Digital Operational Resilience Act (DORA)

Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario

Avv. Filippo Bianchini – e-privacy XXXIV (2024)
Firenze, 16 maggio 2024

Amuse-bouche

- In due frasi:
  - Individuazione e gestione *ex ante* dei **rischi**
  - Applicazione dei principi di **cybersecurity**
- In una *keyword*:
  - (Cyber)**resilienza**

al fine di raggiungere un **“elevato livello di resilienza operativa digitale”**

WhoAmI

- Avvocato cassazionista, iscritto al Foro di Perugia
- DPO e Valutatore privacy certificato UNI 11697 (a breve: UNI EN 17740) - Lead Auditor 27001:2022 - CIPP/E
- Membro supplente dell'Autorità Garante per la protezione dei dati personali di San Marino
- Membro del Consiglio Direttivo di ASSO DPO e AIP-ITCS
- Docente nel Master universitario *Data protection, Cybersecurity e Digital forensics* dell'Università per gli Studi di Perugia e nel progetto Erasmus+ *BuTH-AI, Building Trust in Human Centric Artificial Intelligence* della Link Campus University
- Membro dell'EDPB «Support Pool of Experts»
- Membro del Cybersecurity National Lab, nodo UniPG
- Componente UNI CT 510 e UNI CT 526

Cos’è DORA

- Gestione del rischio TIC
- Segnalazione degli incidenti connessi alle TIC
- Test di resilienza operativa digitale
- Rischi relativi alle TIC derivanti da terzi
- Condivisione delle informazioni
- Autorità competenti

- Modifiche volte ad adeguare la normativa vigente

Resilienza operativa ed evoluzione del rischio digitale: come l'UE sta ridisegnando l'approccio del settore

EU Commission

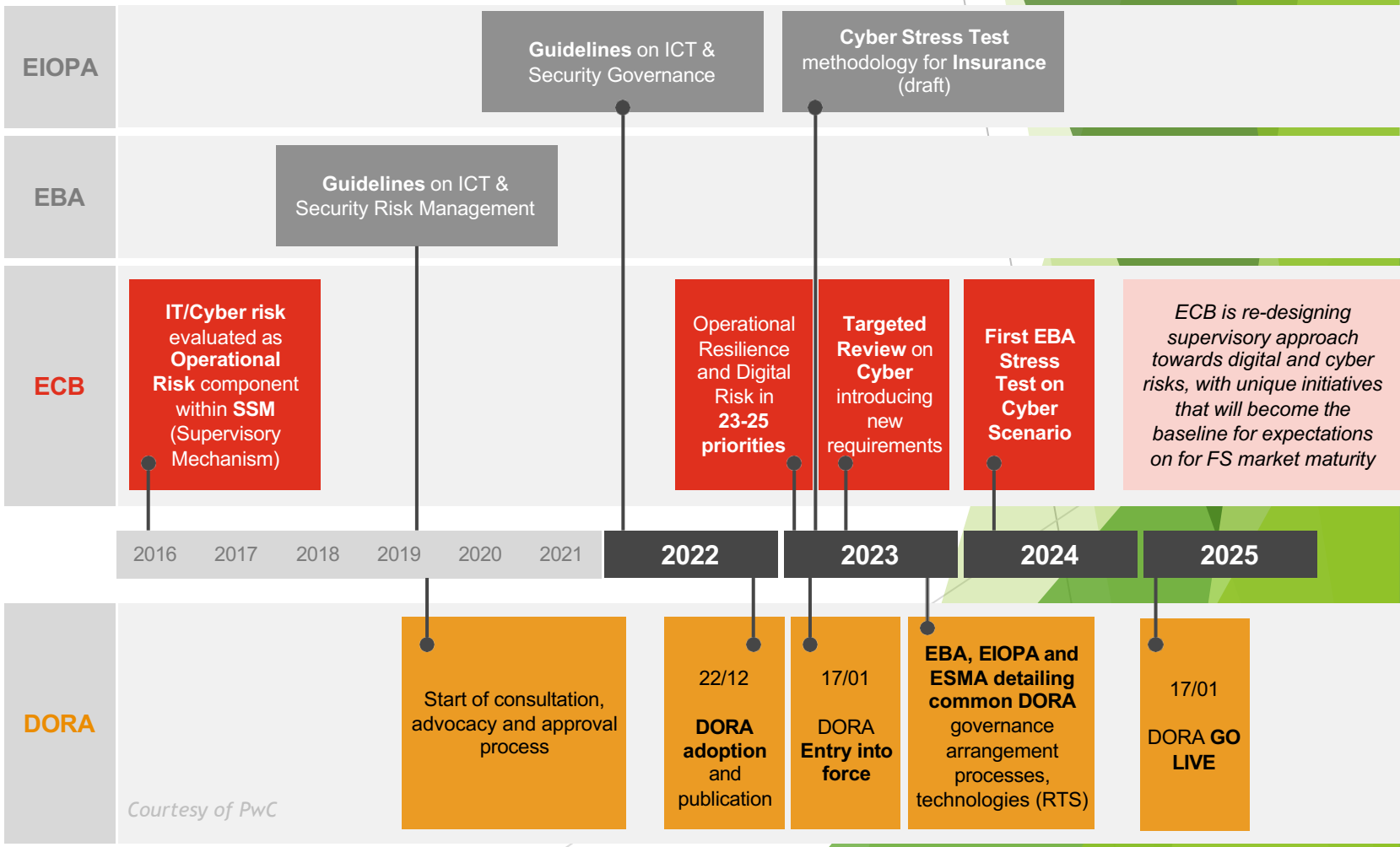
- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- Artificial Intelligence Act
- Data Governance Act
- Data Act
- Cyber Resilience Act
- NIS2 Directive

