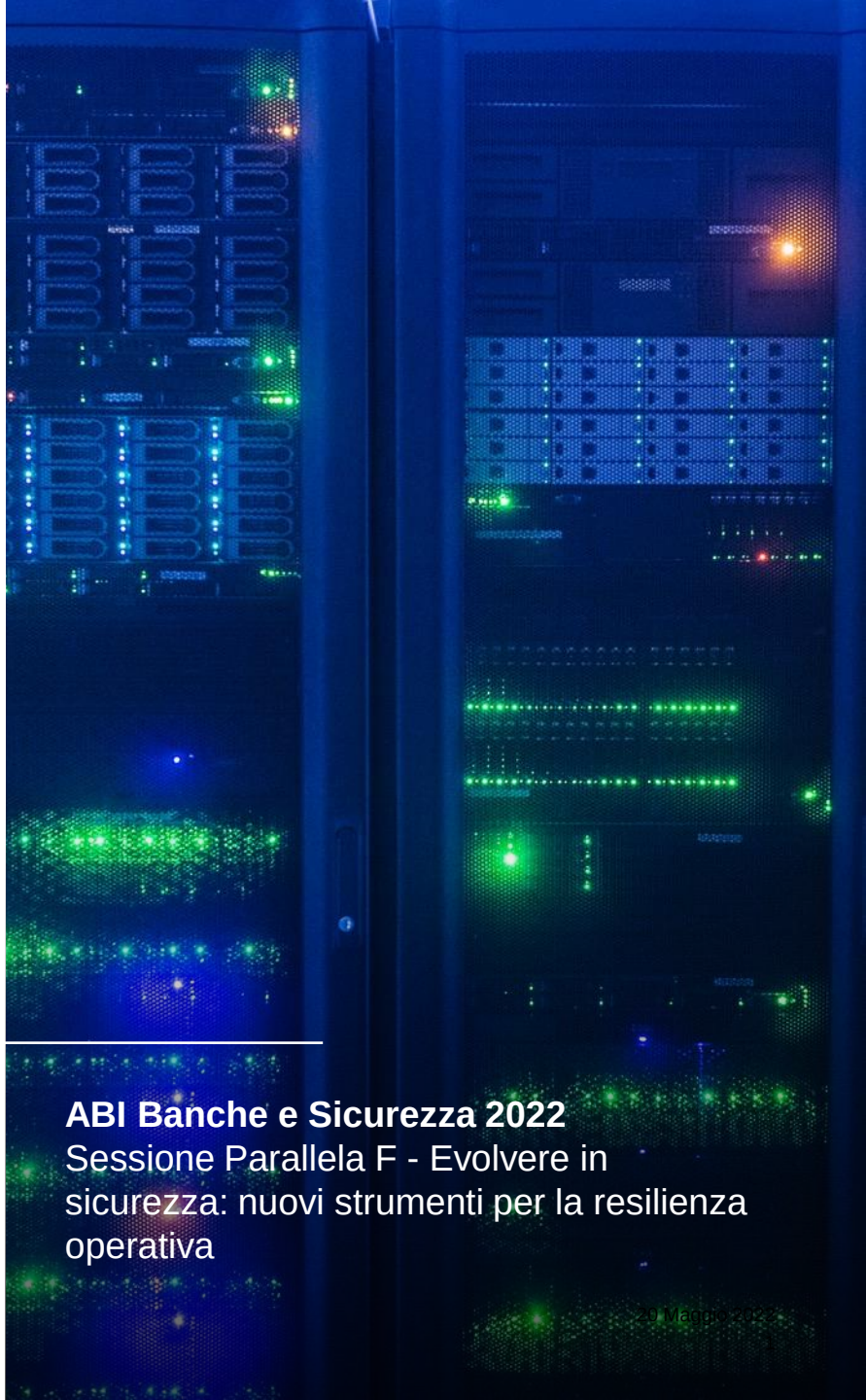
Il Regolamento DORA tra aspettative, percezione del mercato e soluzioni pratiche

