Future evoluzioni regolamentari dalla spinta UE: il Regolamento DORA e il suo impatto nel contesto assicurativo nazionale

Incontro Acorà
luglio 2022

pwc

Agenda

- Le novità regolamentari europee con impatti tecnologici
- Il pacchetto UE sulla Finanza Digitale
- Il Regolamento DORA
- Il confronto tra DORA ed EIOPA
- La percezione del mercato FS italiano: survey PwC
- Il presidio dei temi IT e Cyber da parte dell'Autorità nazionale: il questionario IVASS

Lo Tsunami delle novità Regolamentari Globali ed Europee

Le normative si evolvono secondo un approccio risk-based

Responsabilità

La Cyber Security è un rischio aziendale e in quanto tale è necessaria una corretta gestione e responsabilità del Top Management per supportare i piani strategici. Il Ruolo del CISO ora viene esplicitamente regolamentato.

Gestione Terze Parti

Regole di sicurezza informatica applicabili non solo agli istituti finanziari ma anche alle terze parti. Concentrarsi sui fornitori di servizi cloud.

Cyber resilience

Concentrarsi sulla capacità di poter anticipare, contenere e recuperare rapidamente. Identificare quelle che sono le funzioni aziendali critiche, le risorse informative di supporto, i collegamenti esterni e le dipendenze.

Valutare la reale esposizione ai rischi cyber e la relativa capacità di reazione attraverso verifiche realistiche della sicurezza (Vulnerability Assessment & Penetration Test)

Risk-based

Ci si aspetta che le organizzazioni seguano un approccio basato sul rischio che consideri i rischi informatici e le minacce per la propria attività, definiscano il Cyber Risk e lo colleghino al loro quadro di rischio aziendale.

Gestione degli incidenti

Definire e testare processi per la gestione e risposta agli incidenti, che comprendano la segnalazione di eventi di rischio Cyber alle autorità e ai clienti interessati entro determinati periodi di tempo.

Condivisione delle informazioni

Condivisione delle informazioni con le parti interessate interne ed esterne all'organizzazione, in merito alle minacce, vulnerabilità, incidenti e attività di risposta.

Il fattore umano rimane essenziale per la sicurezza informatica. Le autorità si aspettano l'attuazione di comportamenti sicuri a tutti i livelli dell'organizzazione, dimostrando che la sicurezza informatica è radicata all'interno dei processi aziendali.

Le Regolamentazioni Europee in ambito Technology ed FS

Regulatory Body / Regulation

EU Commission

Digital Services Act (DSA) - *Proposta*
- Stabilire una trasparenza e un chiaro quadro di responsabilità per le piattaforme online, compresa la rimozione dei contenuti illegali

Digital Markets Act (DMA) - *Proposta*
- Alcune grandi piattaforme online fungono da "gatekeeper" nei mercati digitali. Il DMA mira a garantire che queste piattaforme si comportino in modo equo.

Digital Operational Resilience Act (DORA) – *Proposta Settembre 2020*
- Armonizzare i requisiti di rischio ICT in tutta Europa, in modo che il sistema finanziario disponga delle garanzie necessarie per mitigare gli attacchi informatici e altri rischi.

Markets in Crypto-Assets Regulation (MiCA) – *Proposta Settembre 2020*
- Stati membri dell'UE e regolamentare tutti gli emittenti e i fornitori di servizi che si occupano di criptovalute.

Artificial Intelligence Act - *Proposta*
- Norme dell'UE per affrontare le questioni di responsabilità relative alle nuove tecnologie, compresi i sistemi di IA

Data Governance Act - *Proposta*
- Framework per facilitare la condivisione dei dati

Data Act - *Proposta*
- Framework per i diritti di accesso e utilizzo dei dati.

ECB

Cyber Information and Intelligence Sharing Initiative (CIISI-EU) - *2020*
- Facilitare la condivisione di informazioni, intelligence e best practices tra le infrastrutture finanziarie

SREP IT & Cyber Risk Questionnaire - *2017*
- Raccolta standardizzata di informazioni dei soggetti della vigilanza bancaria per la valutazione completa di tutte le aree di rischio IT.

TIBER – EU - *2018*
- In che modo le autorità, le entità, i servizi di threat intelligence e di red teaming devono collaborare per testare e migliorare la resilienza informatica delle entità effettuando un attacco informatico controllato.

EIOPA

Guidelines on Outsourcing to Cloud Service Providers – *Gennaio 2021*
- Aspettative di vigilanza a livello EU per gli outsourcing in ambito cloud computing in ambito assicurativo

Guidelines on ICT & Security Governance – *Aprile 2021*
- Come le imprese assicurative dovrebbero gestire i sistemi ICT ed i rischi per la sicurezza a cui sono esposte
- Gestione dei rischi ICT e di sicurezza attraverso l'istituzione di una sana governance interna e di un quadro di controllo interno che stabilisca chiare responsabilità per il personale delle imprese assicurative, compresi gli organi di gestione.

