

Roma, 20 marzo 2024

DORA: il nuovo Regolamento europeo sulla Resilienza Operativa Digitale per il settore dei Financial Services

- *Le regole europee per la Resilienza Operativa Digitale nel Settore Finanziario*
- *Gli impatti operativi derivanti dagli adeguamenti richiesti dal 40° aggiornamento della Circolare 285/2013 della Banca d'Italia e dal Regolamento DORA*

Chi sono:



Valerio Tomasoni

*Organization, IT & Security Manager
Business Continuity Manager
Change & Incident Manager*

Contributor AIEA_{for}DORA

AGENDA



ISACA
AIEA | Milan Chapter

- ☐ **Chi è AIEA**
- ☐ **L'attenzione del Regolatore al tema della Resilienza Operativa Digitale**
- ☐ **1° Verticale - Resilienza vs Continuità Operativa**
- ☐ **2° Verticale - Framework IT Management**
- ☐ **Il Progetto «AIEA_{for}DORA»**
- ☐ **Pubblicazioni**



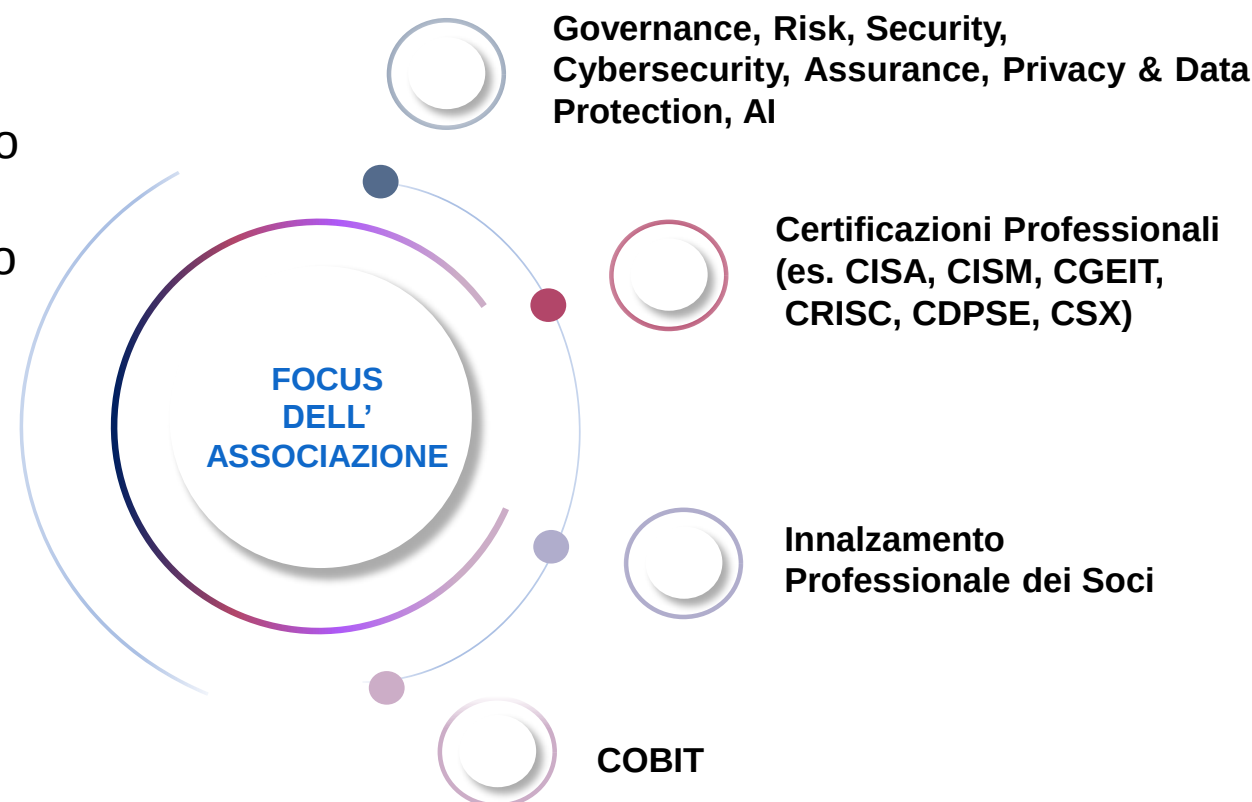
AIEA: l'associazione italiana degli Information Systems Auditors

Associazione No Profit attiva sui temi dell'IT e dell'Information Security, fondata nel 1979 a Milano, che aderisce a ISACA diventando il Capitolo di Milano, primo capitolo europeo per ISACA. Dal 6 Aprile 2022, iscritta al RUNTS (Registro Unico Nazionale Enti Terzo Settore), cambiando la sua denominazione in AIEA ETS

1000+ Soci in tutta Italia e Canton Ticino

ISACA – Associazione Internazionale di Professionisti che operano su tematiche IT/IS, che conta oggi 170.000 Soci e 225 Capitoli nel mondo.

Nel 2022, nasce **ISACA Europe**, basata a Dublino, a cui fanno capo 30.000 Soci e 45 Capitoli



Contesto normativo fine 2022



DORA, Circ. 285/40° e NIS 2

	OBIETTIVI	PRINCIPALI NOVITÀ	DESTINATARI
DORA	Migliorare la gestione del rischio ICT e la resilienza operativa digitale nel settore finanziario.	- Obblighi di governance e risk management per la sicurezza ICT. - Piani di resilienza operativa digitale per gestire e rispondere agli incidenti ICT. - Supervisione da parte delle autorità competenti.	- Enti Creditizi - Imprese di Investimento
Circ. 285/40°	Recepire gli orientamenti EBA, Risk Mangement ICT dedicato	- Proattività del RM - Nuovi ruoli e responsabilità nella gestione dei rischi ICT - Gestione del rischio in change e progetti	- Compagnie di Assicurazione - Prestatori di servizi di pagamento
NIS 2	Aumentare il livello di sicurezza delle reti e dei sistemi informativi in tutta l'UE.	- Misure di sicurezza per reti e sistemi informativi. - Obblighi di notifica degli incidenti informatici. - Cooperazione tra gli Stati membri.	Altri settori Merceologici (NIS 2)

DORA

«Digital Operational Resilience Act»