Samantha Trama, Senior Manager – Cybersecurity & Privacy FS
20 maggio 2022



ABI Banche e Sicurezza 2022
Sessione Parallela F - Evolvere in sicurezza: nuovi strumenti per la resilienza operativa

PwC Security Survey: Digital Operational Resilience

30

Istituzioni Finanziarie


50% Banking


40% Insurance


10% AWM

Definizione dei Servizi ed analisi dei Rischi Cyber

Processi, Servizi ICT e Servizi di Business E-2-E

Il Dialogo tra Cyber e Risk Management

Framework Cyber Risk ed aspetti metodologici

Threat Intelligence & Incident Response

Servizi Threat Intelligence

Early Warning ed Incident Management

Follow up, Perdite Operative e dialogo con il Top Management / BoD

Business Continuity

Posizionamento organizzativo Business Continuity

Modellizzazione degli Scenari

Verifiche di Sicurezza e TLPT

Gestione Sicura delle Terze Parti

Info Sharing

La vostra percezione del Regolamento DORA

100%

Opportunità per attivare temi legati alla **Cyber Hygiene**

50%

Opportunità per evidenziare l'importanza delle **competenze** e dello **staffing Cyber**

40%

Over Regulation

6%

Opportunità per **visibilità** verso il **BoD / Top Management**

Processi, Servizi ICT e Servizi di Business E-2-E

- DORA contribuisce all'**aggiornamento dei processi** verso una migliore **rappresentazione dei servizi vs. Clientela**
- Solo **1 organizzazione su 5** ha già previsto la modellizzazione dei **Servizi di Business** in ottica **End-to-End**
- Le maggiori difficoltà di definizione derivano da un'**attuale** scarsa **integrazione** nei **modelli esistenti**
- **Approcci teorici complessi**, non correlati ai modelli aziendali, possono portare ad un'**effort elevato senza applicabilità** pratica e tangibile
- Una corretta **prioritizzazione delle attività di analisi** può essere effettuata partendo dai modelli di valutazione già esistenti **capitalizzando** gli **investimenti** effettuati nel **tempo**
- Fondamentale l'**ottimizzazione dei processi ICT** per ricostruire la catena tecnologica ed avere una corretta visibilità delle interdipendenze e dei flussi dati

22% Definizione ed aggiornamento dei **Servizi di Business** erogati alla clientela, **correlati** con i **processi** in logica **End-to-End**, i servizi Operations, ICT e Cyber e relativa catena tecnologica

34% Definizione ed aggiornamento dell'**alberatura dei processi** secondo standard di settore, **correlazione** e definizione delle interdipendenze con i processi **Operations, ICT e Cyber** nonché della relativa **catena tecnologica**

11% Definizione ed aggiornamento dell'alberatura dei **processi** aziendali secondo standard di settore e dei **Servizi ICT e Cyber senza correlazioni specifiche**

