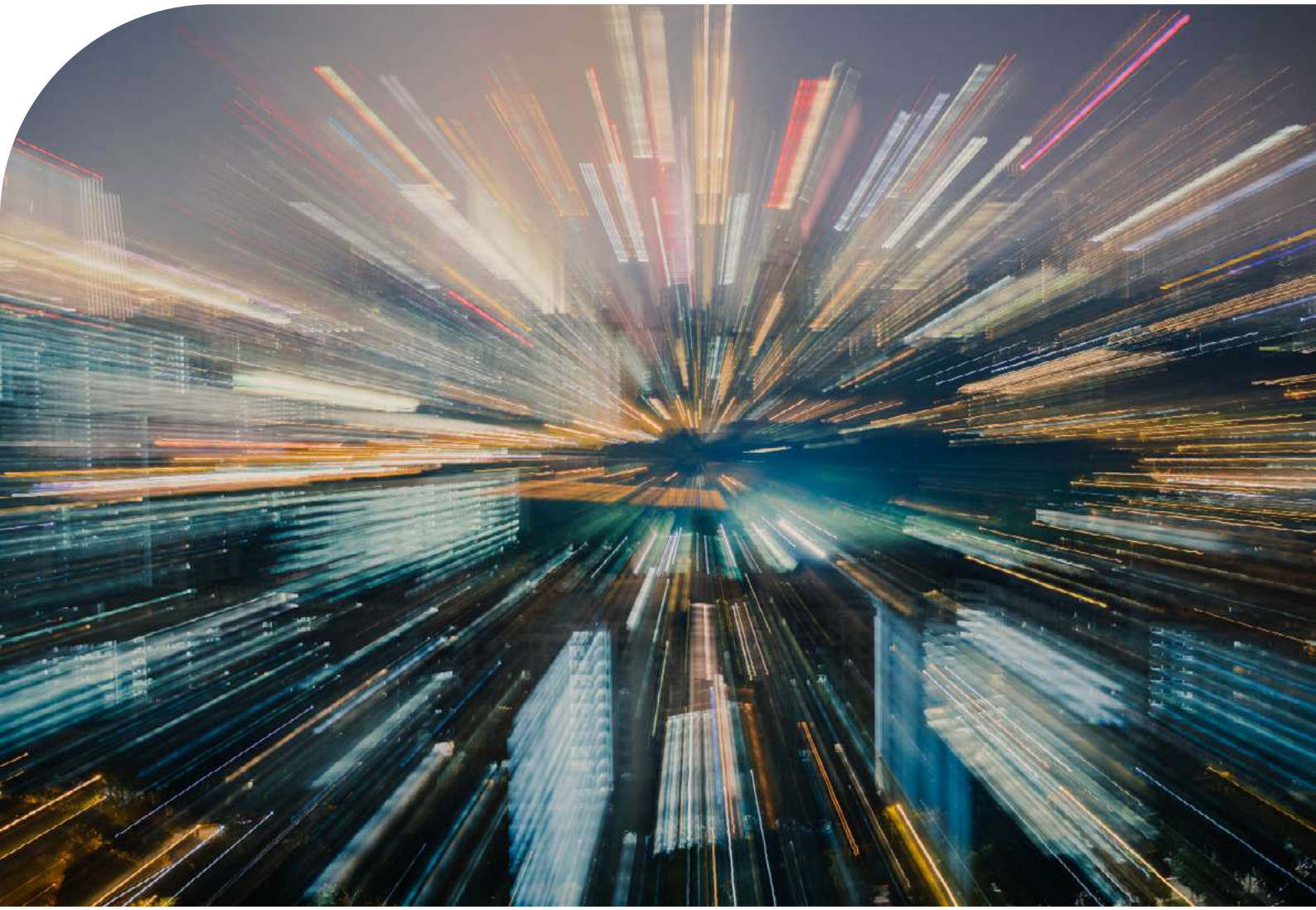
Directory Assessor portale SWIFT

Nello specifico, dal 2017 NTT DATA Italia si occupa di supportare e affiancare uno dei principali gruppi bancari nazionali nelle attività di completamento e inserimento della Self Attestation, offrendo un supporto specialistico per le attività di Self Assessment propedeutiche al processo annuale di rinnovo della compliance al framework normativo SWIFT, e già dal 2019 conduce l’attività di Independent Assesment in qualità di terza parte indipendente. Il perimetro delle attività comprende l’infrastruttura tecnologica della Capo Gruppo, che si articola in una serie di BIC relativi a filiali italiane, estere e Legal Entities, e un ulteriore gruppo di BIC “autonomi” afferenti ad altre Filiali estere, dotati di una propria infrastruttura tecnologica di collegamento alla rete SWIFT e che pertanto si occupano autonomamente di assolvere agli obblighi di compliance verso SWIFT.
Nei loro confronti la Capo Gruppo esercita un’attività di monitoraggio costante, al fine di garantire la compliance dell’intero perimetro del gruppo, e NTT DATA la affianca supportando le comunicazioni verso gli ISO locali e gestendo eventuali richieste da parte di questi ultimi.
Il processo di Independent Assessment viene condotto attraverso interviste (da remoto o in loco) con i referenti della Capo Gruppo competenti per l’area di interesse da analizzare, e con la raccolta di evidenze a supporto di quanto esposto durante gli incontri. Il materiale raccolto costituirà la base per la stesura del report finale, la relazione di Independent Assessment, e il report dei findings, ovvero l’elenco degli ambiti in cui sono state riscontrate specifiche aree di intervento, con la relativa classificazione in base al grado di severità (high, medium, low) e il termine entro cui dovranno essere concluse. In caso di non conformità rispetto ad un requisito mandatory (la cui risoluzione deve avvenire entro il 31 dicembre per poter caricare su KYC una Sef Attestation compliant), deve essere verificata la corretta chiusura delle azioni di rimedio una volta completate, e successivamente aggiornare il report di Independent Assessment.
In entrambe le attività di assessment, NTT DATA è solita prendere in considerazione l’ultima versione normativa del CSCF, nonostante la sua obbligatorietà inizi a decorrere a partire dall’anno successivo. La scelta di NTT DATA è stata quella di adottare un approccio lungimirante rispetto a quelli che saranno i nuovi requisiti e/o ambiti in perimetro delle successive versioni del CSCF, facilitando così le strutture del cliente nella pianificazione delle necessarie attività di adeguamento al framework e riducendo i rischi provenienti da nuove minacce cyber.