I destinatari DORA

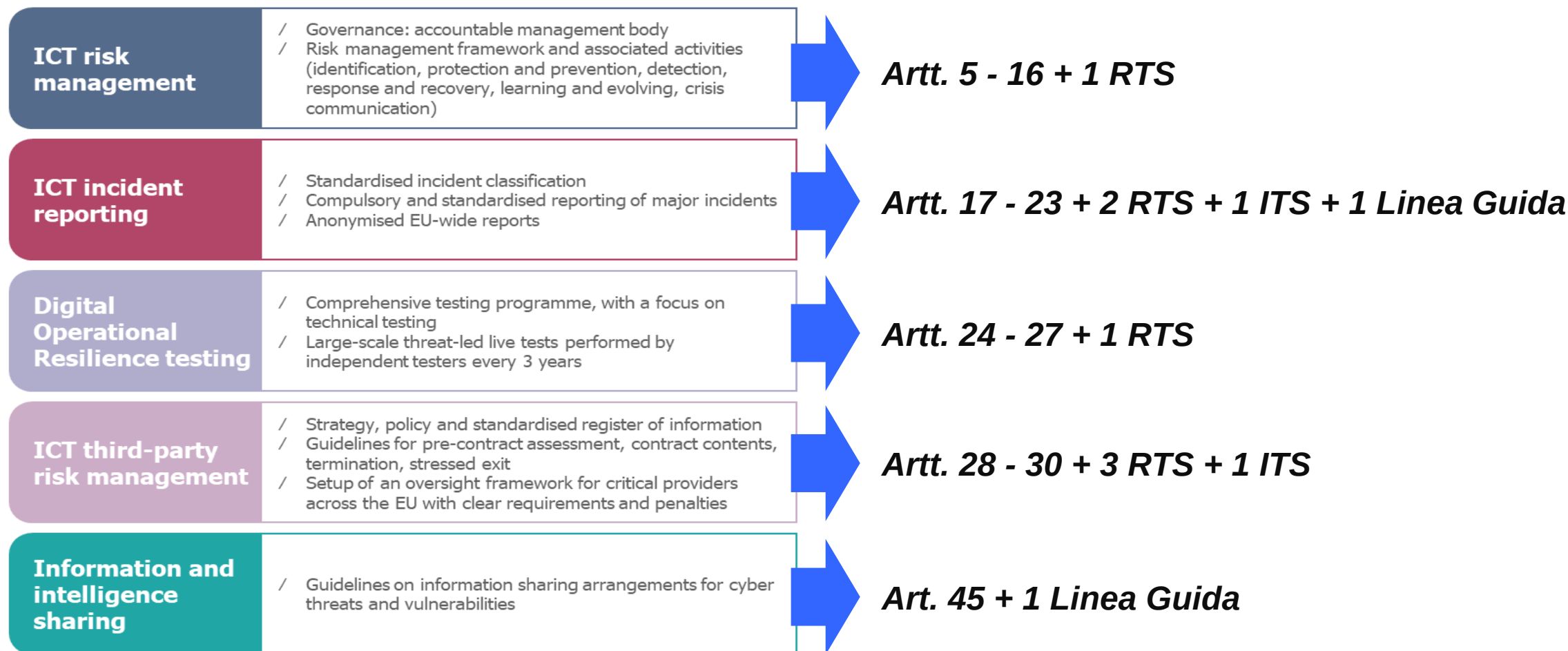
Si stima un impatto su **oltre 22.000 aziende** tra:



Banche, Assicurazioni e Intermediari... ma non solo!!!

Rif. Art. 2, Par.1, Lett. u) del Regolamento

I 5 Pillars DORA



DORA:

«Digital Operational Resilience Act»

La crescente digitalizzazione del Settore Finanziario alla base d DORA:

- **Aumento dell'uso di tecnologie digitali** da parte di banche, assicurazioni e altri intermediari finanziari;
- **Interconnessione** di Organizzazioni, Prodotti e Servizi;
- **Nuovi rischi** informatici e cyber-attacchi, anche su scala globale.



OBIETTIVO

Governance,
Risk, Security,
Cybersecurity,
Assurance,
Privacy, AI



FINE "GRACE PERIOD"

17 Gennaio 2025



DESTINATARI

Banche,
assicurazioni,
operatori di
criptovalute, ecc.
(fornitori servizi IT e
settori finanziari



BENEFICI

Maggiore sicurezza
e stabilità del
sistema finanziario.
Aumento della
fiducia nei servizi
finanziari digitali.



AZIONI PER LE AZIENDE

Valutare l'impatto del
Regolamento.
Adeguare i sistemi e
le procedure interne.
Investire in tecnologie
di sicurezza.

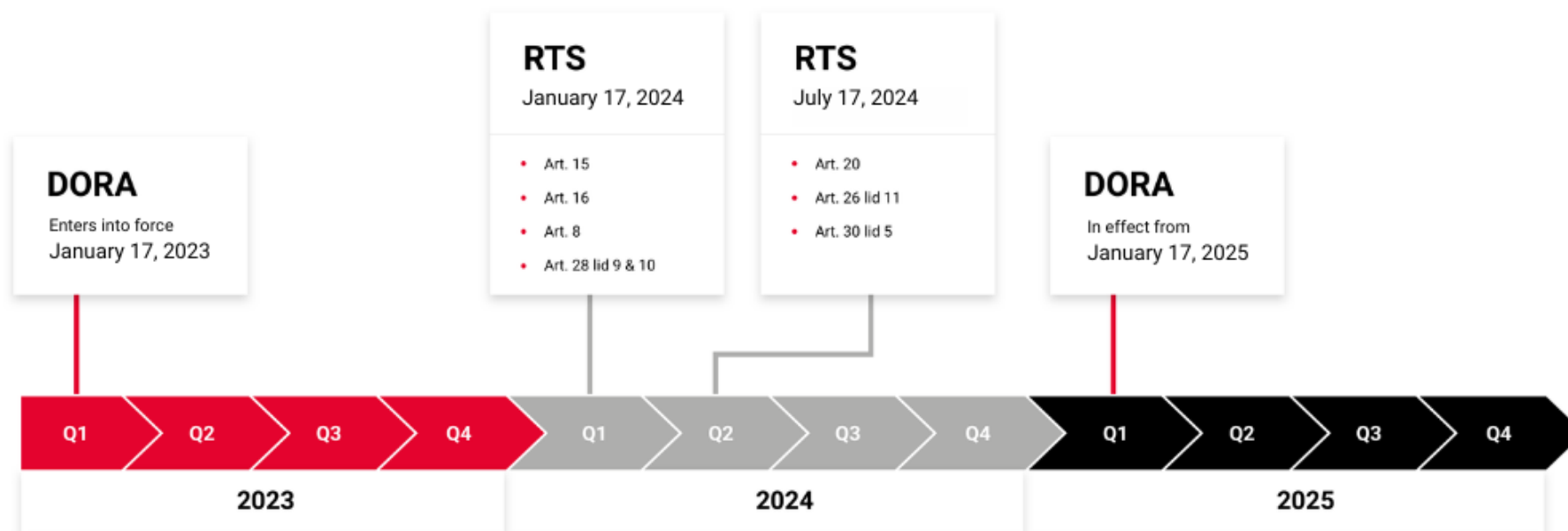


MISURE

Governance dei rischi
ICT, cybersecurity,
ICT risk
management,
incident reporting
Gestione Terze Parti.

Timeline DORA

Attenzione: DORA è già in vigore dal 17 Gennaio 2023.
Dal 17 Gennaio 2025 sarà operativo il relativo regime sanzionatorio



1° Verticale

Resilienza e Continuità Operativa

Cosa significa Resilienza?



Essere pronti a tutto è impossibile...ma possiamo essere preparati



Fonte: [Per affrontare le tempeste aziendali non basta "solo" essere pronti. | LinkedIn](#)

Per affrontare le tempeste aziendali non basta "solo" essere pronti...

- **Essere pronti** significa essere reattivi e capaci di rispondere rapidamente alle sfide immediate (avere «soluzioni»), ma essere «preparati è molto di più».
- **Essere preparati** implica avere una conoscenza approfondita, competenze solide e una mentalità «flessibile» che permetta di adattarsi alle mutevoli ed imprevedibili situazioni esterne.