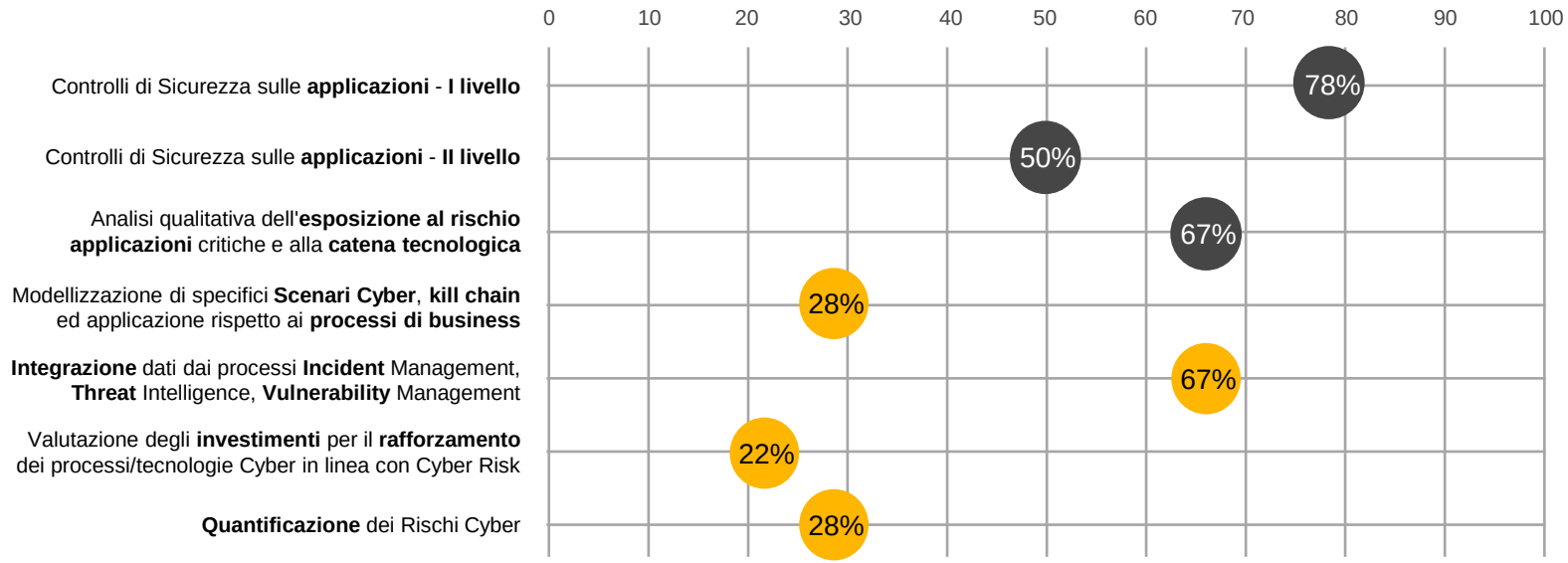
11% Definizione ed aggiornamento dell'**alberatura dei processi aziendali** secondo standard di settore

22% Definizione ed aggiornamento dei **Servizi ICT e Cyber**

Cyber Risk

83%

Collaborazione tra Sicurezza e Rischi Operativi con differenti scope di valutazione



Security
Scope Tecnologico

Op Risk
Impatto Business

- La collaborazione **tra Cybersecurity e Risk Management** è **coerente** con l'applicazione con le **metodologie tradizionali** di valutazione dei rischi, per cui le **analisi tecnologiche** della sicurezza sono input alla **modellizzazione dei rischi operativi.** Tali **rappresentazioni non** risultano, da un punto di vista **Regulatory**, **adeguate** a **rappresentare** i **rischi reali** sottostanti**.**
- La modellizzazione degli scenari **Cyber**, tramite attività di **Threat Modelling**, è fondamentale per ricostruire gli **impatti** rispetto ai **servizi** erogati alla **clientela** e loro **quantificazione**, nonché per indirizzare **investimenti adeguati**

Business Continuity

60% **Posizionamento all'interno della Funzione di Sicurezza**

70%

Scenari di **indisponibilità** derivanti dalle **normative**

- Non sempre implementate le soluzioni per tutti gli scenari di indisponibilità (20%).
- Scenari e soluzioni di contingency ad hoc vengono sviluppati per alcuni ambiti / processi specifici (20%).

40%

Scenario modelling in coerenza con analisi dei **rischi**

- Gli **scenari** considerati nei modelli di gestione della Continuità Operativa stanno **evolvendo progressivamente**: la **modellizzazione** di **scenari plausibili**, diversi dall'indisponibilità totale delle risorse, permette una maggiore **calibrazione degli investimenti** e nella **capacità di reazione** nel day-by-day.

