# Digital Operational Resiliency Act

## La value proposition e l’approccio per la definizione di un programma di «DORA Compliance in a Box»

# Zero Trust | La strategia che indirizza le attuali sfide più importanti degli Enti Finanziari in ambito Sicurezza IT

## Principali sfide in ambito Sicurezza Informatica

Enterprise
**Security Strategy**

Rendere sicuro tutto l'ecosistema aziendale

Hybrid
**Workforce**

Garantire agli impiegati e Terze Parti l'accesso ai sistemi sempre

Network
**Edge Transformation**

Proteggere le reti in un perimetro sempre più ampio

Crown Jewel
**Data**

Proteggere i dati critici ovunque risiedano

Advanced Threats
**& Ransomware**

Rispondere ad attacchi informatici e aumentare la resilienza informatica

Privileged
**Access**

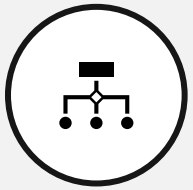
Gestire l'accesso elevato a sistemi e ai workloads critici

Cloud
**DevSecOps**

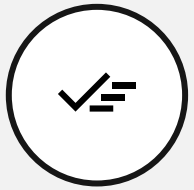
Sviluppare e rilasciare soluzioni sicure

## Principi Fondamentali Zero Trust

**Realizzazione superficie protetta** inclusi dati e applicazioni

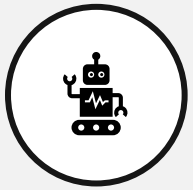


**Mapping transazioni e dati sensibili** per scoprire come si muovono i dati tra identities e applicazioni



**Architettura Zero Trust per ogni microperimetro**, reti Software-Defined (SDN) e protocolli di sicurezza che utilizzano firewall fisici o virtuali

**Policy Zero Trust post realizzazione reti**, usando per es. metodo Kipling, che prende in esame chi, cosa, quando, dove, perché accede alle reti



**Monitoraggio** di tutto il traffico anomalo, **automazione** e **manutenzione** dei processi di ispezione e analisi

# Una strategia end-to-end orientata verso il controllo di tutti i sei elementi fondamentali del digital asset interno consente di presidiare i 5 key pillar di DORA

### Identità

**Persone, Servizi o dispositivi IOT**: in caso di accesso ad una **risorsa**, è necessario verificare l'identità con **autenticazione forte** che garantisca che l'accesso sia **conforme alle policy di sicurezza**

### Device

I dati possono fluire su una **varietà di device diversi**, (dispositivi IoT smartphone, dispositivi in Cloud, ecc..). Necessario monitorare costantemente lo **stato di salute e la conformità dei dispositivi**

### Applications

Applicazioni ed API sono l'interfaccia per l'utilizzo dei dati. Necessario garantire che esse siano **correttamente funzionanti**, monitorando eventuale **comportamento anomalo** o **azioni anomali dell'utente**

### Infrastructure

L'infrastruttura (on-premise, VM, container o Cloud) rappresenta un ***vettore critico per eventuali minacce***. Necessario **valutare le versioni, le configurazione e modalità di accesso** per rafforzarne la sicurezza

### Data

La sicurezza dei dati è tra gli obiettivi principali della Cyber Security. Necessario garantire che i dati siano **classificati, etichettati e criptati** e che l'**accesso** agli stessi sia disciplinato in base alle **policy di sicurezza**

### Network

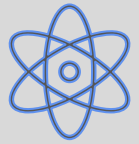
Tutti i dati sono infine **accessibili tramite l'infrastruttura di rete**. Necessario **prevenire attacchi alla rete**: buone pratiche prevedono la segmentazione e la crittografia end-to-end delle stesse

ICT Risk Management Framework

Digital Operational Resilience Testing

ICT Incident Reporting

Outsourcing & Third Party Risk



Information Sharing

IBM

# La definizione di una Test Strategy è indispensabile per l'identificazione di linee guida, processi, strumenti e per la pianificazione di dettaglio di tutte le fasi di test