EBA

Guidelines on ICT & Security Risk Management - *June 2020*
- Come le istituzioni finanziarie dovrebbero gestire i sistemi ICT ed i rischi per la sicurezza a cui sono esposte
- Gestione dei rischi ICT e di sicurezza attraverso l'istituzione di una sana governance interna e di un quadro di controllo interno che stabilisca chiare responsabilità per il personale delle istituzioni finanziarie, compresi gli organi di gestione.

EBA Guidelines on Outsourcing – *September 2019*
- Gli orientamenti definiscono le disposizioni di governance interna che gli enti creditizi, gli istituti di pagamento e gli istituti di moneta elettronica dovrebbero attuare quando esternalizzano servizi, attività o funzioni interne.

Recommendations on Outsourcing to Cloud Service Providers – *July 2018*
- Aspettative di vigilanza a livello EU per gli outsourcing in ambito cloud computing in ambito bancario

Report with advice for the European Commission on Crypto-Assets – *January 2019*
- EBA raccomanda alla Commissione europea di effettuare ulteriori analisi per determinare la risposta appropriata a livello di UE in ambito criptovalute

Il pacchetto UE sulla Finanza Digitale

Il **Regolamento DORA** si innesta nel più ampio «**Pacchetto UE sulla finanza digitale**», volto a consentire e sostenere ulteriormente il potenziale della finanza digitale in termini di innovazione e concorrenza, attenuando nel contempo i rischi che ne derivano per i consumatori, le imprese e, in generale, la stabilità finanziaria dell'Unione.

Attraverso tali proposte normative saranno offerti inoltre ai consumatori e alle imprese una più **ampia scelta di servizi finanziari** e **soluzioni di pagamento moderne**, garantendo al tempo stesso
la tutela dei degli stessi e la stabilità finanziaria.

Regolamento Markets in Crypto-Assets «MICA»

La proposta di regolamento pone quale obiettivo la definizione di un **sistema di regole armonizzato in materia di cripto-attività**, e segnatamente cripto-valute (o valute virtuali), che consenta di coglierne le opportunità per lo sviluppo di servizi digitali finanziari innovativi e mitigarne i rischi per i consumatori, le imprese e la stabilità finanziaria dell'Unione.

Regolamento Digital Ledger Technology «DLT»

La proposta di regolamento, in combinazione con il MiCA, rappresenta il **primo intervento** concreto nell'ambito delle infrastrutture a supporto della negoziazione delle cripto-attività, volto a fornire livelli adeguati di tutela dei consumatori, degli investitori e di certezza del diritto per le stesse cripto- attività, ed a consentire alle imprese innovative **di utilizzare la *blockchain* e la tecnologia Distributed Ledger Technology (DLT)**.

Regolamento Digital Operational Resilience «DORA»

La proposta di regolamento pone quale obiettivo la definizione di un quadro dettagliato e completo di **regole per l'identificazione e gestione dei rischi ICT**, stabilendo obblighi in materia di *testing* delle infrastrutture e dei fornitori e adozione ed applicazione di strategie, politiche, procedure, strumenti e protocolli in materia di resilienza operativa digitale.

Direttiva Digital Operational Resilience «DORA»

La proposta di Direttiva si inserisce ad un più alto livello nel contesto del DORA e pone quale obiettivo la certezza del diritto in materia di operazioni in cripto-attività e il rafforzamento della resilienza operativa digitale mediante un'esenzione temporanea per i sistemi multilaterali
di negoziazione (MTF) e la modifica di talune Direttive UE rilevanti per il settore FS quali **UCITS IV, AIFMD, MiFID II, CRDIV, PSD2** e **Solvency II**.

Perché il Regolamento DORA?

A fronte della crescente importanza che le tecnologie dell'informazione e della comunicazione rivestono nelle attività e nella prestazione dei servizi finanziari da parte delle entità finanziarie, la proposta della Commissione si pone nell'ottica di **armonizzazione ed uniformazione minima delle regole concernenti la sicurezza delle reti e dei sistemi informativi attualmente in essere a livello di Unione Europea**.

