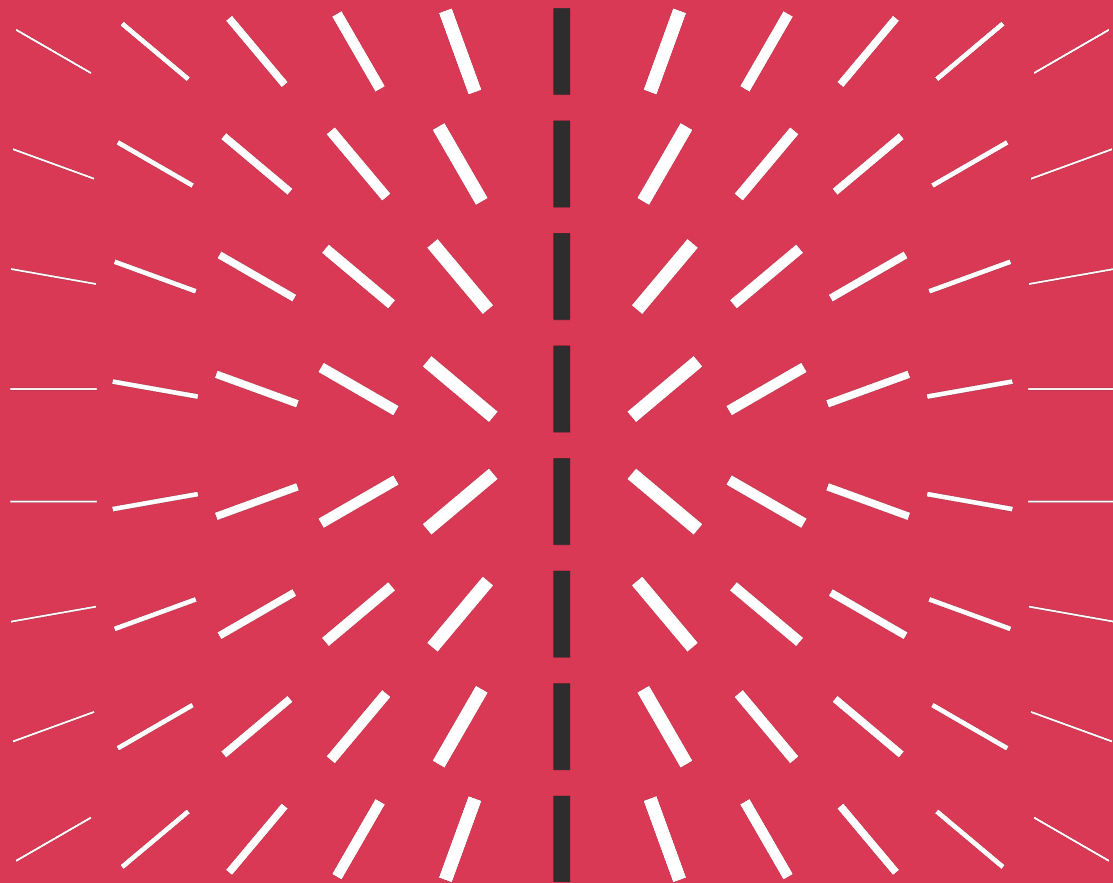


ABI Banche e Sicurezza 2023

Sessione Parallela C - La gestione degli incidenti alla luce dei requisiti normativi che spingono a sempre maggiore reporting dei problemi

Modelli integrati per la gestione degli incidenti

Milano, Auditorium Bezzi - Banco BPM
16 maggio 2022



La Gestione degli Incidenti nei nuovi requisiti del Regolamento DORA: una visione d'insieme



Ulteriori dettagli sono forniti nelle slide successive

Pillar DORA 2  **Gestione End-to-End dei rischi ICT**


Definizione ed adozione di una **strategia** di Digital Operational Resilience che includa **KPI, KRI** e **processi di monitoraggio**, con le seguenti **principali implicazioni**:

- Early warning
- Mappatura Business supportato da tecnologie ICT
- Analisi delle dipendenze con terze parti
- Analisi del rischio basata su scenari
- Integrazione metriche incidenti nei processi di governo
- Strategie di comunicazione
- Reporting rafforzato vs. BoD
- ...

