Il *virtual Information Security Officer* (vISO) a supporto del sistema banca «digitale»

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

1 Uno scenario di cambiamento

Il 2022 ha visto l'emanazione del **40° aggiornamento** della **Circolare della Banca d'Italia n. 285/2013 sulle Disposizioni di vigilanza per le banche.**

Tale aggiornamento, che ha l'obiettivo di attuare le Linee guida EBA sulla gestione dei rischi inerenti le tecnologie dell'informazione (ICT), vede la modificarsi, tra l'altro:

- il Capitolo 3 "Il sistema dei controlli interni"
- il Capitolo 4 "Il sistema informativo",
- il Capitolo 5 "La continuità operativa".

Le Linee guida vogliono inoltre armonizzare il quadro di misure di gestione dei rischi inerenti l'uso delle tecnologie ICT e le misure di sicurezza di cui le Banche devono dotarsi, ma rientrano in un più ampio insieme di norme, regolamenti e direttive che interesseranno gli istituti finanziari nei prossimi anni, tra cui:

1. **Regolamento UE 2022/2554** (noto come *Digital Operational Resilience Act* – **DORA**) volto ad incrementare le misure di sicurezza a favore della resilienza e della sicurezza informatica del settore finanziario ed una Direttiva UE 2022/2556, ad esso collegata, che serve ad armonizzare il quadro normativo.
2. **Direttiva (UE) 2022/2555** (nota come **NIS2** e che va a sostituire la Direttiva 2016/1148 cd. NIS sulla sicurezza delle reti e dei sistemi informativi), che introduce nuovi obblighi per le aziende in materia di sicurezza dei dati e maggiori responsabilità per i soggetti interessati.
3. **Direttiva (UE) 2022/2557** (nota come **CER** – *"Directive on the resilience of critical entities"*) relativa alla resilienza dei soggetti critici.

La timeline di adeguamento

2022

- 40° agg.to Circolare 285/2013
- Pubblicazione DORA (RegUE 2022/2554 – DirUE 2022/2556)
- Pubblicazione CER – Direttiva (UE) 2022/2557
- Pubblicazione NIS2 – Direttiva (UE) 2022/2555
- PCI-DSS v.4.0
- SWIFT Customer Security Controls Framework v.2022

2023

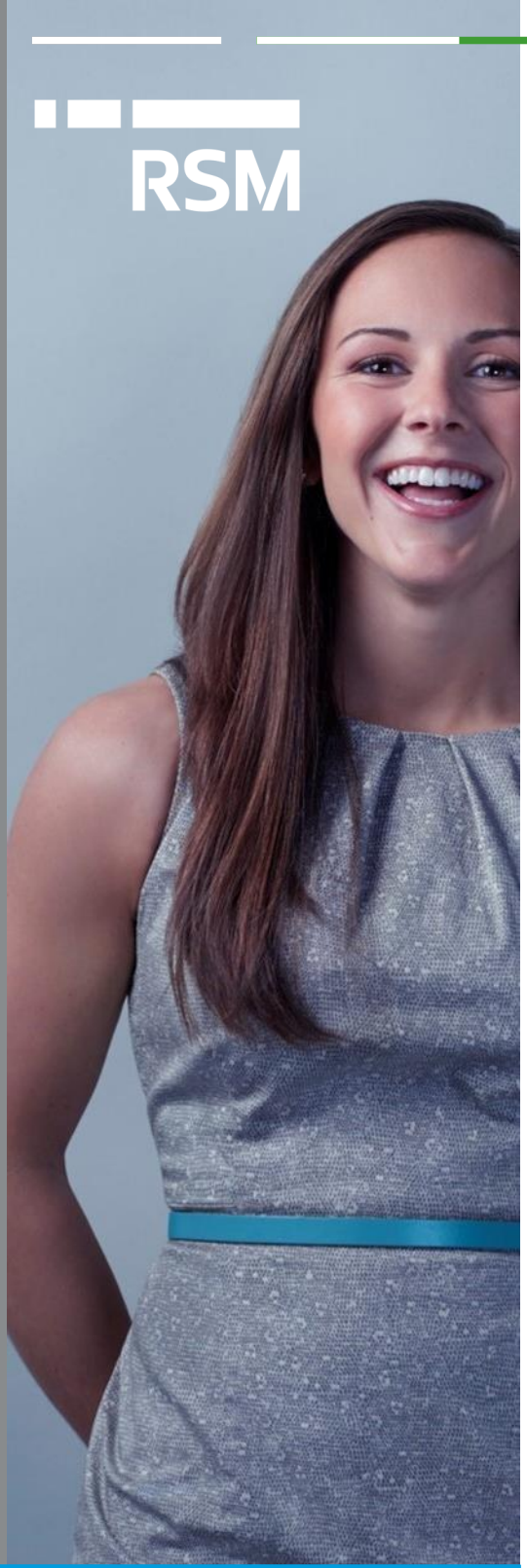
- Termine adeguamento Circ. 285/2013 e relazione a Banca d'Italia
- Entrata in vigore di DORA
- Entrata in vigore di NIS2