RIDUZIONE DELLE DISPARITA' FRA GLI STATI MEMBRI	**Armonizzazione** degli obblighi organizzativi e procedurali in materia di identificazione dei rischi ICT in capo alle entità finanziarie per la **creazione** di un **cd. *level playing field*** tra gli Stati Membri
INNALZAMENTO DELLO STANDARD EUROPEO IN MATERIA DI CYBER SECURITY	Il **Regolamento DORA** è altresì atto ad **anticipare** le **necessità** in materia di ***cyber security*** data l'accelerazione della **digitalizzazione** ed **evoluzione tecnologica dei servizi finanziari**, ancor più marcata in seguito all'emergenza Covid-19
GOVERNANCE DEI RISCHI ICT E RISCHI CYBER	**Valorizzazione** dei rischi ICT e rischi Cyber quali **rischi autonomi in ambito operativo e finanziario**, con conseguente obbligo per le entità finanziarie di definizione di un **quadro organizzativo e procedurale di *governance***, anche finanziaria, degli stessi integrata nel più ampio quadro dei **rischi operativi**
RUOLO DELLE AUTORITÀ DI VIGILANZA	**Centralizzazione** del **ruolo** delle **Autorità di vigilanza** sia in ambito di **controllo** e **valutazione** dei presidi adottati dalle entità finanziarie che nella **gestione** degli **incidenti** e **valutazione** dei **rischi** derivanti dalla **dipendenza** delle **entità finanziarie** dai **fornitori** di servizi ICT terzi

«[...] La BCE accoglie con favore l'obiettivo del regolamento proposto di rimuovere gli ostacoli al mercato interno dei servizi finanziari e di migliorarne il funzionamento attraverso l'armonizzazione delle norme applicabili nel settore della gestione dei rischi delle tecnologie dell'informazione e della comunicazione (ICT) [...]»

Fonte: Opinione BCE del 4 giugno 2021 sulla proposta di Regolamento DORA

Roadmap Regolamentare

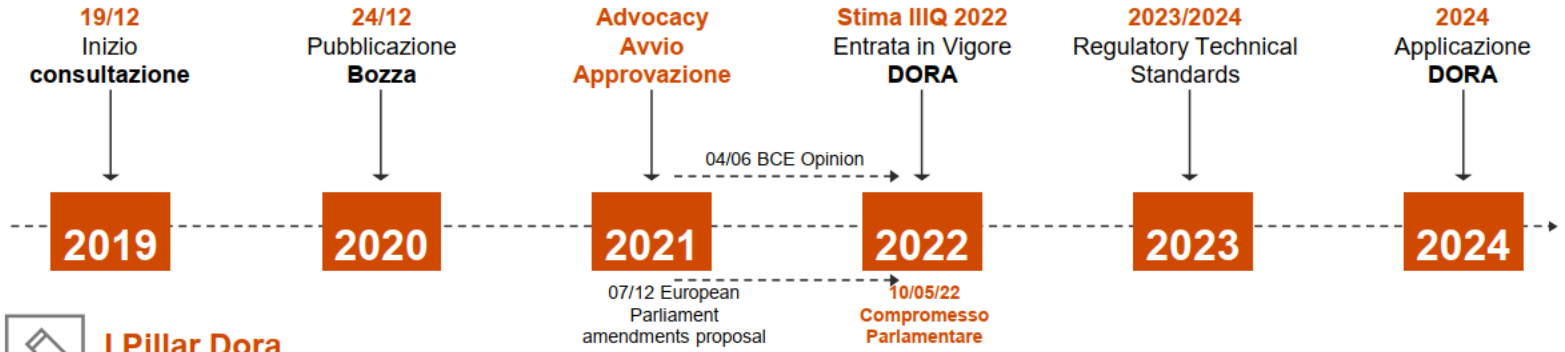
Il carattere fondante della proposta di regolamento UE DORA: un big bang della cyber security per il sistema finanziario comunitario, con obiettivi comuni sfidanti. Un effetto di istantaneo innalzamento dello standard regionale, che rende il sistema finanziario comunitario più forte e con ricadute anche 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 i**n ambito FS**.
- Il perimetro di applicazione DORA ricomprende le **entità del settore finanziario tradizionale** come istituti di credito, borse e stanze di compensazione, **gestori di fondi** alternativi, società di gestione, imprese di **assicurazione**, istituti di **pagamento**, istituti di moneta elettronica, nonché fornitori di servizi di **cripto-valuta**, emittenti di ***cripto-asset*** ed emettenti di ***token***.