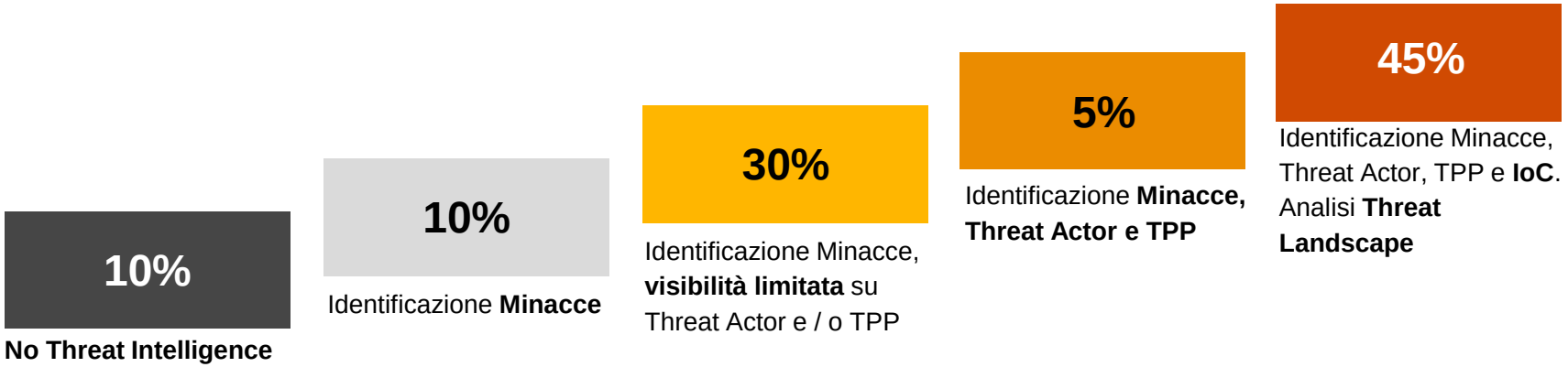
40% **Altro posizionamento organizzativo**