Punti di forza dell’approccio

Per rispondere alla complessità e alla delicatezza dell’argomento trattato, NTT DATA fornisce un supporto costante e puntuale su tutte le attività coinvolte nel raggiungimento della compliance.

L’approccio strutturato, competente e specialistico sulla sicurezza e il vero e proprio “gioco di squadra” ottenuto grazie alla sinergia con i referenti coinvolti nell’assessment, è la chiave di NTT DATA per il raggiungimento dell’obiettivo nel modo più efficace e propositivo possibile.
In linea con il core value foresight dell’azienda, NTT DATA svolge regolarmente attività di Independent Assessment già dal 2019, in anticipo rispetto alle tempistiche standard di SWIFT che ne prevedono l’obbligatorietà solamente dal 2021.
L’approccio utilizzato non si basa solo ed esclusivamente sull’individuazione di non conformità, ma anche di punti di miglioramento. L’esigenza di attestarsi al framework deve essere vista come un’opportunità di miglioramento dell’infrastruttura tecnologica dell’ente e non come un obbligo, in tal modo anche la realizzazione dei requisiti non obbligatori diventa portatrice di valore non solo in ambito di sicurezza cyber, ma anche di reputation nell’intero ecosistema finanziario.



Conclusioni

Il 5 febbraio 2016 la Banca Centrale del Bangladesh si è ritrovata a vivere il peggiore incubo di ogni banca: una rapina. E non una rapina qualsiasi, una delle più grandi della storia, con un bottino di ben 81 milioni di dollari, denaro che ad oggi non è mai stato recuperato. Non si è trattato del classico copione che ben conosciamo: niente sparatorie, niente facce incappucciate, niente gallerie costruite sotto il pavimento della banca fin dentro il caveau. La Banca Centrale del Bangladesh era del tutto impreparata poichè ha dovuto misurarsi con un campo di battaglia diverso, ancora sconosciuto: quello tecnologico. A essere presa di mira è stata la rete SWIFT, utilizzata principalmente dagli istituti bancari per inviare e ricevere messaggi relativi alle transazioni finanziarie. La risposta di SWIFT è stata immediata: ad un anno dall'episodio che ha coinvolto la Banca del Bangladesh, mette a disposizione dei propri utenti la protezione di cui hanno bisogno tramite la pubblicazione di un nuovo sistema di sicurezza pensato ad hoc, composto da controlli puntuali a difesa delle transazioni finanziarie. L'obiettivo dichiarato è bloccare, o almeno scoraggiare, i potenziali criminali. Nasce così nel 2017 il Customer Security Programme.