L'obiettivo di una strategia di test è descrivere l'approccio end-to-end di test del ciclo di sviluppo del software, che garantisca a tutti gli stakeholder la comprensione dell'approccio globale, degli strumenti, dei target e dei tempi delle attività di test

## Principali obiettivi della Strategia di Test

Definizione test **scope**, **portata** dei test e degli **obiettivi** degli **sprint**

Definizione **ambienti** di test, **strumenti** di test, i **dati** di test e **configurazioni**

Pianificazione **attività** di **test** e definizione della **frequenza** dei **test**

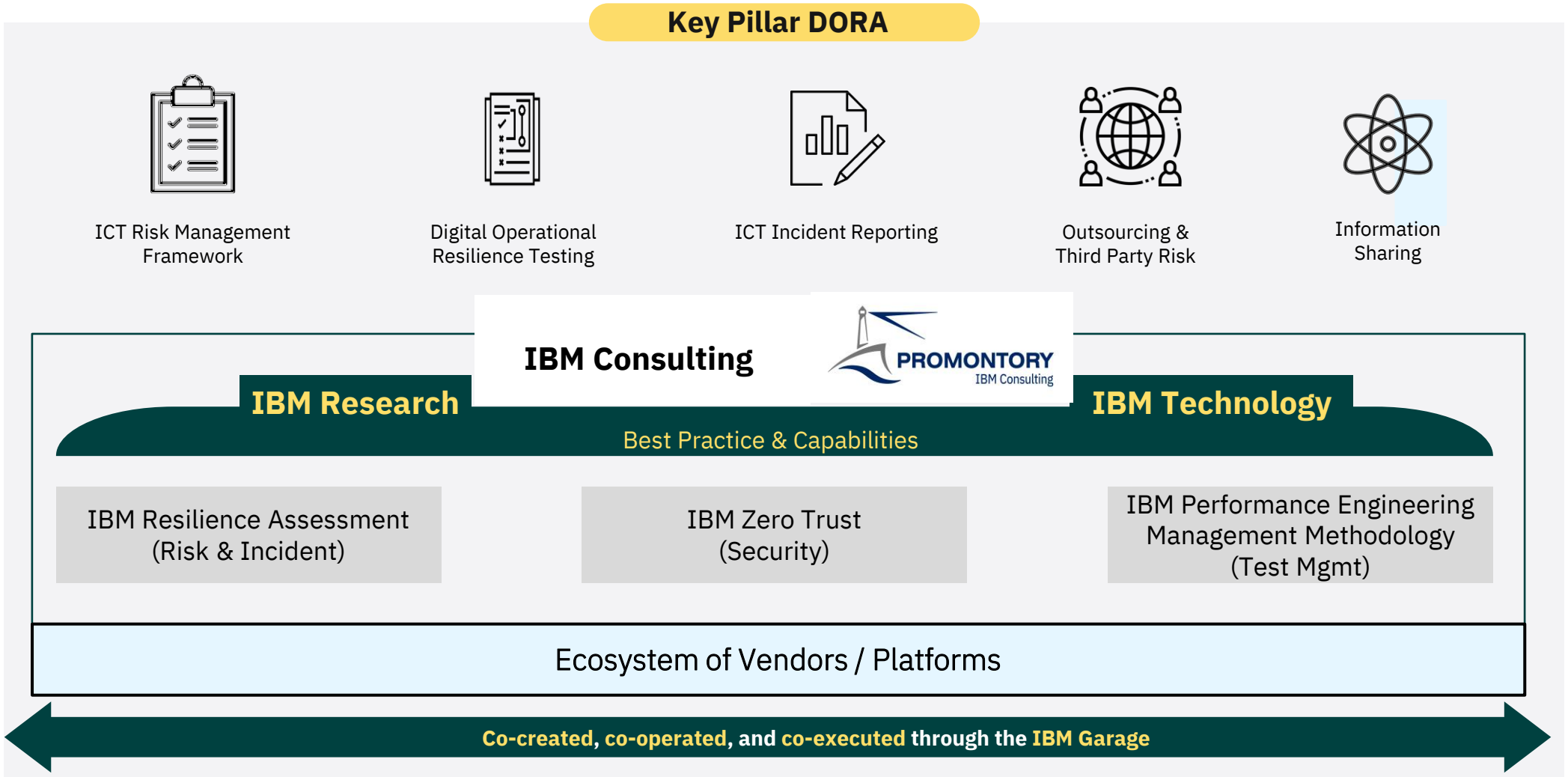
Determinazione dei **prerequisiti**: es **vincoli**, **competenze** e **formazione** utenti