Digital Finance Package

- Markets in Crypto-Assets Regulation (MiCA)
- Digital Ledger Technology (DLT)
- Digital Operational Resilience Act (DORA)

EU Digital agenda is completely evolving how we are defining and dealing with digital risks. FS Sector will play a key role in this journey with DORA and tailored Resilience initiatives

Focus On Financial Services



Resilienza: definizione

- Capacità di **reagire** di fronte ad un evento avverso, sia questo un atto volontario, involontario, fortuito.
- Più in generale è la capacità di un'organizzazione di **resistere** a eventi che comprendono il mutare della congiuntura economica, l'evoluzione del mercato, i cambiamenti tecnologici, ecc.

ISO 22316:2017(en)

Security and resilience — Organizational resilience — Principles and attributes

Introduction

Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context. Enhancing resilience can be a strategic organizational goal, and is the outcome of good business practice and effectively managing risk.

An organization's resilience is influenced by a unique interaction and combination of strategic and operational factors. Organizations can only be more or less resilient; there is no absolute measure or definitive goal.

Cos'è la resilienza operativa digitale?

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «resilienza operativa digitale»: la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni;

- Strumento di integrità, solidità e affidabilità
- Veicolo di consapevolezza dei rischi informatici e di sicurezza
- Strumento di garanzia a tutela dei consumatori

Qual è il ciclo di vita della cyber resilienza?

- La resilienza informatica può essere compresa attraverso un ciclo di vita basato sulle fasi del ciclo di vita dei servizi dell'Information Technology Infrastructure Library (ITIL):