Alla luce degli eventi che hanno spinto SWIFT a pubblicare il Customer Security Control Framework, l'obbligo di compliance per tutti gli utenti operanti nella rete SWIFT deve essere letto non come un semplice, per non dire ennesimo, vincolo di adeguamento ad un quadro normativo, ma come la preziosa opportunità di operare in sicurezza nel complesso mondo delle transazioni finanziarie, in ottica di miglioramento continuo.

NTT DATA Italia si adopera continuativamente dal 2017 per supportare gli istituti bancari e altri utenti della rete SWIFT nelle attività propedeutiche al conseguimento della compliance verso SWIFT, adottando un approccio specialistico, ben consapevole dell'importanza di una solida competenza nel settore; sinergico, poiché promuove la massima collaborazione con le controparti nell'esecuzione delle attività propedeutiche all'assessment; lungimirante, con un occhio sempre proiettato al futuro, sensibile alla necessità di saper andare oltre quanto richiesto nell'immediatezza da SWIFT e giocare d'anticipo sugli interventi di adeguamento necessari per tenere il passo dei costanti aggiornamenti del CSCF.

Key takeaways

1 Il CSCF è un framework di controlli di sicurezza a cadenza annuale pubblicato da SWIFT per la prima volta nel 2017, destinato agli utenti della propria rete, identificati tramite un codice numerico BIC (Bank Identifier Code) di 8 cifre.

2 Il framework si basa su 3 principi (SECURE YOUR ENVIRONMENT, KNOW AND LIMIT ACCESS, DETECT AND RESPOND), 7 obiettivi e 32 controlli. I controlli non devono essere applicati in maniera indiscriminata a tutti i BIC, ma sono suddivisi in obbligatori e opzionali per ognuna delle 5 possibili architetture definite dal framework (A1, A2, A3, A4 e B) in base alle componenti tecnologiche che si collegano alla rete SWIFT e al loro grado di outsourcing.

3 Annualmente gli utenti della rete SWIFT devono dimostrare la propria compliance al framework normativo, attraverso la pubblicazione di una Self Attestation valida sulla piattaforma KYC-SA, e dal 2021 anche tramite l'esecuzione di un Independent Assessment. Le conseguenze legate ad una mancata compliance sono: richiamo al regolatore nazionale, danni d'immagine, esecuzione di un Independent Assessment di terza parte per ordine di SWIFT (Mandated Assessment) e possibile allontanamento dalla rete con conseguenti risvolti economico-finanziari.

4 Dal 2017 NTT DATA Italia lavora per supportare gli istituti bancari e altri utenti della rete SWIFT nel conseguimento della compliance verso il framework SWIFT, operando in qualità di Independent Assessor certificato (censita nel portale SWIFT) e fornendo un supporto specialistico in tutte le attività necessarie al corretto adempimento degli obblighi verso SWIFT.

Irene Polato
Consultant, Cyber Security Strategy & Governance

Francesco Nucci
Consultant, Cyber Security Strategy & Governance

Leonardo Talerico
Analyst, Cyber Security Strategy & Governance

NTT DATA aiuta le organizzazioni a orientarsi nella rapida evoluzione delle tecnologie, a rispondere alle crescenti aspettative dei clienti e, attraverso l'innovazione e la profonda esperienza nel settore, mette a disposizione le competenze e le risorse per guidare lo sviluppo digitale. Offriamo consulenza in ogni fase di progetto, da una prima fase di strategia e concept, passando dagli impatti sui processi, per arrivare all'implementazione finale. Advisory, Design, Tecnologia e Operation sono solo alcune delle nostre aree di competenza. NTT DATA ha sede a Tokyo con oltre 123.000 professionisti in oltre 50 Paesi in tutto il mondo. www.nttdata.com/it

NTT DATA
Trusted Global Innovator

NTT DATA