Iter legislativo



I Pillar Dora

1. **Governance e Struttura Interna ICT / Cyber** *(requisiti già esistenti in ambito banking)*
2. **Gestione dei Rischi ICT e Cyber End-to-End**
3. **Reporting degli Incidenti ICT e Cyber**
4. *Nuovi requisiti in ambito* **Digital Resilience Testing**
5. **Gestione delle Terze Parti ICT** e **TPRM**
6. **Information Sharing** a livello EU
7. *Ruoli e Responsabilità delle* **Autorità Competenti**

Oltre al Regolamento, aspetti di dettaglio saranno definiti mediante le norme tecniche di regolamentazione (RTS):

- **Strumenti**, **metodi**, **processi** e **politiche** di **gestione** del **rischio ICT**.
- **Modalità** di **classificazione** degli **incidenti ICT**.
- Contenuti e formato della **segnalazione** di **incidenti ICT** alle **Autorità competenti**.
- **Contenuti** e **modalità** per l'**implementazione** e l'**aggiornamento** del **registro** contenente informazioni su tutti gli **accordi** con **fornitori ICT**.
- **Contenuti** e **modalità** di vigilanza dei **fornitori** di **funzioni critiche ICT**.

DORA ha effetti *disruptive* nella *regulation* dei Financial Services

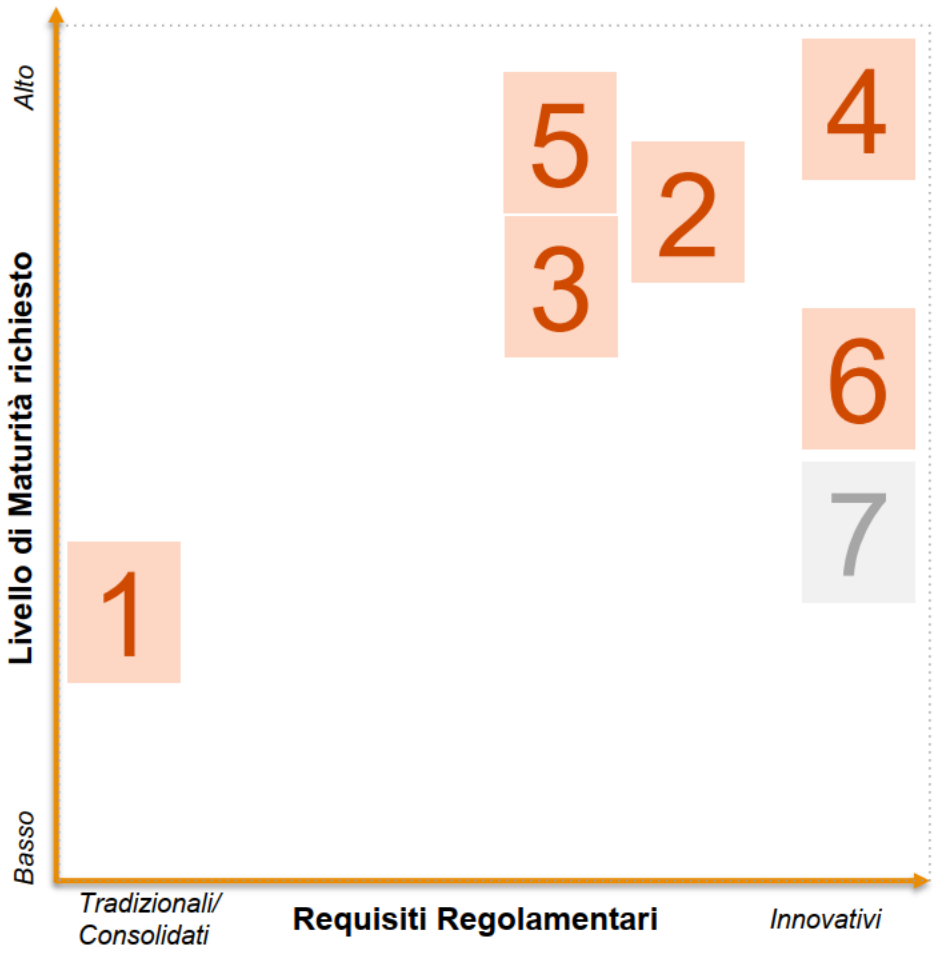
I principali impatti:

- **migliorare** e **semplificare** le attività delle entità finanziarie nella **gestione del rischi ICT e Cyber**.
- stabilire meccanismi di verifica dei sistemi ICT.
- aumentare l'***awareness*** delle autorità di vigilanza e delle entità finanziarie sui **rischi** informatici / cyber e sugli **incidenti** ICT / Cyber.
- introdurre **nuovi poteri per le Autorità di vigilanza** finanziaria per sorvegliare i rischi derivanti dalla dipendenza delle entità finanziarie da **fornitori** di servizi ICT di terze parti.

Inoltre, il Regolamento DORA impone **analisi interpretative approfondite** sotto il **profilo legale** e **regolamentare** degli impatti delle novità introdotte in materia di resilienza operativa digitale sui **diversi quadri normativi** e **regolamentari** degli **operatori del mercato FS**.