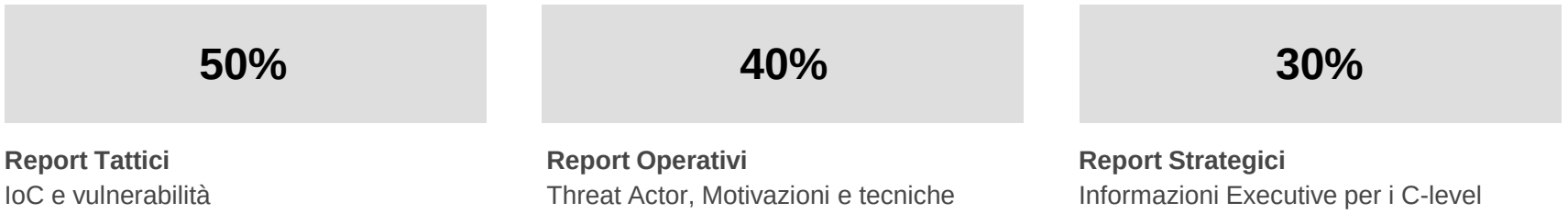
10%

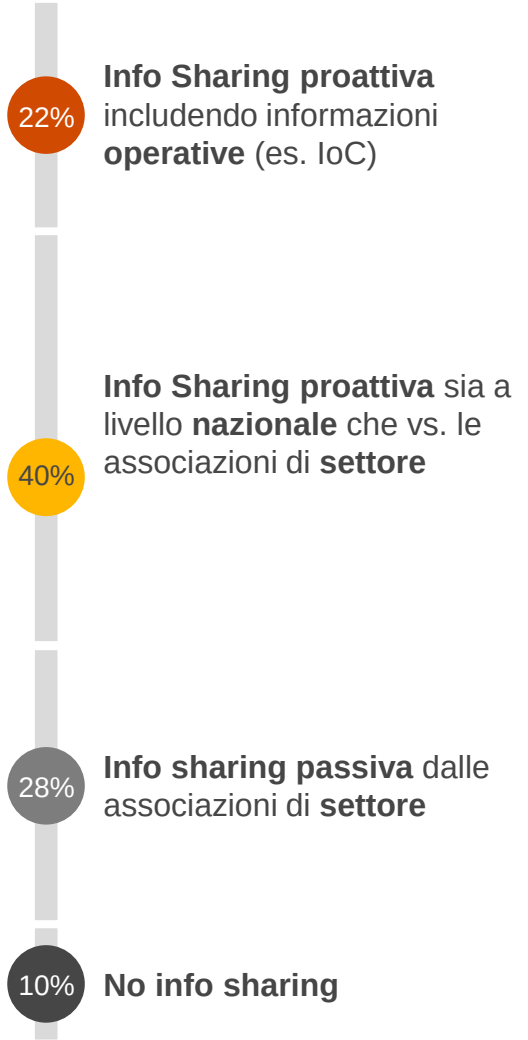
Integrazione degli **Scenari Cyber**

- L'integrazione con le attività di **Cyber threat e scenario modelling**, rispetto ai servizi forniti alla clientela, permettono l'identificazione di contromisure, protocolli di comunicazione e incident response cookbook specialistici.
- Integrazione favorita dal **posizionamento organizzativo.**

Threat Intelligence & Info Sharing







Esercitare attività di **Threat Intelligence** equivale nella maggior parte dei casi ad attivare una TI **«Incident Centric»** legata allo studio dei **feed - spesso con limitazioni informative -** provenienti dagli IoC **senza** attuare ulteriori **attività**, meno tattiche e **strategiche**, che potrebbero invece fornire informazioni su potenziali minacce che potrebbero impattare l'organizzazione, così da **indirizzare** in maniera **preventiva** e **predittiva** gli investimenti Cyber.

Incident Management, Reporting e Comunicazione

Incident Response

70% Integrazione dei Report TI tattici

45% Classificazione Regulatory-driven

40% Adozione tassonomie di settore (MITRE)

80% Monitoraggio dei sistemi critici

60% Monitoraggio dei sistemi non critici

60% Predisposizione Cookbook

67% Personale con skill specializzate

56% Blue Team esterni Incident Retainer

- **Processi e soluzioni** per la gestione degli **incidenti** stanno diventando sempre più **sofisticati**, enfatizzata dalla **scarsità** di **competenze** specialistiche.
- Una processo di **classificazione efficace** permette di affrontare in maniera consapevole **l'evento** tanto in termini di **impatto** quanto di **tecniche** di attacco sfruttate, così da agevolare le successive attività di **analisi** e **monitoraggio.**
- Una classificazione correttamente allineata ai **criteri dei Regulator** ed alle **tassonomie** di settore consente di **efficientare** i processi di incident **response**, **reporting**, nonché di produrre informazioni condivisibili nel rispetto dei nuovi indirizzi di **"knowledge share"** richiamati tanto dal **DORA** quanto dalla **NIS.**

Follow Up

70% Root Cause Analysis

50% Analisi Processi IR e Forensics

78% Avvio remediation IIIe Parti

- L'**analisi** approfondita in seguito alla **risposta** ad un evento permette di indirizzare azioni di rimedio **tecnologiche**, **operative** (incluse possibili azioni di **contingency**) nonché nei confronti delle **Terze Parti.**

Reporting

85% Modelli di Escalation e Reporting interna

67% Reportistica CdA

78% Reportistica Regulatory

45% Perdite Operative ed integrazione Rischi

- Il **Top management** è sempre più coinvolto anche nella **review post incident**, anche su temi tecnologici, con attenzione alle attività di remediation, valutazione dei rischi ed impatti operativi.