STRATEGIA **PROGETTAZIONE** **TRANSIZIONE** **FUNZIONAMENTO** **MIGLIORAMENTO**

Uno sguardo d'insieme

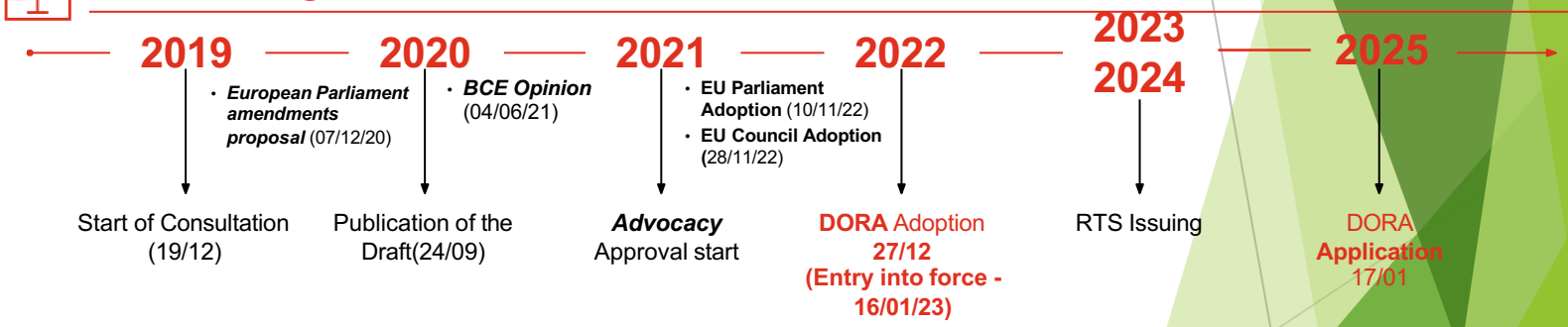
> Il carattere fondante della proposta di regolamento UE DORA: un big bang della cybersecurity per il sistema finanziario comunitario, con obiettivi comuni e sfidanti. Un effetto di innalzamento istantaneo dello standard regionale, che rende il sistema finanziario comunitario più forte e con ripercussioni globali.

Fonte: "Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma»
Paolo Ciocca, Commissario Consob, 18 novembre 2020

Applicabilità

- Il regolamento si applicherà a circa **22.000 entità di servizi finanziari**.
- L'ambito di applicazione del DORA comprende entità del settore finanziario tradizionale come **enti creditizi**, **istituti di pagamento**, **prestatori di servizi di informazione sui conti**, **istituti di moneta elettronica**, **gestori di fondi di investimento alternativi**, **società di gestione**, **imprese di assicurazione**, **enti pensionistici**, **agenzie di rating**.

Processo legislativo



Pilastri DORA

1. *Governance della resilienza operativa digitale*
2. *Gestione del rischio informatico e ICT end-to-end*
3. *Gestione delle TIC e degli incidenti informatici*
4. *Test di resilienza digitale*
5. *Gestione del rischio di terze parti nel settore ICT*
6. *Condivisione delle informazioni*

I 5 pilastri DORA per proteggere i servizi finanziari (FS) dalle minacce digitali

Gestione dei rischi digitali

- Aspettative e requisiti diretti affidati al **CdA** per la gestione e l'assunzione della responsabilità della **gestione dei rischi ICT e cyber lungo l'intera catena del valore** (e di outsourcing).
- Identificazione dei **servizi aziendali critici o importanti, costruzione di una comprensione completa end-to-end e approfondita di tutte le catene del valore** (servizi e gli asset ICT sottostanti, compresi i fornitori ICT di terze parti e i loro fornitori).
- **Alto livello di maturità per la gestione degli asset ICT** - requisiti per mappare, condividere e visualizzare i dati di tutti gli asset ICT e della catena del valore ICT per determinare asset critici, fornitori ICT terzi e **dipendenze chiave**.
- Definire **strategie e misure complete di protezione e prevenzione** per ogni scenario digitale grave ma plausibile che impatta sui servizi aziendali e sulle relative **catene di valore**.
- **Implementare nuovi processi, tecnologie e controlli chiave per la sicurezza informatica e la resilienza**, come IAM, SIEM, segregazione della rete, gestione delle vulnerabilità, sicurezza dei dati e gestione delle modifiche.
- **Allineare le strategie di continuità** (comprese quelle ICT), i **piani** e le **capacità** per rispondere ai nuovi scenari e proteggere i servizi aziendali (ad esempio, ripristino dei dati, misure di emergenza).