	Banking & Payments Markets	Investment Services	Asset Management	Insurance
Normativa UE	CRD/CRR	MiFIR	UCITS IV	Solvency II
	PSD2	EMIR	AIFMD	IDD
	EMD2	MiFID2		IORPII
	EBA Guidelines	ESMA Guidelines		**EIOPA Guidelines**
	NIS Directive			
	GDPR			
	SFDR			
	TIBER EU Framework			
Normativa Nazionale	TUB	TUF		CAP
	BoI Circ. 285	Regolamento Emittenti		**IVASS Reg. 38**
	BoI Circ. 288	Regolamento Intermediari		IVASS Reg. 40
	Disp. Vig. IMEL	Reg. attuat. artt. 4-*undecies* TUF		IVASS Reg. 41
	Perimetro Nazionale di Sicurezza Cibernetica			

I Pillar del Regolamento EU DORA (1/2)



1 GOVERNANCE E STRUTTURA INTERNA

- Ruolo centrale dell'organo di gestione nell'adozione, gestione e monitoraggio del quadro interno di gestione del rischio ICT;
- Formazione specifica / Digital Training per il Top Management;
- Empowerment delle responsabilità per le funzioni interne ICT;
- Monitoraggio della corretta applicazione delle politiche e del processo di gestione interna del rischio ICT;
- Reporting continuo da parte delle funzioni ICT sugli incidenti e sulle soluzioni correttive implementate.

2 GESTIONE END TO END DEI RISCHI ICT E CYBER

Visione End-to-End del processo di Gestione dei Rischi ICT/Cyber tra:

II linea (Risk Management):

- Politiche, Framework e processi di valutazione e gestione del rischio ICT/Cyber come rischio operativo
- Definizione di impact tolerances, scenario analysis ed integrazione RAF (approvazione dell'organo di gestione)
- Revisione / aggiornamento annuale o in caso di incidenti

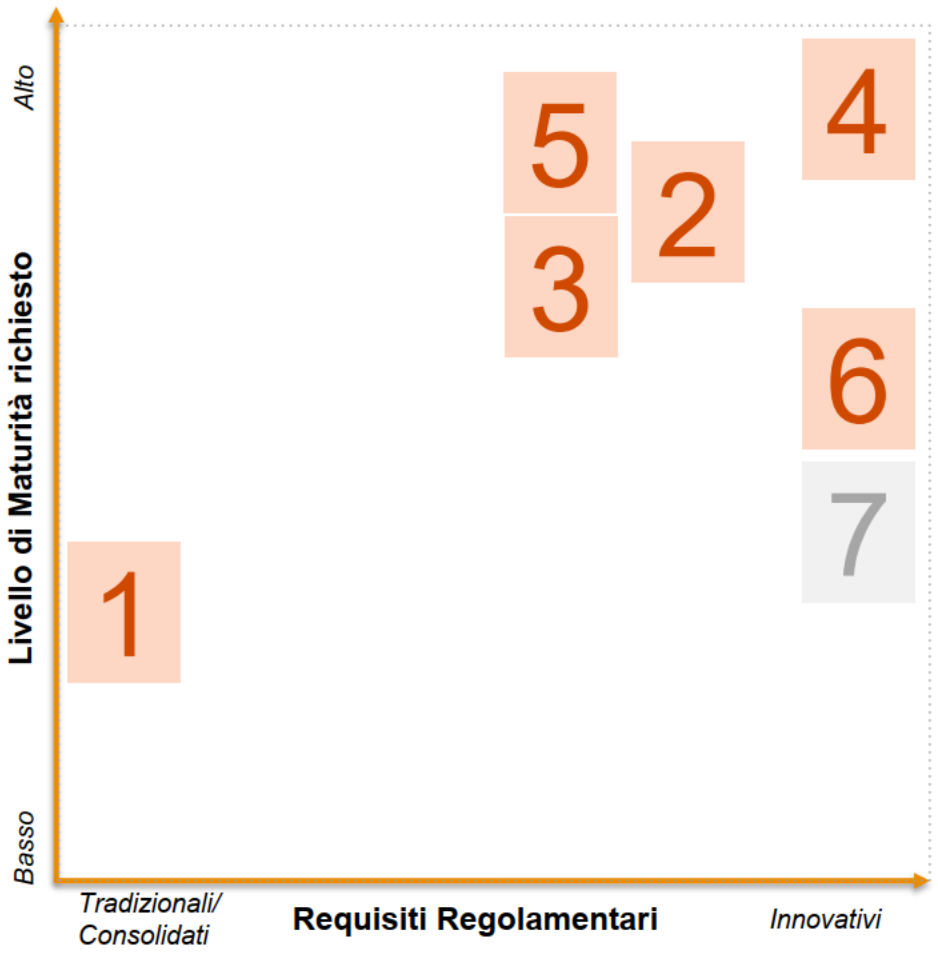
I Linea (Operations):

- Visione per servizi di business (critical functions)
- Threat analysis & scenario management
- Misure tecniche ed organizzative per protezione e la prevenzione ICT/Cyber;
- Progettazione e realizzazione Infrastrutture ed architetture resilienti
- Monitoraggio predittivo e early detection delle anomalie;
- Continuous improvement, root cause e incident post-mortem analysis;
- Strategie di business continuity, back-up e disaster recovery basate su scenari plausibili e con vista per servizi di business.