2024

- Emanazione RTS per DORA
- Attuazione CER e abrogazione Direttiva 2008/114/CE
- Recepimento dagli Stati Membri di NIS2 e abrogazione di NIS1 (Direttiva 2016/1148 e del D.lgs 18/05/2018, n. 65

2025

- Applicazione DORA
- Recepimento nuovi requisiti PCI-DSS v.4.0 e ritiro della v.3.2.1



Il vISO supporta la Vostra organizzazione nell'ideare, mettere in atto e testare un piano efficace ed efficiente per la protezione dei processi, dei sistemi e delle informazioni

2

Il virtual Information Security Officer

Risorse e competenze multidisciplinari che si integrano nella Vostra organizzazione

In questo scenario, in cui si richiede alle organizzazioni del settore bancario e finanziario una evoluzione dal punto di vista dei processi, delle procedure e dell'analisi del rischio ICT, si innesta il **virtual Information Security Officer (vISO)**, il team specialistico di RSM in materia di sicurezza delle informazioni, che include competenze multidisciplinari di **risk management**, **IT compliance, cybersecurity** e **legali**, oltre che risorse tecniche interne ed esterne.

Il vISO riporta al Senior Management della Vostra organizzazione e vi supporta nella gestione del processo e nello sviluppo del programma di **identificazione, valutazione dei rischi informatici e protezione delle informazioni aziendali**.

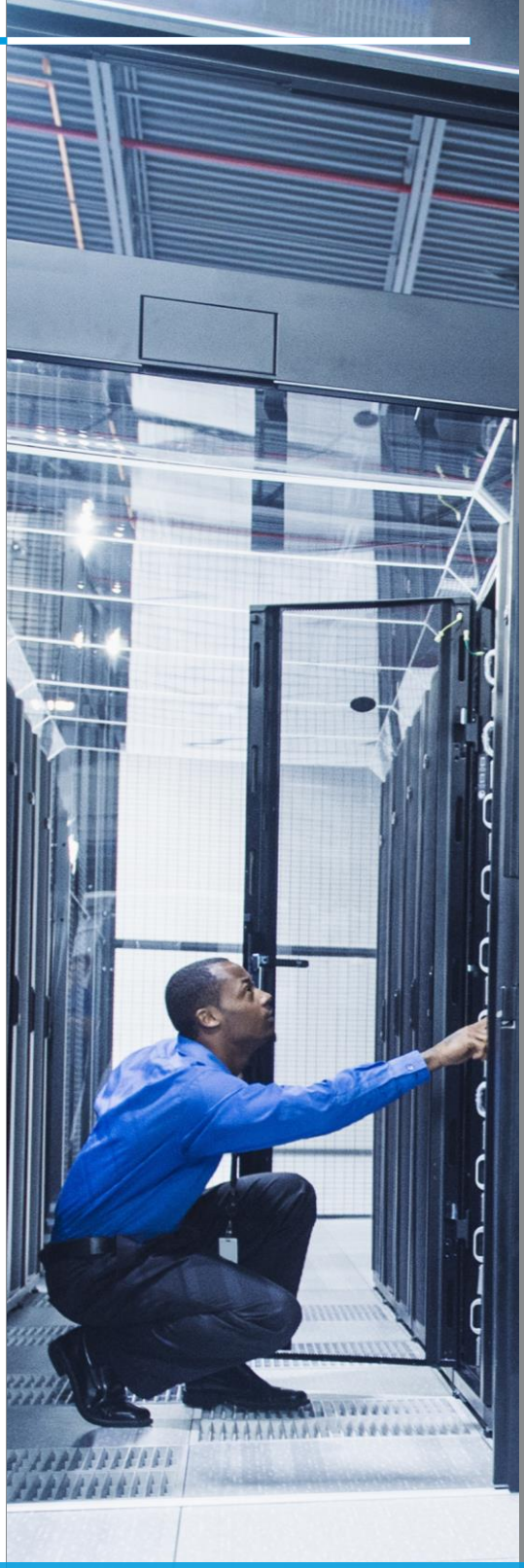
Il vISO:

- Dialoga attivamente con la 1° linea di difesa (es. CISO), con le Vostre altre figure controllo e monitoraggio (es. dipartimento di *Risk Management*, dipartimento di *Compliance*) e con il dipartimento di *Internal Audit*, andando ad inserire come **figura di raccordo** tra le figure di *Governance, Risk & Compliance* e le figure tecniche del dipartimento IT o dell'*outsourcer* tecnologico;
- Supporta nelle attività di ***risk assessment***, fornendo inoltre metodologie e approcci coerenti con la Vostra organizzazione e derivanti da linee guida e *framework* internazionali, al fine di **preservare i sistemi** di sicurezza delle informazioni e di **gestire e mitigare i rischi ICT**;
- Favorisce lo **sviluppo** dell'efficacia dei sistemi di **sicurezza delle informazioni** della Vostra organizzazione, in accordo con gli altri stakeholder,
- Supporta nella analisi, valutazione ed evoluzione dell'attuale **grado di preparazione e maturità in materia di cybersicurezza della Vostra organizzazione e dei Vostri partner tecnologici**, anche tramite piani di sensibilizzazione, training e verifiche interne o presso i Vostri fornitori ICT;
- Garantisce la presenza di una figura autorevole in materia di sicurezza dell'informazione nelle varie fasi di processo dove è necessario assicurare la riduzione e mitigazione dei prima che si verifichino perdite irreversibili (***security by design***);
- Supporta la Vostra organizzazione e gli altri dipartimenti coinvolti nella **gestione e valutazione degli incidenti ICT.**

3

I benefici del vISO

- **Competenze** multidisciplinari e flessibili, che possono essere richieste ***on-demand,*** anche solo in caso di necessità o nei momenti più critici
- **Disponibilità** da remoto oppure *on-site* a seconda delle Vostre esigenze
- Accesso ad un consulente di **fiducia**, che parla la «lingua» del Vostro dipartimento IT, quella delle Vostre funzioni di controllo e quella del revisore interno ed esterno
- Conoscenza delle linee guida e dei *framework* nazionali ed internazionali in materia di sicurezza IT e cybersicurezza ed esperienza sulle attuali **best practices** del Vostro settore
- Conoscenza dettagliata dei **rischi informatici**
- **Assistenza esperta** nel rispondere rapidamente alle problematiche e nel ridurre al minimo le interruzioni
- Possibilità di riunire facilmente tutti i sistemi di sicurezza con un **coordinamento integrato**
- Una **visione indipendente** sulla gestione del rischio ICT
- Una soluzione **economicamente vantaggiosa** per affrontare l'attuale carenza di competenze in materia di sicurezza informatica e la difficoltà di reperire profili con conoscenze multidisciplinari



Il vISO di RSM è:

Stratega:
Definisce le priorità degli interventi da attuare presso la Vostra organizzazione, in accordo con gli altri *stakeholders* del processo, e garantisce che la sicurezza, le risorse e i budget siano pienamente allineati al raggiungimento dei Vostri obiettivi.

Consulente:
Comprende le implicazioni delle nuove possibili minacce in ambito ICT e crea, in accordo con gli *stakeholders* della Vostra organizzazione, una *roadmap* strategica affinché le contromisure in ambito *cybersecurity* siano adeguate alla Vostra propensione al rischio.

Specialista tecnologico:
Seleziona ed implementa e gestisce, sulla base delle Vostre necessità, sistemi di rilevazione e di monitoraggio delle minacce e integra i servizi forniti da terze parti all'interno di un *framework* omogeneo.

Esperto di rischi e processi
Valuta il disegno dei processi e ne monitora l'operatività al fine di salvaguardere la confidenzialità, l'integrità e la disponibilità dei dati e delle applicazione ed inoltre supporta la Vostra organizzazione nello sviluppo ed implementazione della sicurezza, anche in maniera preventiva.