Incidenti legati alle TIC

- Introduzione di un processo di gestione per la **registrazione e il monitoraggio degli incidenti legati alle TIC** (compresa la loro classificazione).
- Presentare un rapporto iniziale, intermedio e finale sugli incidenti legati alle TIC.
- **Armonizzare la segnalazione degli incidenti legati alle TIC** utilizzando i modelli standard sviluppati dalle autorità di vigilanza europee.

Test di resilienza operativa digitale

- **Test di penetrazione avanzati** basati sulle minacce ogni 3 anni.
- **Revisione regolare del quadro di gestione del rischio ICT** e revisione annuale di tutte le applicazioni, i sistemi e i processi ICT critici.
- Misure per **migliorare le eventuali carenze individuate e segnalazione alle autorità di vigilanza**.
- Possibile implementazione regolare di **test di penetrazione guidati dalle minacce con il coinvolgimento di fornitori di servizi terzi**.

Gestione del rischio da parte di fornitori ICT terzi

- **Armonizzazione dei rapporti con i fornitori terzi di TIC** in tutte le fasi degli accordi contrattuali.
- Le **clausole contrattuali standard** devono contenere una descrizione completa dei servizi forniti.
- **Monitorare, documentare e riferire costantemente** su tutti gli accordi contrattuali con i fornitori terzi e **identificare i servizi che supportano funzioni critiche o importanti**.

Condivisione delle informazioni

- Disposizioni per la **condivisione di informazioni e intelligence sulle minacce informatiche** in un ambiente fidato.
- Stabilire meccanismi per verificare le informazioni fornite e intraprendere azioni appropriate.

Incident management

- Processo con lo scopo di evitare o minimizzare impatti di tipo economico o reputazionale e ripristinare nel più breve tempo possibile l'erogazione dei servizi.

PROCESSO DI GESTIONE E SEGNALAZIONE DI INCIDENTI:

1. IDENTIFICAZIONE
2. PROTEZIONE E PREVENZIONE
3. INDIVIDUAZIONE
4. RISPOSTA E RIPRISTINO
5. APPRENDIMENTO ED EVOLUZIONE
6. REPORTING E COMUNICAZIONE

Framework di sicurezza

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
1.ISO/IEC 27005:2018	AB	QT, QL Both can be used to apply the methods described in the document	It supports two main categories: primary and supporting assets (ANNEX B); provides info on primary and supporting assets. New assets can be imported *Interoperability Level:2*	ANNEX B provides criteria and scale suggestions to evaluate assets but scale depends on organisation. New criteria can be imported. *Interoperability Level: 3*	ANNEX C provides examples of typical threats. New threats and threat categories can be added. *Interoperability Level: 3*	ANNEX D provides vulnerabilities and methods for vulnerability assessment. New vulnerabilities and vulnerability catalogues can be imported. *Interoperability Level: 3*	Matrix is used for risk calculation with modifiable scales. ANNEX E provides examples for risk assessment. Other calculation methods can be used. *Interoperability Level: 3*	Measure catalogues are not included. This standard relies on ISO 27002 or other methods to import measure catalogues. Flexibility in RR calculation. No specific one given. *Interoperability Level: 3*	EN, FR	Significant compatibility with other frameworks and standards.
2.NIST SP 800-37	AB	QL	No specific categories of assets provided. As a framework, it can accommodate any asset taxonomy. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No specific asset valuation criteria given. As a framework, it can accommodate any evaluation method. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No specific threat catalogue given. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. RR calculation is flexible. *Interoperability Level: 3*	EN	As a generic method, it can accommodate any risk assessment method.