3 REPORTING DEGLI INCIDENTI ICT E CYBER

- Definizione ed implementazione di processi e procedure per monitorare, gestire e registrare gli incidenti ICT/Cyber
- Classificazione degli incidenti sulla base di soglie di rilevanza definite dalle Autorità
- Segnalazione alle autorità competenti dei soli incidenti ICT/Cyber sulla base della gravità
- Trasparenza al mercato
- Strategie e processi di comunicazione interna/esterna

I Pillar del Regolamento EU DORA (2/2)



4 DIGITAL OPERATIONAL RESILIENCE TESTING

Istituzione, mantenimento ed esecuzione periodica (prevalentemente annuale) di un programma di test di resilienza operativa digitale sull'intero parco dei sistemi ICT, che comprenda anche gli aspetti Cybersecurity ed inclusivo delle logiche TIBER-EU.

5 TPRM, MANAGEMENT & AGREEMENTS

- Adozione, nell'ambito dell'ICT/Cyber Risk Framework, di una strategia per il monitoraggio e la gestione dei rischi derivanti da fornitori di servizi ICT/Cyber di terze parti
- Inclusione di clausole standard nei contratti con fornitori terzi di servizi ICT/Cyber;
- Mantenimento e aggiornamento di un registro con informazioni su tutti gli accordi con fornitori ICT/Cyber;
- Monitoraggio dello stato di implementazione delle misure ICT/Cyber da parte dei fornitori di servizi ICT/Cyber.

6 INFORMATION SHARING

Programma (su base volontaria) di condivisione di informazioni relative a minacce informatiche all'interno della *community* delle entità finanziarie soggette al DORA al fine di:

- migliorare la resilienza operativa digitale del mercato europeo FS
- aumentare la consapevolezza delle minacce informatiche
- contenere la diffusione delle minacce informatiche
- rafforzare le capacità di difesa delle entità finanziarie

7 REPORTING DEGLI INCIDENTI ICT E CYBER

Le AEV, attraverso Comitati congiunti e in collaborazione con le Autorità Competenti, la BCE e il CERS, possono introdurre meccanismi di condivisione di pratiche efficaci e di meccanismi esercitazione a livello EU per la creazione di un piano di condivisione dei rischi ICT/Cyber più comuni con l'obiettivo finale di una maggiore resilienza dei mercati finanziari e promuovere modalità di risposta coordinata a livello UE

DORA vs. EIOPA

- DORA definisce un **approccio olistico e completo** di **gestione dei rischi ICT e Cyber** in ottica **End-to-End,** stabilendo i principi per la **I e II linea**, comprese le **attività operative** e di **governance** della **sicurezza** e dell'**ICT**, oltre che di gestione delle **IIIe Parti**, per tutti i settori dei Financial Services.
- Gli orientamenti **EIOPA** definiscono specifici **requisiti organizzativi, operativi, tecnici** e per **processi specifici**, **dettagliando** principi parzialmente enunciati anche nelle disposizioni DORA.
- Gli orientamenti **EIOPA Outsourcing to Cloud Service Provider** sono focalizzate sui servizi cloud in outsourcing, mentre l'ambito **DORA copre tutti gli accordi di terze parti ICT** (outsourcing e non outsourcing).
- Maggiori **dettagli operativi** sull'applicazione dei **principi DORA** verranno emanati tramite **RTS**, che verranno emanati dalle Autorità Competenti in seguito all'emanazione del Regolamento. Nel mentre, i requisiti EIOPA vengono comunque applicati ai diversi topic organizzativi, operativi ed implementativi.
- Considerati i diversi perimetri e le tempistiche di applicazione, come PwC **suggeriamo** alle istituzioni assicurative la valutazione dell'opportunità di **armonizzare** le attività organizzative, operative e di implementazione in corso per la **conformità EIOPA** rispetto ai **principi DORA**.