Pillar DORA 3  **Gestione, classificazione e reporting degli incidenti**

Definizione di uno **standard**, a livello Europeo, di metodi, **processi** e **template** per il reporting di **incidenti** e **minacce**:

- Identificazione**: Threat intelligence e visibilità delle interdipendenze tecnologiche
- Protezione e Prevenzione**
- Detection**: Early Warning, detection proattiva e analisi del degrado delle performance
- Risposta e Recupero**: Identificazione, analisi e contenimento degli incidenti
- Miglioramento continuo**: Assessment dell'efficacia dei processi e definizione di azioni di rimedio
- Reporting**: Procedure di escalation, pianificazione delle comunicazioni, gestione reclami

Pillar DORA 4  **Digital Operational Resilience Test**

Conduzione di **test** di **Digital Operational Resilience** su **tutte** le **applicazioni** e **sistemi critici** ed **integrazione** delle **lesson learned** nell'ambito del processo di risk assessment.

- Vulnerability Assessment
- Penetration Test
- Network Security Assessment
- Wireless Assessment
- Cybersecurity & Privacy Assessment
- Compatibility Test
- Source Code Analysis
- Physical Penetration Test
- Threat Led Penetration Testing

Gestione degli Incidenti

Il cambio di paradigma nella gestione end-to-end dei rischi ICT impatta il processo di gestione degli Incidenti

Innovazioni introdotte

Inclusione dei **dati** derivanti dalla gestione degli incidenti delle **metriche di governo della resilienza** digitale, oltre che all'interno delle modalità di **valutazione dei rischi** digitali (quantificazione delle impact tolerances).

Il quadro per la gestione dei rischi informatici delinea i differenti **meccanismi introdotti per individuare e prevenire gli incidenti** ICT e per proteggersi dal loro impatto.

Il quadro per la gestione dei rischi informatici consente di **documentare il numero di incidenti ICT gravi** segnalati, nonché l'efficacia delle misure preventive.

Il quadro per la gestione dei rischi informatici delinea una **strategia di comunicazione in caso di incidenti ICT**.

Identificazione

- Visione per **servizi di business** (critical functions), mappatura processi, applicazioni (interdipendenze orizzontali / verticali), infrastrutture, endpoint, dati (evoluzione CMDB).
- Threat analysis & scenario management – definizione e modellizzazione degli scenari di attacco plausibili.

Individuazione

- Meccanismi di individuazione prevedono molteplici livelli di controllo, definiscono soglie di allarme e criteri per l'**individuazione e la risposta degli incidenti** e istituiscono meccanismi di allarme automatico per la risposta agli incidenti.
- Vengono **dedicate risorse e capacità** sufficienti al monitoraggio dell'attività degli utenti e **al verificarsi di anomalie e incidenti**.

Comunicazione

- **Responsabilità formale** per l'attuazione della **strategia di comunicazione per gli incidenti, portavoce** nei confronti del pubblico e dei mezzi di comunicazione.
- **Strategie di comunicazione predefinite**.

Risposta e ripristino

- **Risposta tempestiva, appropriata ed efficace per trovare una soluzione agli incidenti ICT**, per limitare i danni e privilegiare la ripresa delle attività.
- **Piani, procedure e capability dedicati che prevedano tecnologie, processi e misure di contenimento** idonei a ciascun tipo di **incidente ICT** e a scongiurare danni ulteriori.
- **Segnalazione dei costi e perdite causati da incidenti ICT (Autorità / CdA)**.

Politiche di backup e metodi di ripristino

- **Durante il ripristino successivo a un incidente** vengono **effettuate molteplici verifiche**, compresi i controlli incrociati, per assicurare il più elevato livello di integrità dei dati.

Apprendimento ed evoluzione

- **Personale con skill idonee** per analizzare **vulnerabilità** e impatti / cause degli **incidenti ICT**.
- **Follow Up:**
 - **Root cause analysis**
 - Aderenza ed Efficacia delle **procedure**
 - Ricostruzione della **kill chain** al fine di verificare l'efficacia dei **presidi** di prevenzione / protezione.
 - **Tempestività della risposta agli allarmi** di sicurezza e alla **determinazione dell'impatto** degli incidenti e della loro gravità.
 - **Qualità e alla rapidità dell'analisi forense**.
 - **Efficacia della comunicazione** interna ed esterna (incl. clientela).
 - **Revisione** degli **scenari** modellizzati per la gestione dei rischi.
 - **Identificazione dei miglioramenti** da apportare a tutti i diversi processi e tecnologie correlate.