Framework di sicurezza

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
1.ISO/IEC 27005:2018	AB	QT, QL Both can be used to apply the methods described in the document	It supports two main categories: primary and supporting assets (ANNEX B); provides info on primary and supporting assets. New assets can be imported *Interoperability Level:2*	ANNEX B provides criteria and scale suggestions to evaluate assets but scale depends on organisation. New criteria can be imported. *Interoperability Level: 3*	ANNEX C provides examples of typical threats. New threats and threat categories can be added. *Interoperability Level: 3*	ANNEX D provides vulnerabilities and methods for vulnerability assessment. New vulnerabilities and vulnerability catalogues can be imported. *Interoperability Level: 3*	Matrix is used for risk calculation with modifiable scales. ANNEX E provides examples for risk assessment. Other calculation methods can be used. *Interoperability Level: 3*	Measure catalogues are not included. This standard relies on ISO 27002 or other methods to import measure catalogues. Flexibility in RR calculation. No specific one given. *Interoperability Level: 3*	EN, FR	Significant compatibility with other frameworks and standards.
2.NIST SP 800-37	AB	QL	No specific categories of assets provided. As a framework, it can accommodate any asset taxonomy. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No specific asset valuation criteria given. As a framework, it can accommodate any evaluation method. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No specific threat catalogue given. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. RR calculation is flexible. *Interoperability Level: 3*	EN	As a generic method, it can accommodate any risk assessment method.

Processo di gestione degli incidenti connessi alle TIC

- Procedure
- Ruoli e responsabilità
- Comunicazione e *responsible disclousure*
- Segnalazione di incidenti gravi
- Meccanismo di risposta agli incidenti

Classificazione degli incidenti

Articolo 18

Classificazione degli incidenti connessi alle TIC e delle minacce informatiche

1. Le entità finanziarie classificano gli incidenti connessi alle TIC e ne determinano l'impatto in base ai criteri seguenti:

a) il numero e/o la rilevanza di clienti o controparti finanziarie interessati e, ove applicabile, la quantità o il numero di transazioni interessate dall'incidente connesso alle TIC e il fatto che tale incidente abbia provocato o meno un impatto reputazionale;

b) la durata dell'incidente connesso alle TIC, compreso il periodo di inattività del servizio;

c) l'estensione geografica dell'incidente connesso alle TIC, con riferimento alle aree colpite, in particolare se interessa più di due Stati membri;

d) le perdite di dati derivanti dall'incidente connesso alle TIC, in relazione alla disponibilità, autenticità, integrità o riservatezza dei dati;

e) la criticità dei servizi colpiti, comprese le operazioni dell'entità finanziaria;

f) l'impatto economico dell'incidente connesso alle TIC — in particolare le perdite e i costi diretti e indiretti — in termini sia assoluti che relativi.

Segnalazione

3. Qualora si verifichi un grave incidente TIC che eserciti un impatto sugli interessi finanziari dei clienti, le entità finanziarie, senza indebito ritardo e non appena ne vengono a conoscenza, informano i loro clienti in merito a tale incidente e alle misure che sono state adottate per attenuare gli effetti avversi dell'incidente.

In caso di minaccia informatica significativa, le entità finanziarie, se del caso, informano i loro clienti potenzialmente interessati in merito alle opportune misure di protezione che i clienti stessi possono prendere in considerazione.

4. Entro i termini da fissare a norma dell'articolo 20, primo comma, lettera a), punto ii), le entità finanziarie trasmettono all'autorità competente interessata:

a) una notifica iniziale;

b) una relazione intermedia dopo la notifica iniziale di cui alla lettera a), non appena lo stato originario dell'incidente cambia in maniera significativa o il trattamento dell'grave incidente TIC cambia alla luce delle nuove informazioni disponibili, seguita, a seconda dei casi, da notifiche aggiornate, ogni qualvolta sia disponibile un aggiornamento della situazione, nonché su specifica richiesta dell'autorità competente;

c) una relazione finale, quando l'analisi delle cause che hanno dato origine all'incidente sia stata completata, indipendentemente dal fatto che le misure di attenuazione siano già state attuate, e quando al posto delle stime siano disponibili i dati dell'impatto effettivo.