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**

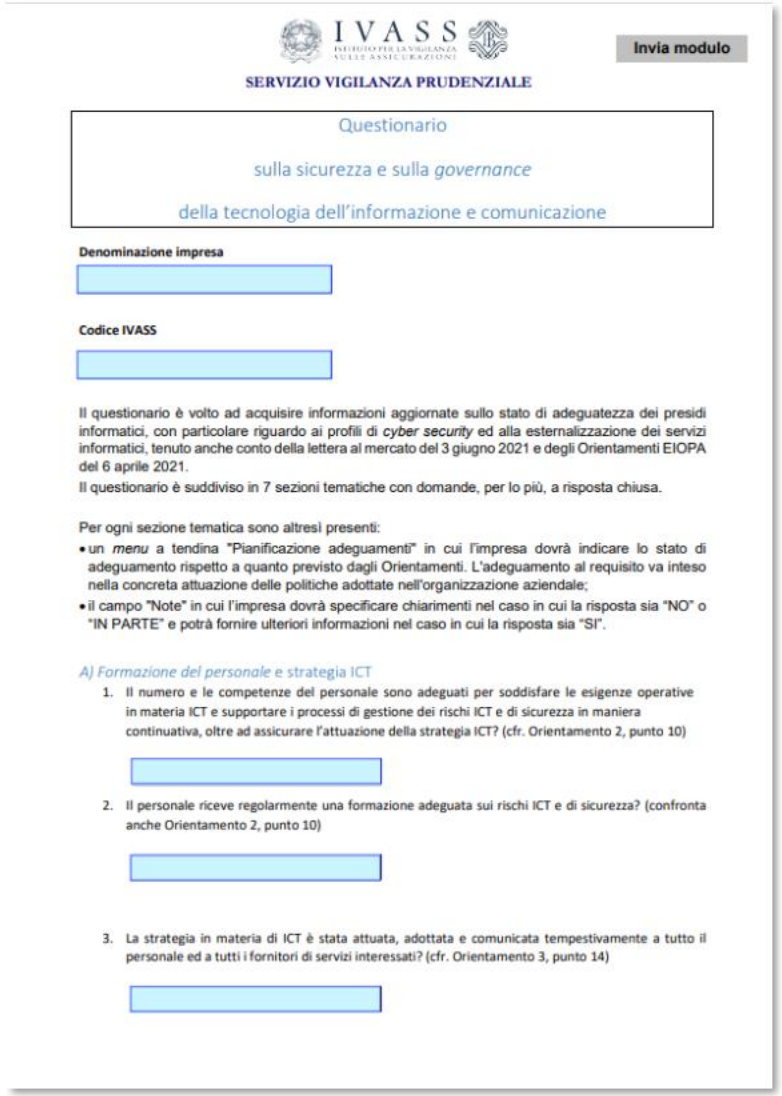
40%

Over Regulation

6%

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

Il questionario IVASS per l'adeguamento EIOPA



IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Invia modulo

SERVIZIO VIGILANZA PRUDENZIALE

Questionario

sulla sicurezza e sulla *governance*

della tecnologia dell'informazione e comunicazione

Denominazione impresa

Codice IVASS

Il questionario è volto ad acquisire informazioni aggiornate sullo stato di adeguatezza dei presidi informatici, con particolare riguardo ai profili di *cyber security* ed alla esternalizzazione dei servizi informatici, tenuto anche conto della lettera al mercato del 3 giugno 2021 e degli Orientamenti EIOPA del 6 aprile 2021.