*I dipendenti preparati sono in grado non solo di affrontare le sfide attuali, ma anche di **anticipare e adattarsi alle sfide future**. Investire nella preparazione significa fornire formazione continua, promuovere lo sviluppo delle competenze e incoraggiare una mentalità di apprendimento costante.*

*In un mondo in continua evoluzione, dove le tecnologie e le strategie aziendali cambiano rapidamente, **avere persone preparate è il vero asset di un'azienda***

Fonte: [Per affrontare le tempeste aziendali non basta "solo" essere pronti. | LinkedIn](#)

Cos'è la Resilienza Operativa?



- **La Resilienza Operativa si riferisce sia alla capacità di un sistema di preservare il suo funzionamento tollerando perdite e interruzioni, sia alla capacità di recuperare in seguito al loro verificarsi.**
- L'attenzione è sempre di più focalizzata sulla gestione del rischio di **terze parti** e sull'affrontare gli eventuali problemi di un determinato provider di **infrastruttura cloud**.
- Nel caso delle società che offrono servizi bancari, assicurativi e finanziari, resilienza operativa può riferirsi più specificamente alla **capacità di fornire servizi critici anche in caso di interruzioni di vasta portata**.

Alcune «definizioni»



- **Lo standard ISO**, già nella sua versione del 2012, **introduceva concetti di resilienza legati alla capacità di identificare e valutare l'impatto** di quelle **minacce** che, se realizzate, possono **causare interruzione dei servizi**, ovvero definire un modello di resilienza (organizzativa) per garantire una risposta efficace
- Il **Comitato di Basilea** definisce la **resilienza (operativa)** la capacità di un'organizzazione di assorbire e adattarsi in un ambiente in evoluzione per consentire il raggiungimento degli obiettivi, sopravvivere e prosperare.
- Il **BCI** all'interno del suo glossario, distribuito gratuitamente sul sito istituzionale, definisce la **resilienza operativa** come, la capacità di un'organizzazione, del personale, dei sistemi (informativi), della rete di telecomunicazioni, delle attività o dei processi di assorbire l'impatto di una discontinuità, interruzione o perdita dell'attività di business e continuare a fornire un accettabile livello di servizio.
- L'**FCA** per ultima, ma non meno importante, definisce la **resilienza (operativa)** come la capacità di prevenire, adattarsi, rispondere, riprendersi e imparare da interruzioni operative, introducendo allo stesso tempo un elemento di novità, ovvero la valutazione dell'impatto sul cliente e del danno (intollerabile) che l'organizzazione gli potrebbe creare in caso di interruzione dei servizi offerti.

Continuità Operativa VS Resilienza Operativa

Si concentra sul mantenimento delle funzioni critiche durante un'interruzione.

L'obiettivo è ripristinare rapidamente i servizi essenziali al livello pre-crisi.

Si basa su piani di continuità operativa (BCP) che definiscono procedure di risposta a specifici scenari di interruzione.

È un approccio reattivo che si concentra sulla gestione degli eventi dopo che si sono verificati.

CONTINUITÀ
OPERATIVA

RESILIENZA
OPERATIVA

Si concentra sulla capacità di adattarsi e prosperare di fronte a eventi avversi, anche inaspettati.

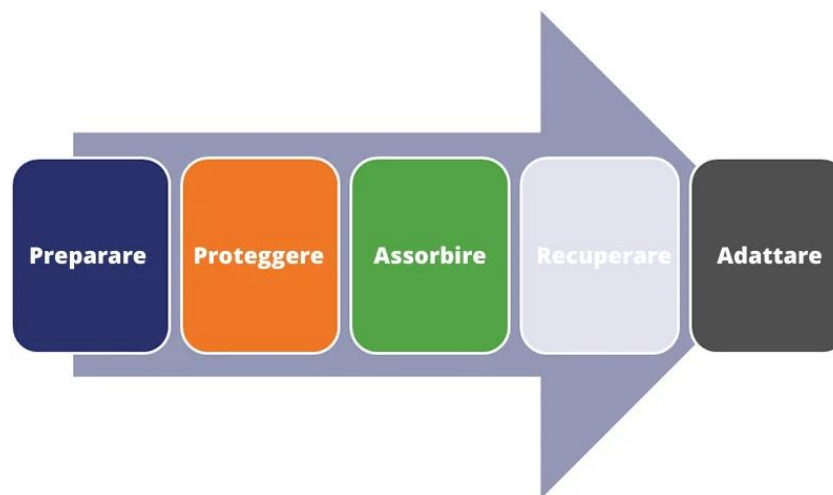
L'obiettivo è assorbire l'impatto di un evento e riprendersi rapidamente, minimizzando i danni.

Si basa su una cultura di resilienza che permea l'intera organizzazione.

È un approccio proattivo che si concentra sulla prevenzione degli eventi e sulla capacità di adattarsi a nuove circostanze.

Quindi...

- essere resilienti, nelle differenti dimensioni di un'azienda (es. operativa, IT ed infrastrutturale, HR, Corporate Security, Digital Security, ecc), **non significa** quindi **essere necessariamente capaci di ripartire complessivamente a fronte di un grave evento straordinario**, ma **riguarda la capacità di continuare ad erogare determinati servizi “importanti”** grazie alla propria flessibilità acquisita
- avere un **processo efficace di continuità operativa è d'altro canto un abilitatore della resilienza (operativa)**



Resilienza



ISACA®
AIEA | Milan Chapter



(<https://www.build-resilience.org/>)



Valerio Tomasoni

Il nuovo Regolamento DORA- AIEA *for* DORA

Resilienza



ISACA®
AIEA | Milan Chapter

Business Continuity / Continuity of Operations

Business Continuity Management (BCM) is a management process that identifies potential threats to an organization and the impacts to business operations if those threats are realized.

[Read More](#)

Crisis Management and Communications

The Crisis Management & Communication Discipline addresses crises that are managed primarily by top management and at a strategic level of the organization.

[Read More](#)

Human Resource Management

Human Resource Management is a business field focused on maximizing employee productivity. It is a function in organizations designed to maximize employee performance in service of an employer's strategic objectives. Human Resource Management also concerns itself with managing and encouraging organizational change.

[Read More](#)

Information & Communication Technology Continuity

The discipline of Information and Communication Technology (ICT) addresses the need for organizations to protect their technology and telecommunication systems and to minimize the impact of disruptions.

[Read More](#)

Critical Environments

The focus of the Critical Environments discipline is on the design, build, operations, management, governance, and audit of data centers and other critical environments used to house computer systems, and associated components such as telecommunications and storage systems.

[Read More](#)

Financial Health & Viability

Organizational resilience is more than managing risk, engaging leadership, and having a healthy culture. The organization must be financially viable and provide a product or service under changing conditions.

[Read More](#)

Incident Response

The focus of this discipline is on the planning needed for an effective response to an incident. Organizations need to have procedures in place to manage an incident that impacts life safety and physical assets.

[Read More](#)

Information Security

Today more than ever, computer system threats need to be both understood and protected against at the highest level possible. With the increase in threats the field of information security has grown and evolved.

[Read More](#)

Legal, Audit, and Compliance

The Legal, Compliance and Audit discipline plays two roles in organizational resilience. First, it is a collection of best practices as determined by various industry groups, oversight organizations, and government agencies. Second, inspection procedures up to and including third-party audits are available to ensure alignment with the practices.