- **Reporting** strutturato nei confronti del **CdA**.
- **Strategie, procedure, canali e tecnologie** per la comunicazione vs. **Clientela**.

La Gestione, Classificazione e Reporting degli Incidenti

Innovazioni introdotte

Armonizzazione a livello Europeo di **modalità, processi e template** per il **reporting** degli **incidenti** (FS – DORA e non FS – NIS2).

Descrizione del **processo** di gestione e relative **fasi, elevando le best practice/ framework** di settore a **livello regolamentare**.

Tassonomia e soglie comuni per la **classificazione** degli **incidenti ICT e Cyber**. **Template standardizzati** per la **notifica** di potenziali **minacce cyber**.

Supporto e feedback da parte delle Autorità in caso di incidenti.

Possibilità di **centralizzazione** in un **HUB** per la **segnalazione e reporting degli incidenti ICT/Cyber** a livello EU e partecipazione ad attività di condivisione delle informazioni.

NIST Cybersecurity Framework

Identify

- Integrazione informazioni threat intelligence (strategica ed operativa).
- Visibilità sulle interdipendenze tecnologiche e potenziali impatti.

Protect

Detect

- Indicatori di early warning.
- Rilevamento proattivo e tempestivo di attività anomale e degrado delle prestazioni in un sistema, rete, etc. (e.g. *tramite SIEM, IDS/IPS, Antivirus*).
- Classificazione degli incidenti sulla base di criteri forniti dalle Autorità

Respond

Rilevamento, analisi e contenimento dell'incidente per garantire la mitigazione dell'incidente ed il ripristino tempestivo dell'operatività dei sistemi impattati (e.g. *tramite DDoS Protection, SOAR, Endpoint Protection*).

Recover

- Valutazione dell'efficacia dei processi e capability.
- Integrazione di nuovi scenari di rischio.
- Definizione di azioni di rimedio.
- Condivisione delle informazioni a livello di mercato.

Reporting e Comunicazione

- Gestione dei reclami.
- Notifica e segnalazione di incidenti gravi alle Autorità.

Gli impatti dell'integrazione DORA sulle modalità di gestione degli incidenti

- **Modellizzazione di scenari cyber**
- **Implementazione** processi di **Cyber Threat Intelligence** (strategica/operativa).
- **Mappatura e manutenzione** di tutti i servizi di business, **processi**, relativa catena tecnologica e dipendenze da fornitori terzi.

- **Predisposizione** di meccanismi di generazione e **monitoraggio** dei **log** di sicurezza, anche su base **predittiva**.
- Definizione di **indicatori di early warning**
- **Classificazione degli incidenti** integrata con le **metriche di gestione dei rischi** e con le **soglie** di impatto definite dalle autorità

- **Definizione** di una **politica** di **backup** dei **dati**, modalità e procedure per la **ricostruzione dei dati**
- **Adozione** di **strumenti** e **metodologie** che garantiscano il **minor tempo** possibile per il **ripristino dei dati**.

- **Definizione piani di comunicazione** ed escalation interna.
- **Implementazione** processi di **reporting** interna (CdA) ed esterna.
- **Reporting vs. Autorità**
- Procedure e canali di **comunicazione vs. clientela finale**

Identificazione

Protezione e Prevenzione

- **Asset visibility**
- Implementazione di **processi e tecnologie di protezione / prevenzione**, anche in riferimento agli **specifici scenari definiti** (e.g. segregazione della rete)

Individuazione

Risposta e Ripristino

- **Capability specialistiche**
- Misure di **contenimento**
- Definizione di **playbook** e procedure di Incident **Response** per gli scenari definiti
- Definizione di **procedure di IT Continuity** e di
- **Procedure di contingency** per ogni scenario / servizio
- **Integrazione** dei processi di gestione degli **incidenti cyber** con **event & crisis management** (allineamento metriche, responsabilità).