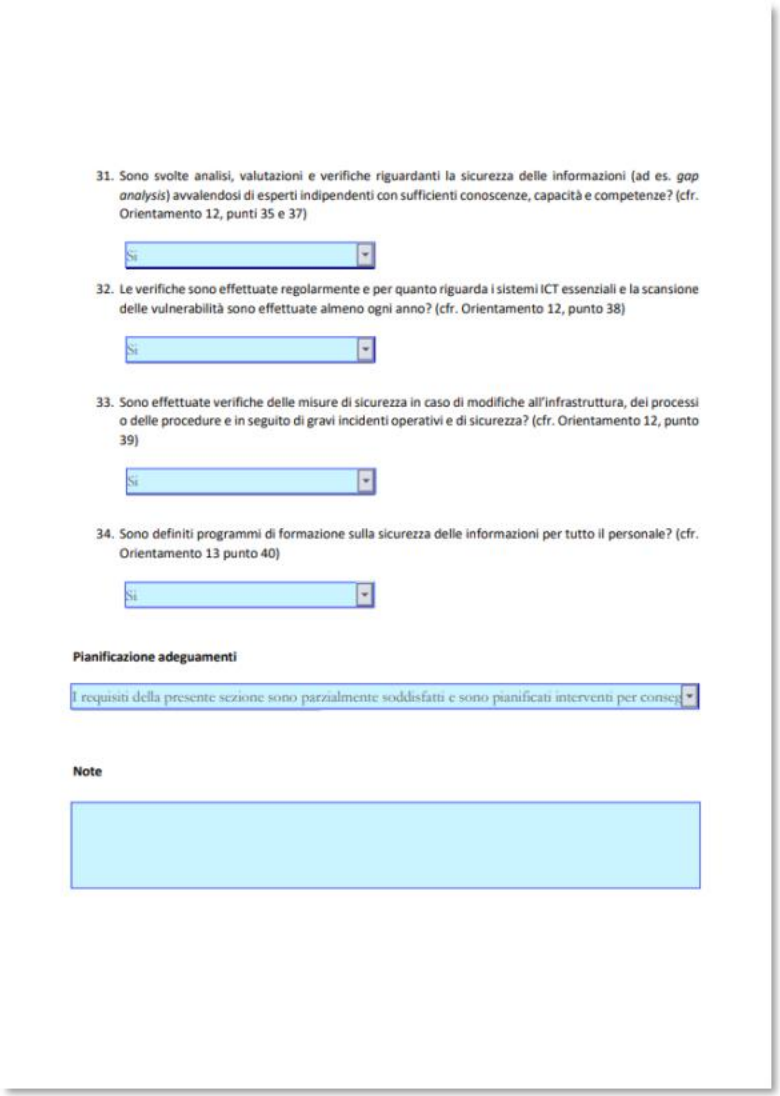
Il questionario è suddiviso in 7 sezioni tematiche con domande, per lo più, a risposta chiusa.

Per ogni sezione tematica sono altresì presenti:

- un *menu* a tendina "Pianificazione adeguamenti" in cui l'impresa dovrà indicare lo stato di adeguamento rispetto a quanto previsto dagli Orientamenti. L'adeguamento al requisito va inteso nella concreta attuazione delle politiche adottate nell'organizzazione aziendale;
- il campo "Note" in cui l'impresa dovrà specificare chiarimenti nel caso in cui la risposta sia "NO" o "IN PARTE" e potrà fornire ulteriori informazioni nel caso in cui la risposta sia "SI".

A) Formazione del personale e strategia ICT

1. Il numero e le competenze del personale sono adeguati per soddisfare le esigenze operative in materia ICT e supportare i processi di gestione dei rischi ICT e di sicurezza in maniera continuativa, oltre ad assicurare l'attuazione della strategia ICT? (cfr. Orientamento 2, punto 10)
2. Il personale riceve regolarmente una formazione adeguata sui rischi ICT e di sicurezza? (confronta anche Orientamento 2, punto 10)
3. La strategia in materia di ICT è stata attuata, adottata e comunicata tempestivamente a tutto il personale ed a tutti i fornitori di servizi interessati? (cfr. Orientamento 3, punto 14)



31. Sono svolte analisi, valutazioni e verifiche riguardanti la sicurezza delle informazioni (ad es. *gap analysis*) avvalendosi di esperti indipendenti con sufficienti conoscenze, capacità e competenze? (cfr. Orientamento 12, punti 35 e 37)

Si

32. Le verifiche sono effettuate regolarmente e per quanto riguarda i sistemi ICT essenziali e la scansione delle vulnerabilità sono effettuate almeno ogni anno? (cfr. Orientamento 12, punto 38)

Si

33. Sono effettuate verifiche delle misure di sicurezza in caso di modifiche all'infrastruttura, dei processi o delle procedure e in seguito di gravi incidenti operativi e di sicurezza? (cfr. Orientamento 12, punto 39)

Si

34. Sono definiti programmi di formazione sulla sicurezza delle informazioni per tutto il personale? (cfr. Orientamento 13 punto 40)

Si

Pianificazione adeguamenti

I requisiti della presente sezione sono parzialmente soddisfatti e sono pianificati interventi per conseg

Note

7 Sezioni tematiche, in cui sono suddivisi 83 Controlli

A. Formazione del personale e strategia ICT
B. Rischi ICT e di sicurezza
C. Sicurezza delle informazioni
D. Gestione degli incidenti operativi o di sicurezza
E. Gestione delle attività ICT
F. Gestione della continuità operativa
G. Esternalizzazione di servizi ICT con riferimento anche al *cloud**

- **Verifica dello stato di adeguatezza rispetto ai singoli requisiti degli Orientamenti EIOPA**
- **Richiesta di visibilità della pianificazione degli Adeguamenti previsti**

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.

Thank you

pwc.com/it

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or exhaustiveness of the information contained in this publication, and, to the extent permitted by law, PwC Business Services, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2022 PwC Business Services. All rights reserved. Not for further distribution without the permission of PwC Business Services. In this document, “PwC” refers to PwC Business Services which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.