[Read More](#)

Organizational Behavior

Organizational Behavior is the study of human behavior in organizational settings, the interface between human behavior and the organization, and the organization itself.

[Read More](#)

Resilience requires a coordinated approach.

While there is no single strategy or solution to make an organization resilient, an organization can enhance its resilience by:

- Strengthening of individual management disciplines of the organization that manage risk and doing so in an integrated and coordinated manner.
- Building a culture that ensures the organization behaves in a healthy manner.
- Increasing its adaptive capacity and ability to manage change.

Each of these aspects plays an important role in building a more resilient organization, but implemented as a framework and as an integrated strategy will bring the most benefit.

Risk Management

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of an incident or to maximize the realization of opportunities.

[Read More](#)

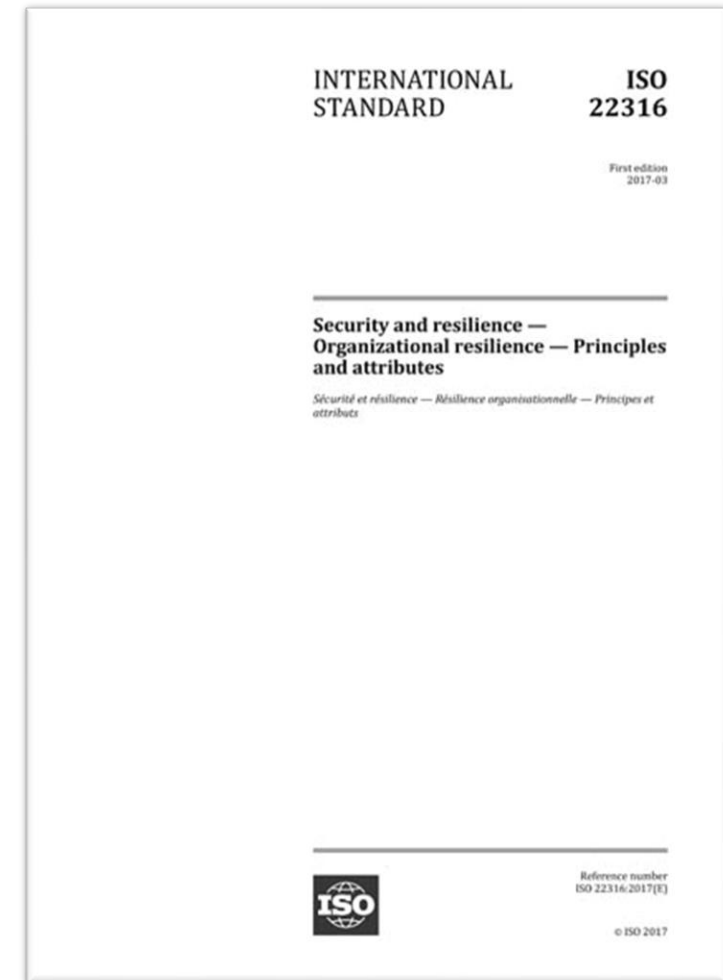
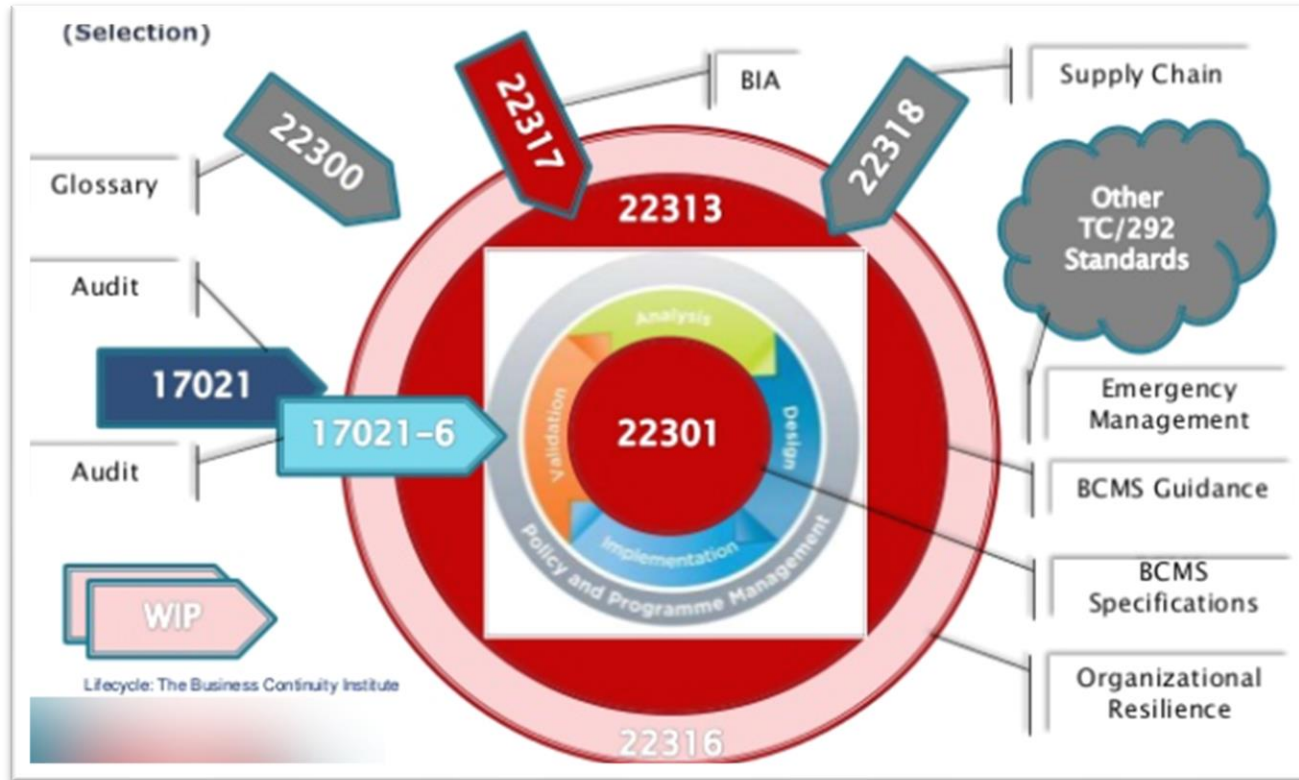
Supply Chain Management

Threats to your supply chain and therefore to your organization abound – their likelihood and consequences heightened by long, global supply chains, ever-shrinking product cycles, and volatile and unpredictable market cycles.

