ADVANCTION
We secure your business

Cyber Security

LA COMPLIANCE CON LE NUOVE RICHIESTE DELLA CIRCOLARE FINMA 2008/21

Il supporto di Advanction in risposta alle nuove richieste della Normativa finalizzate a migliorare la sorveglianza e la gestione della Cyber Security in banca

Advanction SA

Via ala Posta, 31
CH - 6835 Morbio Superiore

www.advanction.com
info@advanction.com

Contenuti

Introduzione

Nel corso del 2016 la FINMA ha sottoposto a revisione la circolare 2008/21 “Rischi operativi – banche” e ha pubblicato il 1 novembre una nuova versione della stessa, con lo scopo di estendere le necessità di controllo sulle infrastrutture tecnologiche includendo requisiti specifici alla gestione dei cyber-rischi. Tali requisiti, che entreranno in vigore il 1 luglio 2017, si applicano a tutte le banche, indipendentemente dalla loro dimensione o categoria di supervisione.

Nuovi requisiti e linee guida

Le banche devono formalizzare la loro strategia di gestione dei cyber-rischi, definendo ruoli e responsabilità così come i processi per coprire le seguenti *cinque dimensioni*:

Identificazione e valutazione dei cyber-rischi

Le banche devono identificare, valutare e pianificare azioni per fronteggiare cyber-incidenti. In particolare devono valutare l'implementazione di soluzioni di threat intelligence e mantenere un censimento dei sistemi e dei dati critici.

Protezione contro gli attacchi

Le banche devono implementare misure che prevengano l’estrazione non autorizzata di dati dall’esterno, monitorando nel contempo i flussi di dati stessi. Devono anche assicurarsi della sicurezza delle loro reti e le interfacce con reti esterne così come implementare diverse linee di difesa (ad es. per bloccare attacchi DDOS).

Identificazione dei cyber-attacchi

Devono essere migliorati gli approcci al monitoraggio, che permettono alle banche di bloccare ogni tentativo di penetrazione non autorizzato verso le reti interne, individuare irregolarità nei flussi dati della rete e gestire allarmi di sicurezza in modo efficiente. Le banche devono anche considerare l’implementazione di soluzioni di SIEM come strumento per migliorare il log sistematico degli attacchi.

Risposta agli attacchi

Le banche devono definire i processi, le persone e gli strumenti necessari per rispondere agli attacchi, allo scopo di mantenere la normale attività operativa. Devono anche formalizzare i loro piani di azione e le modalità di comunicazione con gli stakeholder interni ed esterni.

Ripristino delle attività di business dopo un attacco

Le banche devono definire le misure necessarie ad assicurare il ripristino della disponibilità e dell’integrità dei sistemi e il ripristino dei dati corrotti o perduti dopo un attacco. Inoltre devono formalizzare un processo sistematico, con le relative procedure, per un’analisi forense successiva a ogni attacco significativo, in grado di identificare le cause e le deficienze di

Introduzione

controllo, così come sviluppare un piano d'azione con adeguate misure per migliorare la protezione contro gli attacchi.

Cyber Security Framework

Advanction ha progettato e realizzato un framework partendo da una base consolidata, creata dal NIST (National Institute for Standards and Technology, degli Stati Uniti) base che FINMA stessa ha utilizzato come riferimento per la redazione della circolare 2008/21 “Rischi operativi – banche”.

Il framework è un set di standard è best practice realizzato grazie al contributo di migliaia di esperti di sicurezza e progettato per aiutare le aziende nella gestione dei rischi di violazione della cybersecurity. Grazie all’aiuto del framework, le aziende possono avere un quadro chiaro del loro profilo di sicurezza attuale, definire quale profilo dovrebbero avere e creare un piano per raggingerlo.

Il Cyber Security Framework di Advanction è stato contestualizzato considerando la realtà degli istituti di credito svizzeri. Oltre a ciò prevede due ulteriori concetti in grado di adattarsi ancora meglio alle diverse esigenze di ogni banca:

- Livelli di priorità
- Livelli di maturità

L’applicazione del Cyber Security Framework consente numerosi benefici, come ad esempio:

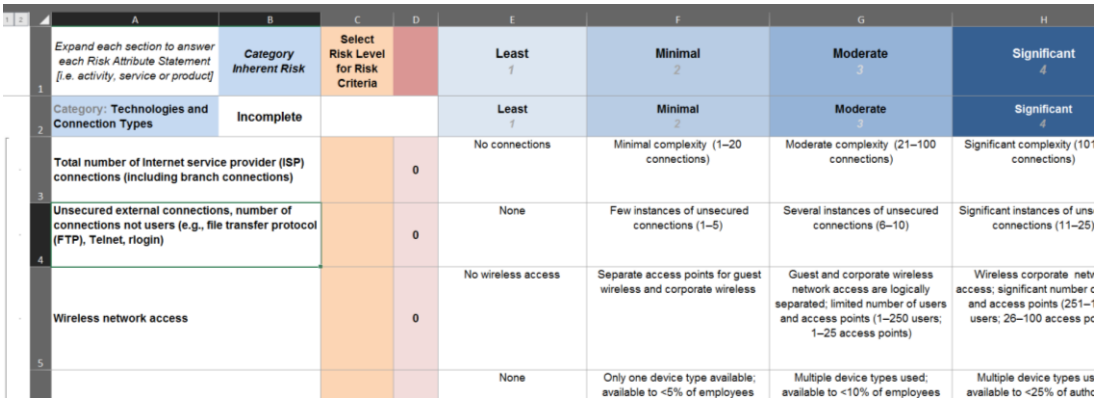
- ✓ Accurata identificazione e valutazione dei fattori di rischio
- ✓ Valutazione della preparazione della banca in ambito Cyber Security
- ✓ Identificazione dei punti di miglioramento a livello di Risk Management
- ✓ Definizione delle azioni da intraprendere per incrementare il livello di sicurezza

Cyber Security Assessment Tool

Advanction ha sviluppato il Cyber Security Assessment Tool allo scopo di aiutare le banche a identificare i rischi e valutarne la preparazione in ambito Cyber Security.

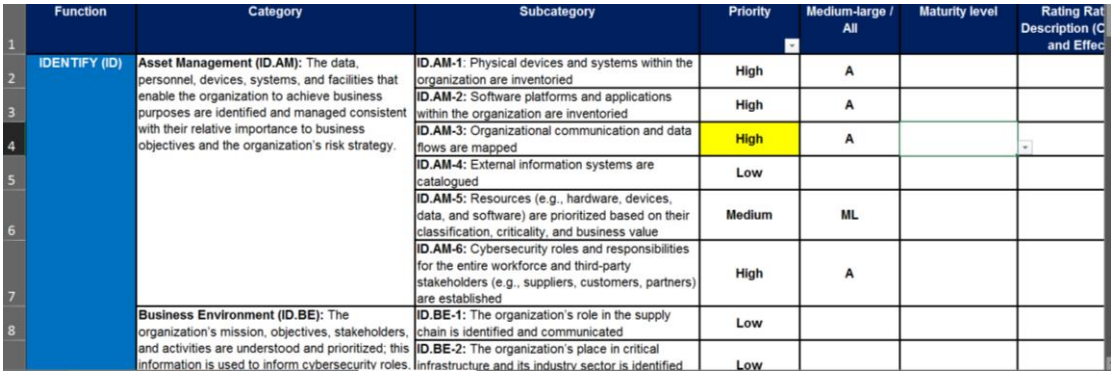
L'Assessment oltre a fornire la fotografia della situazione in un determinato momento, permette di ottenere un processo ripetibile e misurabile. In questo modo le istituzioni finanziarie sono in grado di monitorare costantemente la propria situazione, nel tempo.

Il profilo di rischio prende in considerazione i vari contesti che possiedono un rischio implicito per la banca.



	A	B	C	D	E	F	G	H
1	*Expand each section to answer each Risk Attribute Statement [i.e. activity, service or product]*	*Category Inherent Risk*	Select Risk Level for Risk Criteria		Least 1	Minimal 2	Moderate 3	Significant 4
2	Category: **Technologies and Connection Types**	**Incomplete**			Least 1	Minimal 2	Moderate 3	Significant 4
3	**Total number of Internet service provider (ISP) connections (including branch connections)**			0	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101 connections)
4	**Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)**			0	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of uns connections (11–25)
5	**Wireless network access**			0	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate netv access; significant number c and access points (251–1 users; 26–100 access po
					None	Only one device type available; available to <5% of employees	Multiple device types used; available to <10% of employees	Multiple device types us available to <25% of autho