Comunicazione

6% Automatizzazione

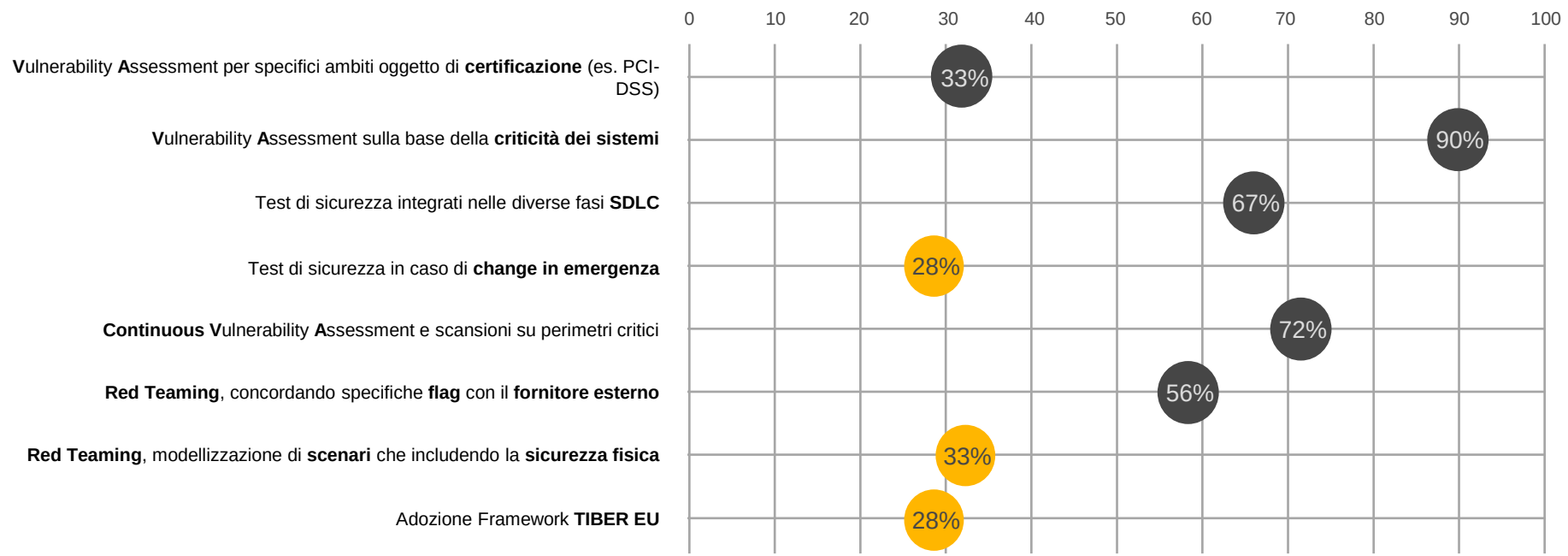
40% Predefinizione comunicazioni per scenari specifici

50% Responsabilità, canali e protocolli

6% Comunicazione gestita on demand

- La **comunicazione** verso la **clientela** è un processo **presidiato** ma che richiede **competenze** specifiche e **tecnologie abilitanti.**

Verifiche di Sicurezza & TLPT



- I **V**ulnerability **A**ssessment sono ancora le attività più **comuni** per testare la presenza di eventuali criticità di sicurezza.
- L'inclusione dei temi di **sicurezza fisica** all'interno delle verifiche di sicurezza e relativi scenari sottolinea la tendenza verso una **sicurezza convergente.**
- Particolare attenzione va dedicata alle verifiche di sicurezza in caso di **change in emergenza**, per una **sicura gestione** degli incidenti operativi **ICT.**
- L'adozione del framework **TIBER EU** diventerà **mandatoria**, integrando Targeted Threat Intelligence, Purple Teaming, valutazioni del Rischio Cyber e challenge ai processi di Incident Response.