[Read More](#)



(<https://www.build-resilience.org/>)



Nella **ISO 22316** sono menzionate le seguenti «discipline» e «sistemi di gestione» che contribuiscono a una buona resilienza organizzativa (Annex A):

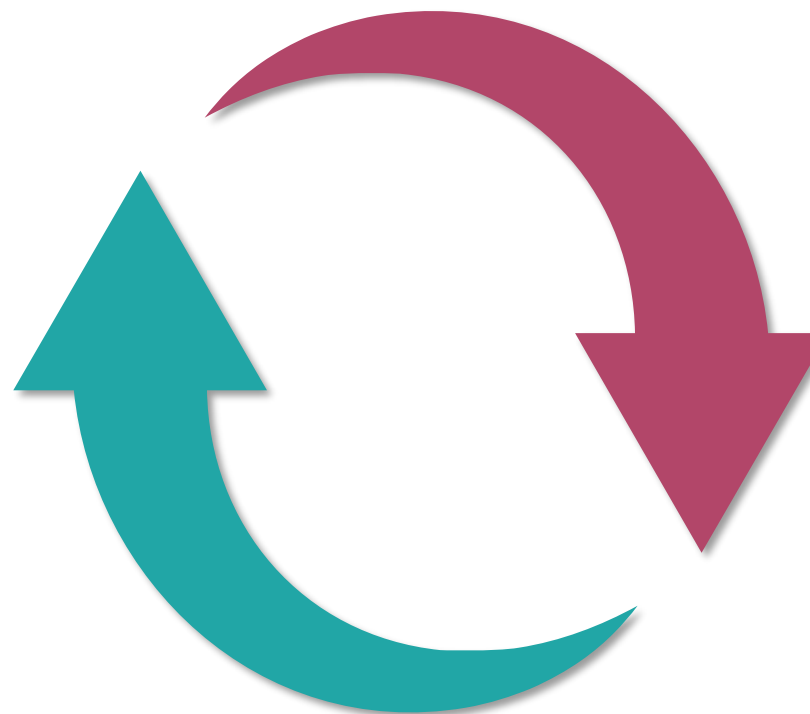
- gestione degli asset;
- gestione della continuità operativa;
- gestione della crisi;
- gestione della sicurezza cyber;
- gestione delle comunicazioni;
- gestione delle emergenze;
- gestione dell'ambiente;
- gestione dei siti;
- controllo finanziario;
- controllo frodi;
- governance;
- gestione della salute e della sicurezza;
- gestione delle risorse umane;
- gestione della sicurezza delle informazioni;
- information, communications and technology;
- gestione della sicurezza fisica;
- gestione della qualità;
- gestione del rischio;
- gestione della catena di fornitura;
- pianificazione strategica.

Continuità Operativa «moderna»



EX ANTE

Proteggendosi e
strutturandosi per
“incassare il colpo”



EX POST

Avendo soluzioni
pronte per
“contenere e reagire”

Continuità Operativa «moderna»



2° Verticale

Risk Management ICT

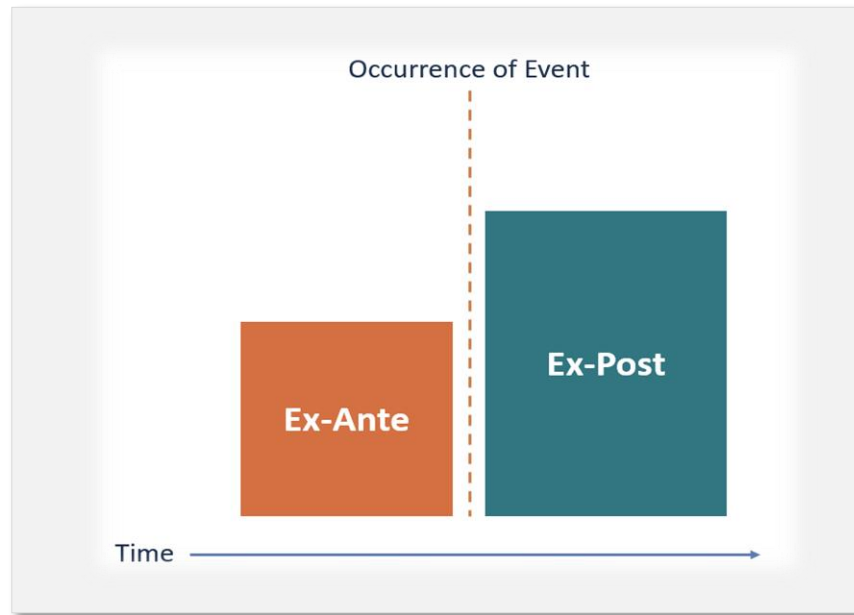
Risk Management



Adottare un approccio orientato alla prevenzione



Piuttosto che un approccio orientato alla reazione a comportamenti illeciti o non conformi



*Significa
essere*



Passaggio da un approccio reattivo ad un
approccio proattivo di gestione dei rischi

E QUINDI?

Supply Chain & Information Technology

Le principali cause di INCIDENTI ALTI e CRITICI



Fornitori



Esternalizzazioni

Il processo di esternalizzazione ha reso più vulnerabile l'infrastruttura organizzativa della banca.

Il crescente grado di digitalizzazione e interconnessione ha amplificato i rischi relativi alle tecnologie dell'informazione e della comunicazione rendendo così il sistema finanziario, più vulnerabile alle minacce informatiche.

Per tali ragioni è necessario essere in grado di:

- Conseguire un elevato livello di sicurezza operativa informativa;
- Contrastare l'esfiltrazione dei dati e attacchi cyber;
- Gestire i rischi, garantire la continuità e la cyber security;



Due Diligence



Valutazione dei Rischi

- Prima di concludere un accordo di esternalizzazione e considerando i rischi operativi connessi alla funzione da esternalizzare, gli enti e gli istituti di pagamento dovrebbero assicurare, nel loro processo di selezione e valutazione, l'idoneità del fornitore di servizi.
- Per quanto riguarda le funzioni essenziali o importanti, gli enti e gli istituti di pagamento dovrebbero far sì che il fornitore di servizi abbia la reputazione commerciale, abilità adeguate e sufficienti, la competenza, la capacità, le risorse (ad esempio umane, informatiche, finanziarie), la struttura organizzativa e, se del caso, le autorizzazioni o le registrazioni regolamentari necessarie per svolgere la funzione essenziale o importante in modo affidabile e professionale al fine di adempiere ai propri obblighi per tutta la durata del contratto proposto.
- Se l'esternalizzazione comporta il trattamento di dati personali o riservati, gli enti e gli istituti di pagamento dovrebbero accertarsi che il fornitore di servizi adotti misure tecniche e organizzative adeguate per proteggere tali dati.
- Gli enti e gli istituti di pagamento dovrebbero adottare misure adeguate per assicurare che i fornitori di servizi agiscano in modo coerente con i loro valori e codici di condotta. In particolare, per quanto riguarda i fornitori di servizi situati in paesi terzi e, se del caso, i relativi subcontraenti, gli enti e gli istituti di pagamento dovrebbero accertarsi che il fornitore di servizi agisca in modo etico e socialmente responsabile e rispetti le norme internazionali in materia di diritti umani (ad esempio la Convenzione europea dei diritti dell'uomo), di protezione dell'ambiente e di condizioni di lavoro adeguate, compreso il divieto del lavoro minorile.