Backup e Ripristino

Apprendimento ed Evoluzione

- **Miglioramento continuo**, tramite la valutazione delle risultanze dei test e lesson learned.
- Integrazione delle **metriche di governo** della resilienza digitale (KPI; KRI)
- **Quantificazione delle perdite**
- **Verifiche incrociate** con i risultati dei test **Digital Operational Resilience**
- Necessità di **verificare tutte le fasi ed integrazioni dei processi di gestione**, supportato dai test TLPT

Reporting e Comunicazione

Focus sul Pillar 4: Digital Operational Resilience Testing

Innovazioni introdotte

Tutte le applicazioni e i sistemi ICT critici devono essere sottoposti a test di Digital Operational Resilience

Vulnerability Assessment

Wireless Assessment

Source Code Analysis

Penetration Test

Cybersecurity & Privacy Assessment

Physical Penetration Test

Network security Assessment

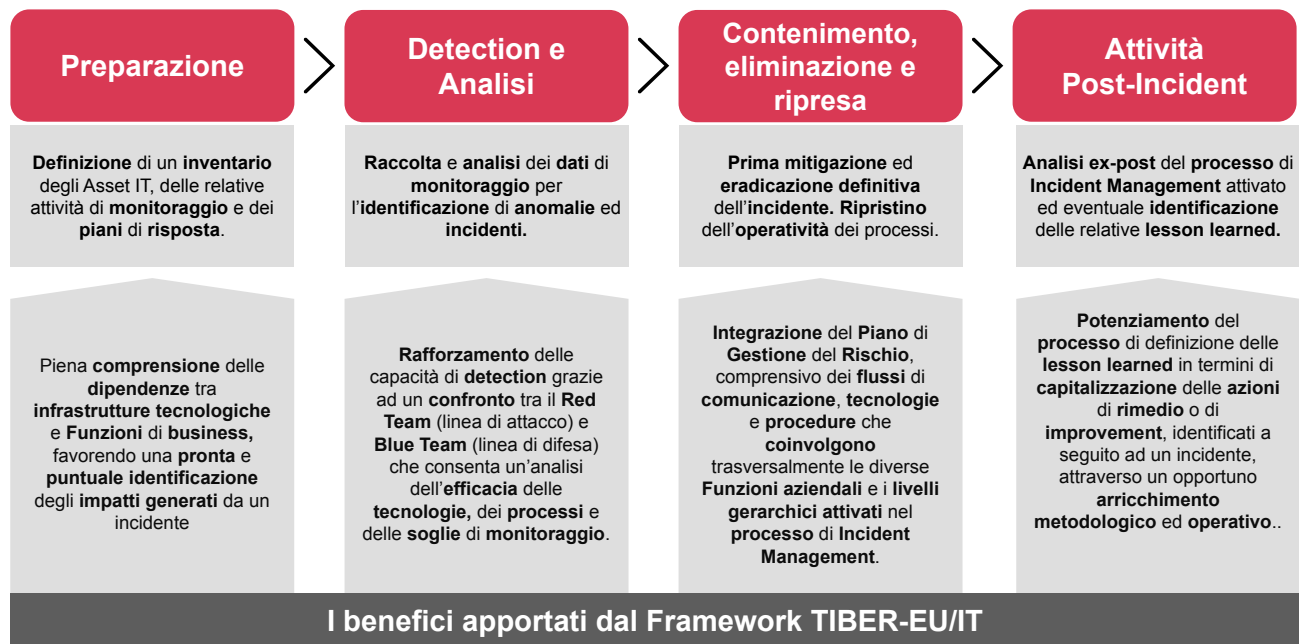
Compatibility test

Threat Led Penetration Testing

- I Threat Led Penetration Testing (TLPT) consistono in vere e proprie simulazioni di attacco, che devono essere svolte secondo quanto stabilito nel Framework TIBER-EU/IT.
- Le Entità Finanziarie chiamate a svolgere test TLPT vengono selezionate dalle autorità competenti sulla base di criteri predefiniti (*).

Lo svolgimento dei Threat Led Penetration Testing (TLPT) abilita una **consapevolezza olistica e trasversale** rispetto a **processi, tecnologie e metodologie** afferenti l'intero ciclo di vita dell'Incident Management:

Ciclo di vita dell'Incident Management



Un caso pratico: la gestione dei Ransomware

L'**approccio olistico** definito dal **DORA** rappresenta il primo tentativo da parte di un Regulator di disciplinare le diverse competenze necessarie ad affrontare le nuove tipologie di minacce cyber.