Strumento di analisi del profilo di rischio

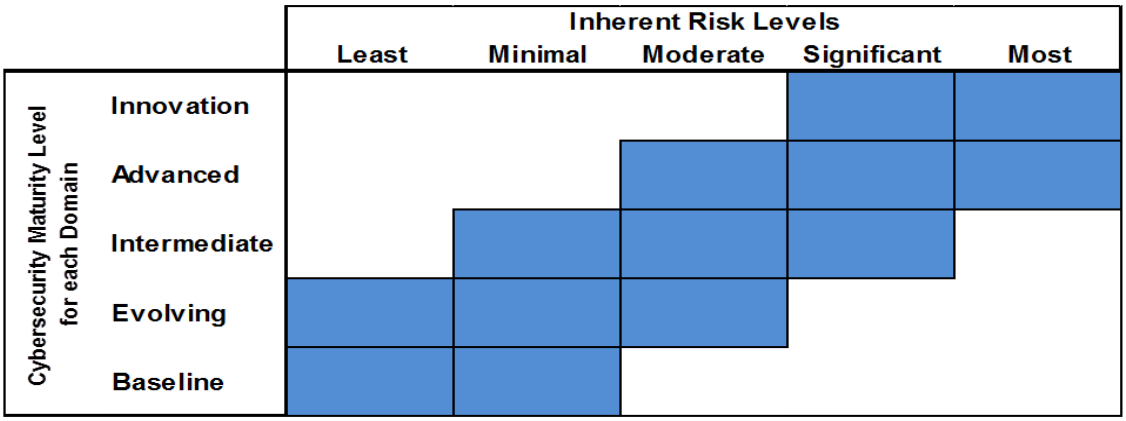


	Function	Category	Subcategory	Priority	Medium-large / All	Maturity level	Rating Rat Description (C and Effec
2	IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	High	A		
3			**ID.AM-2:** Software platforms and applications within the organization are inventoried	High	A		
4			**ID.AM-3:** Organizational communication and data flows are mapped	High	A		
5			**ID.AM-4:** External information systems are catalogued	Low			
6			**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Medium	ML		
7			**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	High	A		
8		**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Low			
			ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified	Low			

Strumento di analisi della maturità del framework

Cyber Security Assessment Tool

L’Assessment consente inoltre di formulare in maniera immediata e facilmente comprensibile il grado di esposizione al rischio combinato con il livello di maturità aziendale:



Ciò rende possibile individuare gli ambiti sui quali intervenire per apportare i miglioramenti necessari in caso di evidente disallineamento tra i due fattori.

Il ruolo di Advanction

Advanction è in grado di aiutare le banche nel miglioramento della loro Compliance nei confronti degli ambiti regolatori.

Tra i servizi che Advanction offre in questo contesto troviamo:

Cyber Security Framework Gap Analysis

Advanction ha sviluppato una metodologia completa per valutare la preparazione delle banche contro i cyber-attacchi e il livello di maturità delle cinque dimensioni sopra descritte, allo scopo di definire il gap nei confronti delle richieste FINMA. Tale metodologia è descritta nel documento “Cyber Security Framework - Implementazione per le banche svizzere”

Cyber Risk Assessment

Alla luce del crescente volume e sofisticazione delle minacce alla Cyber Security, Advanction ha sviluppato il Cyber Security Assessment Tool, finalizzato ad aiutare aiutare le banche a identificare i loro rischi e contemporaneamente riuscire a determinare la loro preparazione in ambito Cyber Security. L’Assessment fornisce un processo ripetibile e misurabile dedicato alle istituzioni finanziarie per misurare la propria preparazione nel tempo.

Tale metodologia viene descritta nel documento “Cyber Security Framework - Implementazione per le banche svizzere”

Roadmap verso la Compliance

La definizione della Roadmap verso la Compliance parte dall’identificazione dei gap definita nel punto precedente e dalla definizione delle attività necessarie per colmare i gap identificati, i *business owner* da coinvolgere e gli *stakeholder* impattati.

Implementazione delle azioni di Compliance

Grazie alle competenze e alle esperienze maturate in ambito Information Security per le istituzioni finanziarie, Advanction è in grado di aiutare le banche nell’ambito delle strategie di Compliance attraverso la

- Formulazione di strategie, policy e procedure nei 5 ambiti del CSF
- Risk Assessment di terze parti
- Revisione delle strategie di protezioni correnti
- Individuazione di soluzioni per la mitigazione dei cyber-rischi (ad es. SIEM; Threat Intelligence)

Servizi di Security Assessment

Advanction propone servizi di *vulnerability assessment* e *penetration testing,* basati su metodologie consolidate e tarati per soddisfare le necessità di banche di varie dimensioni ed esigenze.

Formazione e Coaching

Il personale ed eventualmente i partner dell'organizzazione, vanno formati al fine di raggiungere un adeguato grado di educazione, responsabilità e consapevolezza in ambito Cyber Security. Le risorse devono essere in grado di svolgere le proprie mansioni in accordo con le policy di sicurezza aziendali e le best practice.

Advanction propone servizi di formazione, sensibilizzazione e coaching in ambito Cyber Security.

Informazioni di contatto

Silvestro Maestri
Business Development
Tel +41 (0)76 495 73 15
smaestri@advanction.com

Stefano Bonacina
Information Security Expert
Tel +41 (0)76 575 58 82
sbonacina@advanction.com

Massimiliano Spini
Information Security Expert & Coach
Tel +41 (0)76 819 06 40
mspini@advanction.com

Advanction SA

Via ala Posta, 31
CH - 6835 Morbio Superiore

www.advanction.com

ADVANCTION
We secure your business