Identificare **dipendenze** come **funzioni**, **codice**, **componenti** di sistema, **fornitore**, **tecnologia**, **strumenti**, **attività**, **team, tipi di test**

Impostare le **priorità** considerando l'importanza del **cliente/utente** e le dipendenze

Identificare le **micro-attività** di **dettaglio** per ogni **pianificazione** sprint

# IBM e la Resilienza Operativa Digitale: la nostra Value Proposition per la realizzazione di una «DORA Compliance in a Box»



# L’approccio per la definizione della Dora Compliance in a Box prevede quattro fasi progettuali

## PRINCIPALI ESIGENZE

- Comprendere e analizzare gli attuali **framework** di **gestione E2E** del **rischio**
- **Identificare** possibili **macro gap** da colmare per essere «**Dora Compliant**»
- Valutare l’attuale **capacity interna** a fronte di possibili **adeguamenti** alla **Governance** e ai **Processi attuali**
- Qualificare, pianificare e prioritizzare gli **adeguamenti** per attuare gli interventi del **Remediation Plan**

## Dora Compliance in a Box | Approccio progettuale

### 1 Set-up e analisi contesto

1.1. Set-Up **Progetto** e **Governance**

1.2 **Presentazione tool** di assessment per **Dora Healthcheck**

ZOOM #1

### 2 Raccolta dati per analisi

2.1 Pianificazione delle **interviste** gli SME

2.2 Raccolta **dati** e **compilazione** del **tool** di **Dora Healthcheck**

2.3 Raccolta **principali contratti con i Fornitori Terzi**

2.4 Conferma **primo perimetro dati raccolti**/eventuale **fine tuning**

### 3 Elaborazione dati e analisi di dettaglio

3.1 **Analisi** di **dettaglio** dei dati raccolti

3.2 Analisi di **dettaglio** dei **principali contratti con i Fornitori Terzi**

3.3 Predisposizione **valutazione** di **dettaglio** e **sintesi** per **ogni Funzione**

3.4 **Presentazione** e **discussione** dello **scoring**

### 4 Presentazione Remediation Plan

4.1 Qualifica degli **interventi** di **adeguamento**

4.2 Definizione della **roadmap** di **adeguamento**

4.2 Presentazione del **Remediation Plan**

## Dora Compliance in a Box | Principali acceleratori messi a disposizione

Visione **strategica** in ambiti **trasformativi** e di **change mgmt**

Profonde **conoscenze** di **Industry**, **processi**, **tecnologica** e ambito **Compliance** & **Risk Mgmt**

Profonde **competenze** ed esperienza in **area Legal**

Disponibilità **accesso** a **team** e **best practice global**

Utilizzo **specifici Capability Model** per **assesment tecnico-funzionali** (e.g. DORA Healthcheck)

# IBM ha già definito un modello di assessment (HealthCheck) per effettuare una gap analysis e identificare un remediation plan