Gestione Sicura delle Terze Parti

Pre Contract

67% **Due diligence** con valutazioni Cyber

Contract

50% **Clausole** di Sicurezza in funzione del **rischio**

83% **Clausole** di Sicurezza **standard**

Contracting

50% **Scenari specifici** per le IIIe parti

67% Inclusione nei **modelli BCM**

10% Terze parti incluse nelle verifiche di Sicurezza (VA / PT)

40% Outsourcer inclusi nei test BCM / DR

- **Consolidamento** delle **best practice** per la **sicurezza** nella gestione delle **esternalizzazioni**, da **estendere** anche alla gestione delle forniture e **terze parti.**
- L'integrazione dei **fornitori esterni** come **attori** dei **processi** di sicurezza è basilare per garantire un **corretto presidio** di tutti i rischi associati alla Supply Chain.
- Metodologie di **verifica tradizionali** dovranno essere associate all'inclusione dei fornitori nei **presidi e verifiche di Sicurezza** attualmente previste per gli **scope** gestiti **internamente.**

50% **Controlli** di sicurezza per **specifici scenari**

60% **Controlli** di sicurezza in funzione del **rischio**

40% **Controlli** di sicurezza per servizi **esternalizzati / Cloud**

50% Inclusione dei ruoli e responsabilità dei fornitori all'interno dei processi operativi di Sicurezza, riflessi negli obblighi contrattuali e condivisi con il fornitore

Modelli Tradizionali Evoluzione Resilience

Key takeaway

1

Dal 2020 abbiamo iniziato a seguire l'iter approvativo di **DORA** in quanto **opportunità** per il **Mercato** di **innovazione** e **rafforzamento** delle capability **cyber** del sistema finanziario.

2

Stiamo lavorando molto per costruire meccanismi di **community** a livello di Mercato, iniziando dalle **Pillole DORA** con l'**impegno** di mantenerne **aggiornamenti** ed organizzare **appuntamenti** di rilievo.

3

Dalla nostra esperienza il **ruolo del CISO** è fondamentale e **trainante** nel percorso verso la **Resilience** e, rafforzato da un sempre maggior coinvolgimento del **Top Management**, la roadmap evolutiva DORA è **abilitante** verso un **ruolo trasversale** e di sempre maggiore vicinanza al **business.**

Stay Tuned

https://www.pwc.com/it/it/services/consulting/digital-operational-resilience.html

Digital Operational Resilience Act

La Digital Operational Resilience Act (DORA) come nuovo paradigma europeo per un'efficace ed omnicomprensiva gestione dei temi Cybersecurity ed ICT nei Financial Services, secondo una visione olistica End-to-End basata sull'integrazione dei rischi e che comprende il presidio delle terze parti.

Governo e gestione delle Terze Parti

DORA si ispira ai principi TPRM nel presidio delle Terze Parti, introducendo inoltre nuovi poteri per le Autorità di Vigilanza

Digital Operational Resilience Testing

DORA definisce un programma onnicomprensivo di test di resilienza operativa digitale comprendendo gli aspetti Cyber ed inclusivo delle logiche Tiber EU.

I presidi delle prime linee di difesa ICT e Cybersecurity

Le Responsabilità delle 1e Linee di Difesa Cybersecurity ed ICT nel presidio End-to-End dei Rischi introdotto dal Regolamento EU DORA

La Gestione degli Incidenti ICT e Cybersecurity

DORA evolve la gestione degli incidenti IT e Cyber, richiamando le best practice, ed introducendo novità per la comunicazione e segnalazione alle Autorità.

Operational Resilience e le interconnessioni con il framework di Risk Management

Visione End-to-End del modello di Gestione dei Rischi Operativi, ICT e Cyber come game changer del Regolamento EU DORA.

Contesto di mercato ed implementazione del Regolamento

La view PwC sul contesto del Regolamento EU DORA, una priorità per i Financial Services date le novità in ambito Rischi Operativi, ICT e Cybersecurity.

Grazie

Samantha Trama
Senior Manager – Cybersecurity & Privacy FS
Cybersecurity Strategy & Governance Leader
DORA Integrated Solution Leader

+39 349 3360414
samantha.trama@pwc.com

pwc.com/it