a) **NOTIFICA INIZIALE**

b) **RELAZIONE INTERMEDIA**

c) **RELAZIONE FINALE**

Comunicazione

Articolo 14

Comunicazione

1. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie predispongono piani di comunicazione delle crisi che consentano una divulgazione responsabile di informazioni riguardanti, almeno, gravi incidenti connessi alle TIC o vulnerabilità ai clienti e alle controparti nonché al pubblico, a seconda dei casi.

2. All'interno del quadro per la gestione dei rischi informatici, le entità finanziarie attuano politiche di comunicazione per il personale interno e per i portatori di interessi esterni. Le politiche di comunicazione per il personale tengono conto dell'esigenza di operare un distinguo tra il personale coinvolto nella gestione dei rischi informatici, in particolare il personale responsabile della risposta e del ripristino, e il personale che è necessario informare.

3. Nell'entità finanziaria vi è almeno una persona incaricata di attuare la strategia di comunicazione per gli incidenti connessi alle TIC e assolvere a tal fine la funzione di informazione al pubblico e ai media.

- Piani di comunicazione della crisi
- Politiche di comunicazione per il personale
- Persona incaricata

Poteri dell'Autorità

Articolo 50

Sanzioni amministrative e misure di riparazione

1. Alle autorità competenti sono conferiti tutti i poteri di vigilanza, di indagine e sanzionatori necessari per adempiere i propri compiti ai sensi del presente regolamento.

2. I poteri di cui al paragrafo 1 includono almeno i poteri seguenti:

a) l'avere accesso a qualsiasi documento o dato, detenuto in qualsiasi forma, che l'autorità competente consideri pertinente per lo svolgimento dei propri compiti e la possibilità di riceverne o farne una copia;

b) lo svolgere ispezioni o indagini in loco comprendenti tra l'altro:

   i) la convocazione di rappresentanti delle entità finanziarie per ottenere spiegazioni scritte od orali su fatti o documenti relativi all'oggetto e alle finalità dell'indagine e registrarne le risposte;

   ii) l'audizione di persone fisiche o giuridiche consenzienti allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine;

c) il richiedere l'applicazione di misure correttive e di riparazione per le violazioni dei requisiti del presente regolamento.

Accesso a documenti e dati

Ispezioni e indagini

Misure correttive di riparazione

Tempistica di applicazione

DORA Regulation

Regulation Adoption
2 years from entry into force*

Regulatory Technical Standards (***RTS***)

		Regulation Adoption (2 years from entry into force*)
Pillar 2 ICT & Cyber Risk	• ICT / Cyber Risk Management and reports • Details of Security and ICT measures / processes	1 year
	Harmonization of criteria for incident and cyber threat classification at EU level	1 year
Pillar 3 ICT & Cyber Incident	• Timeframes for incident reporting • Harmonization of templates for incident reporting and cyber threats notification at EU level	18 months
	Establishment of centralized reporting of major ICT-related incidents (ESA Report)	24 months
Pillar 4 Digital Resilience Testing	Test criteria, methodologies, requirements, in particular Threat Led Penetration Test	18 months
	• Third Party Risk Management strategy • Standard templates for the register of information	1 year
Pillar 5 Third Party Risk Management & Agreements	Sub-contract arrangements	18 months
	EU Critical 3rd Parties oversight	18 months

17.01.2024 — 17.07.2024 — ***Application*** *17.01.2025*

DORA Regulation specifies that until the RTS are detailed and published, Financial Institutions shall refer to the following regulations and guidelines as a reference standard:

- **ESA** (European Supervisory Authority) **Guidelines: EBA; EIOPA, ESMA.**
- **TIBER EU**, with reference to Pillar 4 - Digital Resilience Testing.