| Pillar DORA | II livello di analisi |
|---|---|
| I **ICT Risk Mgmt Framework** | ▪ **Governance** e **organizzazione**<br>▪ Quadro per la gestione dei **rischi informatici**<br>▪ **Sistemi**, **protocolli** e **strumenti ICT**<br>▪ **Identificazione**, **protezione** e **prevenzione**, **individuazione**, **risposta** e **ripristino**<br>▪ Politiche e **procedure** di **backup**<br>▪ **Apprendimento** ed **evoluzione**<br>▪ **Comunicazione** |
| II **ICT Incident Reporting** | ▪ Processo di **gestione** degli **incidenti ICT**<br>▪ **Classificazione** degli **incidenti ICT** e delle **minacce informatiche** |
| III **Digital Operational Resilience Testing** | ▪ Test di **strumenti** e **sistemi ICT**<br>▪ Test **avanzati** di **strumenti**, **sistemi** e **processi** ICT basati su **test** di **penetrazione guidati dalla minaccia** (TLPT)<br>▪ Requisiti per **i soggetti incaricati** dello **svolgimento** dei **test** TLPT |
| IV **Outsourcing & Third Party Risk** | ▪ Principi **fondamentali** di una **solida gestione** dei **rischi informatici** derivanti da **terzi**<br>▪ **Valutazione preliminare** del **rischio** di **concentrazione** delle **TIC** a livello di **entità**<br>▪ **Principali disposizioni contrattuali** |
| V **Information Sharing*** | ▪ Disponibilità di una **data platform** che consenta **esposizione** di **dati** in **modo sicuro** e **industrializzato**<br>▪ Adeguata **maturità** delle pratiche **di Data Mgmt / Data Governance**, e.g., **policy** di **governo** per **esposizione dati differenziata**<br>▪ Presenza di **processi** di **audit trail** e **data lineage** che consentano **certificazione** e **verificabilità** dei **dati esposti** |

**DORA HealthCheck Radar**

*Scoring Ente impattato*

CONCETTUALE E ILLUSTRATIVO

Attraverso l'utilizzo del «**DORA HealthCheck**» è possibile:

- **analizzare** gli **attuali framework** di **Risk**, **Incident**, **Test Mgmt** e di **Third-Party Risk Mgmt** per identificare l'**aderenza** del **landscape funzionale** e **applicativo/infrastrutturale** al Regolamento
- **identificare** possibili **adeguamenti** da **attuare**
- **pianificare** e **prioritizzare** le **attività** inerenti il **Remediation Plan**

*Adesione al pillar su base volontaria; non incluso nel Dora Healthcheck

# What’s the next?... DORA Tabletop

Supportare le organizzazioni a gestire in modo proattivo i rischi informatici, migliorare la capacità di reazione operativa e garantire la conformità normativa conducendo DORA Tabletop Exercise

## 1 Governance

**Valutare la risposta di un'organizzazione a una crisi che coinvolge dirigenti e decisori di alto livello.**

Coinvolgere il consiglio di amministrazione e i capi dipartimento sviluppando scenari di interruzione realistici e pertinenti che simulano diversi tipi di minacce e crisi che potrebbero influire sulla resilienza e sulla conformità dell'organizzazione.

## 2 Operational

**Focus sugli aspetti operativi che testano la capacità di garantire la continuità di funzioni e servizi aziendali critici.**

Verificare la prontezza, la risposta e la resilienza delle operazioni aziendali, IT e di sicurezza informatica per servizi e piattaforme specifici, nonché la comunicazione e il coordinamento con altri dipartimenti come sicurezza, legale/conformità e comunicazione esterna.

## 3 Organizational Responsiveness

**Verificare la capacità di rilevare, contenere e rispondere a un attacco e migliorare la reattività e la gestione delle minacce.**

Personalizzato in base ai requisiti specifici, l'obiettivo è valutare gli aspetti tecnici di un incidente informatico valutando e testando i controlli tecnici implementati, le procedure di risposta agli incidenti e i protocolli di comunicazione

# Benefits - Migliorare la comunicazione e il coordinamento tra i team, migliorando la resilienza informatica complessiva dell'organizzazione

| Refining | Improving | Stress Testing | Enhancing | Preparing |
| --- | --- | --- | --- | --- |
| Identificare eventuali punti deboli e lacune in sospeso relativi al DORA Remediation Plan prima dell'applicazione del regolamento (Gen '25) | Comunicazione, coordinamento e processo decisionale tra le parti interessate aziendali, operative e di sicurezza durante una crisi. | Stress test del DORA Remediation plan & recommendations | Resilienza informatica complessiva e capacità di prevenire, rilevare, contenere e rispondere alle minacce informatiche. | L'organizzazione per gli audit e le valutazioni regolamentari e per ridurre il rischio di multe e sanzioni. |