Rischi di Sub-Esternalizzazione



Se l'accordo di esternalizzazione prevede la possibilità che il fornitore di servizi **subesternalizzi funzioni essenziali o importanti ad altri fornitori di servizi**, gli enti e gli istituti di pagamento dovrebbero tener conto di quanto segue:

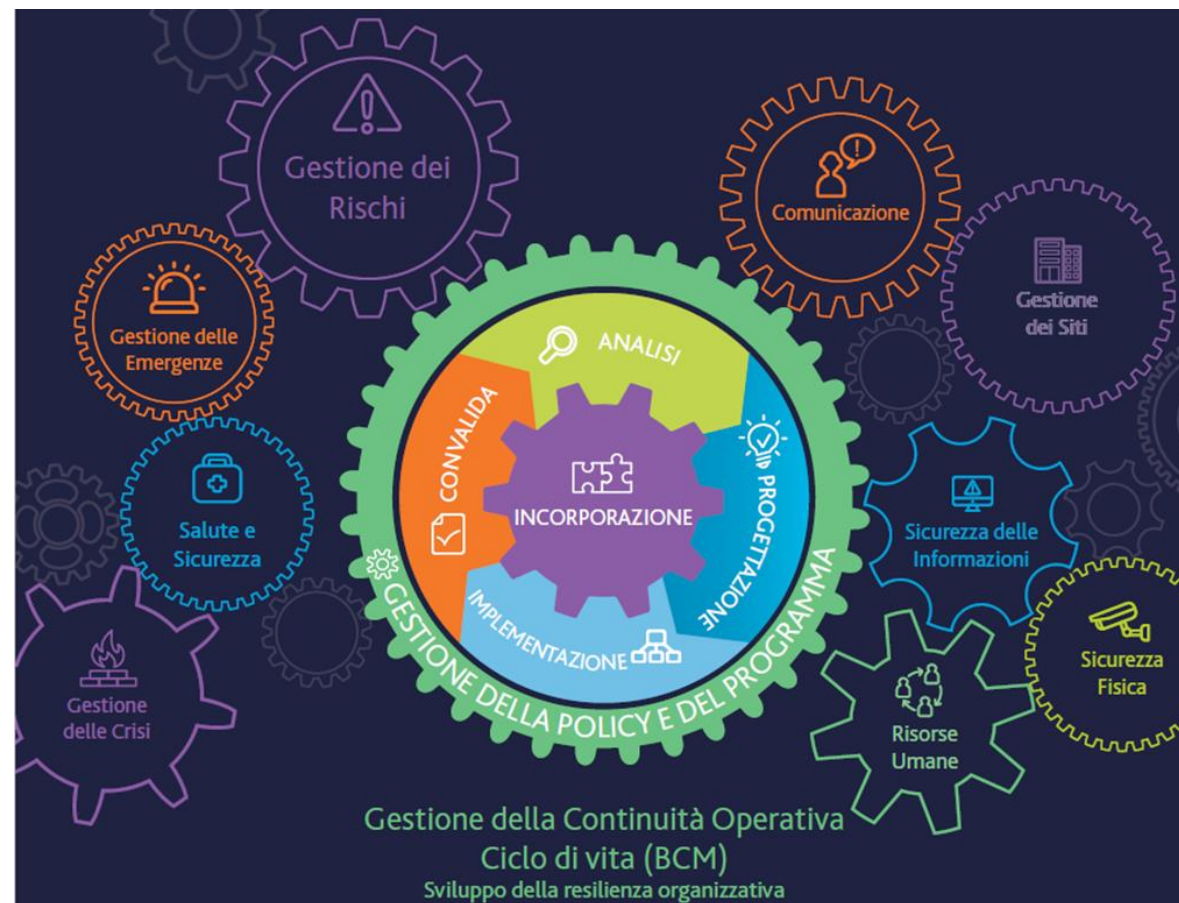
- I rischi associati alla subesternalizzazione, compresi i rischi aggiuntivi che possono sorgere se il subcontraente ha sede in un paese terzo o in un paese diverso da quello del fornitore di servizi;
- Il rischio che lunghe e complesse catene di subesternalizzazione riducano la capacità degli enti o degli istituti di pagamento di vigilare sulla funzione essenziale o importante esternalizzata e la capacità delle autorità competenti di esercitare una efficace vigilanza su essi.

Framework ICT RM



Incorporazione

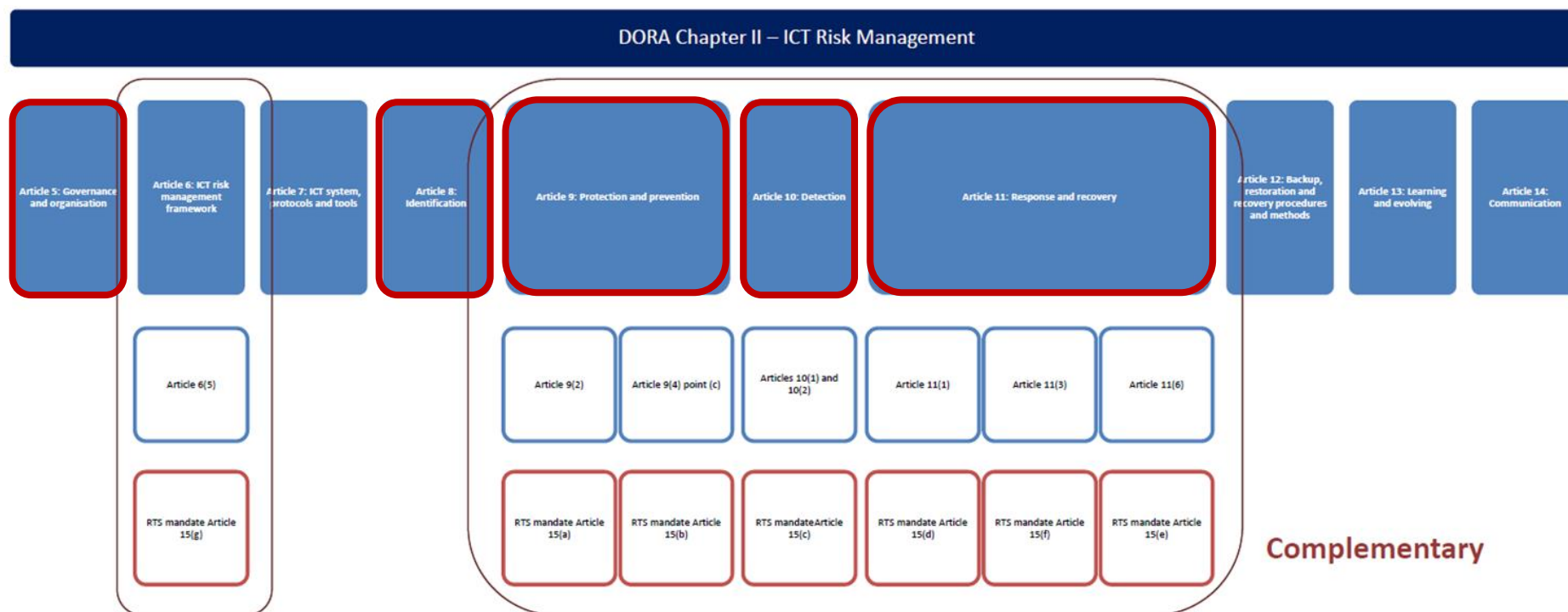
Il **Risk Management** non deve essere visto come un'attività isolata, ma deve essere «integrato» in tutti i «livelli» e «processi» aziendali (**es. BCI**). La cultura del rischio deve essere condivisa da tutti i dipendenti, che devono essere consapevoli dei rischi e delle loro implicazioni.



DORA Chapter II (Articles 1 to 14)



SACA®
A | Milan Chapter



JOINT COMMITTEE OF THE EUROPEAN
SUPERVISORY AUTHORITIES



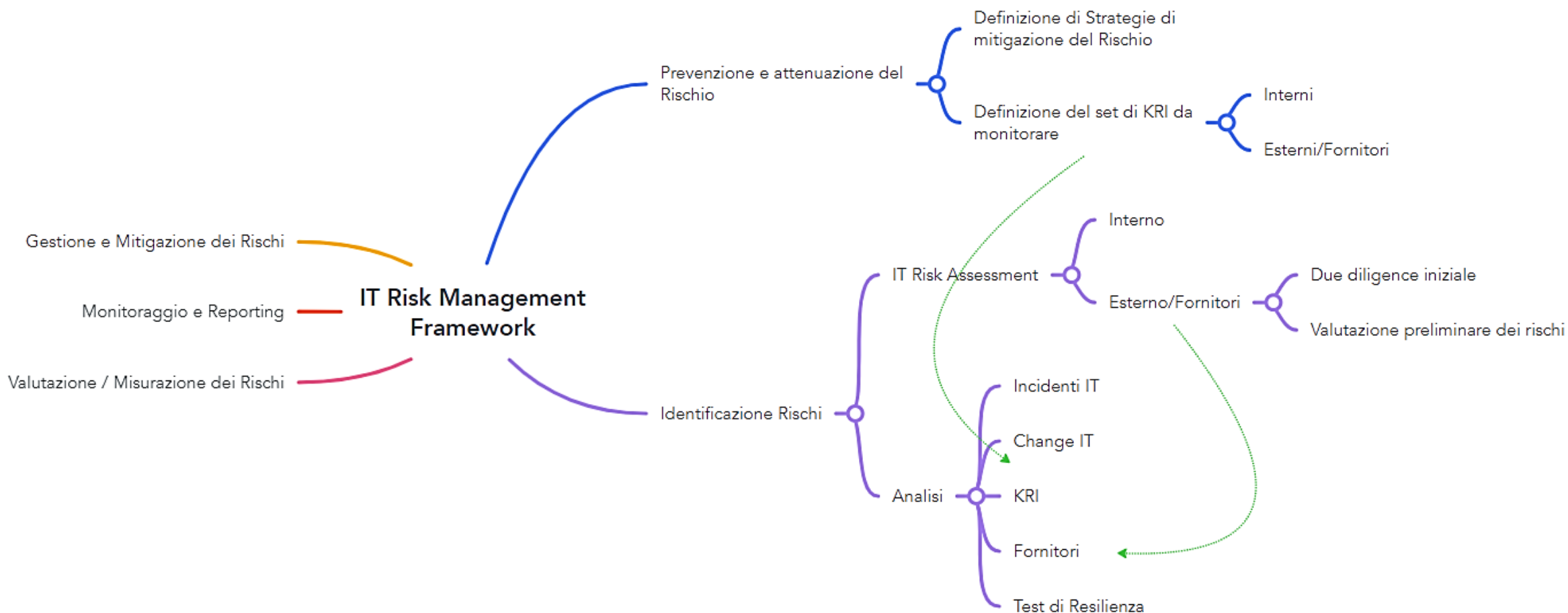
ISACA
AIEA | Milan Chapter



Framework IT Risk Management



ISACA®
AIEA | Milan Chapter





AIEA*for*DORA

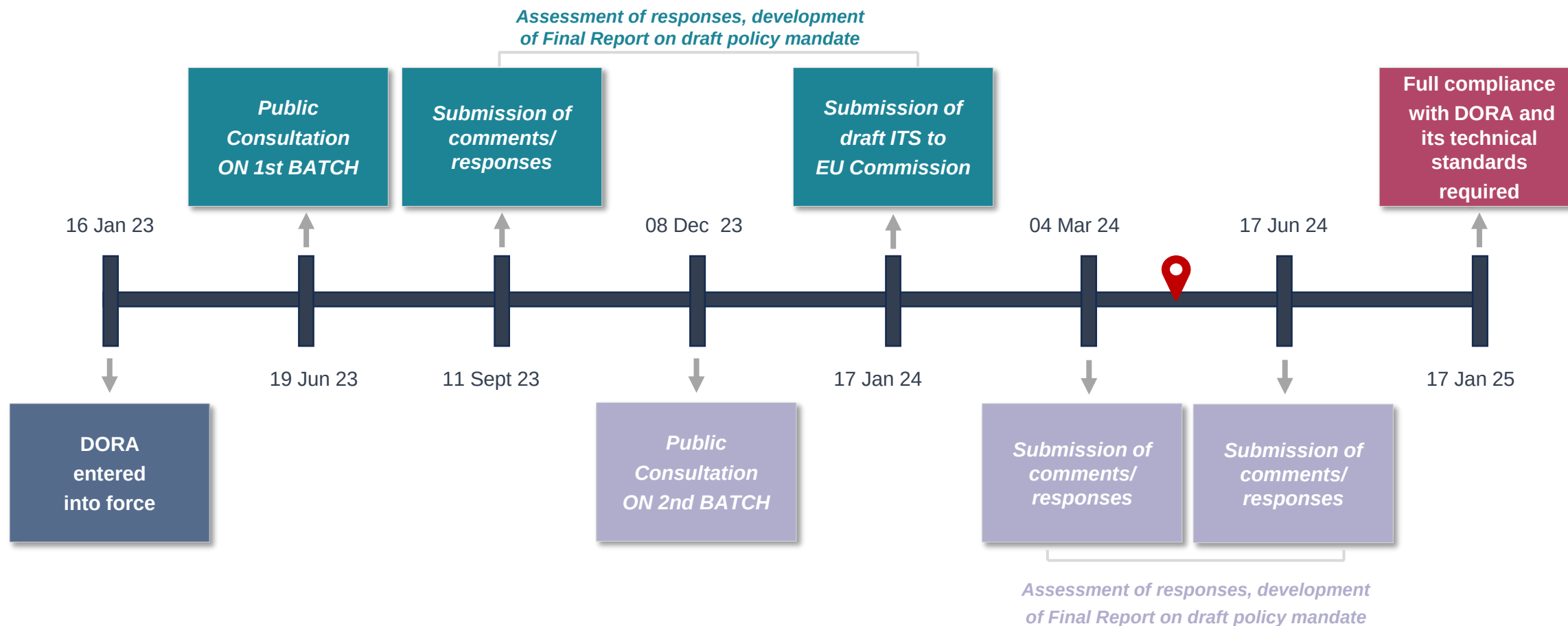
AIEA_{for}DORA, un progetto che nasce con l'ambizione di favorire:



- La creazione di una community di esperti, che possano far fronte comune nei prossimi mesi/ anni, sui temi della Resilienza Operativa Digitale
- Il networking tra persone con skill diverse ma complementari (es. Cybersecurity, IT Strategy, IT Management, Legal, etc.), per una copertura complessiva della tematica
- La sperimentazione di tavoli collaborativi targati AIEA, prolifici di ricerca
- La conoscenza e il divertimento, all'interno dell'Associazione



AIEA_{for}DORA e la timeline delle ESAs



6 Tavoli AIEA per 10 Progetti di Norme Tecniche



Framework per la Gestione dei Rischi ICT



Classificazione degli Incidenti ICT e delle Minacce Significative



Policy per la gestione degli adempimenti contrattuali sull'uso di Servizi ICT forniti da Terze Parti, a supporto di funzioni critiche o importanti



Major Incident ICT-related



Test di Resilienza Operativa Digitale e TLPT



Fornitori Terzi di Servizi ICT

AIEA_{for}DORA: approccio operativo e attività

Fase di analisi e confronto

Attivazione di tavoli di lavoro

Sono stati organizzati 4 incontri per ciascun tavolo tematico, con l'obiettivo di analizzare gli RTS e stimolare il confronto tra i partecipanti.



Raccolta di feedback

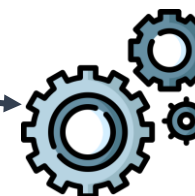
Al termine di ogni incontro, i partecipanti ai tavoli di lavoro hanno compilato un questionario contenente le domande formulate dalle ESA.



Fase di elaborazione e formalizzazione

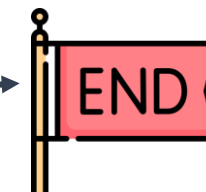
Sintesi e organizzazione

Il Team di Supporto tecnico AIEA ha rielaborato e omogeneizzato le risposte raccolte tramite i questionari.



Condivisione ufficiale

Le risposte finali sono state sottoposte sul portale ESMA, rendendole disponibili per la consultazione ufficiale.



6 Tavoli AIEA_{for}DORA per 8 Progetti di Norme Tecniche (1° batch)

Il **progetto AIEA_{for}DORA** è stato suddiviso in due sessione dove la prima è dedicata alle consultazione del primo lotto di norme tecniche, mentre la seconda è dedicata alla consultazione pubblica sul secondo lotto di norme tecniche.

Framework per la Gestione Rischi ICT

Il Tavolo di Lavoro si è posto l'obiettivo di rispondere al documento di consultazione sugli RTS sull'ICT Management Framework (art.15) e sugli RTS relativi all'ICT Risk Management Framework Semplificato (Art.16).



Classificazione Incidenti ICT e Minacce

Il Tavolo di Lavoro si è posto l'obiettivo di rispondere al documento di consultazione sugli RTS sui criteri per la classificazione degli incidenti legati all'ICT (art.18.3).



Policy per la Contrattualistica verso Fornitori ICT

Il Tavolo di Lavoro si è posto l'obiettivo di rispondere al documento di consultazione sugli ITS per stabilire i modelli per il registro delle informazioni (art. 28.9); e al documento di consultazione sulle RTS per specificare la politica sui servizi ICT forniti da fornitori terzi di ICT (art. 28.10).



6 Tavoli AIEA_{for}DORA per 8 Progetti di Norme Tecniche (2° batch)

Major Incident ICT - related

Per armonizzare e razionalizzare il regime di segnalazione degli incidenti legati alle tecnologie dell'informazione e della comunicazione (ICT) per le entità finanziarie (FE), rispetto a quanto proposto nell'RTS/ITS, il Tavolo di Lavoro si confronterà circa:

- il contenuto delle segnalazioni per gli incidenti ICT rilevanti per riflettere i criteri stabiliti nell'articolo 18(1) e valutare ulteriori elementi,
- la determinazione dei limiti di tempo per la notifica iniziale e per ogni segnalazione di cui all'articolo 19,4

il contenuto della notifica per le minacce

Test di Resilienza Operativa Digitale- TLPT

Il Tavolo di Lavoro si pone come obiettivo quello di approfondire il Framework Tiber- EU e confrontarlo con gli approcci proposti dal TLPT threat-led penetration testing conformemente ai dettati DORA.

Al fine di uniformare ogni aspetto legato alla conduzione dei Test di Resilienza Operativa digitale, sarà necessario analizzare i processi, le tipologie i criteri che guidano tali attività.

Fornitori Terzi di servizi ICT

Tenendo in considerazione gli assunti della precedente consultazione, il Tavolo di Lavoro si pone come obiettivo quello di approfondire con minuzia il tema delle Subforniture.

Si dovrà in particolare valutare con attenzione il Modello proposto per la condivisione di informazioni su accordi di subappalto rivolgendo uno sguardo critico anche ai dettagli sugli scambi di informazioni necessari affinché le autorità competenti garantiscano il seguito delle raccomandazioni di cui all'articolo 35, paragrafo 1, punto d), rivolte ai fornitori critici di servizi di terze parti ICT.

Focus 2° Batch (domande e risposte)

Do you agree with the proposed reporting requirements set out in the draft ITS?

Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT?

Are articles 3 appropriate and sufficiently clear?

TdL 1. Major Incident ICT - related

In linea generale si ritiene l'approccio condivisibile. Tuttavia, è sorto il dubbio di come vengano misurati i requisiti di completezza e accuratezza delle informazioni inserite per notifica iniziale, rapporto intermedio e rapporto finale. Inoltre vi è il dubbio se l'outsourcing infragruppo sia considerato outsourcing.

TdL 2. Test di Resilienza Operativa Digitale - TLPT

In linea generale, l'approccio two-layered è condivisibile ed è sufficientemente esaustivo per quanto concerne il profilo di rischio e il livello di maturità dell'entità finanziaria. Tale approccio, infatti, è funzionale all'individuazione delle misure necessarie a definire la proporzionalità dei test effettuati. Tuttavia, l'approccio sopra menzionato dovrebbe prendere in considerazione eventuali attacchi cyber legati alla Supply chain.

TdL 3. Fornitori Terzi di servizi ICT

Il testo dell'articolo è considerato globalmente chiaro, ma risulta complesso nel suo contenuto e nell'applicazione, specialmente a causa di vincoli rigidi nei punti e) e f). Questi potrebbero obbligare le Entità Finanziarie a gestire i subfornitori come fornitori diretti, limitando le opzioni di selezione. Si suggerisce di focalizzare l'attenzione sull'abilità del fornitore di servizi TIC nel gestire i subfornitori, dando maggiore rilievo ai punti c) e d).



Pubblicazioni



Valerio Tomasoni

Il nuovo Regolamento DORA- AIEAforDORA

L'evoluzione AIEA_{for}DORA: pubblicazioni e approfondimenti su temi-chiave



Dato l'interesse manifestato da «Soci» e da «Non Soci simpatizzanti» verso l'Associazione, AIEA intende continuare il percorso AIEA_{for}DORA avviato nel 2023 con i 6 Tavoli di Lavoro per rispondere alla consultazione pubblica delle AEV (e **circa 50 partecipanti per ogni singolo batch**, oltre allo Staff AIEA_{for}DORA, costituito da 6/8 risorse che si sono dedicate all'organizzazione delle attività, alla preparazione del materiale per facilitare i workshop, all'omogeneizzazione dei contributi ricevuti e alla loro traduzione, etc.).

I prossimi passi saranno:

- **evento AIEA del 19/04 (14.00 - 18.00), per fare il punto su DORA e sui risultati del Progetto AIEA_{for}DORA**
- **Call for Paper, rivolta in primis ai partecipanti ai Tavoli, per lavorare ad una collana di pubblicazioni AIEA sul tema della Resilienza, nella seconda metà del 2024 e primo semestre 2025.**



GRAZIE PER L'ATTENZIONE

Valerio Tomasoni & il Team AIEA *for* DORA
valerio.tomasoni@gmail.com
aieadora@isaca.mi.it