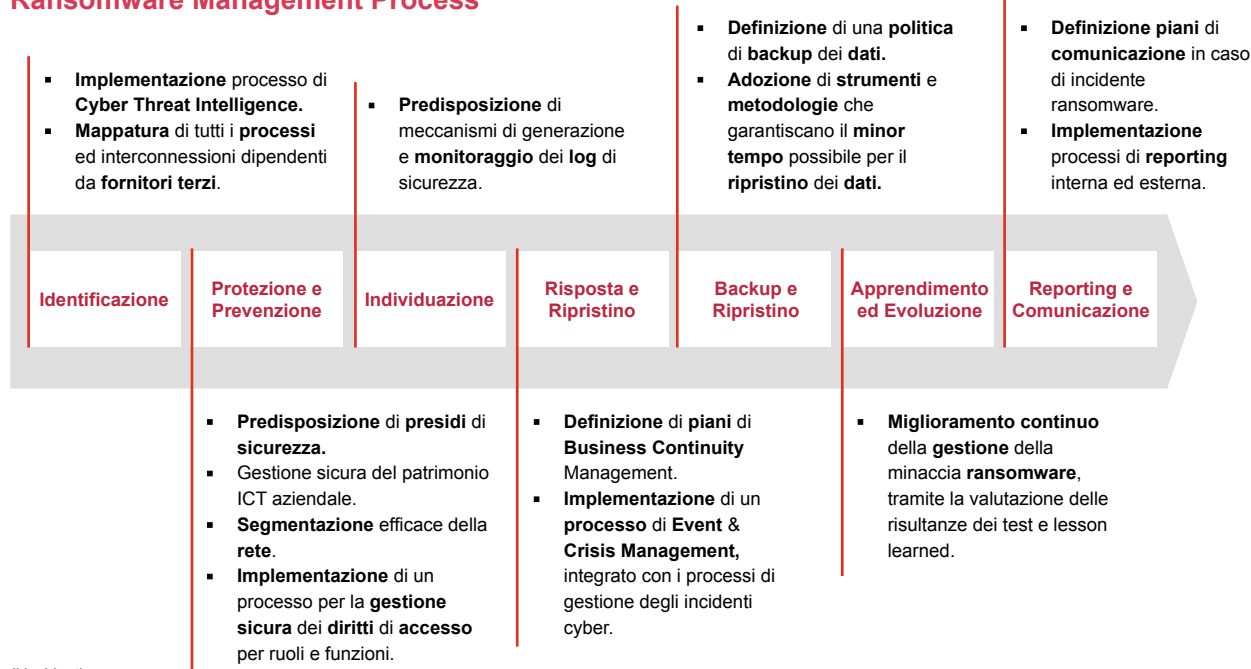
Perché il Ransomware

La minaccia cyber più rappresentativa degli ultimi anni è sicuramente il **Ransomware**, tipologia di malware, che per impatto ed efficacia si è imposta ed è diventata preponderante. I **potenziali impatti** che può produrre un **Ransomware** non sono relegati esclusivamente alla sicurezza, ma riguardano la **totalità** delle **principali Funzioni Aziendali** in quanto tali eventi possono produrre rilevanti **ripercussioni economiche, legali e reputazionali**.

Perché DORA

In virtù di tali considerazioni, si rende **necessaria** l'**adozione** di un **approccio olistico esteso** alle **principali Funzioni Aziendali**, per gestire il fenomeno Ransomware. Si riporta quindi una **vista integrata** delle attività previste dal DORA e volte alla gestione dei Ransomware e delle relative funzioni aziendali responsabili.

Ransomware Management Process





Key Takeaway

1

Completezza informativa della mappatura dei Servizi aziendali End-to-End, processi, operations trasversali e relativa catena tecnologica.

2

Sinergia operativa e metodologica tra le diverse linee di difesa.

3

Potenziamento dei flussi di comunicazione interni ed esterni.

4

Integrazione dei modelli e metriche nella più ampia gestione della digital resilience.

Grazie

Paolo Carcano

Partner | Cyber Security & Privacy FS

paolo.carcano@pwc.com

Dante Niro

Director | Cyber Security & Privacy FS, Security
Emerging Technology Leader

+39 348 1540416

dante.niro@pwc.com

[pwc.com/it](https://www.pwc.com/it)