Focus: RTS timeline

Issuing date	Public Consultation	EU Comm. Approval
17.01.24	Jun/Jul 23 ▼ 15 Set 23	December 23
17.07.24	Nov 23 ▼ Feb 24	May 24

Sistema sanzionatorio

- **Misure e sanzioni:**
  - Efficaci
  - Proporzionate
  - Dissuasive
- Sanzioni **amministrative**
  a) Emanare un ordine che imponga di porre termine al comportamento in violazione
  b) Richiedere la cessazione temporanea o permanente di pratiche
  c) Adottare qualsiasi tipo di misura, anche pecuniaria
  d) Chiedere le registrazione esistenti del traffico di dati
  e) Pubblicazione comunicazione pubbliche indicanti l'identità del trasgressore e la violazione
- Sanzioni **penali** (facoltative)

DORA e NIS2

- L'articolo 1, paragrafo 2, del DORA stabilisce che, in relazione alle entità finanziarie che rientrano nel campo di applicazione della direttiva NIS 2 e delle corrispondenti norme nazionali di recepimento, **il DORA è considerato un atto giuridico dell'Unione specifico del settore** ai fini dell'articolo 4 della direttiva NIS 2. Tale affermazione è rispecchiata nel considerando (1).
- Questa affermazione trova riscontro nel considerando (28) della Direttiva NIS 2.
- Di conseguenza, le disposizioni del DORA relative alla gestione del rischio delle tecnologie dell'informazione e della comunicazione, alla gestione degli incidenti legati alle TIC nonché alle prove di resilienza operativa digitale, agli accordi di condivisione delle informazioni e al rischio di terzi per le TIC **si applicano al posto di quelle previste dalla direttiva NIS 2**
- Gli Stati membri non devono quindi applicare le disposizioni della direttiva NIS 2 sugli obblighi di gestione e segnalazione del rischio di cybersecurity, nonché sulla vigilanza e sull'applicazione della normativa, alle entità finanziarie coperte dalla DORA.

Aspetti salienti e buone pratiche per l'implementazione del DORA

- Considerare il DORA come un'opportunità strategica
  - Fiducia dei clienti + rafforzamento delle capacità TIC e Cyber
- Sfruttare e potenziare le capacità già presenti nell'azienda
  - Non reinventare la ruota, ma valorizzare le *best practice* implementate localmente
- Adottare un approccio integrato e interfunzionale con l'impegno delle parti interessate
  - Integrazione tra processi esistenti, evitando l'approccio a silos
- Coordinamento e direzione di gruppo efficaci
  - Governance di gruppo, con benchmarking sincronizzato tra le filiali
- Se già non implementato, avviare subito un «Programma di trasformazione DORA»

Modello di erogazione

Valutare

Valutazione della maturità

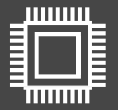
- Gap analysis del TIC risk management
- Progettazione di una roadmap per aumentare la maturità.
- Stima e approvazione del budget.

Implementare

Consegna del programma

- Revisione del report di incidenti.
- Implementare le misure di rimedio.
- Creare capacità di resilienza specifiche; ad esempio, gestione delle terze parti, gestione dell'identità e dell'accesso (IAM), architettura di rete, ecc.

Incorporare



Trasformazione strategica

- Assessment dei fornitori critici e rinegoziazione die contrati.
- Verifica dell'efficacia del controllo.
- Abilitazione digitale attraverso soluzioni basate su strumenti (*compliance by design*).

Grazie per la… tensione!

«[…] se non v'è dispiaciuta affatto, vogliatene bene a chi l'ha scritta, e anche un pochino a chi l'ha raccomodata. Ma se in vece fossimo riusciti ad annoiarvi, credete che non s'è fatto apposta.»

Avv. FILIPPO BIANCHINI

Via Bontempi, 1

06122 PERUGIA

(+39) 075 5723243 – (+39) 349 2864103

info@bianchini.legal

studiolegale

@legale