4 Il nostro approccio integrato

Analisi

- Comprensione degli obiettivi e dell'attuale modello
- GAP Assessment di alto livello

Definizione e Comunicazione della Strategia di ICT Risk e Cybersecurity

- Sviluppo della Strategia gestione del rischio e della Cybersecurity
- Piano di comunicazione
- Adeguamento/allineamento agli obiettivi di business

Implementazione Tecnica e Monitoraggio

Governance

- Definizione delle Policy e delle Procedure

Implementazione dei controlli

- Controllo Accessi
- Gestione centralizzata dei device
- Protezione degli *Endpoint*
- Segregazione delle reti
- Approccio alla Security condiviso per l'organizzazione
- Gestione delle utenze centralizzato

Monitoraggio & Compliance

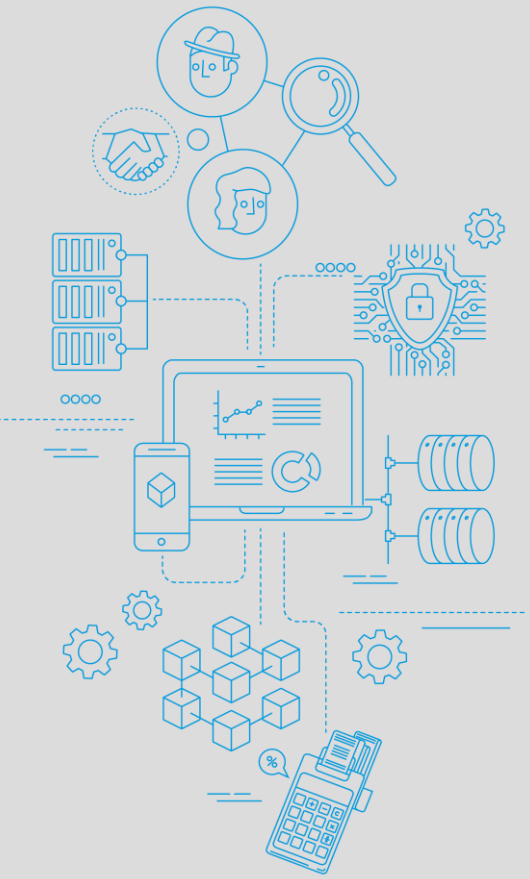
- Verifica delle configurazioni
- Gestione degli incidenti
- Test delle vulnerabilità
- Definizione di *Key Risk Indicator*
- Sviluppo di piani di *awareness* e di formazione
- *Phishing Simulation*
- Definizione di piani di *business continuity*

Reporting

- Predisposizione di relazioni e di strumenti di reporting per gli stakeholder della Società

4

Come il vISO di RSM può supportare concretamente la Vostra organizzazione



ANALISI e VALUTAZIONE

Esecuzione e redazione di un ***ICT Maturity Assessment,*** con l'obiettivo di raggiungere gli obiettivi di adempimento norma e di valorizzare, nel contempo, le informazioni, i modelli di governo e le soluzioni tecnologiche già in essere, evitando l'approccio *"from scratch".*

Effettuazione di un'analisi dei **rischi ICT**, anche derivanti da utilizzo di **fornitori rilevanti**, valutandone la criticità, e definendo, in accordo con gli altri *stakeholders*, contromisure e monitoraggi per permettere la pianificazione di adeguate strategia di contenimento del rischio.

IMPLEMENTAZIONE

Supporto alle altre funzioni interessate per la definizione di **processi, procedure e flussi informativi** (inclusi quelli di *incident reporting*) e revisione di quelli esistenti, per renderli coerenti con i requisiti normativi in essere e allineati alle *best practice* più adatte per l'organizzazione.

Monitoraggio continuo dell'efficacia dei processi e delle procedure adottate, in accordo con le altre funzioni di 2° e 3° livello.

STRATEGIA

Supporto nella definizione di un **«Piano Strategico di Trasformazione digitale»** e di un **«*Cybersecurity Plan*»** , in linea con gli obiettivi dell'organizzazione, ed anche tali da accrescere la consapevolezza delle persone, aumentarne le *skills* digitali e migliorare di conseguenza la resilienza e la sicurezza ICT.

Supporto nella redazione, entro il 1° settembre 2023, della **relazione per Banca d'Italia** con gli interventi (p.e. organizzativi, di processo e tecnologici) effettuati e pianificati per assicurare il rispetto delle disposizioni in materia di rischi ICT.

CONTATTI

Simone Segnalini
Partner
Digital, Risk & Transformation Leader

+39 06 87695257
Simone.Segnalini@rsmitaly.com

Mario Bertoli
Director
Digital, Risk & Transformation

+39 06 87695257
Mario.Bertoli@rsmitaly.com

www.rsm.global/italy

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING