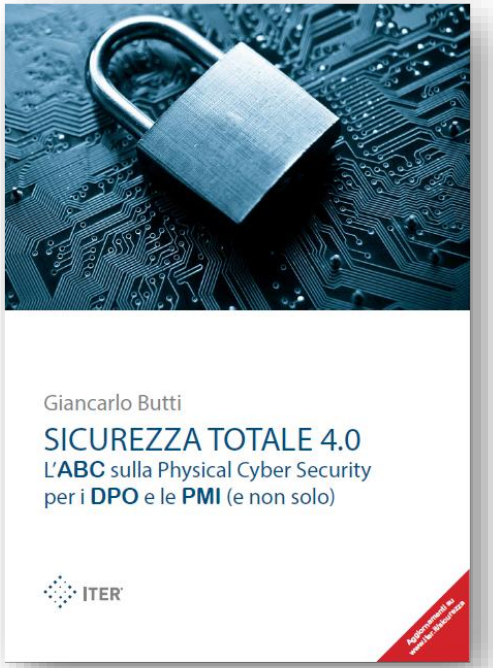
Digital Operational Resilience Act

Giancarlo Butti

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Membro del Comitato Scientifico del CLUSIT.
Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni.
Oltre 150 corsi e seminari tenuti presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CEFRIEL, ABI…; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.
Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate.
Ha pubblicato 26 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 27 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT.
Socio e già proboviro di AIEA è socio del CLUSIT e del BCI.
Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.blog.europrivacy.info .
Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.


Fondamenti per l'implementazione del Digital Operational Resilience Act
Giancarlo Butti
Manuale di resilienza
Guida pratica alla progettazione, gestione e verifica delle soluzioni di business continuity e disaster recovery
ITER


Giancarlo Butti
SICUREZZA TOTALE 4.0
L'ABC sulla Physical Cyber Security per i DPO e le PMI (e non solo)
ITER


Giancarlo Butti - Alberto Piamonte
Governance del rischio
Dall'analisi al reporting e la sintesi per la Direzione
ITER

Resilienza: definizione

Treccani:

1. Nella tecnologia dei materiali, la resistenza a rottura per sollecitazione dinamica, determinata con apposita prova d'urto: prova di r.; valore di r., il cui inverso è l'indice di fragilità.

2. Nella tecnologia dei filati e dei tessuti, l'attitudine di questi a riprendere, dopo una deformazione, l'aspetto originale.

3. In psicologia, la capacità di reagire di fronte a traumi, difficoltà, ecc.

Garzanti:

1. (fis.) proprietà dei materiali di resistere agli urti senza spezzarsi, rappresentata dal rapporto tra il lavoro necessario per rompere una barretta di un materiale e la sezione della barretta stessa

2. capacità di resistere e di reagire di fronte a difficoltà, avversità, eventi negativi ecc.: resilienza sociale

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…

Guerra

Pandemia

Materie prime

Energia

Bank for International Settlements and International Organization of Securities Commissions: Guidance on cyber resilience for financial market infrastructures

…the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption. In the context of operational resilience, the Committee defines tolerance for disruption as the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios.

BCBS

Principles for Operational Resilience

operational resilience as the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption. In the context of operational resilience, the Committee defines tolerance for disruption as the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios

UK Prudential Regulation Authority

"…the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions. The PRA's proposed approach to operational resilience is based on the assumption that, from time to time, disruptions will occur which will prevent firms from operating as usual and see them unable to provide their services for a period. The PRA considers that many firms currently may not sufficiently plan on the basis that disruptions will occur and are therefore not ready to manage effectively when they do."

US: Sound Practices to Strengthen Operational Resilience

"…the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions."

Building a More Resilient Financial System in India through Governance Improvements – Speech by Shri Mahesh Kumar Jain, Deputy Governor, Reserve Bank of India – Friday, June 18, 2021

Dimensions of Resilience

Resilience of the financial system can be tested from many dimensions, viz., financial risks, operational and technological risks, competitive risks, climate risks etc., and the financial system is required to anticipate, absorb and adapt to the same.

- Financial Resilience
- Operational and Technological Resilience
- Competitive Resilience
- Climate Resilience

REGOLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 - (DORA)

«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;

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.

ISO 22316:2017(en)

Security and resilience — Organizational resilience — Principles and attributes

An organization’s resilience:

a) is enhanced when behaviour is aligned with a shared vision and purpose;

b) relies upon an up-to-date understanding of an organization’s context;

c) relies upon an ability to absorb, adapt and effectively respond to change;

d) relies upon good governance and management;

e) is supported by a diversity of skills, leadership, knowledge and experience;

f) is enhanced by coordination across management disciplines and contributions from technical and scientific areas of expertise;

g) relies upon effectively managing risk

ISO 22316:2017(en)

Security and resilience — Organizational resilience — Principles and attributes

The organization should develop a coordinated approach that provides:

— a mandate to ensure its leaders and top management are committed to enhance organizational resilience;

— adequate resources needed to enhance the organization’s resilience;

— appropriate governance structures to achieve the effective coordination of organizational resilience activities;

— mechanisms to ensure investments in resilience activities are appropriate to the organization’s internal and external context;

— systems that support the effective implementation of organizational resilience activities;

— arrangements to evaluate and enhance resilience in support of organizational requirements;

— effective communications to improve understanding and decision making.

Il contesto normativo

EU Commission

- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- Digital Operational Resilience Act (DORA)
- Markets in Crypto-Assets Regulation (MiCA)
- Artificial Intelligence
- Data Governance
- Data Act

ECB

- Cyber Information and Intelligence Sharing Initiative (CIISI-EU) -2020
- SREP IT & Cyber Risk Questionnaire -2017
- TIBER –EU -2018

EBA

- Guidelines on ICT & Security Risk Management -June 2020
- EBA Guidelines on Outsourcing –September 2019
- Recommendations on outsourcing to cloud service providers –July 2018
- Report with advice for the European Commission on Crypto-Assets –January 2019

BCBS

Prudential Treatment of Cryptoasset exposures -September 2021

G7

Fundamental elements of cybersecurity for the financial sector

Element 1: Cybersecurity Strategy and Framework.

Element 2: Governance.

Element 3: Risk and Control Assessment.

Element 4: Monitoring.

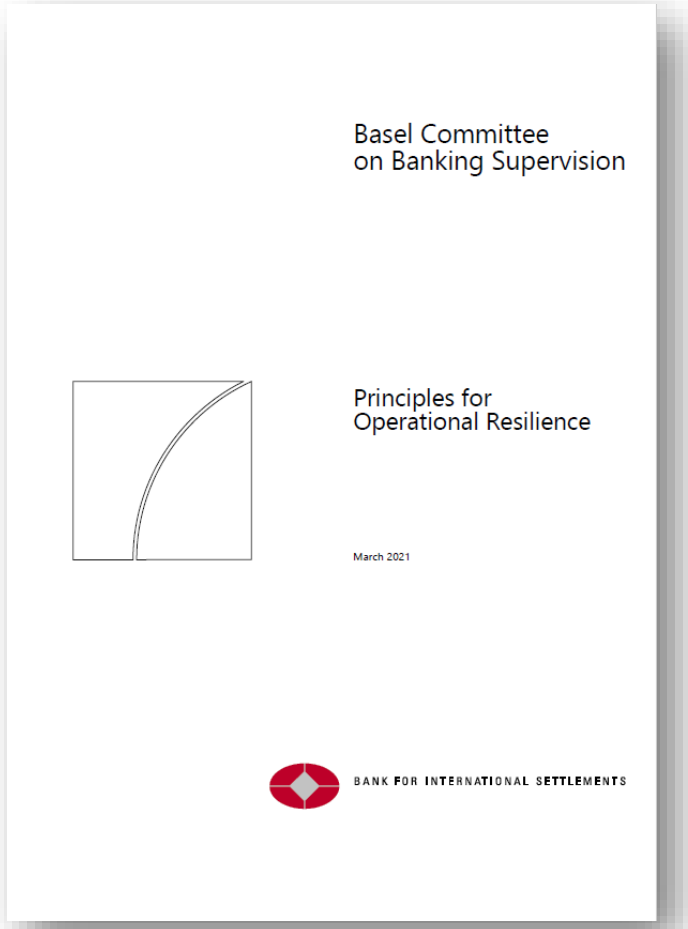
Element 5: Response.

Element 6: Recovery.

Element 7: Information Sharing.

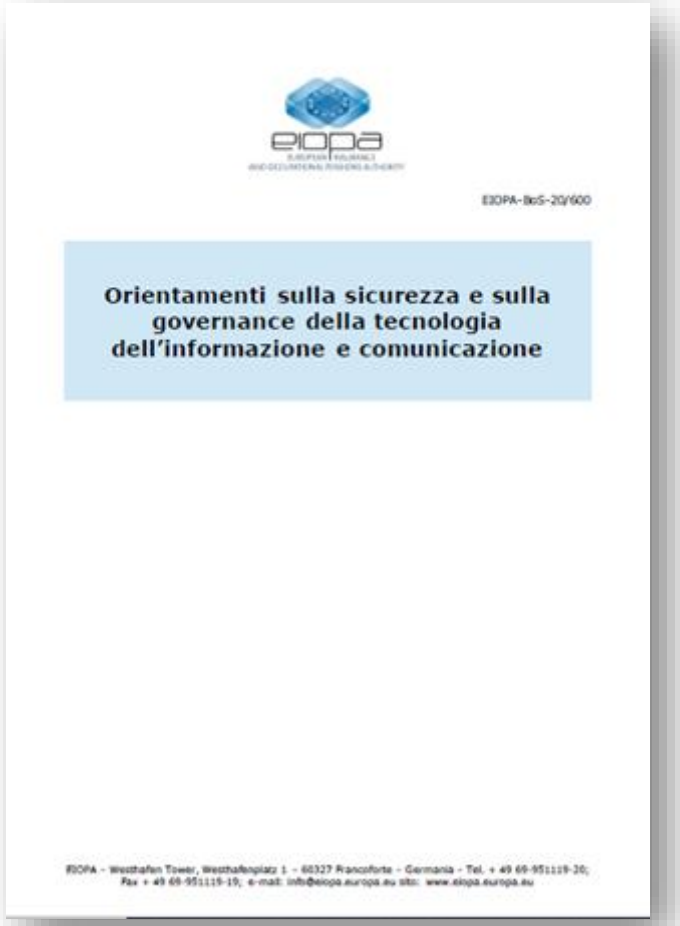
Element 8: Continuous Learning.

Basel Committee on Banking Supervision Principles for Operational Resilience



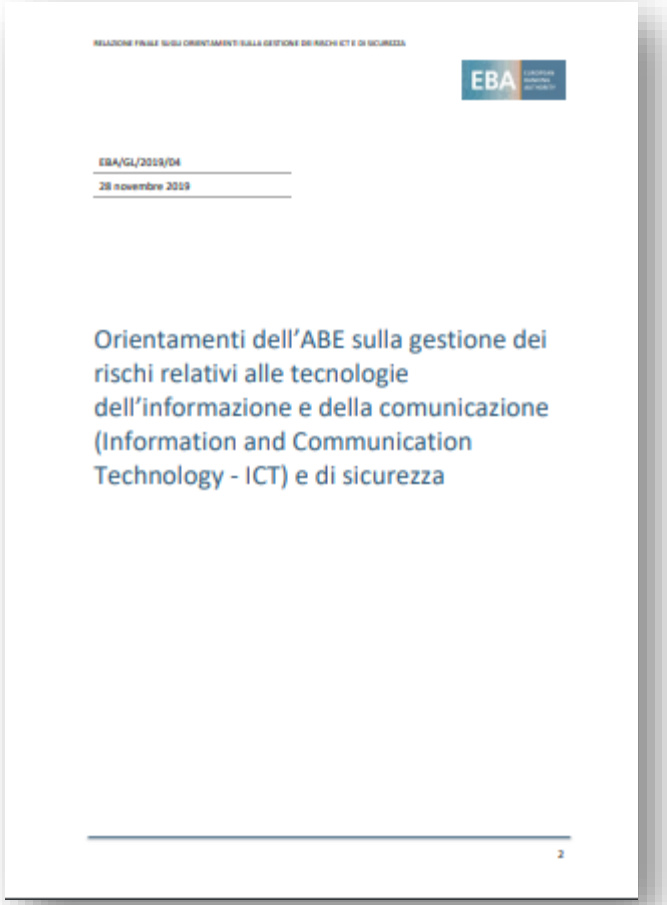
- Governance
- Operational risk management
- Business continuity planning and testing
- Mapping interconnections and interdependencies
- Third-party dependency management
- Incident management
- ICT including cyber security

EIOPA



- Orientamento 1 – Proporzionalità
- Orientamento 2 – Le ICT all'interno del sistema di governance
- Orientamento 3 – Strategia in materia di ICT
- Orientamento 4 – Rischi ICT e di sicurezza nell'ambito del sistema di gestione dei rischi
- Orientamento 5 – Audit
- Orientamento 6 – Politica e misure riguardanti la sicurezza delle informazioni
- Orientamento 7 – Funzione di sicurezza delle informazioni
- Orientamento 8 – Sicurezza logica
- Orientamento 9 – Sicurezza fisica
- Orientamento 10 – Sicurezza delle operazioni ICT
- Orientamento 11 – Monitoraggio della sicurezza
- Orientamento 12 – Analisi, valutazione e verifica della sicurezza delle informazioni
- Orientamento 13 – Sessioni formative e informative sulla sicurezza delle informazioni
- Orientamento 14 – Gestione delle operazioni ICT
- Orientamento 15 – Gestione degli incidenti e dei problemi legati alle ICT
- Orientamento 16 – Gestione dei progetti ICT
- Orientamento 17 – Acquisizione e sviluppo dei sistemi ICT
- Orientamento 18 – Gestione dei cambiamenti riguardanti le ICT
- Orientamento 19 – Gestione della continuità operativa
- Orientamento 20 – Analisi dell'impatto sulle attività
- Orientamento 21 – Pianificazione della continuità operativa
- Orientamento 22 – Piani di risposta e ripristino
- Orientamento 23 – Verifica dei piani
- Orientamento 24 – Comunicazioni in caso di crisi
- Orientamento 25 – Esternalizzazione di servizi ICT e sistemi ICT

EBA



- 1.1. Proporzionalità
- 1.2. Governance e strategia
- 1.2.1. Governance
- 1.2.3. Ricorso a fornitori terzi
- 1.3. Quadro di riferimento per la gestione dei rischi ICT e di sicurezza
- 1.3.1. Organizzazione e obiettivi
- 1.3.2. Individuazione delle funzioni, dei processi e delle risorse
- 1.3.3. Classificazione e valutazione dei rischi
- 1.3.4. Attenuazione dei rischi
- 1.3.5. Segnalazione
- 1.3.6. Audit
- 1.4. Sicurezza dell'informazione
- 1.4.1. Policy di sicurezza dell'informazione
- 1.4.2. Sicurezza logica
- 1.4.3. Sicurezza fisica
- 1.4.5. Monitoraggio della sicurezza
- 1.4.6. Analisi, valutazione e verifica della sicurezza dell'informazione
- 1.4.7. Formazione e sensibilizzazione sulla sicurezza dell'informazione
- 1.5. Gestione delle operazioni ICT
- 3.5.1 Gestione di incidenti e problemi ICT
- 1.6. Gestione dei progetti e dei cambiamenti ICT
- 1.6.1. Gestione dei progetti ICT
- 1.6.2. Acquisizione e sviluppo di sistemi ICT
- 1.6.3. Gestione dei cambiamenti ICT
- 1.7. Gestione della continuità operativa
- 1.7.1. Analisi di impatto sull'operatività
- 1.7.2. Pianificazione della continuità operativa
- 1.7.3. Piani di risposta e di ripristino
- 1.7.4. Verifica dei piani
- 1.7.5. Comunicazione in caso di crisi

Le ragioni di DORA

BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Strengthening digital operational resilience in the financial sector

The IA identifies eight problems:

- i) 'insufficient regulatory response to increased levels of ICT risks';
- ii) 'incomplete view over the frequency and significance of incidents';
- iii) 'complex, inconsistent and overlapping reporting obligations';
- iv) 'insufficient information sharing and cooperation on threat intelligence' (between financial institutions);
- v) 'fragmentation due to multiple testing and no cross-border recognition of results';
- vi) 'insufficient assessment of preventive and resilience capabilities';
- vii) 'challenges for financial institutions to assure compliance with the regulatory framework'; and
- viii) 'unmonitored ICT third-party providers' (TPP) risks'.

Strengthening digital operational resilience in the financial sector

- i) relates to the fragmentation in managing ICT risks, such as a lack of specific requirements on ICT risks and disparity of ICT risk requirements across financial sectors. Problems
- ii-iv) result from ineffective reporting of and limited awareness about threats and incidents, in particular a lack of, or multiple, incident reporting requirements for some financial institutions, insufficient trust in sharing threat intelligence and uncertainty over legal compliance when sharing. Limited and uncoordinated testing, namely a lack of and overlapping testing for some financial institutions, leads to problems
- v-vi). The drivers for problems
- vii-viii) concern risks linked to ICT third-party providers (e.g. data providers, cloud service providers), on which the financial sector increasingly relies, mentioning contractual limitations or gaps in written agreements with ICT third-party providers for example (e.g. outsourcing, sub-outsourcing), and a lack of coherent oversight for ICT TPPs (IA, pp. 8, 10-22).

Cosa è DORA

http://documenti.camera.it/leg18/dossier/pdf/ES050.pdf?_1648451353503

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla **resilienza operativa digitale** per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

“DORA mira a creare un quadro normativo sulla resilienza operativa digitale grazie a cui tutte le imprese garantiscono di poter far fronte a tutti i tipi di malfunzionamenti e minacce connessi alle TIC, al fine di prevenire e mitigare le minacce informatiche.”

https://www.consilium.europa.eu/it/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/

Cosa 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 alla proposta di regolamento DORA

ARTICOLO 1

Oggetto

1.Al fine di conseguire un livello comune elevato di resilienza operativa digitale, il presente regolamento stabilisce i seguenti obblighi uniformi in relazione alla sicurezza dei sistemi informatici e di rete che sostengono i processi commerciali delle entità finanziarie:

a) obblighi applicabili alle entità finanziarie in materia di:

i) **gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);**

ii) **segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC e notifica, su base volontaria, delle minacce informatiche significative;**

iii) **segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), di gravi incidenti operativi o relativi alla sicurezza dei pagamenti;**

iv) **test di resilienza operativa digitale**;

v) **condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;**

vi) **misure relative alla solida gestione dei rischi informatici derivanti da terzi;**

b) **obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi TIC ed entità finanziarie**;

c) norme per **l'istituzione e l'attuazione di un quadro di sorveglianza per i fornitori terzi critici** di servizi TIC, allorché forniscono i loro servizi a entità finanziarie;

d) norme sulla **cooperazione tra autorità competenti e norme sulla vigilanza** e l'applicazione da parte delle autorità competenti in relazione a tutte le materie trattate dal presente regolamento.

2. Quanto alle **entità finanziarie identificate come soggetti essenziali o importanti** ai sensi delle norme nazionali che recepiscono l'articolo 3 della direttiva 2022/2555, il presente regolamento è considerato un **atto giuridico settoriale** dell'Unione ai sensi dell'articolo 4 di tale direttiva.

3. Il presente regolamento lascia impregiudicata la responsabilità degli Stati membri per quanto riguarda le funzioni essenziali dello Stato concernenti la sicurezza pubblica, la difesa e la sicurezza nazionale conformemente al diritto dell'Unione.

---

(29) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

(30) GU C 229 del 15.6.2021, pag. 16.

Gestione del rischio TIC

la gestione del rischio TIC (Capitolo II) che prevede di:

- disporre di una governance interna e di un quadro di controllo che assicuri una gestione efficace e prudenti di tutti i rischi TIC;
- attribuire una serie ben definita di compiti all'organo di gestione, fra i quali la responsabilità della gestione dei rischi TIC;
- disporre di un solido framework per la gestione dei rischi TIC;
- utilizzare strumenti e sistemi di TIC resilienti, tali da ridurre al minimo l'impatto dei relativi rischi;
- identificare costantemente tutte le fonti di rischi relativi alle TIC;
- mettere in atto politiche di continuità operativa e sistemi e piani di ripristino in caso di disastro relativo alle TIC;

Gestione del rischio TIC

- introdurre misure di protezione e prevenzione;
- individuare tempestivamente le attività anomale;
- predisporre capacità e personale idonei a raccogliere informazioni in relazione alle vulnerabilità, minacce, incidenti e attacchi informatici ed ai loro effetti sulla loro resilienza operativa digitale:
- riesaminare gli incidenti e condividere gli insegnamenti, monitorare nel continuo l'efficacia dell'attuazione della strategia di resilienza e gli sviluppi tecnologici, sensibilizzare e formare il personale;
- definire piani di comunicazione nei confronti dei vari stakeholder;
- definire norme tecniche e regolamentazione da parte degli AEV in consultazione con ENISA;

Segnalazione degli incidenti connessi alle TIC

- Le entità finanziarie devono stabilire e attuare un processo di gestione per monitorare e registrare gli incidenti connessi alle TIC, per classificarli e determinarne l'impatto (sulla base di alcuni criteri) e segnalarli, tramite una relazione, alle autorità competenti se ritenuti gravi.
- Per il trattamento della segnalazione deve essere utilizzato un modello comune e le entità finanziarie devono inviare segnalazioni iniziali, intermedie e finali, informando utenti e clienti qualora l'incidente abbia o possa avere un impatto sui loro interessi finanziari.
- Possibilità di istituire un polo unico dell'UE per la segnalazione degli incidenti gravi connessi alle TIC da parte delle entità finanziarie;

Segnalazione degli incidenti connessi alle TIC

- l'Autorità competente fornisce riscontro in merito alle segnalazioni ricevute; le AEV producono un report annuale anonimo sugli incidenti ed emettono allarmi e statistiche;
- estensione dell'applicazione di questo capitolo anche agli operational or security payment-related incidents e major operational or security payment-related incidents.

Test di resilienza operativa digitale

- … anche al fine di accrescere la consapevolezza da parte delle autorità di vigilanza dei rischi informatici e degli incidenti cui sono esposte le entità finanziarie.
- L’entità finanziarie dovranno eseguire una serie di test periodici, anche al fine di identificare punti deboli, carenze o lacune, nonché verificare la capacità di attuare tempestivamente misure correttive, con un'applicazione proporzionata alle proprie dimensioni e del profilo commerciale e di rischio. Solo quelle significative e mature sotto il profilo informatico hanno l'obbligo di svolgere prove avanzate mediante test di penetrazione basati su minacce.
- I soggetti che svolgono le attività di test devono rispondere ai requisiti previsti dall’art. 27.

Rischi relativi alle TIC derivanti da terzi

…che prevede, fra gli altri, di conferire alle autorità di vigilanza finanziaria poteri di sorveglianza sui rischi dovuti alla dipendenza delle entità finanziarie da fornitori terzi di servizi. In tale contesto:

gli aspetti contrattuali chiave (stipula, esecuzione, fase post-contrattuale) saranno armonizzati per garantire che le società finanziarie monitorino i rischi di terzi;

i fornitori terzi di servizi TIC critici saranno sottoposti a un quadro di sorveglianza dell'Unione. In tale contesto per ciascun fornitore terzo di servizi TIC critico sarà definita una autorità di sorveglianza capofila alla quale sono conferiti poteri idonei a garantire l'adeguato monitoraggio dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario.

Condivisione delle informazioni

- …tramite l’istituzione di accordi fra le entità finanziarie per lo scambio di informazioni e dati sulle minacce informatiche.

La struttura della normativa

- 106 considerando
- 64 articoli

- In attesa di pubblicazione di una serie di documenti entro:
  - Il 17 gennaio 2024
  - il 17 luglio 2024

In attesa di emissione

Article 28(10) To further specify the content of the policy on the use of ICT services concerning critical or important functions provided by ICT third-party service providers	Article 30(5) To specify elements when sub-contracting services supporting critical or important functions
Under Article 28 (2) of DORA, as part of their ICT risk management framework, financial entities, other than financial entities referred to in Article 16(1) and other than microenterprises, shall adopt, and regularly review, **a strategy on ICT third-party risk**, taking into account the multi-vendor strategy referred to in Article 5(9) where applicable. **The strategy on ICT third-party risk shall include a policy** on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and shall apply on an individual and, where relevant, on a sub-consolidated and consolidated basis. [...]	In accordance with Article 30(2) (a) of DORA, the contractual arrangements on the use of ICT services shall include at least the following: (a) a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, **indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when this is the case, the conditions applying to such subcontracting.**
In accordance with Article 28 (10) of DORA, the ESAs shall, through the Joint Committee, develop **draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2** in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities.	Article 30 (5) of DORA sets out that the ESAs shall, through the Joint Committee, develop **draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.**

In attesa di emissione

Article 18(3) and (4)
RTS on criteria for classification of major ICT-related incidents and significant cyber threats

The ESAs shall, through the Joint Committee, and in consultation with the ECB and ENISA, develop draft RTS to further specify the following:

a) *the **criteria** set out in paragraph 1, including **materiality thresholds for determining major ICT-related incidents** or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1);*

b) *the **criteria** to be applied by competent authorities for the purpose of **assessing the relevance** of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, **to relevant competent authorities in other Member States**', and the **details of reports** of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, **to be shared with other competent authorities** pursuant to Article 19(6) and (7)*

c) *the criteria set out in paragraph 2 of this Article, including high materiality thresholds for determining significant cyber threats.*

*When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2) **[proportionality principle]**, as well as **international standards, guidance and specifications developed and published by ENISA**, including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly.*

In attesa di emissione

Article 20(a)
RTS specifying the content of the major ICT-related incident reports and notifications for significant cyber threats, as well as the time limits for incident reporting

The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop common draft regulatory technical standards in order to:

i. *establish the **content of the reports for major ICT-related incidents** in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not;*

ii. *determine the **time limits for the initial notification and for each report** referred to in Article 19(4);*

iii. *establish the **content of the notification for significant cyber threats**.*

*When developing those draft regulatory technical standards, the ESAs shall take into account the **size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations**, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), **different time limits may reflect, as appropriate, specificities of financial sectors**, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555. The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of that Directive;*

In attesa di emissione

Article 28(9) ITS on Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third–party service providers

The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the ***register*** *of* ***information*** *referred to in paragraph 3,* ***including information that is common to all contractual arrangements on the use of ICT services****.*

Article 28 (3) Register of Information

As part of their ***ICT risk management framework****, financial entities shall* ***maintain and update*** *at* ***entity level*** *and, at* ***sub-consolidated*** *and* ***consolidated levels****, a* ***Register of Information*** *in relation to* ***all contractual arrangements on the use of ICT services provided by ICT third-party service providers.***

The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not.

Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided.

Financial entities shall make available to the competent authority, upon its request, the full Register of Information or as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity.

Financial entities shall inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services concerning critical or important functions and when a function has become critical or important.

ARTICOLO *2*

Ambito di applicazione

1. Fatti salvi i paragrafi 3 e 4, il presente regolamento si applica alle entità seguenti:

a) enti creditizi;

b) istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366;

c) prestatori di servizi di informazione sui conti;

d) istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE;

e) imprese di investimento;

f) fornitori di servizi per le cripto-attività autorizzati a norma del regolamento del Parlamento europeo e del Consiglio concernente i mercati delle cripto-attività e recante modifica dei regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e delle direttive 2013/36/UE e (UE) 2019/1937 (regolamento sui mercati delle cripto-attività) ed emittenti di token collegati ad attività;

g) depositari centrali di titoli;

h) controparti centrali;

i) sedi di negoziazione;

j) repertori di dati sulle negoziazioni;

k) gestori di fondi di investimento alternativi;

l) società di gestione;

m) fornitori di servizi di comunicazione dati;

n) imprese di assicurazione e di riassicurazione;

o) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;

p) enti pensionistici aziendali o professionali;

q) agenzie di rating del credito;

r) amministratori di indici di riferimento critici;

s) fornitori di servizi di crowdfunding;

t) repertori di dati sulle cartolarizzazioni;

u) fornitori terzi di servizi TIC.

2. Ai fini del presente regolamento le entità di cui al paragrafo 1 lettere **da a) a t) sono definite collettivamente «entità finanziarie».**

3. Il presente regolamento non si applica a:

a) gestori di fondi di investimento alternativi di cui all'articolo 3, paragrafo 2, della direttiva 2011/61/UE;

b) imprese di assicurazione e di riassicurazione di cui all'articolo 4 della direttiva 2009/138/UE;

c) enti pensionistici aziendali o professionali che gestiscono schemi pensionistici che contano congiuntamente non più di 15 aderenti in totale;

d) persone fisiche o giuridiche esentate a norma degli articoli 2 e 3 della direttiva 2014/65/UE;

e) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio che sono microimprese o piccole o medie imprese;

f) uffici dei conti correnti postali di cui all'articolo 2, paragrafo 5, punto 3), della direttiva 2013/36/UE.

4. Gli Stati membri possono escludere dall'ambito di applicazione del presente regolamento le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE che sono situati nei rispettivi territori. Qualora uno Stato membro si avvalga di tale facoltà, e in occasione di ogni successiva modifica, ne informa la Commissione. La Commissione mette tali informazioni a disposizione del pubblico sul suo sito web o attraverso altri canali facilmente accessibili.

ARTICOLO *4*

Principio di proporzionalità

1. Le entità finanziarie attuano le norme di cui al capo II conformemente al principio di proporzionalità, tenendo conto delle loro **dimensioni e del loro profilo di rischio complessivo**, nonché **della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività.**

2. Inoltre, l'applicazione dei capi III e IV e del capo V, sezione I, da parte delle entità finanziarie è proporzionata alle loro dimensioni e al loro profilo di rischio complessivo, nonché alla natura, alla portata e alla complessità dei loro servizi, delle loro attività e della loro operatività, come specificamente previsto dalle pertinenti norme di tali capi.

3. Le **autorità competenti prendono in considerazione l'applicazione del principio di proporzionalità** da parte delle entità finanziarie in sede di **riesame della coerenza del quadro per la gestione dei rischi informatici** sulla base delle relazioni presentate su richiesta delle autorità competenti a norma dell'articolo 6, paragrafo 5, e dell'articolo 16, paragrafo 2.

Rischi

Governance

ARTICOLO *5*

Governance e organizzazione

1. Le entità finanziarie predispongono un **quadro di gestione e di controllo interno** che garantisce **una gestione efficace e prudente di tutti i rischi informatici**, conformemente all'articolo 6, paragrafo 4, al fine di acquisire un elevato livello di resilienza operativa digitale.

2. **L'organo di gestione dell'entità finanziaria definisce e approva l'attuazione di tutte le disposizioni concernenti il quadro per la gestione dei rischi informatici** di cui all'articolo 6, paragrafo 1, vigila su tale attuazione e ne è responsabile.

Ai fini del primo comma, l'organo di gestione:

a) **assume la responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria;**

b) **predispone politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati;**

c) **definisce chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC e stabilisce adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni**;

d) **ha la responsabilità generale di definire e approvare la strategia di resilienza operativa digitale** di cui all'articolo 6, paragrafo 8, compresa la **determinazione del livello appropriato di tolleranza per i rischi informatici dell'entità finanziaria,** ai sensi dell'articolo 6, paragrafo 8, lettera b);

e) approva, **supervisiona e riesamina periodicamente l'attuazione della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC** dell'entità finanziaria, di cui rispettivamente all'articolo 11, paragrafi 1 e 3, che possono

essere adottati come politica specifica dedicata che costituisce parte integrante della politica generale di continuità operativa e del piano di risposta e ripristino dell'entità finanziaria;

f) **approva e riesamina periodicamente i piani interni di audit in materia di TIC** dell'entità finanziaria, gli **audit in materia di TIC e le più importanti modifiche a essi apportate;**

g) **assegna e riesamina periodicamente le risorse finanziarie adeguate per soddisfare le esigenze di resilienza operativa digitale** dell'entità finanziaria **rispetto a tutti i tipi di risorse**, compresi i pertinenti **programmi di sensibilizzazione sulla sicurezza** delle TIC e le attività di formazione sulla resilienza operativa digitale di cui all'articolo 13, paragrafo 6, nonché le **competenze in materia di TIC per tutto il personale**;

h) **approva e riesamina periodicamente la politica** dell'entità finanziaria relativa alle **modalità per l'uso dei servizi TIC prestati dal fornitore terzo di servizi TIC;**

i) i**stituisce a livello aziendale canali di comunicazione** che gli **consentono di essere debitamente informato** in merito a quanto segue:

i) gli **accordi conclusi con i fornitori terzi di servizi TIC** sull'uso di tali servizi;

ii) le **relative eventuali modifiche importanti e pertinenti** previste riguardo ai fornitori terzi di servizi TIC;

iii) il potenziale impatto di tali modiche sulle funzioni essenziali o importanti soggette agli accordi in questione, compresa una sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché almeno gli gravi incidenti TIC e il loro impatto, le misure di risposta e ripristino e le misure correttive.

3. Le entità finanziarie diverse dalle microimprese **istituiscono un ruolo al fine di monitorare gli accordi conclusi con i fornitori terzi di servizi TIC per l'uso di tali servizi, oppure designano un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente**.

4. I **membri dell'organo di gestione dell'entità finanziaria mantengono attivamente aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria, anche seguendo una formazione specifica** su base regolare, commisurata ai rischi informatici gestiti.

EBA

Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza

1.2. Governance e strategia

1.2.1. Governance

- 2. L'organo di gestione dovrebbe garantire che l'istituto finanziario disponga di un quadro di riferimento per la governance e i controlli interni adeguato ai propri rischi ICT e di sicurezza. L'organo di gestione dovrebbe stabilire chiaramente ruoli e responsabilità per le funzioni ICT, per la gestione dei rischi relativi alla sicurezza dell'informazione e per la continuità operativa, compresi quelli dell'organo di gestione e dei suoi comitati.
- 3. L'organo di gestione dovrebbe garantire che la quantità e le abilità del personale dell'istituto finanziario siano adeguate a supportare le esigenze operative dell'ICT e dei processi di gestione dei rischi ICT e di sicurezza dell'istituto su base continuativa, oltre ad assicurare l'attuazione della propria strategia ICT. L'organo di gestione dovrebbe garantire che il bilancio stanziato sia adeguato a soddisfare i requisiti di cui sopra. Inoltre, gli istituti finanziari dovrebbero garantire che tutto il personale, compreso quello che riveste ruoli chiave, riceva una formazione adeguata sui rischi ICT e di sicurezza, compresa la sicurezza dell'informazione, con cadenza annuale o con maggiore frequenza se necessario (cfr. anche la sezione 1.4.7).
- 4. L'organo di gestione ha la responsabilità generale di definire, approvare e supervisionare l'attuazione della strategia ICT dell'istituto finanziario nell'ambito della sua strategia aziendale, nonché di istituire un quadro di riferimento efficace per la gestione dei rischi ICT e di sicurezza.

NIS2

Articolo 20 - Governance

- 1. Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21, sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo. L'applicazione del presente paragrafo lascia impregiudicato il diritto nazionale per quanto riguarda le norme in materia di responsabilità applicabili alle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.
- Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

Framework di sicurezza

ARTICOLO *6*

Quadro per la gestione dei rischi informatici

1. Nell'ambito del sistema di gestione globale del rischio, le entità finanziarie predispongono un **quadro per la gestione dei rischi informatici** solido, esaustivo e adeguatamente **documentat**o, che consenta loro di **affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale**.

2. Il quadro per la gestione dei rischi informatici comprende almeno strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per **proteggere debitamente e adeguatamente tutti i patrimoni informativi e i risorse TIC, compresi software, hardware e server, nonché tutte le pertinenti infrastrutture e componenti fisiche, quali i locali, i centri di elaborazione dati e le aree designate come sensibili**, così da garantire che tutti i patrimoni informativi e i risorse TIC siano adeguatamente **protetti contro i rischi, compresi i danneggiamenti e l'accesso o l'uso non autorizzati.**

3. Conformemente al proprio quadro per la gestione dei rischi informatici, le entità finanziarie riducono al minimo l'impatto dei rischi informatici applicando **strategie, politiche, procedure, protocolli e strumenti in materia di TIC adeguati. Forniscono alle autorità competenti, su richiesta di queste ultime, informazioni complete e aggiornate sui rischi informatici e sul proprio quadro per la gestione dei rischi informatici**.

4. Le entità finanziarie diverse dalle microimprese **attribuiscono la responsabilità della gestione e della sorveglianza dei rischi informatici a una funzione di controllo, di cui assicurano un livello appropriato d'indipendenza** per evitare conflitti d'interessi. Le entità finanziarie garantiscono un'opportuna **separazione e indipendenza tra funzioni di gestione dei rischi informatici, funzioni di controllo e funzioni di audit intern**o, secondo il modello delle **tre linee di difesa** o secondo un modello interno di controllo e gestione del rischio.

5. **Il quadro per la gestione dei rischi informatici è documentato e riesaminato almeno una volta all'anno,** o periodicamente in caso di microimprese, **nonché in occasione di gravi incidenti TIC e in seguito a indicazioni o conclusioni delle autorità di vigilanza formulate a seguito di pertinenti test di resilienza** operativa digitale o di **processi di audit. Il quadro è costantemente migliorato sulla base degli insegnamenti tratti dall'attuazione e dal monitoraggio. È presentata all'autorità competente, su sua richiesta, una relazione in merito al riesame del quadro per la gestione dei rischi informatici.**

6. Il **quadro** per la gestione dei rischi informatici delle entità finanziarie, diverse dalle microimprese, è **sottoposto periodicamente a verifiche di audit interne** effettuate da addetti all'audit in linea con i piani di audit delle entità finanziarie. Tali **addetti all'audit possiedono conoscenze, competenze ed esperienze adeguate in materia di rischi informatic**i, nonché **un'adeguata indipendenza**. La **frequenza e l'oggetto** delle verifiche di audit in materia di TIC sono **commisurati ai rischi** connessi alle TIC cui è esposta l'entità finanziaria.

7. Sulla base delle **conclusioni dell'audit** interno in materia di TIC, le entità finanziarie istituiscono un **procedimento formale per darvi seguito, comprendente regole per la verifica tempestiva delle risultanze critiche e l'adozione di rimedi**.

8. Il **quadro** per la gestione dei rischi informatici **comprende una strategia di resilienza operativa digitale che definisce le modalità di attuazione del quadro**. A tal fine, la strategia di resilienza operativa digitale include metodi per affrontare i rischi informatici e conseguire specifici obiettivi in materia di TIC:

a) **spiegando in che modo il quadro per la gestione dei rischi informatici sostiene gli obiettivi e la strategia commerciale** dell'entità finanziaria;

b) **fissando il livello di tolleranza per i rischi informatici**, conformemente alla **propensione al rischio** dell'entità finanziaria e **analizzando la tolleranza d'impatto per le perturbazioni a livello di TIC**;

c) indicando **chiari obiettivi in materia di sicurezza delle informazioni**, **compresi indicatori chiave di prestazione e parametri chiave di rischio;**

d) **spiegando l'architettura di riferimento a livello di TIC** e le **eventuali modifiche necessarie per conseguire specifici obiettivi commerciali;**

e) delineando i differenti **meccanismi** introdotti per **individuare incidenti connessi alle TIC, prevenire il loro impatto e proteggersi dallo stesso;**

f) **documentando l'attuale situazione di resilienza** operativa digitale **sulla base del numero di gravi incidenti TIC segnalati, nonché l'efficacia delle misure preventive;**

g) attuando test di resilienza operativa digitale, conformemente al capo IV del presente regolamento;

h) delineando una strategia di comunicazione in caso di incidenti connessi alle TIC di cui è richiesta la divulgazione a norma dell'articolo 14.

9. Le entità finanziarie **possono**, nel contesto della strategia di resilienza operativa digitale di cui al paragrafo 8, **definire una strategia olistica per le TIC a livello di gruppo o di entità, basata su una varietà di fornitori**, che indichi le principali dipendenze da fornitori terzi di servizi TIC e che spieghi la **logica sottesa alla ripartizione degli appalti tra i fornitori** terzi di servizi TIC.

10. Le entità finanziarie **possono**, conformemente alla normativa settoriale dell'Unione e nazionale, **esternalizzar**e a imprese interne o esterne al gruppo i **compiti di verifica della conformità ai requisiti in materia di gestione dei rischi informatici.** In caso di esternalizzazione, l'entità finanziaria rimane pienamente responsabile di verificare la conformità ai requisiti in materia di gestione dei rischi informatici.

ENISA
Interoperable EU risk management framework

A risk management framework or methodology should address at least the following phases (ISO 27005, EU ITSRM) which can be considered as its main functional components:

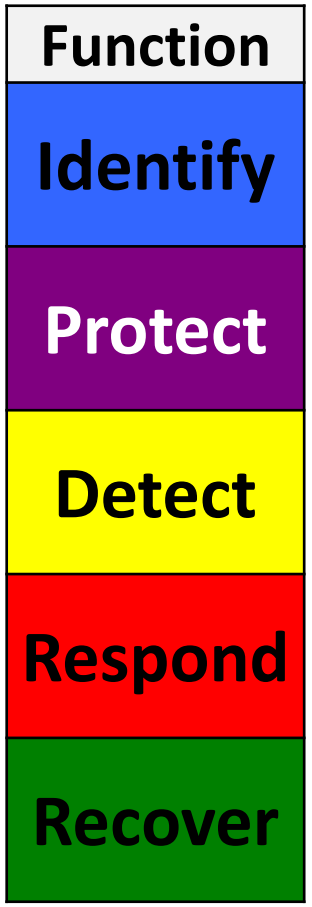
- Risk Identification (Assets, Threats and Vulnerabilities),
- Risk Assessment (Risk Calculation and Evaluation),
- Risk Treatment (Selection and Implementation of Security Controls, and Calculation of Residual Risk),
- Risk Monitoring (Assess effectiveness of measures and monitor risks).

Functional Characteristics	Parameters to Check
Asset Taxonomy	Does the framework or methodology use or describe specific categories of assets?
	Is the taxonomy used modifiable?
	Can the analyst introduce new categories of assets or import taxonomies from other sources?
Asset Evaluation	Does the framework or methodology use or describe specific guidelines for the evaluation of assets (i.e. scale and criteria for assessment of asset value and impact)?
	Are the proposed scales or criteria modifiable?
	Can the analyst introduce new scales or criteria?
Threat Catalogues	Does the framework or methodology use or describe specific threat catalogues and/or threat categories?
	Are the proposed threat catalogues and/or threat categories modifiable?
	Can the analyst introduce new threats and/or threat categories and import them from other sources?
Vulnerability Catalogues	Does the framework or methodology describe specific vulnerability catalogues and/or categories of vulnerabilities?
	Are the proposed vulnerability catalogues and/or categories of vulnerabilities modifiable?
	Can the analyst introduce new vulnerabilities and/or categories of vulnerabilities and import them from other sources?
Risk Calculation	Does the framework or methodology describe specific guidelines for the calculation of risk (i.e. formulas, scale, matrix)?
	Is the proposed calculation method modifiable?
	Can the analyst introduce or import (from other sources) new methods of calculation?
Measure Catalogues & Calculation of Residual Risk	Does the framework or methodology describe specific control catalogues and/or categories of controls?
	Are the proposed control catalogues and/or categories of controls modifiable?
	Can the analyst introduce new controls and/or categories of controls and import them from other sources?
	Is the Calculation of Residual Risk (either on a Calculation of Residual Risk formula or on an Impact of Measures formula) modifiable?

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.

NIST The Framework Core

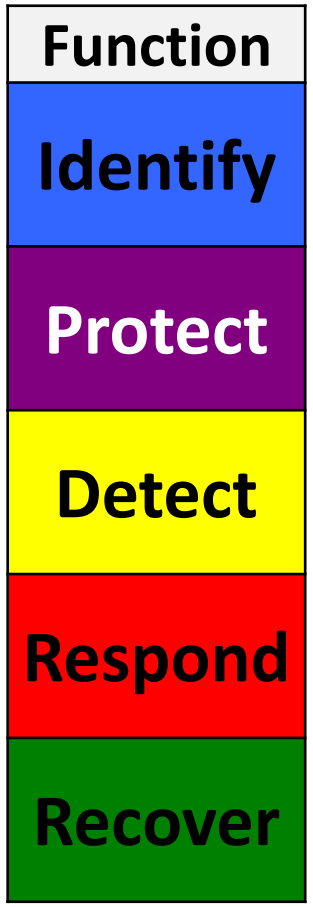
Establishes a Common Language



- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

NIST The Framework Core

Establishes a Common Language



- Articolo 8 - **Identificazione**
- Articolo 9 - **Protezione e prevenzione**
- Articolo 10 - **Individuazione**
- Articolo 11 - **Risposta e ripristino**

An Excerpt from the Framework Core

The Connected Path of Framework Outcomes

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions 23 Categories 108 Subcategories 6 Informative References

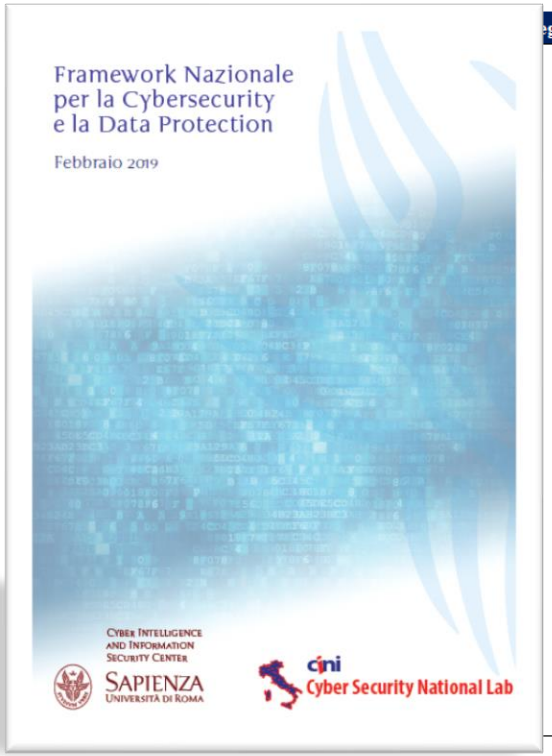
Implementation Tiers

The Cybersecurity Framework Version 1.1

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk[1.1]** • benefits my sharing or receiving information from outside parties			

Framework Nazionale

Cybersecurity e Data Protection



egory	Subcategory	Classe	Livello di Priorità
	PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	**Consigliata**	**ALTA**
	PR.AC-3: L'accesso remoto alle risorse è amministrato	**Consigliata**	**ALTA**
	PR.AC-4: Gli accessi alle risorse e le autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**Consigliata**	**ALTA**
	PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	**Consigliata**	**ALTA**
	PR.AC-6: Le identità sono comprovate, associate a credenziali e verificate durante le interazioni	**Consigliata**	**ALTA**
	PR.AC-7: Le modalità di autenticazione (es. autenticazione a singolo o multi fattore) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	**Consigliata**	**ALTA**

Misurare

NIST Special Publication 800-55 Revision 1

Performance Measurement Guide for Information Security

National Institute of Standards and Technology
U.S. Department of Commerce

Elizabeth Chew, Marianne Swanson, Kevin Stine,
Nadya Bartol, Anthony Brown, and Will Robinson

3.3.1 Implementation Measures

Implementation measures are used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures. Examples of implementation measures related to information security programs include the *percentage of information systems with approved system security plans* and the *percentage of information systems with password policies configured as required*. At first, the results of these measures might be less than 100 percent. However, as the information security program and its associated policies and procedures mature, results should reach and remain at 100 percent. At this point, the organization should begin to focus its measurement efforts on effectiveness/efficiency and impact measures.

Implementation measures can also examine system-level areas—for example, the *percentage of servers within a system with a standard configuration.* At first, the results of this system-level measure will likely be less than 100 percent. When the implementation measure results reach and remain at 100 percent, it can be concluded that the information systems have fully implemented the security controls addressed by this measure, and measurement activities can refocus on other controls in need of improvement. After most implementation measures reach and remain at 100 percent, the organization should begin to focus its measurement efforts on effectiveness/efficiency and impact measures. Organizations should never fully retire implementation measures because they are effective at pointing out specific security controls that are in need of improvement; however, as an organization matures, the emphasis and resources of the measurement program should shift away from implementation and towards effectiveness/efficiency and impact measures.

Implementation measures require data that can be easily obtained from information security assessment reports, quarterly and annual FISMA reports, plans of action and milestones (POA&M), and other commonly used means of documenting and tracking information security program activities.

NIST Special Publication 800-55 Revision 1

Performance Measurement Guide for Information Security

National Institute of Standards and Technology
U.S. Department of Commerce

Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson

3.3.2 Effectiveness/Efficiency Measures

Effectiveness/efficiency measures are used to monitor if program-level processes and systemlevel security controls are implemented correctly, operating as intended, and meeting the desired outcome. These measures concentrate on the evidence and results of assessments and may require multiple data points quantifying the degree to which information security controls are implemented and the resulting effect(s) on the organization's information security posture. For example, the *percentage of enterprise operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated* is both an implementation and effectiveness measure. It measures the implementation of the security control Flaw Remediation (SI-2) in SP 800-53 because the result of the measure demonstrates whether or not vulnerabilities are mitigated through patches or other means. At the same time, the result indicates the effectiveness of the Security Alerts and Advisories (SI-5) security control because any result less than the target indicates a lack of ability to receive alerts and use them to successfully mitigate vulnerabilities.

Effectiveness/efficiency measures address two aspects of security control implementation results: the robustness of the result itself, referred to as ***effectiveness***, and the timeliness of the result, referred to as ***efficiency.*** For example, the **effectiveness**/efficiency measure—*percentage of information security incidents caused by improperly configured access controls*—relies on information regarding the implementation and ***effectiveness*** of the following security controls: Incident Monitoring (IR-5); Audit Monitoring, Analysis, and Reporting (AU-6); and Monitoring Configuration Changes (CM-4).

NIST Special Publication 800-55 Revision 1

Performance Measurement Guide for Information Security

National Institute of Standards and Technology
U.S. Department of Commerce

Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson

Additionally, the effectiveness/**efficiency** measure—*the percentage of system components that undergo maintenance on schedule*—relies on information regarding the ***efficiency*** of the following security controls: Periodic Maintenance (MA-2) and Life Cycle Support (SA-3).

Effectiveness/efficiency measures provide key information for information security decision makers about the results of previous policy and acquisition decisions. These measures can offer insight for improving performance of information security programs. Furthermore, effectiveness/efficiency measures can be used as a data source for continuous monitoring efforts because they help determine the effectiveness of security controls. The results of effectiveness/efficiency measures can be used to ascertain whether selected security controls are functioning properly and are helping facilitate corrective action prioritization.

Effectiveness/efficiency measures may require fusing information security program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be directly tied to security controls implementation.

NIST Special Publication 800-55 Revision 1

Performance Measurement Guide for Information Security

National Institute of Standards and Technology
U.S. Department of Commerce

Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson

3.3.3 Impact Measures

Impact measures are used to articulate the impact of information security on an organization's mission. These measures are inherently organization-specific since each organization has a unique mission. Depending upon the organization's mission, impact measures can be used to quantify:

Cost savings produced by the information security program or through costs incurred from addressing information security events;

The degree of public trust gained/maintained by the information security program; or Other mission-related impacts of information security.

These measures combine information about the results of security controls implementation with a variety of information about resources. They can provide the most direct insight into the value of information security to the organization and are the ones that are sought out by executives. For example, *the percentage of the agency's information system budget devoted to information security* relies on information regarding the implementation, effectiveness, and outcome of the following NIST SP 800-53 security controls: Allocation of Resources (SA-2) and Acquisitions (SA-4). Another, more generalized budget-related impact measure would be *the number of information security investments reported to OMB in an Exhibit 300.* Rather than examining the impact of a security control or controls, this measure evaluates the relationship between the portfolio of information security investments and the budget process.

Impact measures require tracking a variety of resource information across the organization in a manner that can be directly tied to information security activities and events.

Field	Data
Measure ID	State the unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	Statement of strategic goal and/or information security goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Statement of measurement. Use a numeric statement that begins with the word "percentage," "number," "frequency," "average," or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Security controls that provide supporting data should be stated in Implementation Evidence. If the measure is applicable to a specific FIPS 199 impact level (high, moderate, or low), state this level within the measure.
Type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.
Implementation Evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. • For manual data collection, identify questions and data elements that would provide the data inputs necessary to calculate the measure's formula, qualify the measure for acceptance, and validate provided information. • For each question or query, state the security control number from NIST SP 800-53 that provides information, if applicable. • If the measure is applicable to a specific FIPS 199 impact level, questions should state the impact level. • For automated data collection, identify data elements that would be required for the formula, qualify the measure for acceptance, and validate the information provided.
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. Select the frequency of data collection based on a rate of change in a particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.

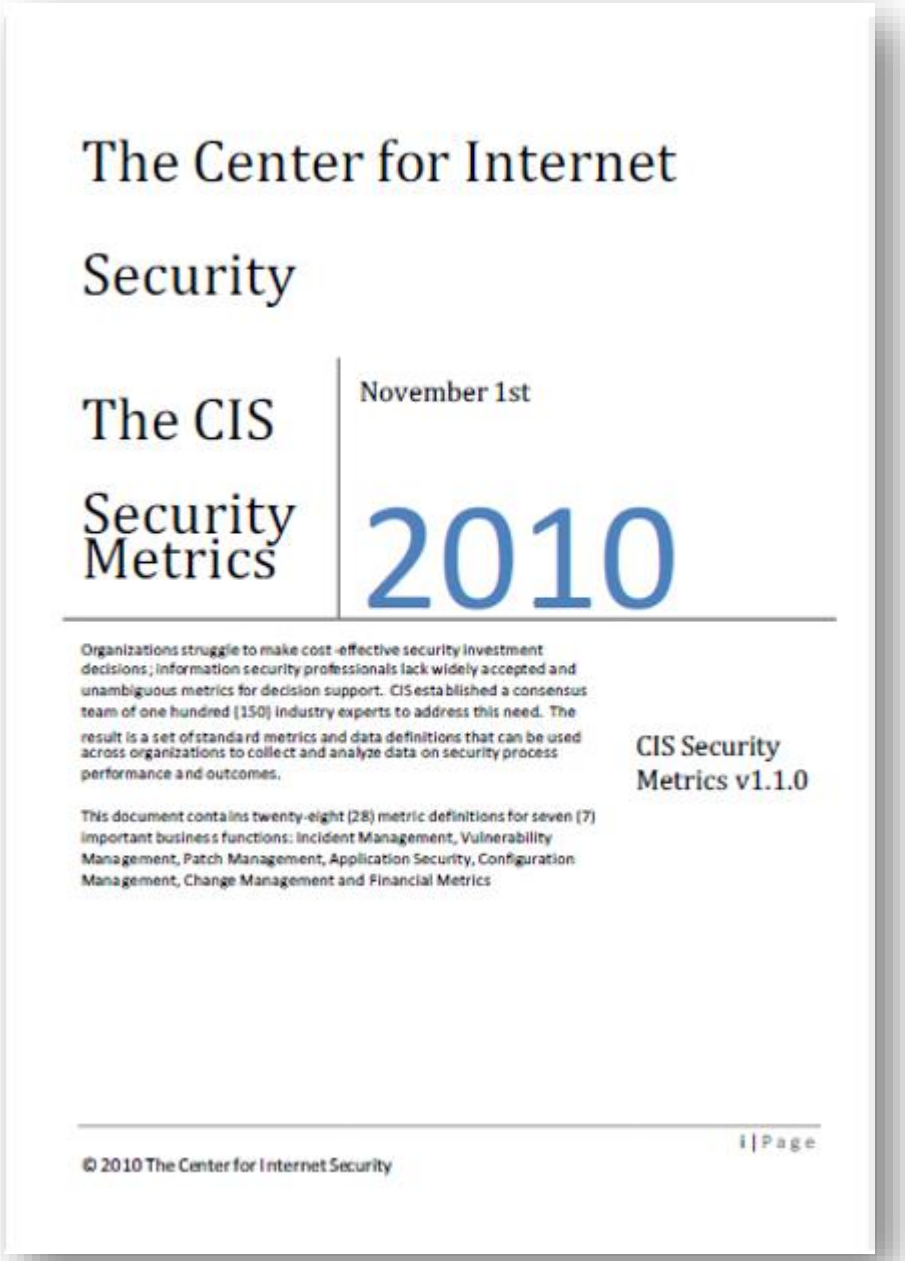
Field	Data
Responsible	Indicate the following key stakeholders:
Parties	• Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Key Performance SECURITY INDICATORS

Name	Inventory of software or devices		
KPSI Index	1		
CAG Critical Control(s)	1, 2		
Description/rationale	This KPSI reflects the concept that asset inventory is at the basis of every ISMS. 70 % of all incidents are not registered or not managed devices.		
Core ISI 001 [1] mapping	IWH_UNA.1, VTC_NRG.1		
Additional ISI 001 [1] mapping	IWH_VNP.1 to 3, IWH_VCN.1, IWH_UNA.1, VTC_WFI.1, VTC_NRG.1		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process, no tools	Processes characterized for the organization but often reactive (reset after incidents). No tools	Processes systematically implemented. Tools usage	Processes continuously checked with the level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Information **SECURITY INDICATORS**

IEX_PHI.1: Phishing targeting company's customers' workstations spoiling company's image or business
Phishing involves a growing number of business sectors (financial organizations, e-commerce sites, online games, social sites etc.). It includes attacks via e-mail with messages that contain either malicious URL links (to forged websites) or malicious URL links (to malware laden genuine websites).
Base events
Customer reporting of a phishing attempt. **Frequency:** High frequency and strong impact on the image **Severity:** 2 **Detection means:** Manual production (via periodic tests of customers or users) **Detection level:** 2 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Number of unique campaigns detected during the last 30 days. A unique campaign consists of a series of coordinated phishing attacks coming from a single origin within a given time slot, with an average of 6 attacks per campaign. **Indicator value:** Ratio of Derived Measure 2 to the media exposure (communication measurement specific to each professional sector) **State-of-the-art value:** (Derived measure 2) 20 campaigns per month in English language (relatively high scattering between companies in a given business sector, primarily depending on the media exposure)
Link with ISO/IEC 27002 [2]
No
Maturity KPSI
Will be available in the next version of the present document.



The Center for Internet Security

The CIS Security Metrics

November 1st

2010

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (150) industry experts to address this need. The result is a set of standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document contains twenty-eight (28) metric definitions for seven (7) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management, Change Management and Financial Metrics

CIS Security Metrics v1.1.0

Number of Applications

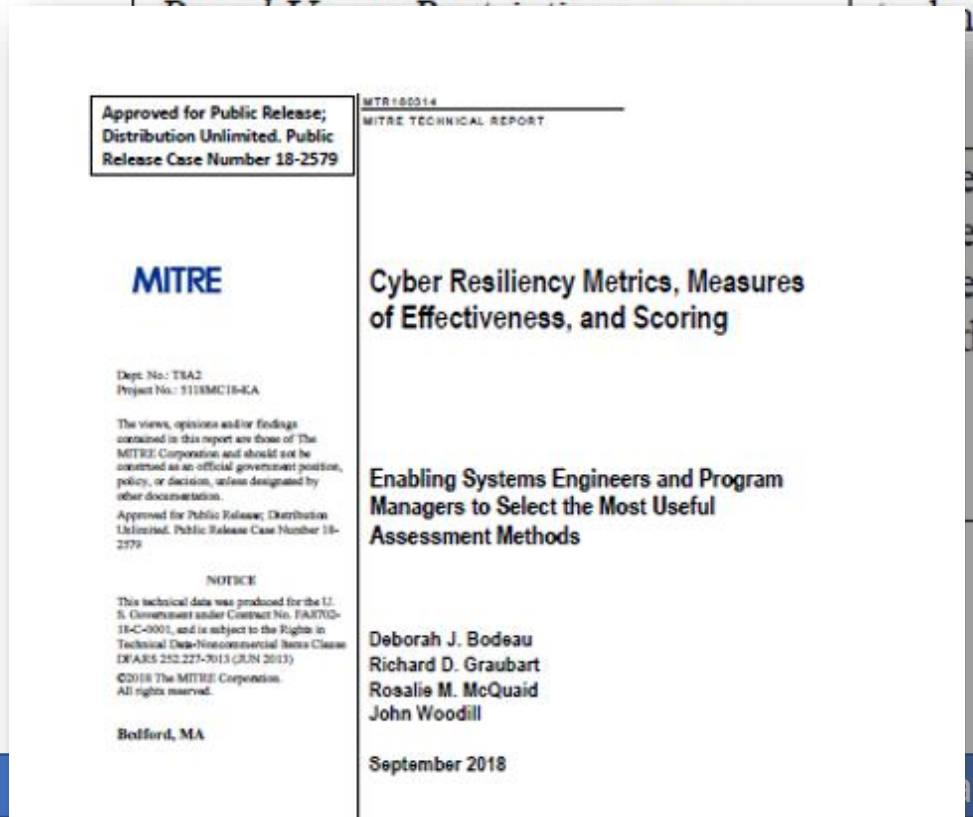
Objective

The goal of this metric is to provide managers with the number of applications in the organization and to help translate the results of other metrics to the scale of the organization's environment.

Table 64: Number of Applications

Metric Name	Number of Applications
Version	1.0.0
Status	Final
Description	This metric counts the number of applications in the organization's environment.
Type	Technical
Audience	Security Operations
Question	What is the number of applications in the organization?
Answer	A positive integer value that is greater than or equal to zero. A value of "0" indicates that the organization does not have any applications.
Formula	The number of applications (NOA) is determined by simply counting the number of applications in the organization: $NOA = Count(Applications)$
Units	Number of applications
Frequency	Weekly, Monthly, Quarterly, Annually.
Targets	NOA values generally should trend lower over time although this number will depend on the organization's business, structure, acquisitions, growth and use of IT. This number will also help organizations interpret the results of other applications security metrics. Because of the lack of experiential data from the field, no consensus on the range of acceptable goal values for Number of Applications exists.

Sub-Objective: Apply basic hygiene and risk-tailored controls	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S1-A1: Restrict access to resources based on criticality and sensitivity (i.e., on resource attractiveness to adversaries)[30] *[Privilege Restriction: Trust-Based Privilege Management, Attribute-*	Percentage of cyber resources to which access is controlled based on criticality [PA-S1-A1-2] Percentage of cyber resources to which access is controlled based on sensitivity [PA-S1-A1-3] Percentage of users with privileged/administrator access [PA-S1-A1-4] Percentage of [administrative, operational] activities [procedurally, ically] enforced by 2-person controls [PA-S1-A1-5]
	ntage of users for which behaviors are restricted based on assigned ee of trust [PA-S1-A2-1] ntage of types of cyber entities for which behaviors are restricted l on assigned degree of trust [PA-S1-A2-2]



Approved for Public Release; Distribution Unlimited. Public Release Case Number 18-2579

MTR180314
MITRE TECHNICAL REPORT

MITRE

Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring

Dept. No.: T8A2
Project No.: 5118MC18-KA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release; Distribution Unlimited. Public Release Case Number 18-2579

NOTICE

This technical data was produced for the U. S. Government under Contract No. FA8702-18-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

©2018 The MITRE Corporation. All rights reserved.

Bedford, MA

Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods

Deborah J. Bodeau
Richard D. Graubart
Rosalie M. McQuaid
John Woodill

September 2018

Identificazione

Mappatura

- **Risorse**
- **Processi**
- **Vulnerabilità e minacce**
- **Correlazioni**
- **Rischi**
- **Fornitori**
- **…**

ARTICOLO *8*

Identificazione

1 Nell'ambito del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie **identificano, classificano e documentano adeguatamente tutte le funzioni commerciali supportate dalle TIC, i ruoli e le responsabilità, i patrimoni informativi e le risorse TIC** a supporto delle suddette funzioni, nonché **i ruoli e le dipendenze rispettivi in materia di rischi informatici**. Le entità **finanziarie riesaminano, secondo necessità e almeno una volta all'anno, l'adeguatezza di tale classificazione** e di altri documenti eventualmente pertinenti.

2 Le entità finanziarie **identificano costantemente tutte le fonti di rischio** relative alle TIC, **in particolare** l'esposizione al rischio **da e verso altre entità finanziarie, e valutano le minacce informatiche e le vulnerabilità** in materia di TIC pertinenti per le loro funzioni commerciali supportate dalle TIC, per i loro patrimoni informativi e per i loro risorse TIC. Le entità finanziarie **riesaminano periodicamente, e almeno una volta all'anno, gli scenari di rischio** che esercitano un impatto su di loro.

3 Le entità finanziarie diverse dalle microimprese **effettuano una valutazione del rischio in occasione di ogni modifica di rilievo dell'infrastruttura del sistema informatico e di rete, dei processi o delle procedure** che incidono sulle loro funzioni commerciali supportate dalle TIC, sui loro **patrimoni informativi o sulle loro risorse TIC.**

4 Le entità finanziarie **identificano tutti i patrimoni informativi e le risorse TIC**, compresi quelli su siti remoti, le risorse di rete e le attrezzature hardware, e **mappano quelle considerate essenziali**. Effettuano la **mappatura della configurazione** dei patrimoni informativi e delle risorse TIC, nonché **dei collegamenti e delle interdipendenze** tra i diversi patrimoni informativi e risorse TIC**.**

5 Le entità finanziarie identificano e **documentano tutti i processi dipendenti da fornitori** terzi di servizi TIC e **identificano le interconnessioni con detti fornitori** che offrono servizi a supporto di funzioni essenziali o importanti.

6. Ai fini dei paragrafi 1, 4 e 5, le entità finanziarie **mantengono inventari pertinenti e li aggiornano periodicamente e in occasione di ogni modifica di rilievo** di cui al paragrafo 3.

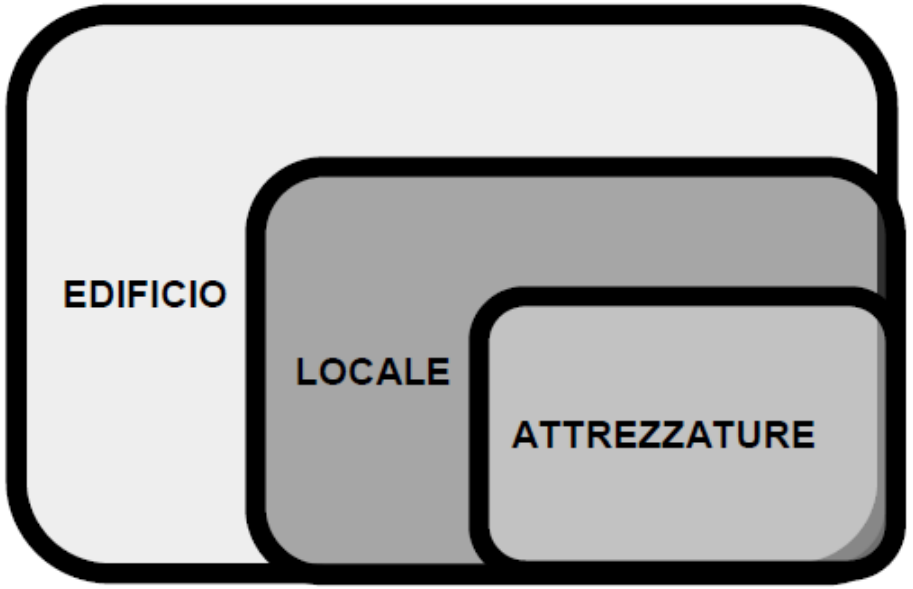
7. Le entità finanziarie diverse dalle microimprese effettuano **periodicamente, almeno una volta all'anno e in ogni caso prima e dopo la connessione di tecnologie, applicazioni o sistemi, una valutazione del rischio specifica per tutti i sistemi legacy.**

Mappatura asset

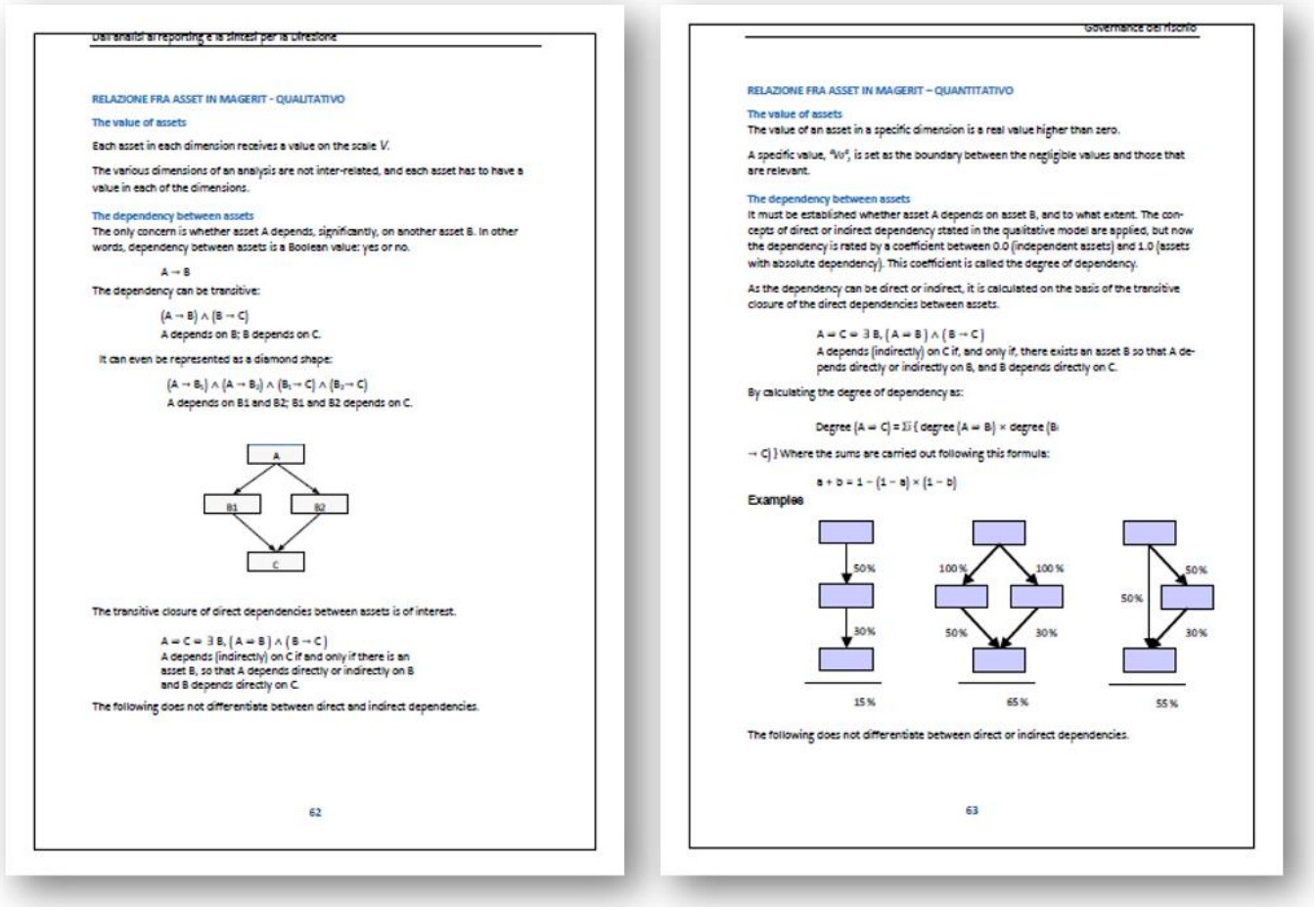
- Qual è il livello di dettaglio richiesto per il censimento degli asset?
- DORA non si occupa solo di resilienza operativa, ma anche di continuità operativa

Mappatura asset

- I componenti di un'analisi del rischio quali asset, probabilità, impatti e gli stessi rischi non sono fra loro indipendenti. Ad esempio: un asset è contenuto in un altro asset (… i dati sono presenti su un disco fisso che è presente in un pc, che è all'interno di un edificio…).
- Un evento che impatta sull'edificio può avere conseguenze quindi sul pc e quindi sui dati.
- Questo non vale per qualunque evento e quindi la valutazione delle conseguenze deve essere molto puntuale; analogamente vale per le contromisure. Alcune contromisure applicate all'edificio hanno effetto anche sugli oggetti che contiene. La valutazione delle relazioni quindi ha effetti sia sulla valutazione del rischio, ma anche sugli effetti delle contromisure, il cui costo può essere ripartito su più asset.



Mappatura asset



Dall'analisi al reporting e la sintesi per la direzione

RELAZIONE FRA ASSET IN MAGERIT - QUALITATIVO

The value of assets

Each asset in each dimension receives a value on the scale *V*.

The various dimensions of an analysis are not inter-related, and each asset has to have a value in each of the dimensions.

The dependency between assets

The only concern is whether asset A depends, significantly, on another asset B. In other words, dependency between assets is a Boolean value: yes or no.

$A \rightarrow B$

The dependency can be transitive:

$(A \rightarrow B) \wedge (B \rightarrow C)$

A depends on B; B depends on C.

It can even be represented as a diamond shape:

$(A \rightarrow B_1) \wedge (A \rightarrow B_2) \wedge (B_1 \rightarrow C) \wedge (B_2 \rightarrow C)$

A depends on B1 and B2; B1 and B2 depends on C.

The transitive closure of direct dependencies between assets is of interest.

$A \Rightarrow C \Leftrightarrow \exists B, (A \Rightarrow B) \wedge (B \rightarrow C)$

A depends (indirectly) on C if and only if there is an asset B, so that A depends directly or indirectly on B and B depends directly on C.

The following does not differentiate between direct and indirect dependencies.

62

Governance del rischio

RELAZIONE FRA ASSET IN MAGERIT – QUANTITATIVO

The value of assets

The value of an asset in a specific dimension is a real value higher than zero.

A specific value, $^{a}V^{d}$, is set as the boundary between the negligible values and those that are relevant.

The dependency between assets

It must be established whether asset A depends on asset B, and to what extent. The concepts of direct or indirect dependency stated in the qualitative model are applied, but now the dependency is rated by a coefficient between 0.0 (independent assets) and 1.0 (assets with absolute dependency). This coefficient is called the degree of dependency.

As the dependency can be direct or indirect, it is calculated on the basis of the transitive closure of the direct dependencies between assets.

$A \Rightarrow C \Leftrightarrow \exists B, (A \Rightarrow B) \wedge (B \rightarrow C)$

A depends (indirectly) on C if, and only if, there exists an asset B so that A depends directly or indirectly on B, and B depends directly on C.

By calculating the degree of dependency as:

Degree $(A \Rightarrow C) = \sum_i \{ \text{degree}(A \Rightarrow B_i) \times \text{degree}(B_i \rightarrow C) \}$ Where the sums are carried out following this formula:

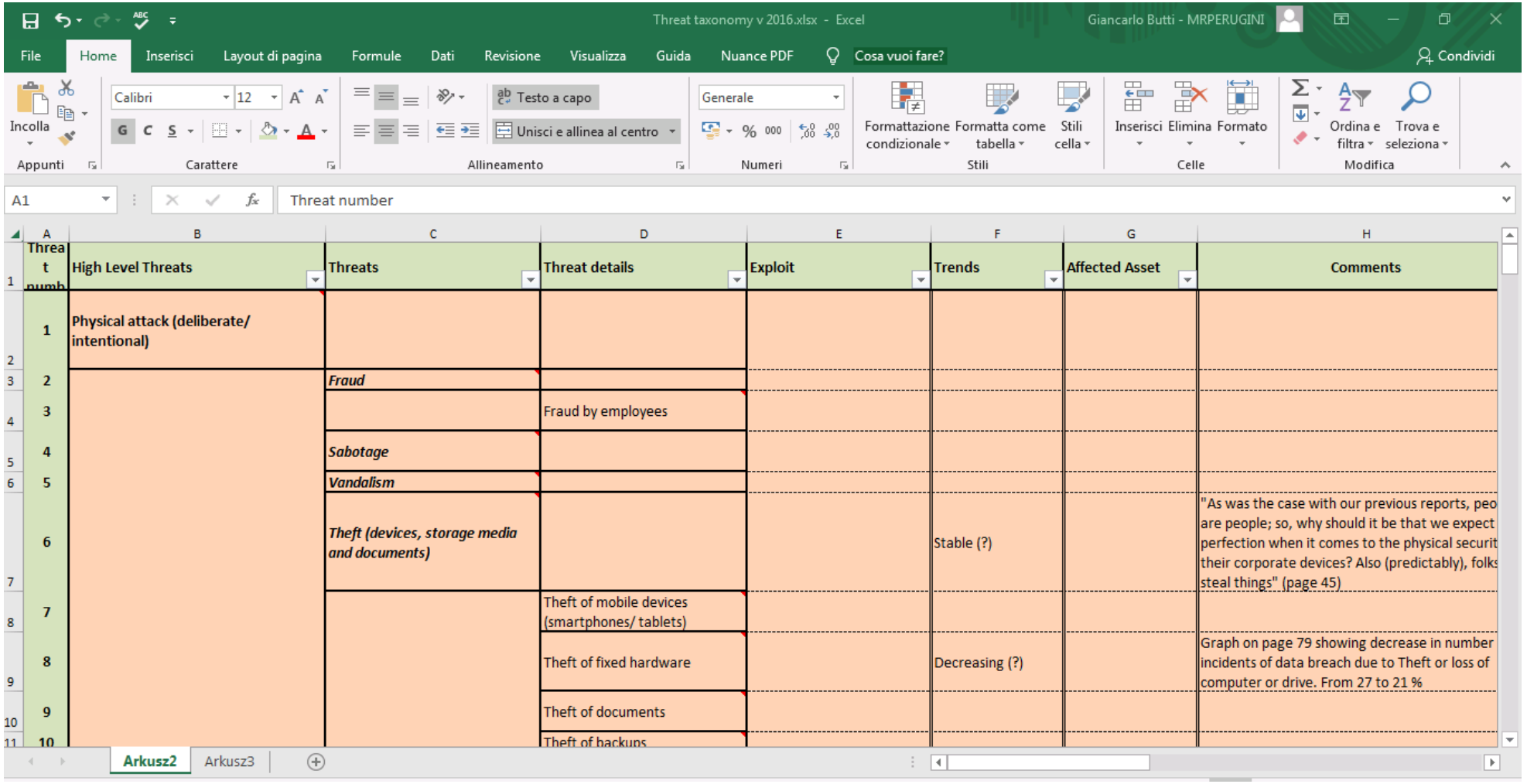
$a + b = 1 - (1 - a) \times (1 - b)$

Examples

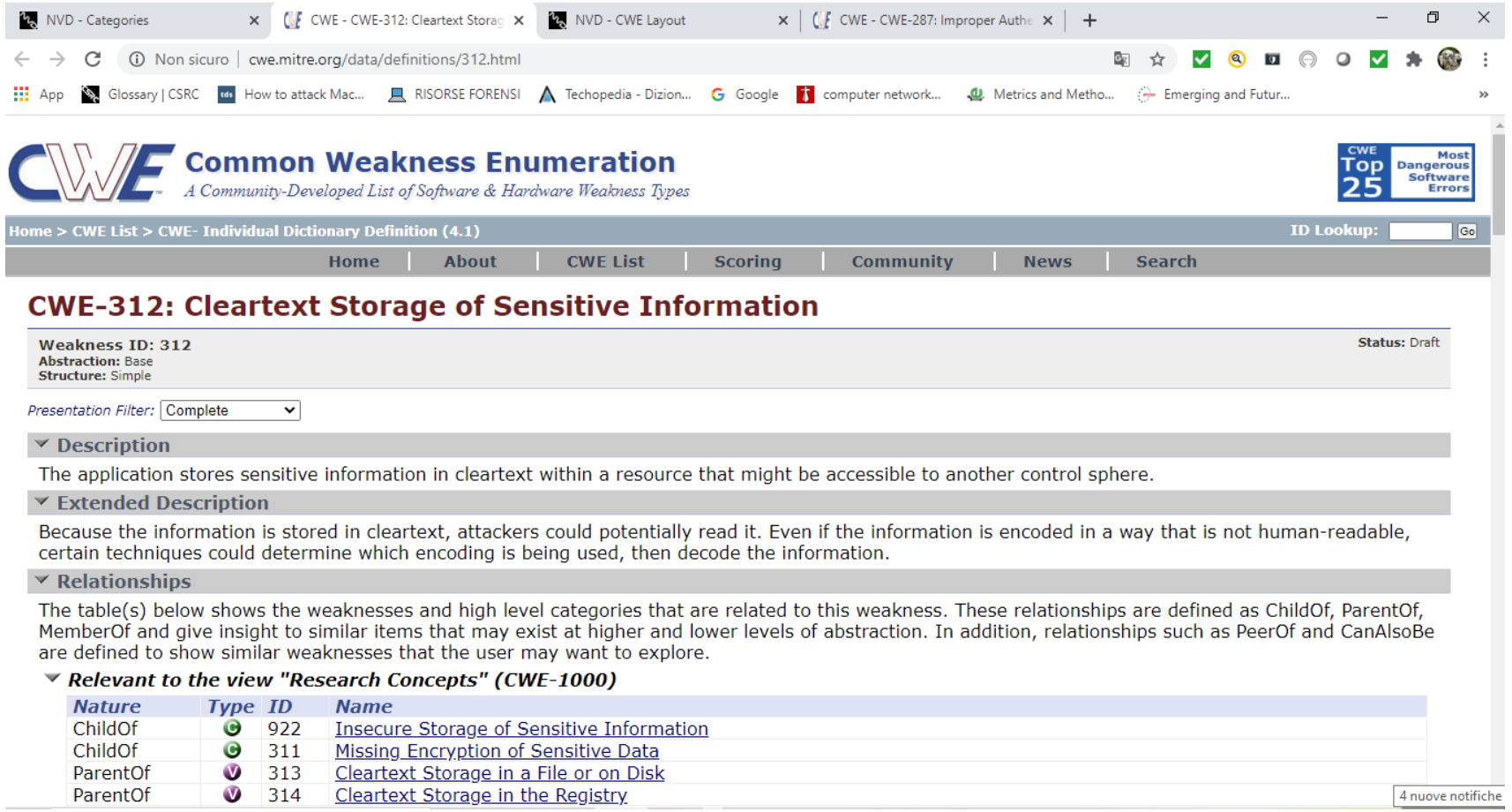
The following does not differentiate between direct or indirect dependencies.

63

ENISA - Threat taxonomy



Vulnerabilità



Analisi del rischio

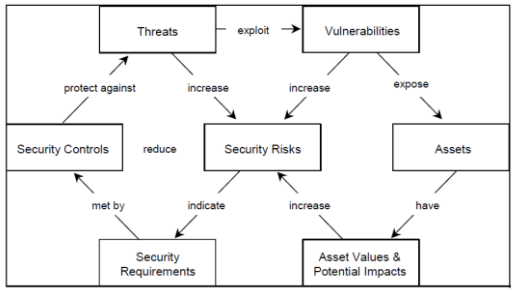
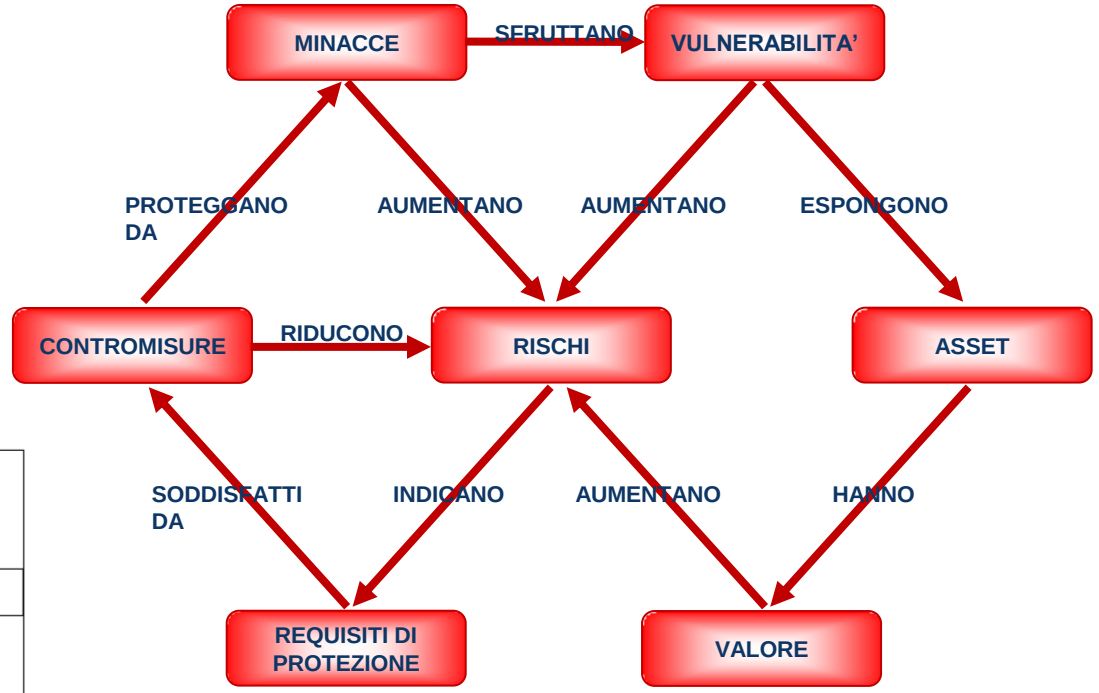


Figure 3: Risk concept relationship
(Source: Australian Standard Handbook of Information Security Risk Management – HB231:2000)



Il rischio secondo la ISO 31000

- *Le organizzazioni di tutti i tipi e di tutte le dimensioni si trovano di fronte a fattori ed influenze esterni ed interni che rendono incerto il conseguimento dei loro obiettivi.*
- *Gestire il rischio è un'attività iterativa ed assiste le organizzazioni nello stabilire le strategie, nel conseguire gli obiettivi e nel prendere decisioni consapevoli.*
- *Gestire il rischio fa parte della governance e della leadership, ed è fondamentale per il modo in cui l'organizzazione viene gestita a tutti i livelli. Questo contribuisce al miglioramento del sistema di gestione.*
- *Gestire il rischio fa parte di tutte le attività riconducibili ad un'organizzazione e comprende l'interazione con le parti interessate.*
- *Gestire il rischio prende in considerazione il contesto esterno ed interno dell'organizzazione, compresi il comportamento umano ed i fattori culturali.*

Il concetto di rischio ICT

Rischi ICT

Orientamenti sulla valutazione dei rischi relativi… SREP

- **Rischio di disponibilità e continuità ICT**
  Il rischio che le prestazioni e la disponibilità dei sistemi e dei dati ICT siano influenzati negativamente, incluso il rischio di incapacità di ripristinare tempestivamente i servizi dell'ente a causa di un guasto delle componenti ICT hardware o software; debolezze nella gestione dei sistemi ICT; o qualsiasi altro evento, come ulteriormente esposto nell'allegato.
- **Rischio di sicurezza ICT**
  Il rischio di accesso non autorizzato ai sistemi e ai dati dei sistemi ICT dell'ente, dall'interno o dall'esterno (ad esempio nel caso di attacchi informatici), come ulteriormente esposto nell'allegato.
- **Rischio relativo ai cambiamenti ICT**
  Il rischio derivante dall'incapacità dell'ente di gestire i cambiamenti dei sistemi ICT in modo tempestivo e controllato, in particolare per quanto concerne programmi di modifica complessi e di grandi dimensioni, come ulteriormente esposto nell'allegato.

(Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP))

Rischi ICT

Orientamenti sulla valutazione dei rischi relativi… SREP

- **Rischio di integrità dei dati ICT**
  Il rischio che i dati archiviati ed elaborati dai sistemi ICT siano incompleti, inesatti o incoerenti nei vari sistemi, in seguito, ad esempio, a controlli ICT carenti o assenti durante le varie fasi del ciclo di vita dei dati ICT (vale a dire, progettazione dell'architettura dei dati, costruzione del modello e/o dei dizionari di dati, verifica degli inserimenti dei dati, controllo delle estrazioni, dei trasferimenti e delle elaborazioni dei dati, inclusi i risultati forniti), tali da compromettere la capacità di un ente di fornire servizi e di produrre le informazioni finanziarie e relative alla gestione (del rischio) in modo corretto e tempestivo come ulteriormente esposto nell'allegato.

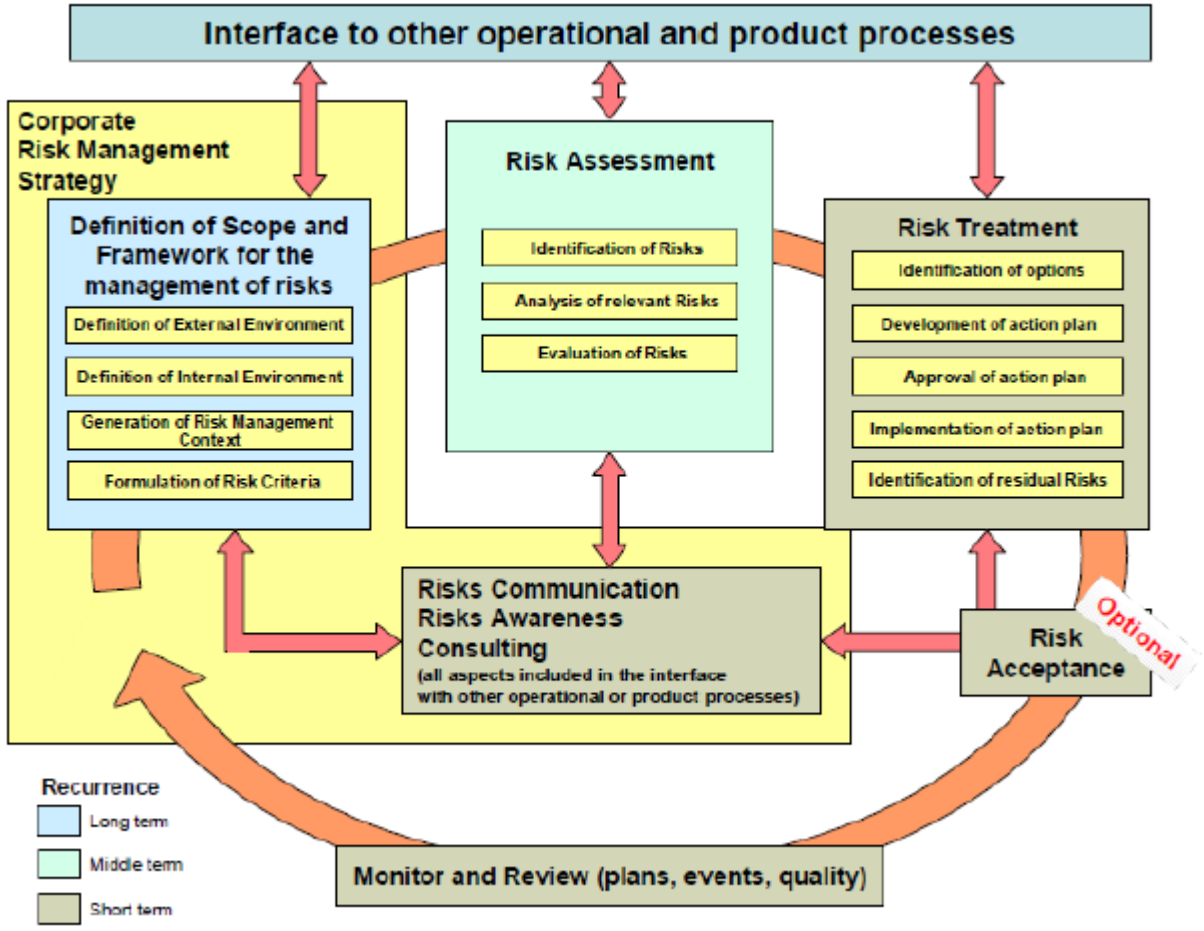
- **Rischio di esternalizzazione ICT**
  Il rischio che il ricorso a una terza parte o a un'altra entità del gruppo (esternalizzazione intra-gruppo), per la fornitura di sistemi ICT o servizi connessi incida negativamente sulle prestazioni e sulla gestione del rischio dell'ente, come ulteriormente esposto nell'allegato.

Metodologie per la gestione del rischio

- La valutazione del rischio nel suo complesso è specificatamente trattata nel già citato standard ISO 31010 Risk management – Risk assessment techniques:
- identificazione del rischio;
- analisi del rischio - analisi delle conseguenze;
- analisi del rischio - stima della probabilità qualitativa, semiquantitativa o quantitativa;
- analisi del rischio - valutazione dell'efficacia di eventuali controlli esistenti;
- analisi del rischio - stima del livello di rischio;
- valutazione del rischio.

Gestione del rischio

ISO 27005:2008



Analisi del rischio in ambito cyber

- La rapidità della evoluzione delle minacce in ambito cyber considerare in primo luogo le minacce
- Vengono considerati gli elementi più esposti alle minacce specifiche
- Vengono considerati gli eventi più gravi e con alta probabilità di accadimento

Analisi dei rischi quali/quantitativi

Probabilità	Impatto 1	2	3	4	5	6
1	€ 4	€ 23	€ 145	€ 917	€ 5,785	€ 36,500
2	€ 23	€ 145	€ 917	€ 5,785	€ 36,500	€ 230,299
3	€ 145	€ 917	€ 5,785	€ 36,500	€ 230,299	€ 1,453,091
4	€ 917	€ 5,785	€ 36,500	€ 230,299	€ 1,453,091	€ 9,168,385
5	€ 5,785	€ 36,500	€ 230,299	€ 1,453,091	€ 9,168,385	€ 57,848,602
6	€ 36,500	€ 230,299	€ 1,453,091	€ 9,168,385	€ 57,848,602	€ 365,000,000

	Insignificante	Minore	Moderato	Maggiore	Severo
Molto probabile	B	B	M	A	MA
Probabile	B	B	M	A	MA
Possibile	MB	B	B	M	A
Improbabile	MB	MB	B	B	M
Raro	MB	MB	MB	B	B

Funzioni essenziali e importanti

Circolare 285

— “funzione aziendale”: l’insieme dei compiti e delle responsabilità assegnate per l’espletamento di una determinata fase dell’attività aziendale. Sulla base della rilevanza della fase svolta, la funzione è incardinata presso una specifica unità organizzativa;

Circolare 285

— “funzione essenziale o importante”: una funzione per la quale risulta verificata almeno una delle seguenti condizioni:

i. un’anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente:

a. i risultati finanziari, la solidità o la continuità dell’attività della banca; ovvero

b. la capacità della banca di conformarsi nel continuo alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;

ii. riguarda funzioni relative ad attività sottoposte a riserva di legge, nella misura in cui la prestazione di tali attività richiede l’autorizzazione da parte di un’autorità di vigilanza;

iii. riguarda compiti operativi delle funzioni aziendali di controllo, a meno che la valutazione dell’essenzialità e dell’importanza della funzione svolta dalla banca non stabilisca che la mancata o inadeguata esecuzione di questi compiti operativi non avrebbe impatti negativi sull’efficacia delle funzioni aziendali di controllo.

Il sistema dei controlli interni, il sistema informativo e la continuità operativa

Nota di chiarimenti (1)(2) Banca d'Italia

4. Quali sono esempi di funzioni operative importanti?

Secondo quanto previsto dalla Sezione I, par. 3, lett. i), sono funzioni operative importanti quelle funzioni per le quali risulta verificata almeno una delle seguenti condizioni:

— un'anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente almeno uno tra i seguenti:

a) i risultati finanziari, la solidità o la continuità delle attività della banca;

b) la capacità della banca di conformarsi alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;

— attività sottoposte a riserva di legge;

— riguarda processi operativi delle funzioni aziendali di controllo o ha un impatto significativo sulla gestione dei rischi aziendali.

Rientra nella responsabilità delle banche l'individuazione delle funzioni aziendali per le quali sussistono le condizioni previste dalla normativa e che quindi si qualificano come funzioni operative importanti. A titolo meramente esemplificativo, rientrano tra le funzioni operative importanti le funzioni di *back office*, il servizio archivio digitale e/o cartaceo, il recupero crediti, il sistema informativo, la delega di gestione di proprie attività, il trasporto valori, le segnalazioni di vigilanza.

BANK OF ENGLAND

FCA FINANCIAL CONDUCT AUTHORITY

Building operational resilience: Impact tolerances for important business services

Business services

A business service is a service that a firm provides to an external end user or participant. Business services deliver a specific outcome or service and should be distinguished from lines of business, eg retail and commercial mortgages, which are a collection of services and activities. They will vary from firm to firm.

In the proposals, the supervisory authorities would require firms and FMIs to consider the chain of activities which make up a business service, from taking on an obligation, to delivery of the service, and determine which part of the chain is critical to delivery. The supervisory authorities propose that all resources that are required to deliver that part of the service should be operationally resilient.

BANK OF ENGLAND

FCA FINANCIAL CONDUCT AUTHORITY

Building operational resilience: Impact tolerances for important business services

‘Important’ business services

The supervisory authorities’ view, originally set out in the DP, is that business services will qualify as ‘important’ when their failure could cause an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, the safety and soundness of individual firms, or financial stability. Often important business services will be linked to the ability to make timely payments such as making mortgage disbursements but this need not always be the case. Further guidance and expectations are provided in the proposals published by each supervisory authority.

Protezione e prevenzione

ARTICOLO *9*

Protezione e prevenzione

1. Allo scopo di proteggere adeguatamente i sistemi di TIC e nella prospettiva di organizzare misure di risposta, le entità finanziarie **monitorano e controllano costantemente la sicurezza e il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto dei rischi informatici** sui sistemi di TIC **adottando politiche, procedure e strumenti adeguati per la sicurezza** delle TIC.

2. Le entità finanziarie **definiscono, acquisiscono e attuano politiche, procedure, protocolli e strumenti per la sicurezza delle TIC miranti a garantire la resilienza, la continuità e la disponibilità** dei sistemi di TIC, in particolare quelli a supporto di funzioni essenziali o importanti, nonché a **mantenere standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati** conservati, in uso o in transito.

3. **Al fine di conseguire gli obiettivi di cui al paragrafo 2** le entità finanziarie **usano soluzioni e processi TIC appropriati** conformemente all'articolo 4. Tali soluzioni e processi TIC:

a) **garantiscono la sicurezza dei mezzi di trasferimento dei dati**;

b) **riducono al minimo i rischi di corruzione o perdita di dati, di accesso non autorizzato nonché di difetti tecnici** che possono ostacolare l'attività commerciale;

c) **prevengono** la **mancanza** di **disponibilità**, il deterioramento **dell'autenticità o dell'integrità**, le **violazioni della riservatezza e la perdita di dati;**

d) assicurano la protezione dei dati contro i **rischi derivanti dalla gestione dei dati, compresi la cattiva amministrazione, i rischi relativi al trattamento dei dati e l'errore umano**.

4. **All'interno del quadro** per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie:

a) **elaborano e documentano una politica di sicurezza dell'informazione** che definisce **le norme per tutelare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, dei patrimoni informativi e delle risorse TIC, compresi quelli dei loro clienti, se del caso;**

b) seguendo un approccio basato sul rischio, realizzano una **solida struttura di gestione della rete e delle infrastrutture** impiegando **tecniche, metodi e protocolli** adeguati, che **possono includere l'applicazione di meccanismi automatizzati, per isolare i patrimoni informativi colpiti in caso di attacchi informatici**;

c) attuano politiche che **limitano l'accesso fisico o logico ai patrimoni informativi e alle risorse TIC** unicamente a **quanto è necessario per funzioni e attività legittime e approvate**, e stabiliscono a tale scopo una serie di **politiche, procedure e controlli** concernenti i **diritti di accesso** e garantiscono una **solida amministrazione degli stessi;**

d) attuano politiche e protocolli riguardanti **robusti meccanismi di autenticazione**, basati su **norme pertinenti e sistemi di controllo dedicati, e misure di protezione delle chiavi crittografiche di cifratura dei dati** sulla scorta dei risultati di processi approvati per la **classificazione dei dati e la valutazione dei rischi informatici;**

e) attuano **politiche, procedure e controlli documentati** per la **gestione delle modifiche** delle TIC, comprese le modifiche apportate a componenti software, hardware e firmware, sistemi o parametri di sicurezza, che adottano un approccio basato sulla valutazione del rischio e sono parte integrante del processo complessivo di gestione delle modifiche dell'entità finanziaria, in modo che **tutte le modifiche apportate ai sistemi di TIC siano registrate, testate, valutate, approvate, attuate e verificate in maniera controllata**;

f) si dotano di politiche **documentate**, idonee ed esaustive in materia di **correzioni ed aggiornamenti**.

Ai fini della lettera b) del primo comma, le entità finanziarie **progettano l'infrastruttura di connessione di rete in modo che sia possibile isolarla o segmentarla istantaneamente,** al fine di ridurre al minimo e **prevenire il contagio, soprattutto per i processi finanziari interconnessi.**

Ai fini della lettera e) del primo comma, il **processo di gestione delle modifiche delle TIC è approvato da linee di gestione adeguate e comprende protocolli specifici in essere.**

ARTICOLO *7*

Sistemi, protocolli e strumenti di TIC

Al fine di **affrontare e gestire i rischi informatici**, le entità finanziarie **utilizzano e mantengono aggiornati sistemi, protocolli e strumenti di TIC** che sono:

a)idonei alle dimensioni delle operazioni a supporto dello svolgimento delle attività delle entità finanziarie, conformemente al principio di proporzionalità di cui all'articolo 4;

b) affidabili;

c) **dotati di capacità sufficiente** per elaborare in maniera accurata i dati necessari per lo svolgimento delle attività e la tempestiva fornitura dei servizi, **nonché per sostenere i picchi di volume** di ordini, messaggi od operazioni, a seconda delle necessità, anche in caso di introduzione di nuove tecnologie;

d) **tecnologicamente resilienti, in modo da fare adeguatamente fronte alle esigenze di informazioni supplementari richieste da condizioni di stress del mercato o da altre situazioni avverse.**

Le misure di sicurezza

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Low Impact Controls

Showing **115** controls:

No.	Control	Priority	Low	Moderate	High
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	ACCESS ENFORCEMENT	P1	AC-3	AC-3	AC-3
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7	AC-7	AC-7
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8	AC-8	AC-8
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	P3	AC-14	AC-14	AC-14
AC-17	REMOTE ACCESS	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)

800-53

(Rev. 4)

Security Controls

Low-Impact

Moderate-Impact

High-Impact

Other Links

Families

Search

Risposta e Ripristino

ARTICOLO *11*

Risposta e ripristino

1. All'interno del **quadro** per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, e in base ai requisiti di identificazione stabiliti all'articolo 8, le entità finanziarie predispongono una **politica di continuità operativa delle TIC** esaustiva, la quale può essere adottata come una politica specifica dedicata che **costituisce parte integrante della politica generale di continuità operativa dell'entità finanziaria.**

2. Le entità finanziarie **attuano la politica di continuità operativa** delle TIC **tramite accordi, piani, procedure e meccanismi appositi, appropriati e documentati, miranti a:**

a) **garantire la continuità delle funzioni essenziali o importanti** dell'entità finanziaria;

b) **rispondere in maniera rapida, appropriata ed efficace e trovare una soluzione a tutti gli incidenti connessi alle TIC, in modo da limitare i danni e privilegiare la ripresa delle attività e le azioni di ripristino;**

c) **attivare senza ritardo piani dedicati che prevedano tecnologie, processi e misure di contenimento idonei a ciascun tipo di incidente** connesso alle TIC e a **scongiurare danni ulteriori**, **nonché procedure mirate di risposta e ripristino** stabilite in conformità dell'articolo 12;

d) **stimare in via preliminare impatti, danni e perdite;**

e) stabilire **azioni di comunicazione e gestione delle crisi** che assicurino **la trasmissione di informazioni aggiornate a tutto il personale interno interessato e ai portatori di interessi esterni**, conformemente all'articolo 14, e comunicare tali informazioni alle **autorità competenti**, conformemente all'articolo 19.

3. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie **attuano i piani di risposta e ripristino** relativi alle TIC associati; per le entità finanziarie diverse dalle microimprese **tali piani sono soggetti a un audit interno indipendente**.

4. Le entità finanziarie p**redispongono, mantengono e testano periodicamente opportuni piani di continuità operativa** delle TIC**, in particolare** per quanto riguarda le funzioni essenziali o importanti **esternalizzate o appaltate tramite accordi con fornitori terzi di servizi TIC.**

5. Nell'ambito della politica generale di continuità operativa, le entità finanziarie effettuano un'analisi dell'impatto sulle attività aziendali (***Business Impact Analysis*** — BIA) delle loro esposizioni a gravi perturbazioni delle attività. Nel quadro della BIA, le entità finanziarie valutano l'impatto potenziale di gravi perturbazioni delle attività **mediante criteri quantitativi e qualitativi, utilizzando, se del caso, dati interni ed esterni e analisi di scenario**. La BIA tiene conto della **criticità delle funzioni commerciali, dei processi di supporto, delle dipendenze da terzi** e dei patrimoni informativi individuati e mappati, nonché delle loro i**nterdipendenze**. Le entità finanziarie provvedono affinché le risorse TIC e i servizi TIC siano progettati e utilizzati in piena conformità con la BIA, in particolare **garantendo adeguatamente la ridondanza di tutte le componenti essenziali.**

6. All'interno della gestione complessiva dei rischi informatici, le entità finanziarie:

a) **testano i piani di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC** in relazione ai sistemi di TIC a supporto di tutte le funzioni **almeno una volta all'anno nonché in caso di modifiche di rilievo** ai sistemi di TIC a supporto di funzioni essenziali o importanti;

b) **testano i piani di comunicazione delle crisi** istituiti in conformità dell'articolo 14.

Ai fini del primo comma, lettera a), le entità finanziarie diverse dalle microimprese **inseriscono nei piani dei test scenari di attacchi informatici** e del **passaggio tra le infrastrutture delle TIC primarie e la capacità ridondante, i backup e le attrezzature ridondanti** necessarie per soddisfare gli obblighi di cui all'articolo 12.

Le entità finanziarie **riesaminano periodicamente la politica di continuità operativa delle TIC e i piani di risposta e ripristino** relativi alle TIC, **tenendo conto dei risultati dei test svolti** in conformità del primo comma e delle raccomandazioni formulate sulla base dei **controlli di audit o degli esami di vigilanza**.

7. Le entità finanziarie diverse dalle microimprese si **dotano di una funzione di gestione delle crisi** che, in caso di attivazione dei piani di continuità operativa delle TIC o dei piani di risposta e ripristino relativi alle TIC, **fissa, tra l'altro, procedure chiare per la gestione della comunicazione interna ed esterna delle crisi,** in conformità dell'articolo 14.

8. Le entità finanziarie **rendono prontamente accessibili le registrazioni delle attività svolte prima e durante le perturbazioni in cui vengono attivati i piani di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC.**

9. Le **controparti centrali** **trasmettono alle autorità** competenti **copie dei risultati dei** test di continuità operativa delle TIC o di esercizi analoghi.

10. **Le entità finanziarie**, diverse dalle microimprese, **comunicano alle autorità competenti, su loro richiesta di queste ultime, una stima dei costi e delle perdite annuali aggregati causati da incidenti gravi connessi alle TIC.**

11. ***A norma dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV elaborano, tramite il comitato congiunto, entro il 17 luglio 2024 orientamenti comuni sulla stima dei costi e delle perdite annuali aggregati di cui al paragrafo 10.***

***ARTICOLO** 12*

Politiche e procedure di backup — Procedure e metodi di ripristino e recupero

1.Al fine di assicurare che i sistemi e i dati di TIC siano ripristinati riducendo al minimo il periodo di inattività e limitando la perturbazione e le perdite, all'interno del proprio quadro per la gestione dei rischi informatici le entità finanziarie elaborano e documentano:

a) l**e politiche e procedure di backup** che precisano il perimetro dei dati soggetti a backup e **la frequenza minima del backup,** in base alla criticità delle informazioni o al livello di riservatezza dei dati;

b) le procedure e i metodi di ripristino e recupero.

2. Le entità finanziarie si dotano di sistemi di backup che possono essere attivati conformemente alle politiche e alle procedure di backup, come pure alle procedure e ai metodi di ripristino e recupero. **L'attivazione dei sistemi di backup non mette a repentaglio la sicurezza dei sistemi informatici e di rete né, la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati. I test delle procedure di backup e di ripristino nonché delle procedure e dei metodi di recupero sono effettuati periodicamente.**

3. **Nel ripristino dei dati di backup** effettuato utilizzando i propri sistemi, le entità finanziarie **impiegano sistemi di TIC che sono fisicamente e logicamente segregati dal sistema di TIC sorgente. I sistemi di TIC sono protetti in maniera sicura da qualsiasi accesso non autorizzato o corruzione delle TIC e consentono il tempestivo ripristino dei servizi attraverso il backup dei dati e dei sistemi ove necessario.**

Per le **controparti centrali**, i piani di ripristino consentono il ripristino di tutte le operazioni in corso al momento della perturbazione, così da permettere alla controparte centrale di continuare a operare con certezza e di completare la liquidazione alla data programmata.

I **fornitori di servizi di comunicazione dati** mantengono inoltre risorse adeguate e dispongono di attrezzature di back-up e ripristino per offrire e mantenere in ogni momento i loro servizi.

4. Le entità finanziarie, diverse dalle microimprese, mantengono **capacità di TIC ridondanti**, dotate di risorse e funzioni sufficienti e adeguate a soddisfare le esigenze commerciali. Le microimprese valutano la necessità di mantenere tali capacità di TIC ridondanti sulla base del loro profilo di rischio.

5. **I depositari centrali di titoli** mantengono **almeno un sito secondario** di trattamento dati dotato di risorse, capacità, funzioni e personale adeguati a soddisfare le esigenze commerciali.

Il sito secondario di trattamento dati è:

a) **ubicato geograficamente a distanza dal sito primario** per garantire che esso abbia un profilo di rischio distinto e impedire che venga colpito dall'evento che ha interessato il sito primario;

b) **in grado di garantire la continuità delle funzioni essenziali o importanti in maniera identica al sito primario, oppure di fornire il livello di servizi** necessario a garantire che l'entità finanziaria svolga le proprie operazioni essenziali **nell'ambito degli obiettivi di ripristino**;

c) **immediatamente accessibile al personale** dell'entità finanziaria per garantire la continuità delle funzioni essenziali o importanti **qualora il sito primario di trattamento dati divenga indisponibile**.

6. **Nel determinare gli obiettivi in materia di punti di ripristino** e tempi di ripristino di ciascuna funzione, le entità finanziarie tengono conto del fatto che si tratti di una funzione essenziale o importante e del **potenziale impatto complessivo sull'efficienza del mercato**. Questi obiettivi in materia di tempi **garantiscono che i livelli di servizi concordati siano rispettati anche in scenari estremi.**

7. **Durante il ripristino successivo a un incidente** connesso alle TIC, le entità finanziarie effettuano **le verifiche necessarie, comprese eventuali verifiche multiple e controlli incrociati, per assicurare che sia mantenuto il più elevato livello di integrità dei dati. Questi controlli sono effettuati anche al momento di ricostruire i dati provenienti da portatori di interessi esterni, per assicurare la piena coerenza di tutti i dati tra i sistemi.**

Soluzioni: DR

- Le soluzioni di DR comprendono una casistica pressoché illimitata, in quanto molteplici sono le composizioni dei sistemi informativi delle aziende di grosse dimensioni.
- È possibile distinguere alcune macro soluzioni:
  - disponibilità di un sito, nel quale è possibile collocare i sistemi su cui far ripartire applicazioni e servizi
  - disponibilità di un sito, con già disponibili i sistemi su cui far ripartire applicazioni e servizi, lasciati inattivi
  - disponibilità di un sito, nel quale sono disponili sistemi già attivi che erogano applicazioni e servizi; in questo caso si utilizza normalmente un bilanciamento di carico fra i due siti (quello primario e quello secondario) nella erogazione dei servizi. In caso di fault di uno dei siti l'altro è in grado di erogare il 100% dei servizi, eventualmente con prestazioni degradate.

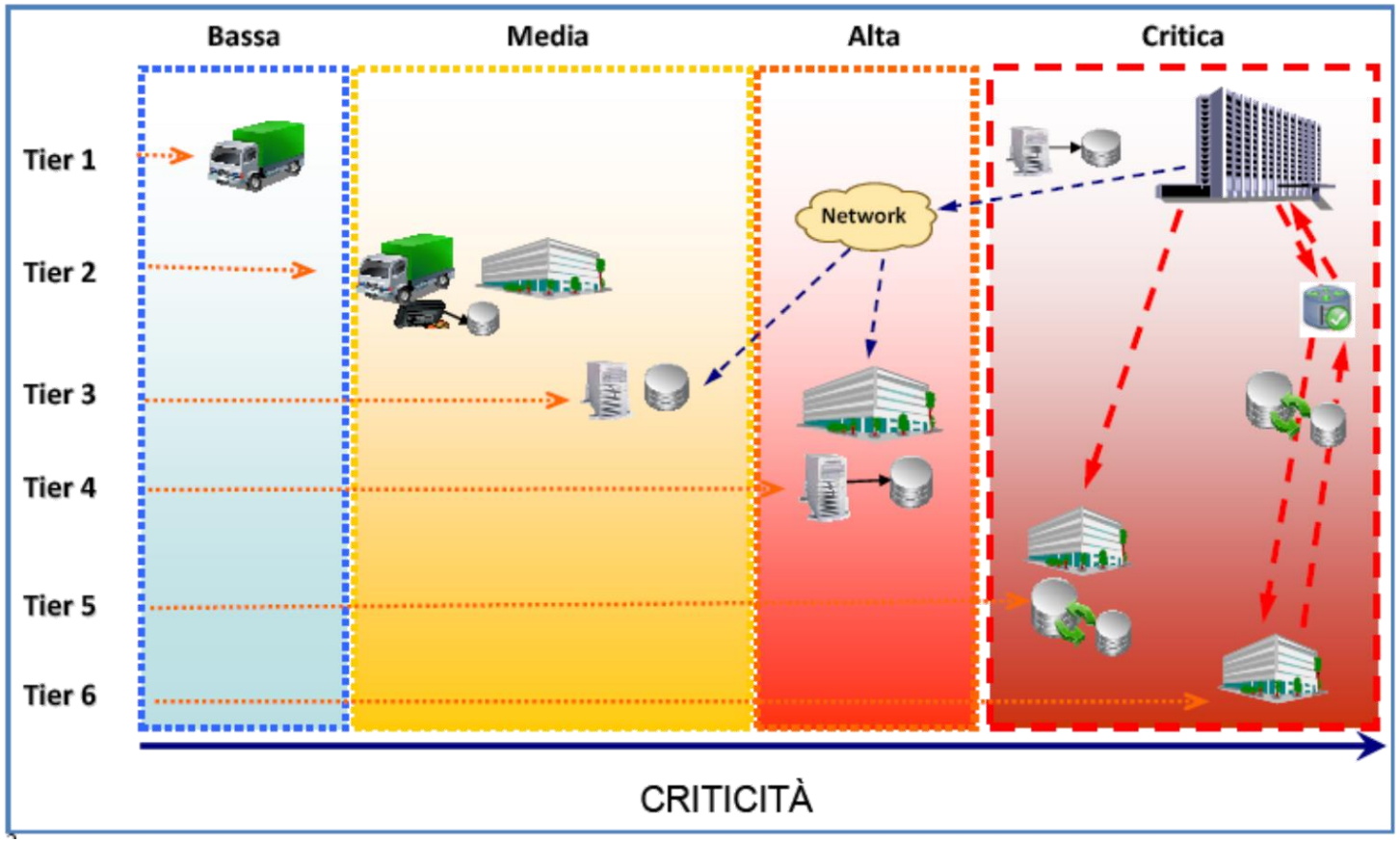
Soluzioni: DR

- disponibilità di un sito, nel quale sono disponili sistemi già attivi che erogano applicazioni e servizi [*]; in questo caso si utilizza normalmente un bilanciamento di carico fra i due siti (quello primario e quello secondario) nella erogazione dei servizi. In caso di fault di uno dei siti l'altro è in grado di erogare il 100% dei servizi, eventualmente con prestazioni degradate.

- [*] in alcuni casi sono usati per sviluppo e test ed è quindi comunque necessaria una ripartenza

G.Butti I rischi nascosti nelle soluzioni di continuità operativa e disaster recovery - CLUSIT Education

Soluzioni: DR



Linee guida PA

Incidenti cyber: *es. ransomware*

- Misure di prevenzione
- Cifratura dei dati
- Air gapping
- Backup off line

Indisponibilità applicativi

- Contratti che garantiscono interventi di assistenza in tempi rapidi e certi 24x7 con fornitori di applicazioni e componenti che supportano processi critici
- Organizzazione dei turni del personale ICT compatibile con interventi 24x7 sui componenti che gestiscono i processi critici

Indisponibilità edifici

- Definizione di unità organizzative di backup presso altre sedi
- Spostamento del personale presso altre sedi
- Smartworking
- …

Indisponibilità personale essenziale

- Definizione di unità organizzative di backup presso altre sedi o in smartworking
- Organizzazione dell'attività con turni
- …

Scenari di rischio

Linee guida per il disaster recovery delle pubbliche amministrazioni

- Da quanto detto consegue che la continuità dei servizi informatici rappresenta un impegno inderogabile per la PA che deve operare in modo da limitare al massimo gli effetti negativi di possibili **fermi prolungati dei servizi ICT**.
- A titolo esemplificativo, la compromissione della continuità di un sistema informatico, può essere conseguenza di:
  - **errori/malfunzionamenti dei processi** (il processo organizzativo che usa il servizio ICT non ha funzionato come avrebbe dovuto per errori materiali, errori nell'applicazione di norme ovvero per il verificarsi di circostanze non adeguatamente previste dalle stesse);
  - **malfunzionamento dei sistemi, delle applicazioni e delle infrastrutture;**
  - **attacchi o eventi naturali di tipo accidentale**;
  - **disastri**.

Scenari di rischio

Circolare 285

- Il piano di continuità operativa prende in considerazione diversi scenari di crisi basati almeno sui seguenti fattori di rischio, conseguenti a **eventi naturali o attività umana**, inclusi danneggiamenti gravi da parte di dipendenti:
  - distruzione o inaccessibilità di **strutture** nelle quali sono allocate unità operative o apparecchiature critiche;
  - indisponibilità di **sistemi informativi critici**;
  - indisponibilità di **personale essenziale** per il funzionamento dei processi aziendali;
  - interruzione del funzionamento delle **infrastrutture** (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
  - alterazione o perdita di **dati e documenti critici**.

Scenari di rischio

Circolare 285

Allegato A – Requisiti per la continuità operativa

- *2.3 Scenari di rischio*
- Gli scenari di rischio rilevanti per la continuità operativa dei processi a rilevanza sistemica sono documentati e costantemente aggiornati. Essi includono, in aggiunta a quanto previsto per tutti gli operatori: eventi catastrofici con distruzioni fisiche su larga scala, a dimensione metropolitana o superiore, che investano infrastrutture essenziali dell'operatore e di terzi; situazioni di crisi gravi anche non connesse ad eventi con distruzioni materiali (ad es., **pandemie, attacchi biologici, attacchi informatici su larga scala**).

Individuazione

ARTICOLO *10*

Individuazione

1. Le entità finanziarie predispongono **meccanismi per individuare tempestivamente le attività anomale, conformemente all'articolo 17, compresi i problemi di prestazione della rete delle TIC e gli incidenti a esse connessi, nonché per individuare i potenziali singoli punti di vulnerabilità (*points of failure*)** importanti.

Tutti i meccanismi di individuazione di cui al primo comma sono periodicamente testati in conformità dell'articolo 25.

2. **I meccanismi di individuazione** di cui al paragrafo 1 **prevedono molteplici livelli di controllo**, definiscono **soglie di allarme e criteri per l'attivazione e l'avvio dei processi di risposta agli incident**i connessi alle TIC, **compresi meccanismi di allarme automatico per il personale incaricato** della risposta agli incidenti connessi alle TIC.

3. Le entità finanziarie **dedicano risorse e capacità sufficienti al monitoraggio dell'attività degli utenti** e **di eventuali anomalie e incidenti** connessi alle TIC, **in particolare attacchi informatici.**

4. I **fornitori di servizi di comunicazione dati** predispongono inoltre **sistemi in grado di controllare efficacemente le comunicazioni sulle operazioni per verificarne la completezza, individuare omissioni ed errori palesi e chiederne la ritrasmissione.**

Intercettare un incidente

National Cyber Security Centre

Security Monitoring: Requirements

The following table highlights Key Aspects security monitoring to consider, and a relevant Security Monitoring Requirement for each. It also recommends examples of what your organisation can do to meet each of the requirements.

Key Aspects	Security Monitoring Requirement	Recommended steps to meet the Security Monitoring Requirements
Business traffic crossing a boundary	Traffic exchanges are authorised and conform to security policy. Transport of malicious content and other forms of attack by manipulation of business traffic are detected and alerted.	• Collect details of imports and exports executed by internal users. • Track cross-boundary information exchange operations. • Collect information on the use of any externally visible interfaces. • Collect information and alerts from content checking and quarantining services.
Activity at a boundary	Detect suspect activity indicative of the actions of an attacker attempting to breach the system boundary, or other deviation from normal business behaviour.	• Collect information from firewalls and other network devices for traffic and traffic-trend. • Collect information from any Intrusion Detection Service (IDS) at the boundary with any un-trusted network.
Internal workstation, server or device	Detect changes to device status and configuration from accidental or deliberate acts by a user, or by malware.	• Record changes to device configuration. • Record indications that could be attributed to accidental or malicious activity (eg system restarts or undefined system processes). • Record indications of unauthorised actions in tightly controlled environments such as the attachment of USB storage devices. • Collect information relating to access to any business critical file areas.
Internal network activity	Detect suspicious activity that may indicate attacks by internal users, or external attackers who have penetrated the internal network.	• Monitor critical internal boundaries and resources within internal networks. Possible candidates for heightened internal monitoring include: core electronic messaging infrastructure (eg email servers & directory servers) sensitive databases (eg HR databases, finance, procurement/contracts, etc.) project servers and file stores with restricted access requirements
Network connections	Prevent unauthorised connections to the network made by remote access, VPN, wireless or any other transient means of network connection.	• Monitor network access points that are open to connection attempts by anyone (eg WiFi access points). • Monitor mobile users and remote working solutions. • Monitor restrictive environments in which the attachment of modems and wireless access points are prohibited. • Monitor network ports of the wired network environment.
Session activity by user & work station	Detect unauthorised activity and access that is suspicious or violates security policy requirements.	• Monitor user activity and sensitive data accesses to ensure they can be made accountable for their actions. • Monitor workstation connectivity, connected peripherals and data ports. • Profile normal user activity to enable detection of abnormal behaviour. • Tightly control and monitor administration and service accounts.
Alerting on events	Be able to respond to security incidents in a time frame appropriate to the perceived criticality of the incident.	• Ensure events classed as critical are notified in as close to real-time as is achievable. • Ensure automation and filtering is sufficient to bring events to the attention of the right people using the right mechanism. • Establish the correct level of monitoring for the organisation, ranging from simple monitoring to integrated solutions using enterprise level centralised security. • Consider combining functions such as security and network management, taking into account maintaining segregation requirements. • Implement secondary alerting channels (eg SNMP, email, SMS, etc.) using in-hours or out-of-hours services when continuous console manning cannot be provided
Accurate time in logs	Be able to correlate event data collected from disparate sources.	• Provide a master clock system component which is synchronised to an atomic clock • Update device clocks from the master clock using the Network Time Protocol (NTP) • Record time in logs in a consistent format - Universal Co-ordinated Time (UTC) is recommended • Provide a process to check and update device clocks on a regular basis (eg weekly) • Define the error margin for time accuracy according to business requirements • Provide manual maintenance for devices that do not support clock synchronisation • Provide support for local time on human interfaces • Provide a process to correct clock drift on mobile devices upon reconnection
Data backup status	Be able to recover from an event that compromises the integrity or availability of information assets.	• Provide an audit trail of backup and recovery to enable identification of the last known good state of the information assets. • Alert storage failure events.

For more information go to: **www.ncsc.gov.uk** **@ncsc_hmg**

Punti di attenzione

Dora esplicitamente si riferisce alla cybersecurity, ma in realtà richiede anche di garantire la continuità operativa.

Quindi l'identificazione va estesa a tutti gli eventi che possono compromettere la continuità anche in ambito sicurezza fisica, personale…

Apprendimento ed evoluzione

ARTICOLO *13*

Apprendimento ed evoluzione

1. Le entità finanziare dispongono **capacità e personale per raccogliere informazioni in relazione alle vulnerabilità e alle minacce informatiche, agli incidenti connessi alle TIC, in particolare agli attacchi informatici, e analizzarne i probabili effetti sulla loro resilienza operativa digitale.**

2. **Dopo che un grave incidente** connesso alle TIC ha perturbato le loro attività principali, le entità finanziarie **svolgono un riesame** successivo a tale incidente che **analizzi le cause** della perturbazione e **identifichi i miglioramenti** che è necessario apportare **alle operazioni** riguardanti le TIC o nell'ambito della **politica di continuità operativa** delle TIC di cui all'articolo 11.

Le entità finanziarie diverse dalle microimprese comunicano, su richiesta, alle autorità competenti le modifiche attuate a seguito del riesame successivo all'incidente connesso alle TIC di cui al primo comma.

Il **riesame successivo all'incidente** connesso alle TIC di cui al primo comma **determina se le procedure stabilite siano state seguite e se le azioni adottate siano state efficaci, anche in relazione:**

a) **alla tempestività della risposta** agli allarmi di sicurezza e alla **determinazione dell'impatto degli incidenti** connessi alle TIC e **della loro gravità**;

b) alla **qualità e alla rapidità dell'analisi forense, ove ritenuto opportuno;**

c) **all'efficacia della procedura di attivazione dei livelli successivi di intervento** in caso di incidenti all'interno dell'entità finanziaria;

d) **all'efficacia della comunicazione interna ed esterna**.

3. Gli **insegnamenti tratti dai test** sulla resilienza operativa digitale effettuati in conformità degli articoli 26 e 27 **e da incidenti connessi alle TIC realmente avvenuti, in particolare attacchi informatici, insieme alle difficoltà riscontrate al momento dell'attivazione dei piani di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC, nonché le informazioni pertinenti scambiate con le controparti e valutate nel corso degli esami di vigilanza sono debitamente e costantemente integrati nel processo di valutazione dei rischi informatici. Tali risultanze costituiscono la base per opportune revisioni delle relative componenti del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1**.

4. Le entità finanziarie **monitorano l'efficacia dell'attuazione della loro strategia di resilienza operativa** digitale stabilita all'articolo 6, paragrafo 8. **Tracciano l'evoluzione nel tempo dei rischi informatici, analizzano la frequenza, i tipi, le dimensioni e l'evoluzione degli incidenti connessi alle TIC,** in particolare **gli attacchi informatici e i relativi schemi, al fine di comprendere il livello di esposizione ai rischi informatici** — segnatamente in relazione alle funzioni essenziali o importanti — e **migliorare la maturità informatica** e la preparazione dell'entità finanziaria.

5. Il personale addetto alle TIC di grado più elevato **comunica almeno una volta all'anno all'organo di gestione le risultanze di cui al paragrafo 3 e formula raccomandazioni.**

6. Le entità finanziarie elaborano **programmi di sensibilizzazione sulla sicurezza** delle TIC nonché **attività di formazione** sulla resilienza operativa digitale, che rappresentano **moduli obbligatori nei programmi di formazione del personale**. Tali programmi e attività di formazione riguardano tutti i **dipendenti e gli alti dirigenti**, e presentano un **livello di complessità commisurato all'ambito delle loro funzioni**. **Se del caso**, le entità finanziarie **includono anche i fornitori terzi di servizi TIC nei loro sistemi di formazion**e pertinenti, conformemente all'articolo 30, paragrafo 2, lettera i).

7. Le entità finanziarie diverse dalle microimprese monitorano costantemente i pertinenti sviluppi tecnologici, anche al fine di comprendere i possibili effetti dell'impiego di tali nuove tecnologie sui requisiti in materia di sicurezza delle TIC e sulla resilienza operativa digitale. Si tengono aggiornate sui più recenti processi di gestione dei rischi informatici, in modo da contrastare efficacemente le forme nuove o già esistenti di attacchi informatici.

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.

Incidenti

ARTICOLO 17

Processo di gestione degli incidenti connessi alle TIC

1. Le entità finanziarie definiscono, stabiliscono e attuano un **processo di gestione degli incidenti connessi alle TIC al fine di individuare, gestire e notificare tali incidenti**.

2. Le entità finanziarie **registrano tutti gli incidenti** connessi alle TIC e le **minacce informatiche significative.** Le entità finanziarie istituiscono procedure e processi appropriati per garantire, in maniera coerente e integrata, il **monitoraggio e il trattamento degli incidenti** connessi alle TIC, **nonché il relativo seguito, in modo da identificare, documentare e affrontare le cause di fondo e prevenire il verificarsi di tali incidenti**.

3. **Il processo** di gestione degli incidenti connessi alle TIC di cui al paragrafo 1:

a) **predispone indicatori di allerta precoce**;

b) stabilisce procedure per **identificare, tracciare, registrare, categorizzare e classificare gli incidenti** connessi alle TIC in base alla loro **priorità e gravità** e in base alla **criticità dei servizi colpiti**, conformemente ai criteri di cui all'articolo 18, paragrafo 1;

c) assegna i **ruoli e le responsabilità** che è necessario attivare **per i diversi scenari e tipi di incidenti** connessi alle TIC;

d) elabora **piani per la comunicazione al personale**, ai **portatori di interessi esterni** e ai **mezzi di comunicazione** conformemente all'articolo 14, nonché per la **notifica ai clienti**, **per le procedure di attivazione dei livelli successivi di intervento, compresi i reclami dei clienti** in materia di TIC, e per la comunicazione di informazioni **alle entità finanziarie che agiscono da controparti**, a seconda dei casi;

e) assicura la **segnalazione almeno degli incidenti gravi** connessi alle TIC **agli alti dirigenti** interessati e **informa l'organo di gestione** almeno in merito a detti incidenti, **illustrandone l'impatto e la risposta e i controlli supplementari da introdurre**;

f) stabilisce **procedure di risposta agli incidenti** connessi alle TIC per **attenuarne l'impatto** e **garantisce tempestivamente l'operatività e la sicurezza dei servizi.**

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**.

2. Le entità finanziarie **classificano le minacce** informatiche come significative **in base alla criticità dei servizi a rischio**, comprese le operazioni dell'entità finanziaria, il n**umero** e/o la **rilevanza di clienti o controparti** finanziarie interessati e **l'estensione geografica** delle aree a rischio.

3. *In consultazione con la BCE e l'ENISA, le AEV elaborano, tramite il comitato congiunto, progetti di norme tecniche di regolamentazione comuni che specificano ulteriormente gli aspetti seguenti:*

a) *i criteri di cui al paragrafo 1, comprese le soglie di rilevanza per la determinazione dei gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o relativi alla sicurezza dei pagamenti, che sono oggetto dell'obbligo di segnalazione di cui all'articolo 19, paragrafo 1;*

b) *i criteri che le autorità competenti devono applicare per valutare la rilevanza degli gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o relativi alla sicurezza dei pagamenti per le autorità competenti interessate in altri Stati membri, nonché i dettagli delle segnalazioni di incidenti gravi connessi alle TIC o, ove applicabile, di gravi incidenti operativi o di sicurezza dei pagamenti da condividere con altre autorità competenti ai sensi dell'articolo 19, paragrafi 6 e 7.*

c) *i criteri di cui al paragrafo 2 del presente articolo, comprese soglie di rilevanza elevate per la determinazione delle minacce informatiche significative.*

4. All'atto dell'elaborazione dei progetti di norme tecniche di regolamentazione comuni di cui al paragrafo 3 del presente articolo, le AEV tengono conto dei criteri di cui all'articolo 4, paragrafo 2, come pure delle norme internazionali, degli orientamenti e delle specifiche elaborati e pubblicati dall'ENISA, tra cui, se del caso, le specifiche riguardanti altri settori economici. Ai fini dell'applicazione dei criteri di cui all'articolo 4, paragrafo 2, le AEV tengono debitamente conto della necessità delle microimprese e delle piccole e medie imprese di mobilitare risorse e capacità sufficienti per garantire una gestione rapida degli incidenti connessi alle TIC.

Le AEV presentano tali progetti di norme tecniche di regolamentazione comuni alla Commissione **entro il 17 gennaio 2024.**

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al paragrafo 3 in conformità degli articoli da 0 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

ARTICOLO *19*

Segnalazione dei gravi incidenti TIC e notifica volontaria delle minacce informatiche significative

1. Le entità finanziarie **segnalano gli gravi incidenti TIC all'autorità competente interessata** di cui all'articolo 46 a norma del paragrafo 4 del presente articolo.

Se un'entità finanziaria **è soggetta alla vigilanza di più di un'autorità** nazionale competente di cui all'articolo 46, gli **Stati membri designano un'unica autorità** competente quale autorità competente interessata responsabile dell'espletamento delle funzioni e dei compiti di cui al presente articolo.

Gli **enti creditizi classificati come significativi** ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 **segnalano i gravi incidenti** TIC **all'autorità nazionale competente** designata ai sensi dell'articolo 4 della direttiva 2013/36/UE, che trasmette immediatamente tale segnalazione alla BCE.

Ai fini del primo comma, le entità finanziarie redigono, dopo aver raccolto e analizzato tutte le informazioni pertinenti, **la notifica iniziale** e le relazioni di cui al paragrafo 4 del presente articolo utilizzando i **modelli di cui all'articolo 20** e le **trasmettono all'autorità competente**. **Qualora un impedimento tecnico non consenta la trasmissione della notifica iniziale utilizzando il modello, le entità finanziarie informano in merito l'autorità competente con mezzi alternativi**.

La notifica iniziale e le relazioni di cui al paragrafo 4 contengono tutte le informazioni necessarie all'autorità competente per determinare la rilevanza dell'grave incidente TIC e valutarne i possibili impatti transfrontalieri.

Fatta salva la segnalazione a norma del primo comma da parte dell'entità finanziaria all'autorità competente interessata, gli **Stati membri possono stabilire**, in aggiunta, che alcune o tutte le entità finanziarie forniscano a**ltresì la notifica** iniziale e ciascuna relazione di cui al paragrafo 4 del presente articolo utilizzando i modelli di cui all'articolo 20 alle autorità competenti o ai gruppi di intervento per la sicurezza informatica in caso di incidente (*computer security incident response teams* — **CSIRT) designati o istituiti a norma della direttiva (UE) 2022/2555**.

2. Le entità finanziarie **possono, su base volontaria, notificare le minacce informatiche significative all'autorità** competente interessata **qualora ritengano che la minaccia sia rilevante per il sistema finanziario**, **gli utenti dei servizi o i clienti**. **L'autorità competente interessata può fornire tali informazioni alle altre autorità pertinenti di cui al paragrafo 6.**

Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 **possono notificare, su base volontaria**, le minacce informatiche significative all'autorità nazionale competente, designata ai sensi dell'articolo 4 della direttiva 2013/36/UE, che trasmette immediatamente la notifica alla BCE.

Gli Stati membri possono stabilire che le entità finanziarie che procedono alla **notifica su base volontaria** e a norma del primo comma possano altresì trasmettere tale notifica ai **CSIRT** nazionali designati o istituiti a norma della direttiva (UE) 2022/2555.

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**.

5. Ai sensi del presente articolo, le entità finanziarie **possono esternalizzare**, conformemente al diritto settoriale dell'Unione e nazionale, gli **obblighi di segnalazione a un fornitore terzo** di servizi. In caso di esternalizzazione, l'entità finanziaria rimane pienamente responsabile di espletare gli obblighi di segnalazione degli incidenti.

6. *Dopo aver ricevuto la notifica iniziale e ciascuna delle relazioni di cui al paragrafo 4, l'autorità competente trasmette tempestivamente i dettagli dell'grave incidente TIC ai seguenti destinatari sulla base, ove applicabile, delle rispettive competenze:*

a) all'ABE, all'ESMA o all'EIOPA;

b) alla BCE, qualora siano coinvolte le entità finanziarie di cui all'articolo 2, paragrafo 1, lettere a), b) e d);

c) *alle autorità competenti, ai punti di contatto unici o ai CSIRT designati o istituiti conformemente alla direttiva (UE) 2022/2555*;

d) *alle autorità di risoluzione di cui all'articolo 3 della direttiva 2014/59/UE e al Comitato di risoluzione unico (SRB) per quanto riguarda le entità di cui all'articolo 7, paragrafo 2, del regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio ([37]) nonché le entità e i gruppi di cui all'articolo 7, paragrafo 4, lettera b), e all'articolo 7, paragrafo 5, del regolamento (UE) n. 806/2014, qualora tali dettagli riguardino incidenti che comportano un rischio per le funzioni essenziali definite all'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE; e*

e) *ad altre pertinenti autorità pubbliche ai sensi del diritto nazionale*.

7. Una ***volta ricevute le informazioni*** conformemente al paragrafo 6, l'ABE, l'ESMA o l'EIOPA e la BCE, in consultazione con l'ENISA e in collaborazione con l'autorità competente interessata, *valutano la pertinenza dell'grave incidente TIC rispetto alle autorità competenti in altri Stati membri*. A seguito di tale valutazione, l'ABE, l'ESMA o l'EIOPA inviano una notifica al riguardo il prima possibile alle autorità competenti interessate in altri Stati membri. La BCE notifica i membri del Sistema europeo di banche centrali in merito a questioni afferenti il sistema di pagamenti. Sulla base di tale notifica, le autorità competenti adottano, se del caso, tutte le misure necessarie per proteggere l'immediata stabilità del sistema finanziario.

([37]) Regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio, del 15 luglio 2014, che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010 (GU L 225 del 30.7.2014, pag. 1).

8. La notifica che l'ESMA deve effettuare a norma del paragrafo 7 del presente articolo lascia impregiudicata la responsabilità dell'autorità competente di trasmettere urgentemente i dettagli dell'grave incidente TIC all'autorità pertinente dello Stato membro ospitante, laddove uno dei depositari centrali di titoli svolga una cospicua attività transfrontaliera nello Stato membro ospitante, laddove l'incidente grave connesso alle TIC possa comportare serie conseguenze per i mercati finanziari dello Stato

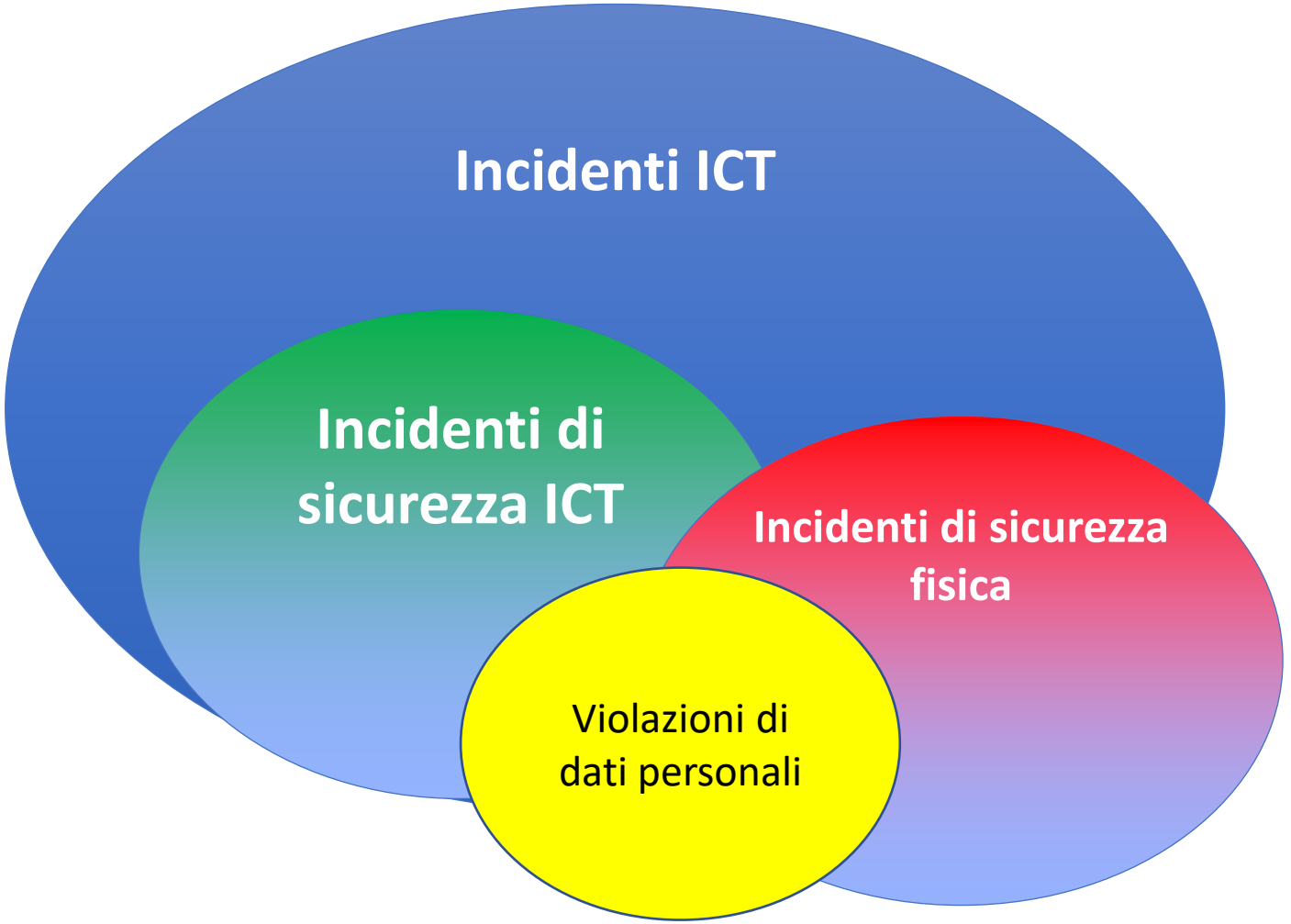
membro ospitante e laddove vi siano accordi di cooperazione tra le autorità competenti in relazione alla vigilanza delle entità finanziarie.

ARTICOLO *23*

Incidenti operativi o relativi alla sicurezza dei pagamenti riguardanti enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica

I requisiti contenuti nel presente capo si applicano anche agli incidenti operativi o relativi alla sicurezza dei pagamenti ovvero ai gravi incidenti operativi o relativi alla sicurezza dei pagamenti allorché riguardano enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica.

Perimetro


Incidenti ICT
Incidenti di sicurezza ICT
Incidenti di sicurezza fisica
Violazioni di dati personali

Definizioni

Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza

Incidente operativo o di sicurezza

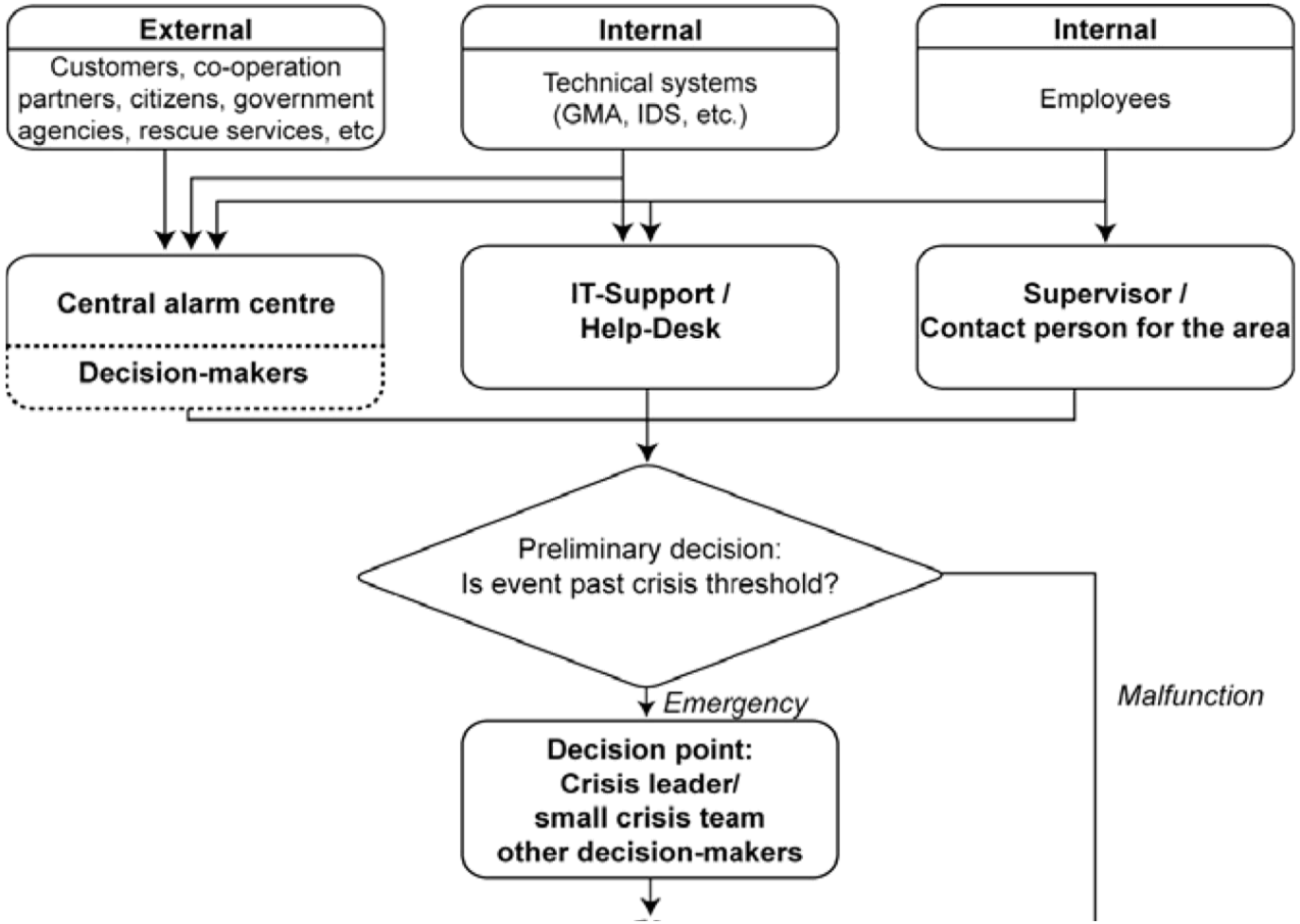
- *Singolo evento o serie di eventi collegati, non pianificati dall'istituto finanziario, che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi.*

Definizioni

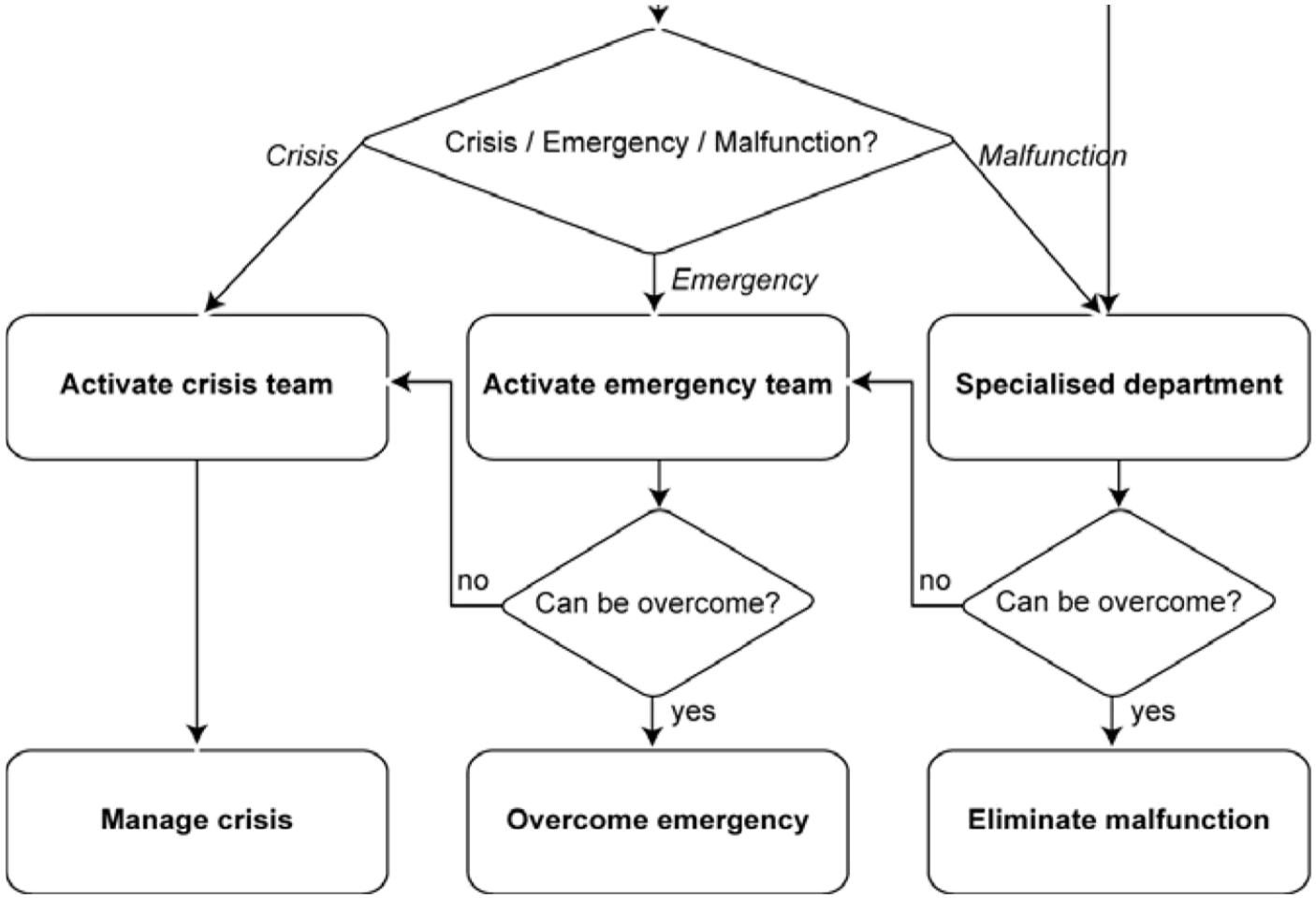
Regolamento del parlamento europeo e del consiglio
relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

*"**incidente connesso alle TIC** (tecnologie dell'informazione e della comunicazione): un evento imprevisto identificato, verificatosi nella rete e nei sistemi informativi e derivante o meno da attività dolose, che compromette la sicurezza della rete e dei sistemi informativi, delle informazioni da essi trattate, conservate o trasmesse, o che ha effetti avversi sulla disponibilità, la riservatezza, la continuità o l'autenticità dei servizi finanziari forniti dall'entità finanziaria".*

La gestione degli incidenti: BSI



La gestione degli incidenti: BSI



Formazione e formalizzazione

Tutti gli utenti devono essere formati in merito agli incidenti di qualunque natura e sulle modalità con cui effettuare una segnalazione

Devono essere definiti i canali di segnalazione, anche per qualunque soggetto esterno

Deve esistere un raccordo con la procedura di gestione dei reclami e di problem solving

Apprendimento

Le analisi delle motivazioni che hanno provocato l'incidente vanno analizzate al fine di individuare:

- contromisure
- soluzioni da inserire nel database dei casi noti

Elementi di valutazione: esempio PSD2

Criteri	Livello di impatto minore	Livello di impatto maggiore
1) Transazioni interessate (solo per servizi di pagamento)	> 10 % del livello normale delle transazioni di servizi di pagamento dell'intermediario (in termini di numero di transazioni) e > 100 000 EUR	> 25 % del livello normale delle transazioni di servizi di pagamento dell'intermediario (in termini di numero di transazioni) o > 5 milioni di EUR
2) Utenti interessati	> 5 000 e > 10 % degli utenti del servizio interessato dall'incidente	> 50 000 o > 25 % degli utenti del servizio interessato dall'incidente
3) Periodo di indisponibilità di componenti critiche del sistema informativo	> 2 ore	Non applicabile
4) Impatto economico	Non applicabile	> Max (0,1 % capitale di tipo "Tier 1"[6], 200 000 EUR) o > 5 milioni di EUR
5) Alto livello di escalation interna	Sì	Sì e probabilmente si ricorrerà alla modalità di crisi aziendale (o equivalente)
6) Altri intermediari, operatori o infrastrutture connesse potenzialmente coinvolti	Sì	Non applicabile
7) Impatto sulla reputazione	Sì	Non applicabile

Notifica degli incidenti

GDPR
Articolo 33 **Notifica di una violazione dei dati personali all'autorità di controllo** 1.In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

NIS
Art. 12 Obblighi in materia di sicurezza e notifica degli incidenti

5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.

Valutazione di una violazione di dati personali

Valutazione di impatto:

- Linee guida EDPB
- Metodologia ENISA

Test

ARTICOLO 24

Requisiti generali per lo svolgimento dei test di resilienza operativa digitale

1. Allo scopo di **valutare la preparazione alla gestione degli incidenti** connessi alle TIC, di **identificare punti deboli, carenze e lacune della resilienza operativa digitale e** di **attuare tempestivamente misure correttive**, le entità finanziarie diverse dalle microimprese, tenuto conto dei criteri di cui all'articolo 4, paragrafo 2, stabiliscono, mantengono e riesaminano un **programma di test** di resilienza operativa digitale solido ed esaustivo quale parte integrante del **quadro** per la gestione dei rischi informatici di cui all'articolo 6.

2. Il programma di test di resilienza operativa digitale comprende una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare conformemente agli articoli 25 e 26.

3. Nello svolgimento del programma di test di resilienza operativa digitale di cui al paragrafo 1 del presente articolo, le entità finanziarie, diverse dalle microimprese, adottano un approccio basato sul rischio che prende in considerazione i criteri di cui all'articolo 4, paragrafo 2, **tenendo debitamente conto del mutevole contesto dei rischi informatici, di eventuali rischi specifici cui l'entità finanziaria interessata è o potrebbe essere esposta, della criticità dei patrimoni informativi e dei servizi forniti, nonché di qualsiasi altro fattore giudicato rilevante dall'entità finanziaria stessa.**

4. Le entità finanziarie, diverse dalle microimprese, assicurano che i **test siano svolti da soggetti indipendenti, interni o esterni**. Se i test sono svolti da un soggetto incaricato dello svolgimento dei **test interno, le entità finanziarie dedicano risorse sufficienti e garantiscono che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test.**

5. Le entità finanziarie, diverse dalle microimprese, definiscono procedure e politiche per dare un **ordine di priorità ai problemi riscontrati durante lo svolgimento dei test, per classificarli e porvi rimedio**; stabiliscono inoltre **metodologie di convalida interne per accertare che tutti i punti deboli, le carenze o le lacune che sono stati individuati siano pienamente affrontati.**

6. Le entità finanziarie, diverse dalle microimprese, provvedono affinché, **con cadenza almeno annuale, siano eseguiti test adeguati su tutti i sistemi e le applicazioni di TIC a supporto di funzioni essenziali o importanti.**

ARTICOLO *25*

Test di strumenti e sistemi di TIC

1. Il programma di test di resilienza operativa digitale di cui all'articolo 24 prevede, conformemente ai criteri di cui all'articolo 4, paragrafo 2, **l'esecuzione di test adeguati**, tra cui **valutazione e scansione delle vulnerabilità**, **analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test end-to-end e test di penetrazione.**

2. **I depositari centrali di titoli e le controparti centrali effettuano valutazioni della vulnerabilità prima di ciascun rilascio o nuovo rilascio di nuovi o già esistenti applicazioni e componenti infrastrutturali, e servizi TIC a supporto delle funzioni essenziali o importanti dell'entità finanziaria.**

3. Le microimprese eseguono i test di cui al paragrafo 1 combinando un approccio basato sul rischio con una pianificazione strategica dei test relativi alle TIC, tenendo debitamente conto della necessità di mantenere un approccio equilibrato tra l'entità delle risorse e il tempo da assegnare ai test relativi alle TIC di cui al presente articolo, da un lato, e l'urgenza, il tipo di rischio, la criticità dei patrimoni informativi e dei servizi forniti nonché qualsiasi altro fattore rilevante, compresa la capacità dell'entità finanziaria di assumere rischi calcolati, dall'altro.

ARTICOLO *26*

Test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (TLPT)

1. Le entità finanziarie, diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese, che sono identificate conformemente al paragrafo 8, terzo comma, del presente articolo, effettuano **test avanzati sotto forma di test di penetrazione basati su minacce con cadenza almeno triennale**. Sulla base del profilo di rischio dell'entità finanziaria e tenuto conto delle circostanze operative, **l'autorità competente può, se necessario, chiedere all'entità finanziaria di ridurre o aumentare tale frequenza.**

2. Ciascun test di penetrazione guidato dalla minaccia riguarda **alcune o tutte le funzioni essenziali o importanti** dell'entità finanziaria ed **è effettuato sui sistemi attivi di produzione a supporto di tali funzioni.**

Le entità finanziarie identificano tutti i sistemi, i processi e le tecnologie TIC sottostanti a supporto delle funzioni essenziali o importanti e tutti i pertinenti servizi TIC, **compresi quelli a supporto di funzioni essenziali o importanti che sono stati esternalizzate o appaltate** a fornitori terzi di servizi TIC.

Le entità finanziarie **valutano quali funzioni essenziali o importanti debbano essere interessate dai TLPT**. Il risultato della valutazione determina il preciso ambito di applicazione dei TLPT ed è **convalidato dalle autorità competenti**.

3. Qualora i fornitori terzi di servizi TIC rientrino nell'ambito di applicazione dei TLPT, l'entità finanziaria adotta le misure e le salvaguardie necessarie per garantire la partecipazione di tali **fornitori terzi di servizi TIC ai TLPT** ed è sempre pienamente responsabile di garantire il rispetto del presente regolamento.

4. Fatto salvo il paragrafo 2, primo e secondo comma, laddove si ritiene ragionevolmente che la **partecipazione di un fornitore terzo di servizi** TIC ai TLPT di cui al paragrafo 3 **possa avere un impatto avverso sulla qualità o la sicurezza dei servizi offerti** dal fornitore terzo di servizi TIC **a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento**, **ovvero sulla riservatezza dei dati relativi a tali servizi**, l'entità finanziaria e il fornitore terzo di servizi TIC **possono concordare per iscritto che il fornitore terzo di servizi TIC stipuli direttamente accordi contrattuali con un soggetto incaricato dello svolgimento dei test esterno**, allo scopo di condurre, sotto la direzione di un'entità finanziaria designata, un **TLPT congiunto che coinvolga diverse entità finanziarie (*pooled testing*) a cui il fornitore terzo di servizi TIC fornisce tali servizi.**

Detto test congiunto **riguarda la pertinente gamma di servizi TIC a** supporto delle funzioni essenziali o importanti appaltate dalle entità finanziarie al rispettivo fornitore terzo di servizi TIC. I **test congiunti sono considerati TLPT effettuati dalle entità finanziarie che partecipano ai test congiunti**.

Il numero di entità finanziarie che partecipano ai test congiunti è debitamente calibrato tenendo conto della complessità e dei tipi di servizi interessati.

5. **Le entità finanziarie, cooperando con i fornitori terzi di servizi TIC e altre parti coinvolte, inclusi i soggetti incaricati dello svolgimento dei test ma escluse le autorità competenti, applicano efficaci controlli** di gestione del rischio **per attenuare i rischi di potenziali impatti sui dati, danni alle attività e perturbazioni delle funzioni essenziali o importanti, delle operazioni o dei servizi delle entità finanziarie, delle loro controparti o del settore finanziario.**

6. **Alla fine dei test, dopo che le relazioni e i piani correttivi siano stati concordati**, **l'entità finanziaria e, ove applicabile, i soggetti incaricato dello svolgimento dei test esterni trasmettono all'autorità**, designata conformemente al paragrafo 9 o 10, **una sintesi delle pertinenti risultanze, i piani correttivi e la documentazione attestante che i TLPT sono stati svolti conformemente ai requisiti.**

7. *Le autorità forniscono alle entità finanziarie un attestato che conferma che i test sono stati svolti conformemente ai requisiti, come si evince dalla documentazione, in modo da consentire il riconoscimento reciproco dei TLPT tra le autorità competenti. L'entità finanziaria notifica all'autorità competente interessata l'attestato, la sintesi delle pertinenti risultanze e i piani correttivi.*

Fatto salvo tale attestato, le entità finanziarie rimangono sempre pienamente responsabili degli impatti dei test di cui al paragrafo 4.

8. Per l'effettuazione dei TLPT, le entità finanziarie si avvalgono di **soggetti incaricati dello svolgimento dei test in conformità dell'articolo 27**. Quando ricorrono a soggetti incaricati dello **svolgimento dei test interni per l'effettuazione di TLPT, le entità finanziarie si avvalgono di un soggetto incaricato dello svolgimento dei test esterno ogni tre test**.

Gli enti creditizi classificati come significativi a norma dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013, ricorrono esclusivamente a soggetto incaricato dello svolgimento dei test esterni conformemente all'articolo 27, paragrafo 1, lettere da a) a e).

*Le autorità competenti **identificano le entità finanziarie** che hanno l'obbligo di svolgere TLPT tenendo conto dei criteri di cui all'articolo 4, paragrafo 2, sulla base della valutazione degli elementi seguenti:*

a) *i **fattori correlati all'impatto**, in particolare la **portata dell'impatto sul settore finanziario dei servizi forniti** e delle attività svolte dall'entità finanziaria;*

b) *i **possibili problemi di stabilità finanziaria**, tra cui il **carattere sistemico dell'entità finanziaria** a livello di Unione o nazionale, a seconda dei casi;*

c) *lo specifico **profilo dei rischi informatici**, il **livello di maturità delle TIC** dell'entità finanziaria o **le caratteristiche tecnologiche in questione**.*

9. *Gli Stati membri possono designare un'autorità pubblica unica nel settore finanziario responsabile delle questioni relative ai TLPT nel settore finanziario a livello nazionale e le affidano tutte le competenze e tutti i compiti a tal fine.*

10. *In assenza di una designazione a norma del paragrafo 9 del presente articolo e fatto salvo il potere di identificare le entità finanziarie tenute a svolgere TLPT, un'autorità competente può delegare l'esercizio di alcuni o di tutti i compiti di cui al presente articolo e all'articolo 27 a un'altra autorità nazionale nel settore finanziario*.

11. *Di concerto con la BCE, le AEV elaborano progetti di norme tecniche di regolamentazione comuni conformemente al quadro di riferimento TIBER-EU al fine di specificare ulteriormente quanto segue:*

a) *i criteri utilizzati ai fini dell'applicazione del paragrafo 8, secondo comma;*

b) *i requisiti e le norme che disciplinano il ricorso a soggetto incaricato dello svolgimento dei test interni;*

c) *i requisiti concernenti:*

i) l'ambito dei TLPT di cui al paragrafo 2;

ii) l'approccio e la metodologia da seguire per i test in ciascuna fase del relativo processo; iii) i

risultati, la chiusura e le fasi correttive dei test;

d) il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco di tali test, nel contesto di entità finanziarie che operano in più di uno Stato membro, al fine di consentire un livello adeguato di partecipazione alla vigilanza, nonché un'attuazione flessibile per tener conto delle specificità dei sottosettori finanziari o dei mercati finanziari locali.

All' atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono debitamente conto di eventuali caratteristiche specifiche derivanti dalla natura distinta delle attività nei diversi settori dei servizi finanziari.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

ARTICOLO *27*

Requisiti per i soggetti incaricati dello svolgimento dei test per lo svolgimento dei TLPT

1.Per lo svolgimento dei test di penetrazione basati su minacce, le entità finanziarie **ricorrono unicamente a soggetto incaricato dello svolgimento dei test che:**

a) **possano vantare il più alto grado di idoneità e reputazione**;

b) possiedano **capacità tecniche e organizzative e dimostrino esperienza specifica nel campo delle analisi delle minacce, dei test di penetrazione e dei test red team;**

c) **siano certificati** da un ente di accreditamento in uno Stato membro **o rispettino codici formali di condotta o quadri etici**;

d) **forniscano una garanzia indipendente** o **una relazione di audit concernente la solida gestione dei rischi derivanti dallo svolgimento di TLPT, comprese la dovuta protezione delle informazioni riservate dell'entità finanziaria e il risarcimento dei rischi commerciali dell'entità finanziaria;**

e) siano **debitamente e pienamente coperti da un'assicurazione di responsabilità professionale, anche contro i rischi di colpa e negligenza.**

2.Quando ricorrono a soggetto incaricato dello svolgimento dei **test interni**, le entità finanziare devono provvedere affinché, oltre all'obbligo di cui al paragrafo 1, siano soddisfatte le condizioni seguenti:

a) **tale ricorso è stato approvato dall'autorità competente** interessata o dall'autorità pubblica unica designata conformemente all'articolo 26, paragrafi 9 e 10;

b) **l'autorità competente** interessata ha verificato che l'entità finanziaria **dispone di risorse dedicate sufficienti** e che essa ha garantito che siano **evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test**; e

c) il soggetto che fornisce **analisi delle minacce è esterno all'entità finanziaria**.

3. Le entità finanziarie **garantiscono che i contratti conclusi con i soggetti incaricati dello svolgimento dei test esterni prevedano una solida gestione dei risultati dei TLPT** e **che qualsiasi trattamento dei dati**, comprese la generazione, la conservazione, l'aggregazione, l'elaborazione, la segnalazione, la comunicazione o la distruzione, **non comporti rischi per l'entità finanziaria**.

G-7

Fundamental elements for threat-led penetration testing

Executive Summary

In light of the increasing sophistication and persistence of cyber risks, which can threaten to disrupt our interconnected global financial systems, the G-7 continues to promote the development of frameworks to enhance public and private sector approaches to strengthening cyber resilience of critical entities in the financial system following its publication in 2016 of the *G-7 Fundamental Elements of Cybersecurity for the Financial Sector* (*"G7FE"*).

These efforts include steps to ensure strong cyber resilience measures are assessed and evaluated, as highlighted by the *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector* (*"G7FE-Assessment"*), published in 2017. The G7FE-Assessment included components to consider and embed when developing cyber resilience assessment frameworks.

The *G-7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT)* provide entities with a guide for the assessment of their resilience against malicious cyber incidents through simulation and a guide for authorities considering the use of Threat-Led Penetration Testing (TLPT) within their jurisdictions. These fundamental elements are intended to complement a wider suite of cyber resilience assessment tools and techniques, and are not meant to be considered as a singular approach.

G-7

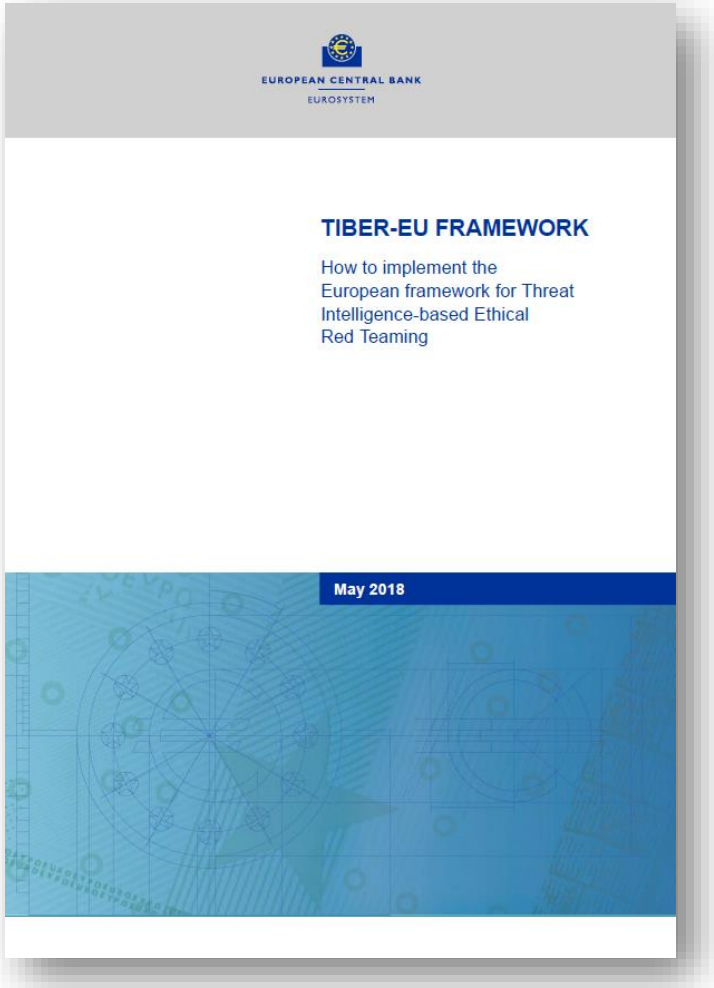
Fundamental elements for threat-led penetration testing

The core objectives of the *G7FE-TLPT* are to enhance and assess the cyber resilience of entities and the financial sector more generally, by:

- Providing core elements of and approaches for the conduct of TLPT across G-7 jurisdictions. The G7FE-TLPT aim to facilitate greater compatibility among TLPT approaches, whilst also encouraging flexibility and local tailoring based on the unique markets and regulations within each jurisdiction;
- Providing a guide to authorities considering the use of TLPT within their jurisdiction;
- Providing a guide to entities with respect to conducting their own TLPT assessments; and
- Supporting cross-authority interaction and cross-jurisdictional TLPT for multinational entities, facilitating mutual acceptance of test results.

The *G7FE-TLPT* seek to drive greater compatibility among TLPT approaches and do not invalidate existing frameworks or prevent their continuous adaptations to the evolving threat landscape.

TIBER-EU FRAMEWORK



Il Consiglio direttivo della BCE ha approvato nella primavera del 2017 la strategia di supervisione per la resilienza cibernetica delle infrastrutture di mercato europee con il fine di assicurare un'applicazione comune e coerente con la ***Guidance on cyber resilience for financial market infrastructures*** *nell'ambito dell'Eurosistema. Fra le iniziative vi è anche la predisposizione di un quadro di riferimento per l'esecuzione di test avanzati sui sistemi informativi.*

TIBER-EU FRAMEWORK

Gli obiettivi di TIBER-EU comprendono fra gli altri:

- migliorare la cyber resilienza delle entità e del settore finanziario in generale;
- standardizzare e armonizzare il modo in cui le entità eseguono i test in tutta l'UE, garantendo al contempo a ciascuna giurisdizione un certo grado di flessibilità per adattare il quadro in base alle sue specificità;
- fornire indicazioni alle autorità su come stabilire, attuare e gestire questa forma di test a livello nazionale o europeo;
- valutare anche gli aspetti giurisdizionali per i test di entità multinazionali;
- favorire la cooperazione internazionale fra i vari soggetti coinvolti;
- …

TIBER-EU FRAMEWORK

Le pubblicazioni del framework

La descrizione della metodologia è raccolta in 3 diverse pubblicazioni:

- TIBER-EU FRAMEWORK - How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

Che descrive nel dettaglio le modalità per l'esecuzione dei test.

- TIBER-EU Framework - Services Procurement Guidelines

Che fornisce, ad esempio, i requisiti dei Threat Intelligence Provider, dei Red Team Provider e gli strumenti per la loro valutazioni, quali ad esempio questionari e check list.

Viene anche fornita una tabella con un elenco delle possibili certificazioni che qualificano il personale addetto alle operazioni e le stesse strutture che si offrono quali TI o RT provider.

- TIBER-EU White Team Guidance - The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test

Che indica i ruoli e le responsabilità del White Team.

BANK OF ENGLAND

CBEST

CBEST Intelligence-Led Testing - CBEST Services Assessment Guide

3.2. Assessment criteria

3.2.1 Reputation, history and ethics

3.2.2 Service quality and value-for-money

3.2.3 Research and development capability

3.2.4 Staff competence

3.2.5 Security and risk management

3.2.6 Professional accreditation and complaint process

3.2.7 Collaborative working

Condivisione informazioni

ARTICOLO 45

Meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche

1.Le entità finanziarie possono scambiarsi reciprocamente informazioni e analisi delle minacce informatiche, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cibersicurezza e strumenti di configurazione, nella misura in cui tale condivisione di informazioni e dati:

a) **mira a potenziare la resilienza operativa digitale delle entità finanziarie, in particolare aumentando la consapevolezza in merito alle minacce informatiche, contenendo o inibendo la capacità di diffusione delle minacce informatiche, sostenendo le capacità di difesa, le tecniche di individuazione delle minacce, le politiche di mitigazione o le fasi di risposta e ripristino;**

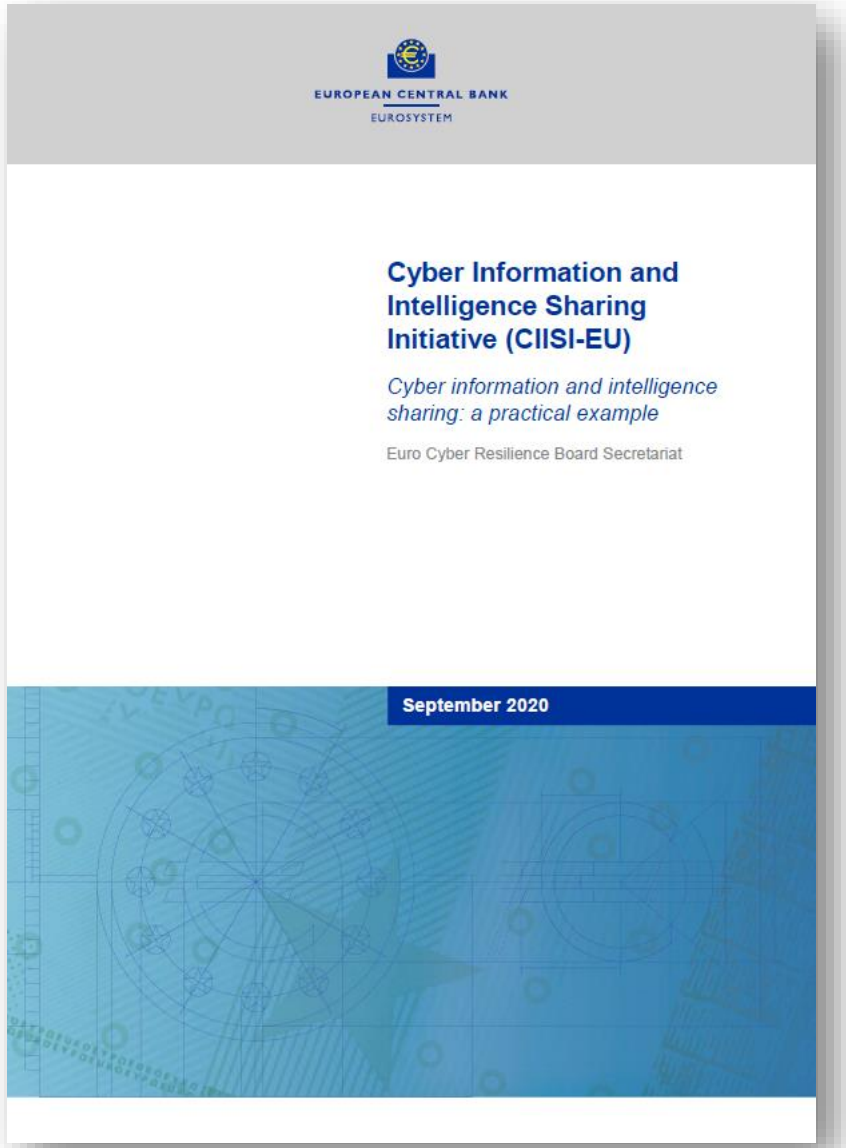
b) **si svolge entro comunità fidate di entità finanziarie;**

c) si realizza mediante meccanismi di condivisione delle informazioni che tutelano la natura potenzialmente sensibile delle informazioni condivise e sono disciplinati da norme di condotta pienamente rispettose della riservatezza dell'attività economica, della protezione dei dati personali ai sensi del regolamento (UE) 2016/679 e delle linee guida sulla politica in materia di concorrenza.

2. Ai fini del paragrafo 1, lettera c), i meccanismi di condivisione delle informazioni definiscono le condizioni per la partecipazione e, se del caso, definiscono i dettagli concernenti il coinvolgimento delle autorità pubbliche e la veste in cui queste

possono partecipare ai meccanismi di condivisione delle informazioni, il coinvolgimento dei fornitori terzi di servizi TIC, nonché gli elementi operativi tra cui l'utilizzo di piattaforme informatiche apposite.

3. Le entità finanziarie notificano alle autorità competenti la propria partecipazione ai meccanismi di condivisione delle informazioni di cui al paragrafo 1, al momento della convalida della propria adesione o, se del caso, della cessazione dell'adesione, quando quest'ultima abbia effetto.



Core Objectives of CIISI-EU

The core objectives of CIISI-EU are to:

- Prevent, detect, respond and raise awareness of cybersecurity threats to the CIISI-EU Community members, thereby discharging a public interest responsibility;
- Enable relevant and actionable intelligence sharing within the CIISI-EU Community, with Law Enforcement and potentially to the wider ecosystem to better protect the European financial sector against cybersecurity threats;
- Encourage active contribution and active participation within a 'trusted circle', rather than passive consumption or weak usage;
- Synthesize and actively propagate the sharing of strategic intelligence in addition to operational TTPs and tactical IOCs; and
- Continuously learn and evolve, as a collective, with regard to the process of analysing, developing and sharing cyber information and intelligence.

Terzi

CAPO V

Gestione dei rischi informatici derivanti da terzi

Sezione I

Principi fondamentali di una solida gestione dei rischi informatici derivanti da terzi

ARTICOLO *28*

Principi generali

1.Le entità finanziarie gestiscono i **rischi informatici derivanti da terzi** quali componenti integranti dei rischi informatici nel contesto del proprio **quadro** per la gestione di detti rischi di cui all'articolo 6, paragrafo 1, e conformemente ai principi indicati di seguito:

a) le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi TIC per lo svolgimento delle proprie operazioni commerciali rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla normativa applicabile in materia di servizi finanziari;
b) la gestione dei rischi informatici derivanti da terzi da parte delle entità finanziarie si svolge nel rispetto del **principio di proporzionalità**, tenendo conto:

   i) della **natura, della portata, della complessità e dell'importanza delle dipendenze** connesse alle TIC;

   ii) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, tenendo conto della **criticità o dell'importanza dei rispettivi servizi**, **processi o funzioni** e del **potenziale impatto sulla continuità** e la **disponibilità** delle attività e dei servizi finanziari a livello individuale e di gruppo.

2. Nel contesto del quadro per la gestione dei rischi informatici TIC, le entità finanziarie diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese **adottano e riesaminano periodicamente una strategia per i rischi informatici derivanti da terzi**, tenendo conto della **strategia basata su una varietà di fornitori** di cui all'articolo 6, paragrafo 9, ove applicabile. Tale strategia comprende una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti

prestati da fornitori terzi e **si applica su base individuale** e, se del caso, su base **subconsolidata e consolidata**. Sulla base di una valutazione del profilo di rischio complessivo dell'entità finanziaria e della portata e della complessità dei servizi operativi, **l'organo di gestione riesamina periodicamente i rischi individuati in relazione agli accordi contrattuali** per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti.

3. Nel contesto del **quadro** per la gestione dei rischi informatici, le entità finanziarie mantengono e aggiornano a livello di entità, e su base subconsolidata e consolidata, un **registro di informazioni su tutti gli accordi contrattuali** per l'utilizzo di servizi TIC prestati da fornitori terzi.

Gli accordi contrattuali di cui al primo comma sono opportunamente documentati, distinguendo quelli che si riferiscono a servizi TIC a supporto di funzioni essenziali o importanti dagli altri.

Le entità finanziarie **comunicano almeno una volta all'anno alle autorità competenti** il numero di **nuovi accordi** per l'utilizzo di servizi TIC, le categorie di fornitori terzi di servizi TIC, il tipo di accordi contrattuali e le funzioni e i servizi TIC forniti.

Su richiesta, le entità finanziarie **mettono a disposizione dell'autorità competente** il **registro delle informazioni** completo o, a seconda della richiesta, determinate sezioni del registro insieme alle informazioni giudicate necessarie per consentire l'efficace vigilanza sull'entità finanziaria.

Le entità finanziarie **informano tempestivamente l'autorità competente in merito a eventuali accordi** contrattuali previsti per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti, **nonché del momento in cui una funzione diventa essenziale o importante.**

4. **Prima di stipulare un accordo contrattuale** per l'utilizzo di servizi TIC, le entità finanziarie:

a) **valutano se l'accordo** contrattuale **riguardi** l'utilizzo di servizi TIC a supporto di **una funzione essenziale o importante**;

b) **verificano se siano soddisfatte le condizioni di vigilanza per la conclusione del contratto**;

c) **identificano e valutano tutti i rischi** pertinenti relativi all'accordo contrattuale, compresa la possibilità che tale accordo contrattuale possa aggravare il **rischio di concentrazione** delle TIC di cui all'articolo 29;

d) effettuano **controlli di dovuta diligenza** (*due diligence*) **sui potenziali fornitori** terzi di servizi TIC e ne garantiscono l'idoneità lungo tutto il processo di selezione e valutazione;

e) individuano e valutano i **conflitti d'interessi** che possano derivare dall'accordo contrattuale.

5. Le entità finanziarie **possono stipulare accordi** contrattuali **soltanto con fornitori terzi** di servizi TIC che **soddisfano standard appropriati in materia di sicurezza delle informazion**i. Laddove tali accordi contrattuali riguardino funzioni essenziali o importanti, le entità finanziarie, prima di concludere detti accordi, prendono in debita considerazione l'utilizzo da parte dei fornitori terzi di servizi TIC degli **standard di qualità più aggiornati ed elevati in materia di sicurezza delle informazioni.**

6. Nell'esercizio dei **diritti di accesso, ispezione e audit** nei confronti del fornitore terzo di servizi TIC, le entità finanziarie **predeterminano**, sulla base di un approccio basato sul rischio, la **frequenza delle verifiche di audit e delle ispezioni nonché i settori da sottoporre ad audit, aderendo a standard di audit comunemente accettate in conformità di eventuali indicazioni di vigilanza** sull'uso e l'integrazione di tali standard di audit.

Laddove gli accordi contrattuali conclusi con fornitori terzi di servizi TIC per l'utilizzo di servizi TIC comportino un'elevata complessità tecnica, l'entità finanziaria **verifica che i revisori**, indipendentemente dal fatto che siano revisori interni o esterni o

siano un gruppo di revisori, **possiedano competenze e conoscenze adeguate** per svolgere efficacemente gli audit e le valutazioni del caso.

7. Le entità finanziarie stabiliscono clausole che consentano la **risoluzione degli accordi contrattuali** per l'utilizzo di servizi TIC in una qualsiasi delle circostanze seguenti:

a) **rilevante violazione**, da parte del fornitore terzo di servizi TIC, **di leggi, regolamenti o condizioni contrattuali** applicabili;

b) **circostanze, identificate nel corso** del **monitoraggio dei rischi informatici** derivanti da terzi, **ritenute suscettibili di alterare l'esercizio** delle funzioni previsto a norma dell'accordo contrattuale, **tra cui modifiche di rilievo** che incidano sull'accordo o sulla situazione del fornitore terzo di servizi TIC;

c) **punti deboli del fornitore** terzo di servizi TIC **emersi riguardo alla sua gestione complessiva dei rischi informatici** e, in particolare, nel modo in cui il fornitore garantisce la **disponibilità, autenticità, integrità e riservatezza** dei dati, siano essi dati personali o altrimenti sensibili, oppure dei dati non personali;

d) laddove **l'autorità competente non sia più in grado di vigilare efficacemente** sull'entità finanziaria **per via delle condizioni dell'accordo contrattuale in questione o delle circostanze ivi afferenti.**

8. Per i servizi TIC a supporto di funzioni essenziali o importanti, le entità finanziarie predispongono **strategie di uscita**. Tali strategie tengono conto dei rischi che possono emergere a livello dei fornitori terzi di servizi TIC, in particolare **possibili disfunzioni dei fornitori** stessi, il **deterioramento della qualità dei servizi** TIC forniti, una **perturbazione dell'attività commerciale conseguente a una fornitura di servizi TIC inadeguata o carente**, oppure gravi rischi connessi **all'adeguatezza e alla continuità** dell'esercizio del rispettivo servizio TIC oppure la risoluzione di accordi contrattuali con fornitori terzi di servizi TIC in una delle circostanze di cui al paragrafo 7.

Le entità finanziarie garantiscono di **poter porre termine agli accordi contrattuali senza:**

a) **perturbare l**e proprie attività commerciali;

b) **limitare il rispetto dei requisiti normativi;**

c) **pregiudicare la continuità e la qualità dei servizi** forniti ai clienti.

I piani di uscita sono esaustivi, **documentati** e, conformemente ai criteri di cui all'articolo 4, paragrafo 2, sottoposti a **test adeguati** e **riesaminati periodicamente.**

Le entità finanziarie identificano **soluzioni alternative ed elaborano piani di transizione** che consentano loro di **trasferire** i servizi TIC previsti dal contratto e i relativi dati dal fornitore terzo di servizi TIC, in maniera sicura e nella loro interezza, **a fornitori alternativi oppure reintegrarli** al proprio interno.

Le entità finanziarie **dispongono di misure di emergenza idonee per mantenere la continuità operativa qualora si verifichino le circostanze di cui al primo comma.**

9. *Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di attuazione per definire modelli standard in relazione al registro delle informazioni di cui al paragrafo 3, comprese le informazioni comuni a tutti gli accordi contrattuali per l'utilizzo di servizi TIC. Le AEV presentano tali progetti di norme tecniche di attuazione alla Commissione entro il 17 gennaio 2024.*

Alla Commissione è conferito il potere di adottare le norme tecniche di attuazione di cui al primo comma in conformità dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

10. *Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per precisare ulteriormente il contenuto dettagliato della politica di cui al paragrafo 2, in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC.*

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni. Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione 17 gennaio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

ARTICOLO *29*

Valutazione preliminare del rischio di concentrazione delle TIC a livello di entità

1.All'atto dell'identificazione e della valutazione dei rischi di cui all'articolo 28, paragrafo 4, lettera c), le entità finanziarie tengono conto altresì dell'eventualità che la prevista conclusione di un accordo contrattuale relativo a servizi TIC a supporto di funzioni essenziali o importanti possa avere una delle seguenti conseguenze:

a) la conclusione di un contratto con un **fornitore** terzo di servizi TIC **non facilmente sostituibile**; o

b) la presenza di **molteplici accordi** contrattuali relativi alla prestazione di servizi TIC a supporto di funzioni essenziali o importanti **con lo stesso fornitore** terzo **oppure con fornitori terzi strettamente connessi**.

Le entità finanziarie **vagliano i benefici e i costi di soluzioni alternative**, **quali il ricorso a diversi fornitori** terzi di servizi TIC, **verificando se e come le soluzioni previste soddisfino le esigenze commerciali e consentano di conseguire gli obiettivi fissati nella propria strategia di resilienza digitale**.

2. Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prevedano la possibilità che un fornitore terzo di servizi TIC **subappalti** a sua volta servizi TIC a supporto di una funzione essenziale o importante ad altri

fornitori terzi di servizi TIC, le entità finanziarie vagliano i **benefici e i rischi che possono derivare da tale subappalto**, in particolare nel caso di un **subappaltatore di TIC stabilito in un paese terzo**.

Qualora gli accordi contrattuali riguardino servizi TIC a supporto delle funzioni essenziali o importanti, le entità finanziarie tengono in debita considerazione le disposizioni del **diritto fallimentare** applicabili in caso di fallimento del fornitore terzo di servizi TIC come pure **eventuali restrizioni relative all'urgente ripristino dei dati dell'entità finanziaria.**

Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti siano conclusi con un fornitore terzo di servizi TIC stabilito in un **paese terzo**, le entità finanziarie, in aggiunta alle considerazioni di cui al secondo comma, tengono conto altresì del rispetto delle **norme dell'UE sulla protezione dei dati e dell'effettiva applicazione della legge in tale paese terzo.**

Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prevedano un s**ubappal**to, le entità finanziarie valutano se **e come catene di subappalti potenzialmente lunghe e complesse possano incidere sulla loro capacità di monitorare pienamente le funzioni appaltate e sulla capacità dell'autorità competente di vigilare efficacemente**, a tal proposito, sull'entità finanziaria.

ARTICOLO *30*

Principali disposizioni contrattuali

1. I **diritti e gli obblighi** dell'entità finanziaria e del fornitore terzo di servizi TIC sono attribuiti chiaramente e **definiti per iscritto**. Il testo integrale del contratto comprende gli **accordi sul livello dei servizi** ed è **contenuto in un documento scritto** disponibile alle parti in **formato cartaceo** oppure in un documento in altro formato scaricabile, durevole e accessibile.

2. Gli accordi contrattuali per l'utilizzo di servizi TIC comprendono almeno gli elementi seguenti:

a) la **descrizione chiara e completa di tutte le funzioni** che il fornitore terzo di servizi TIC deve svolgere e tutti i servizi TIC che deve prestare, comprese l'indicazione **dell'eventuale autorizzazione a subappaltare** un servizio TIC a sostegno di una funzione essenziale o importante o parti significative di essa e, in caso affermativo, le **condizioni di tale subappalto**;

b) le località, segnatamente le regioni o i paesi, in cui si devono svolgere le funzioni e prestare i servizi TIC appaltati o subappaltati e in cui si devono **trattare i dati, compreso il luogo di conservazione**, nonché l'**obbligo**, per il fornitore terzo di servizi TIC, di **segnalare in anticipo all'entità finanziaria l'intenzione di cambiare tale o tali località;**

c) le disposizioni in materia di **disponibilità, autenticità, integrità e riservatezza** in relazione alla protezione dei **dati**, compresi i dati personali;

d) le disposizioni relative alle **garanzie di accesso, ripristino e restituzione, in un formato facilmente accessibile, di dati** personali e non personali trattati dall'entità finanziaria **in caso di insolvenza, risoluzione o interruzione** delle operazioni commerciali del fornitore terzo di servizi TIC **o in caso di risoluzione degli accordi commerciali;**

e) le descrizioni dei **livelli di servizio**, compresi **relativi aggiornamenti e revisioni**;

f) l'obbligo per il fornitore terzo di servizi TIC di **prestare assistenza all'entità finanziaria senza costi aggiuntivi o a un costo stabilito ex ante**, qualora si verifichi un incidente connesso alle TIC relativo al servizio TIC fornito all'entità finanziaria;

g) **l'obbligo per il fornitore** terzo di servizi di TIC di **operare senza riserve con le autorità** competenti e con le autorità di risoluzione dell'entità finanziaria, comprese le persone da queste nominate;

h) i **diritti di risoluzione e il relativo termine minimo di preavviso** per la risoluzione degli accordi contrattuali, conformemente alle attese delle autorità competenti e delle autorità di risoluzione;

i) le **condizioni riguardanti la partecipazione dei fornitori** terzi di servizi TIC ai **programmi di sensibilizzazione** sulla sicurezza delle TIC e alle **attività di formazione sulla resilienza** operativa digitale delle entità finanziarie conformemente all'articolo 13, paragrafo 6.

3.Gli **accordi contrattuali** per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti comprendono, in aggiunta agli elementi di cui al paragrafo 2, almeno quanto segue:

a) la **descrizione completa dei livelli di servizio**, comprendente i **relativi aggiornamenti e revisioni** con precisi **obiettivi quantitativi e qualitativi**, **in termini di prestazioni**, nell'ambito dei livelli di servizio concordati, in modo da **consentire un monitoraggio efficace** da parte dell'entità finanziaria dei servizi TIC e l'applicazione, senza indebito ritardo, di opportune **azioni correttive qualora i livelli di servizio concordati non siano rispettati**;

b) termini di preavviso e **obblighi di segnalazione per il fornitore** terzo di servizi TIC nei confronti dell'entità finanziaria, tra cui la **notifica di eventuali sviluppi che potrebbero esercitare un impatto significativo sulla capacità del fornitore** terzo di servizi TIC di prestare servizi a supporto di funzioni essenziali o importanti efficacemente, **in linea con i livelli di servizio concordati**;

c) l'obbligo per il fornitore terzo di servizi TIC di **attuare e testare i piani operativi d'emergenza** e di **predisporre misure, strumenti e politiche per la sicurezza** delle TIC che offrano un adeguato livello di sicurezza per la fornitura dei servizi da parte dell'entità finanziaria, in linea con il proprio **quadro** normativo;

d) l'obbligo per il fornitore terzo di servizi TIC di **partecipare e cooperare pienamente al TLPT** dell'entità finanziaria di cui agli articoli 26 e 27;

e) il diritto di **monitorare** costantemente le prestazioni del fornitore terzo di servizi TIC, che comporta quanto segue:

i) **diritti incondizionati di accesso, ispezione e audit** da parte dell'entità finanziaria — o di un terzo designato a tal fine — e dell'autorità competente nonché il diritto di **ottenere copia della documentazione** pertinente in loco, se di importanza critica per le operazioni del fornitore terzo di servizi TIC, il cui effettivo esercizio non sia impedito o limitato da altri accordi contrattuali o politiche di attuazione;

ii) il diritto di concordare **livelli di garanzia alternativi**, **qualora siano interessati i diritti di altri clienti**;

iii) l'obbligo per il fornitore terzo di servizi TIC di **cooperare senza riserve nel corso delle ispezioni e degli** audit in loco svolti dalle autorità competenti, dall'autorità di sorveglianza capofila, dall'entità finanziaria o da un terzo designato; e

iv) l'obbligo di fornire **dettagli sull'ambito di applicazione, sulle procedure da seguire** e sulla **frequenza di tali ispezioni e audit**;

f) le **strategie di uscita,** in particolare la definizione di un **adeguato periodo di transizione obbligatorio**:

i) durante il quale il **fornitore terzo di servizi TIC continuerà a prestare i suoi servizi TIC o a esercitare le sue funzioni** allo scopo di **ridurre il rischio di perturbazioni** presso l'entità finanziaria o di garantire la sua efficace risoluzione e ristrutturazione;

ii) che **permetta all'entità finanziaria di migrare** verso un altro fornitore terzo di servizi TIC oppure di adottare soluzioni interne coerenti con la complessità del servizio prestato.

In deroga alla lettera e), il fornitore terzo di servizi TIC e l'entità finanziaria che è una microimpresa possono convenire che i diritti di accesso, ispezione e audit dell'entità finanziaria possano essere delegati a un terzo indipendente, nominato dal fornitore terzo di servizi TIC, e che l'entità finanziaria possa richiedere in qualsiasi momento al terzo informazioni e garanzie sulle prestazioni del fornitore terzo di servizi TIC.

4. All'atto della negoziazione degli accordi contrattuali, le entità finanziarie e i fornitori terzi di servizi TIC **prendono in considerazione il ricorso a clausole contrattuali standard elaborate dalle autorità pubbliche per servizi specifici.**

5. *Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare ulteriormente gli elementi di cui al paragrafo 2, lettera a), che l'entità finanziaria deve determinare e valutare quando subappalta servizi TIC a supporto di funzioni essenziali o importanti.*

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

Rischi legati ai fornitori (*)

Supplier risk includes but is not limited to:

- Political risk—Unstable regimes, closed borders, customs and tariffs may affect suppliers.
- Environmental risk—Natural disasters (floods, fires, etc.) and epidemics may affect the supplier area and disrupt logistics and the supplier workforce.
- Social risk—Industrial unrest, labor actions, strikes, sabotage and crime may affect supplier and partner locations.
- Technical / operational risk—Machine or equipment failure, quality defects, IT supplier failure and loss of knowledgeable workforce can jeopardize a given enterprise project.
- Legal and regulatory compliance risk—Suppliers may fail to comply with legal and regulatory requirements, or fall under court order to stop work at a given supplier location.
- Economic risk—Financial instability and lack of cash flow can cripple day-to-day supplier operations.

(*) ISACA - SUPPLY CHAIN RESILIENCE AND CONTINUITY

Rischi legati ai fornitori

- Concentration risk (single point of failure)—Enterprises should not rely on a single supplier for all service and product needs. In certain industries, concentration risk can accrue whenever a single niche supplier or vendor provides fundamental services or infrastructure to an entire industry (e.g., SAP, core banking software, processor chips for hardware manufacturers, industry-specific technologies and robotic automation).
- Financial risk—Suppliers encounter a business scenario that threatens their financial health. Inappropriate investment decisions by supplier management results in financial instability of the supplier.
- Geopolitical risk—The contracting enterprise supply chain is disrupted by global political events. Political decisions may affect the capability of the supplier to provide productand services.
- Reputational risk—Risk associated with loss of reputation reflects the possibility that a supplier will engage in activities that negatively affect the enterprise image. Risk associated withreputation materializes when an enterprise fails to fulfill the commitments to its stakeholders. In the current era of using suppliers for many product components and services, supply chain providers can exacerbate reputation risk. A security breach by a supplier's employees may impact the reputation of the enterprise.11 The enterprise can delegate responsibility forperforming tasks, but the accountability for outcomes remains with the enterprise and has an impact on reputation.

Rischi legati ai fornitori

Suppliers can be categorized into four major groups, based on the nature of the relationship and dependencies of the organization. Categories of suppliers include:

- Strategic—Suppliers whose relationship is based on mutual benefits for both organizations. The relationship is strongly coupled where dependency on suppliers may not be very high, like tactical or niche suppliers, but essential for mutual benefits. Some examples include large enterprises that support start-up incubation centers where the outcome is beneficial for the start-up as well as for the enterprise. Another example is when enterprises invest in the supplier organization to provide essential supplies to the organization. These suppliers may also be available in the market but the enterprise prefers the strategic supplier where it has invested.
- Tactical—Suppliers that help in managing operations. These suppliers cannot be replaced easily and, hence, need to be considered for continuity.
- Commodity—Suppliers of material and spare parts for manufacturing and maintaining infrastructure and other consumables. There can be multiple suppliers, which is better for continuity.

Rischi legati ai fornitori

- Niche—Providers of exclusive products and services without which it will be difficult to sustain enterprise operations. These suppliers are most difficult to replace and are critical for continuity. Examples include a provider of complex solutions like SAP, SIEM and IDAM, or suppliers of a niche component without which a product cannot be distributed.

EBA
Orientamenti in materia di esternalizzazioni

7 Politica di esternalizzazione

8 Conflitti di interesse

9 Piani di continuità operativa

10 Funzione di audit interno

11 Requisiti in materia di documentazione

12 Analisi preventiva dell'esternalizzazione

12.2 Valutazione dei rischi degli accordi di esternalizzazione

12.3 Due diligence

13 Fase contrattuale

13.1 Subesternalizzazione di funzioni essenziali o importanti

13.2 Sicurezza dei dati e dei sistemi

13.3 Diritti di accesso, di informazione e di audit

13.4 Diritti di cessazione

14 Controllo delle funzioni esternalizzate

15 Strategie di uscita (exit strategies)

Orientamenti EBA
12 Due diligence

- 69. 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.
- 70. 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.

Orientamenti EBA
12 Due diligence

- 71. Ulteriori fattori da prendere in considerazione nell'effettuare la due diligence su un potenziale fornitore di servizi comprendono, tra l'altro:
- a. il modello di business, la natura, le dimensioni, la complessità, la situazione finanziaria, la struttura proprietaria e di gruppo del fornitore di servizi;
- b. le relazioni a lungo termine con i fornitori di servizi già valutati e che prestano servizi per l'ente o l'istituto di pagamento;
- c. se il fornitore di servizi è un'impresa madre o una filiazione dell'ente o dell'istituto di pagamento, se rientra nel perimetro di consolidamento contabile dell'ente o se è membro dello stesso sistema di tutela istituzionale al quale appartiene l'ente oppure è controllato da enti che ne fanno parte;
- d. se il fornitore di servizi è vigilato dalle autorità competenti.

Orientamenti EBA
12 Due diligence

- 72. 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.
- 73. 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.

ESMA

Orientamenti in materia di esternalizzazione a fornitori di servizi cloud

- …
- Orientamento 1 Governance, sorveglianza e documentazione
- Orientamento 2 Analisi di pre-esternalizzazione e due diligence
- Orientamento 3 Principali elementi contrattuali
- Orientamento 4 Sicurezza delle informazioni
- Orientamento 5 Strategie di uscita
- Orientamento 6 Diritti di accesso e di audit
- Orientamento 7 Subesternalizzazione
- Orientamento 8 Notifica scritta alle autorità competenti
- Orientamento 9 Supervisione degli accordi di esternalizzazione nel cloud

EIOPA

Orientamenti in materia di esternalizzazione a fornitori di servizi cloud

- Orientamento 1 – Servizi cloud ed esternalizzazione nel cloud
- Orientamento 2 – Principi generali di governance per l'esternalizzazione nel cloud
- Orientamento 3 – Aggiornamento della politica scritta di esternalizzazione
- Orientamento 4 – Notifica scritta all'autorità di vigilanza
- Orientamento 5 – Requisiti documentali
- Orientamento 6 – Analisi pre-esternalizzazione
- Orientamento 7 – Valutazione delle funzioni e delle attività operative cruciali o importanti
- Orientamento 8 – Valutazione dei rischi dell'esternalizzazione nel cloud
- Orientamento 9 – Dovuta diligenza in merito al fornitore di servizi cloud

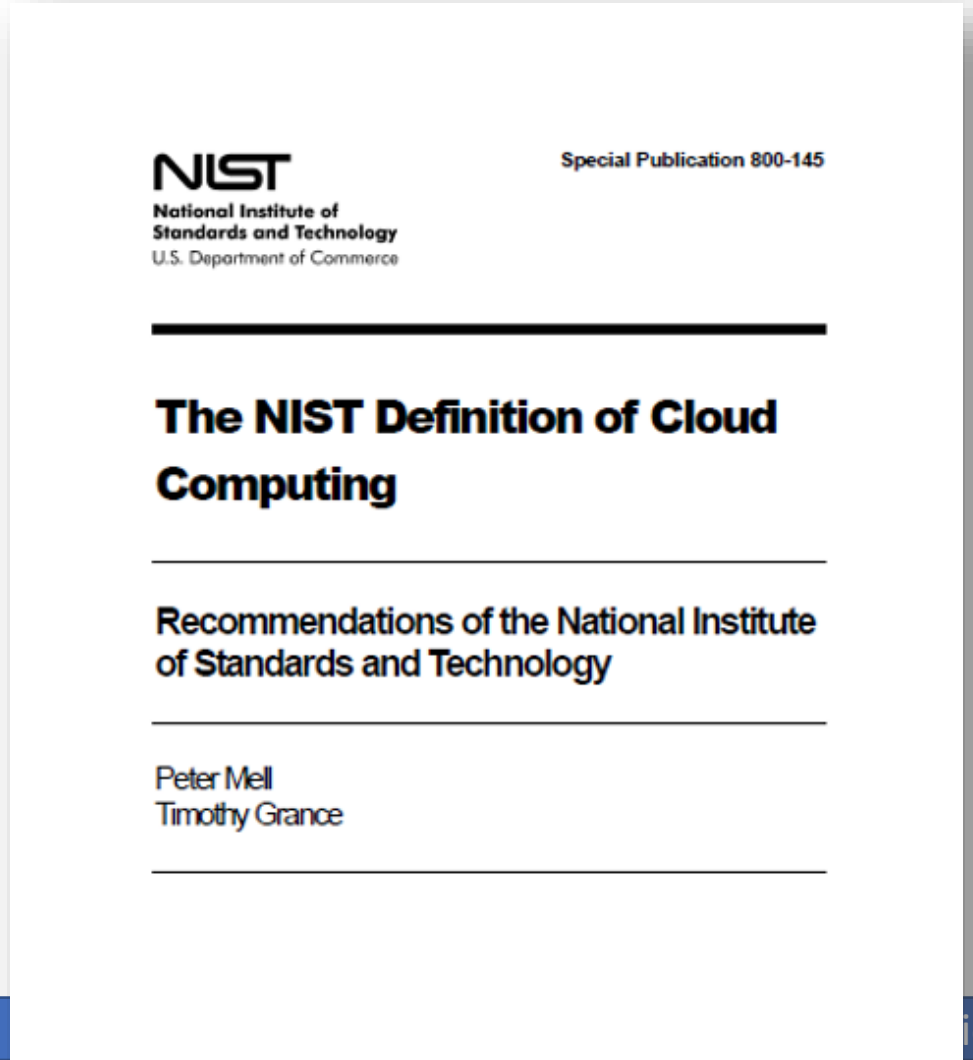
EIOPA

Orientamenti in materia di esternalizzazione a fornitori di servizi cloud

- Orientamento 10 – Obblighi contrattuali
- Orientamento 11 – Diritti di accesso e di audit
- Orientamento 12 – Sicurezza dei dati e dei sistemi
- Orientamento 13 – Subesternalizzazione di funzioni e attività operative cruciali o importanti
- Orientamento 14 – Monitoraggio e supervisione degli accordi di esternalizzazione nel cloud
- Orientamento 15 – Diritti di recesso e strategie di uscita
- Orientamento 16 – Supervisione degli accordi di esternalizzazione nel cloud da parte delle autorità di vigilanza
- Norme sulla conformità e sulla segnalazione
- Disposizione finale sulle revisioni

Cloud

Concetti base

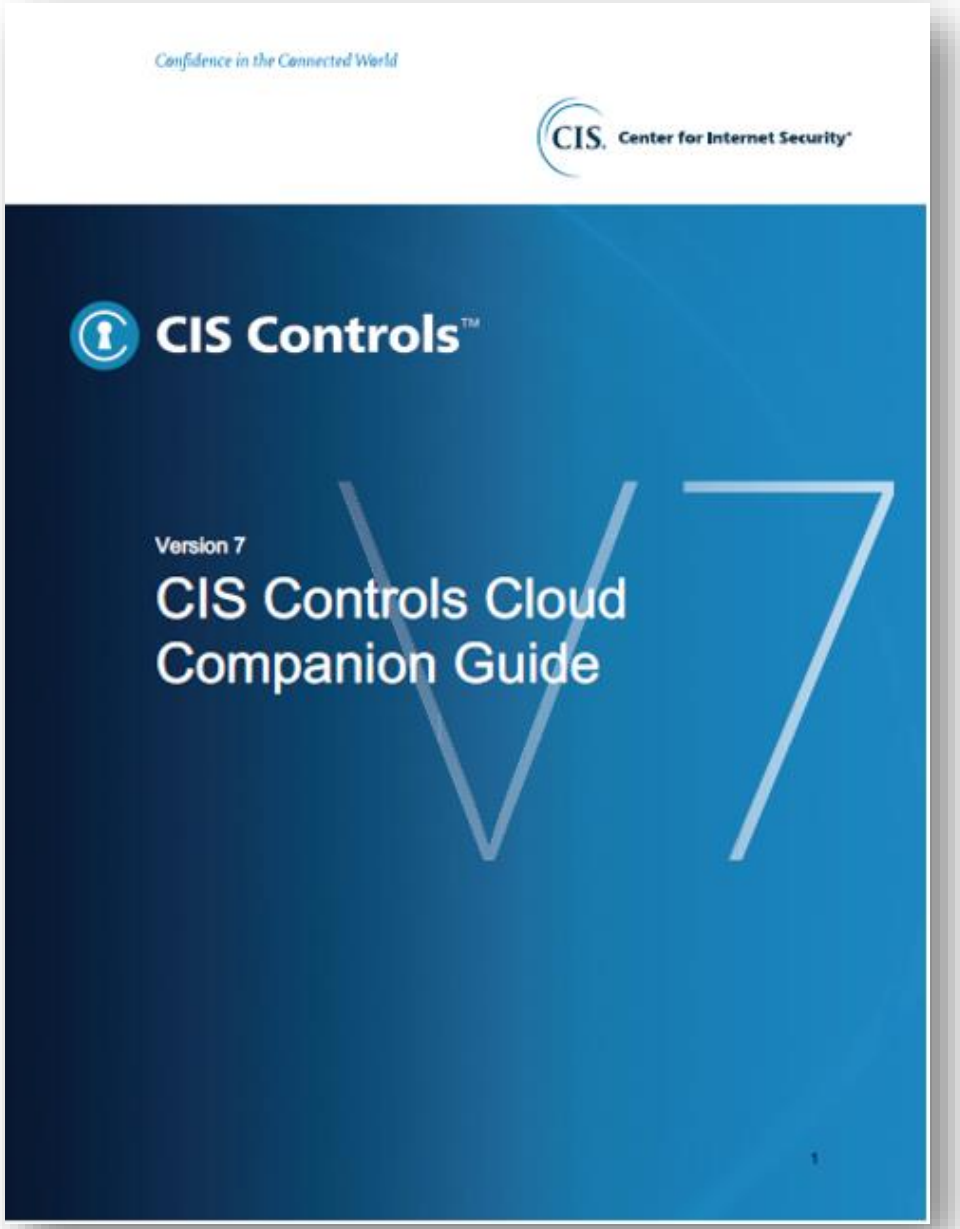

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance


Confidence in the Connected World

CIS Center for Internet Security®

CIS Controls™

Version 7

CIS Controls Cloud Companion Guide

NIST: Essential Characteristics

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

NIST + CIS : Service Models

- Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

NIST + CIS : Service Models

- *FaaS (Function as a Service) is a cloud computing service that allows the consumer to develop, manage, and run their application functionalities without having to manage and maintain any of the infrastructure that is required. The consumer can execute code in response to events that happen within the CSP or the application without having to build out or maintain a complex underlying infrastructure.*

NIST + CIS: Deployment Models

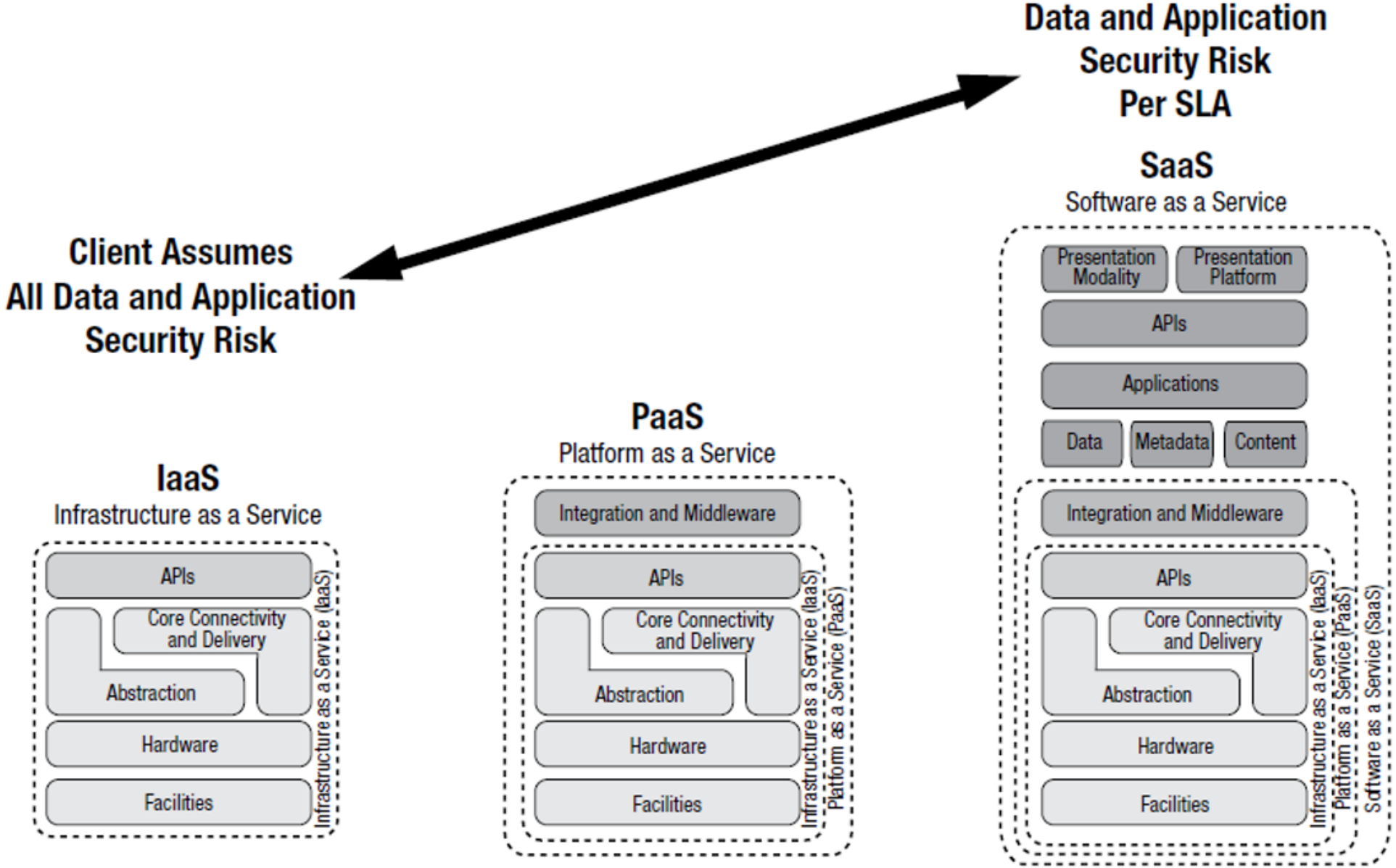
- Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
  - *Private cloud (on-prem) consists of all the computing resources being hosted and used exclusively by one consumer (organization) within its own offices and data centers. The consumer is responsible for the operational costs, hardware, software, and the resources required to build and maintain the infrastructure. This is best used for critical business operations and applications that require complete control and configurability.*
  - *Private cloud (third-party hosted) is a private cloud that is hosted by an external third party provider. The third party provides an exclusive cloud environment for the consumer and manages the hardware. All costs associated with the maintenance is the responsibility of the consumer.*

NIST + CIS: Deployment Models

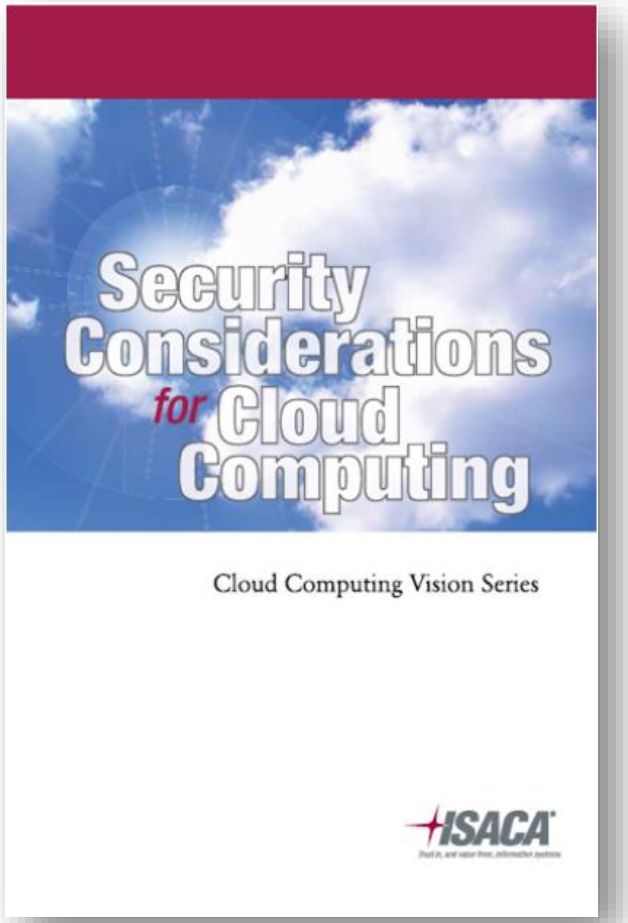
- Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Client Assumes All Data and Application Security Risk

Data and Application Security Risk Per SLA



Risk Factors by Service Model



Esempio: PAAS

Risk-decreasing factor:

- S2.A Short development time—Using the service oriented architecture (SOA) library provided by the CSP, applications can be developed and tested within a reduced time frame because SOA provides a common framework for application development.

Risk affected—Unavailability, loss

Risk-increasing factors:

- *S2.B Application mapping—If current applications are not perfectly aligned with the capabilities provided by the CSP, additional undesirable features (and vulnerabilities) could be introduced.*

Risk affected—Theft, disclosure

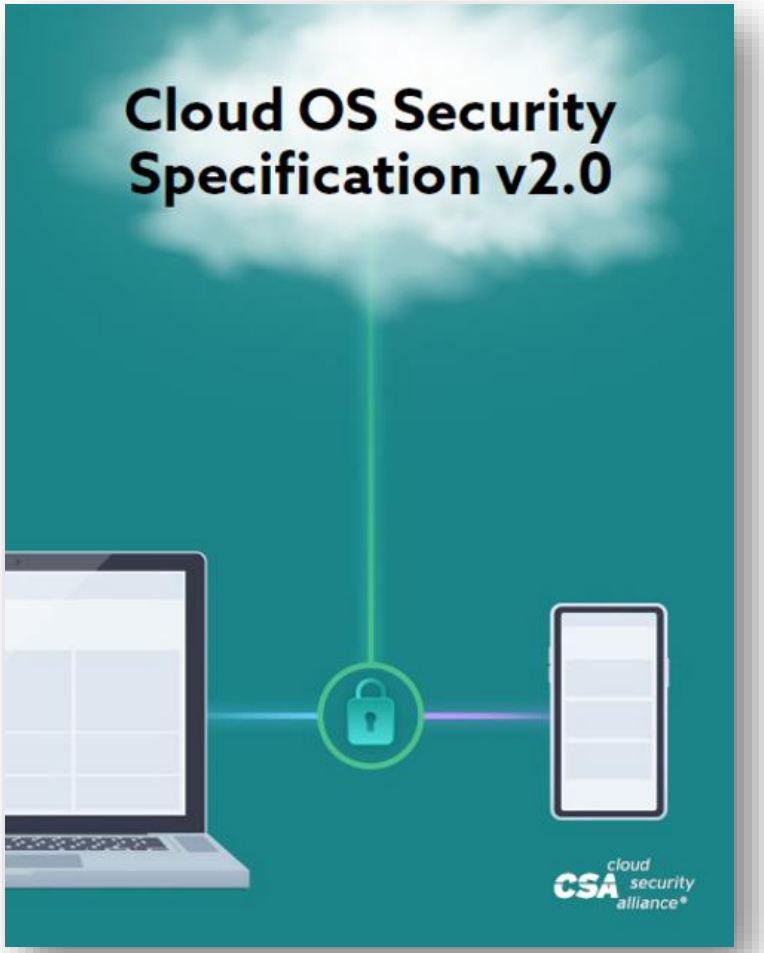
- *S2.C SOA-related vulnerabilities—Security for SOA presents new challenges because vulnerabilities arise not only from the individual elements, but also from their mutual interaction. Because the SOA libraries are under the responsibility of the CSP and are not completely visible to the enterprise, there may exist unnoticed application vulnerabilities.*

Risk affected—Unavailability, loss, theft, disclosure

- *S2.D Application disposal—When applications are developed in a PaaS environment, originals and backups should always be available. In the event of a contract termination, the details of the application could be disclosed and used to create more selective attacks on applications.*

Risk affected—Theft, disclosure

Risks and threats for administrators include



- The virtualization management layer becomes the new high-risk area. Cloud computing systems enable computing resources for large numbers of users using virtualization technology. Therefore, the virtualization management layer becomes the new high-risk area.
- Malicious users are difficult to track and isolate. The on-demand and self-service allocation of resources within a cloud computing system make it much easier for malicious users to launch attacks. Unfortunately, these users are difficult to track and isolate due to dynamically varying resource allocation and network settings.
- Open interfaces make the cloud computing system vulnerable to external attacks.
- Administrators commonly use open interfaces to access the cloud computing system through networks, making the system vulnerable to attacks from external networks.

Risks and threats for end users include

Risks cannot be controlled for data stored in the cloud. Computing resources and data are retained and managed entirely by cloud service providers. The risks brought by this resource management mode are as follows:

- Malicious cloud service provider administrators may invade CSC systems illegally.
- Data security cannot be ensured after the computing resources or storage space is released.
- The selection and formulation of laws and regulations used for data processing can be complex.

- Multi-tenant resource sharing may cause data leakage and lead to attacks.

- Resources shared among multiple tenants pose the following security risks:
  - User data may leak because of inappropriate isolation methods.
  - Users are susceptible to attacks by other malicious users within the same physical environment.

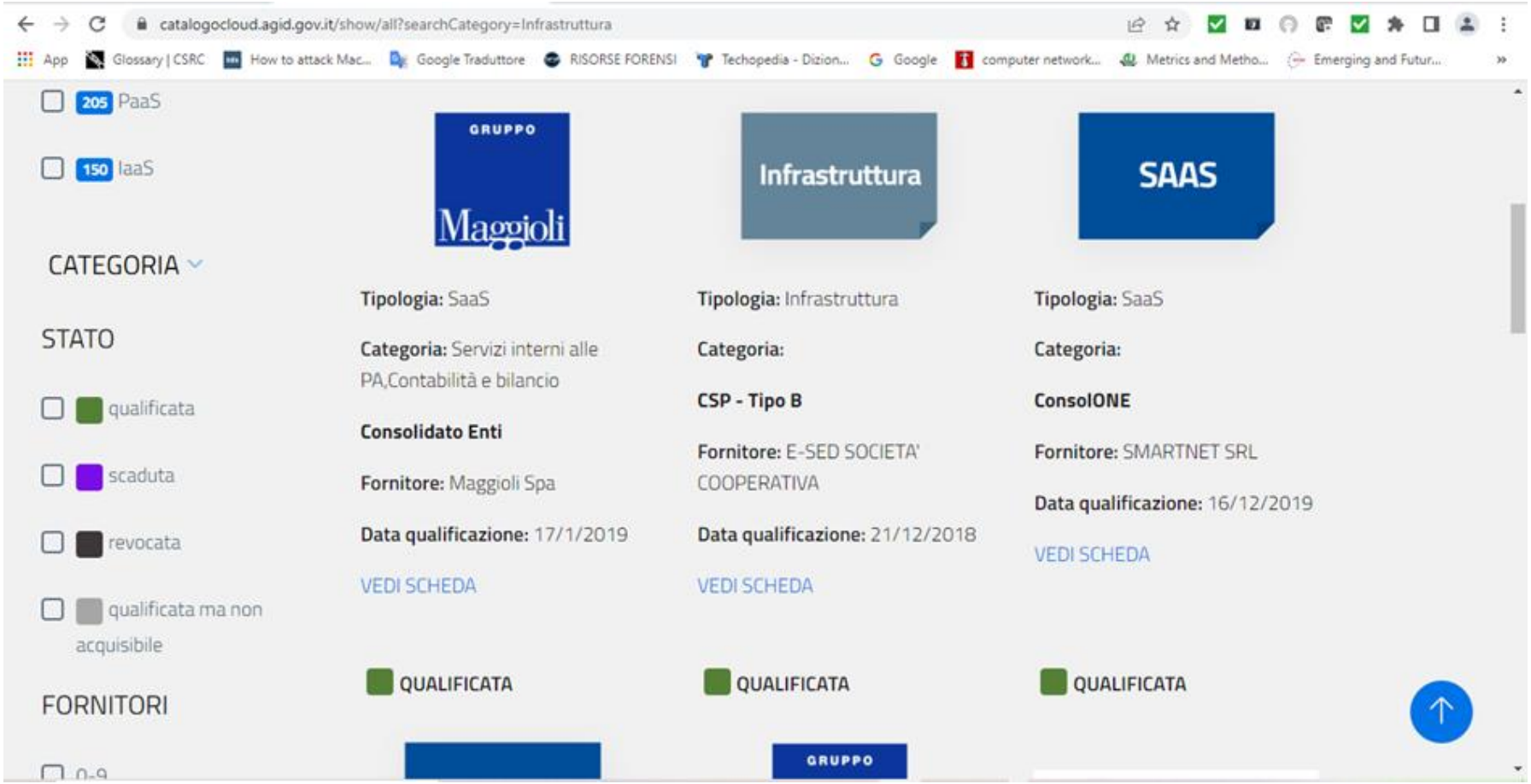
- Open network interfaces carry security risks. In a cloud computing environment, users operate and manage computing resources through the internet. The openness of network interfaces brings more security risks.

- Hardware resource security can be challenging to control. Since computing resources are allocated and utilized through virtualization technology, users have limited and control of the original hardware resources which are actually in use.

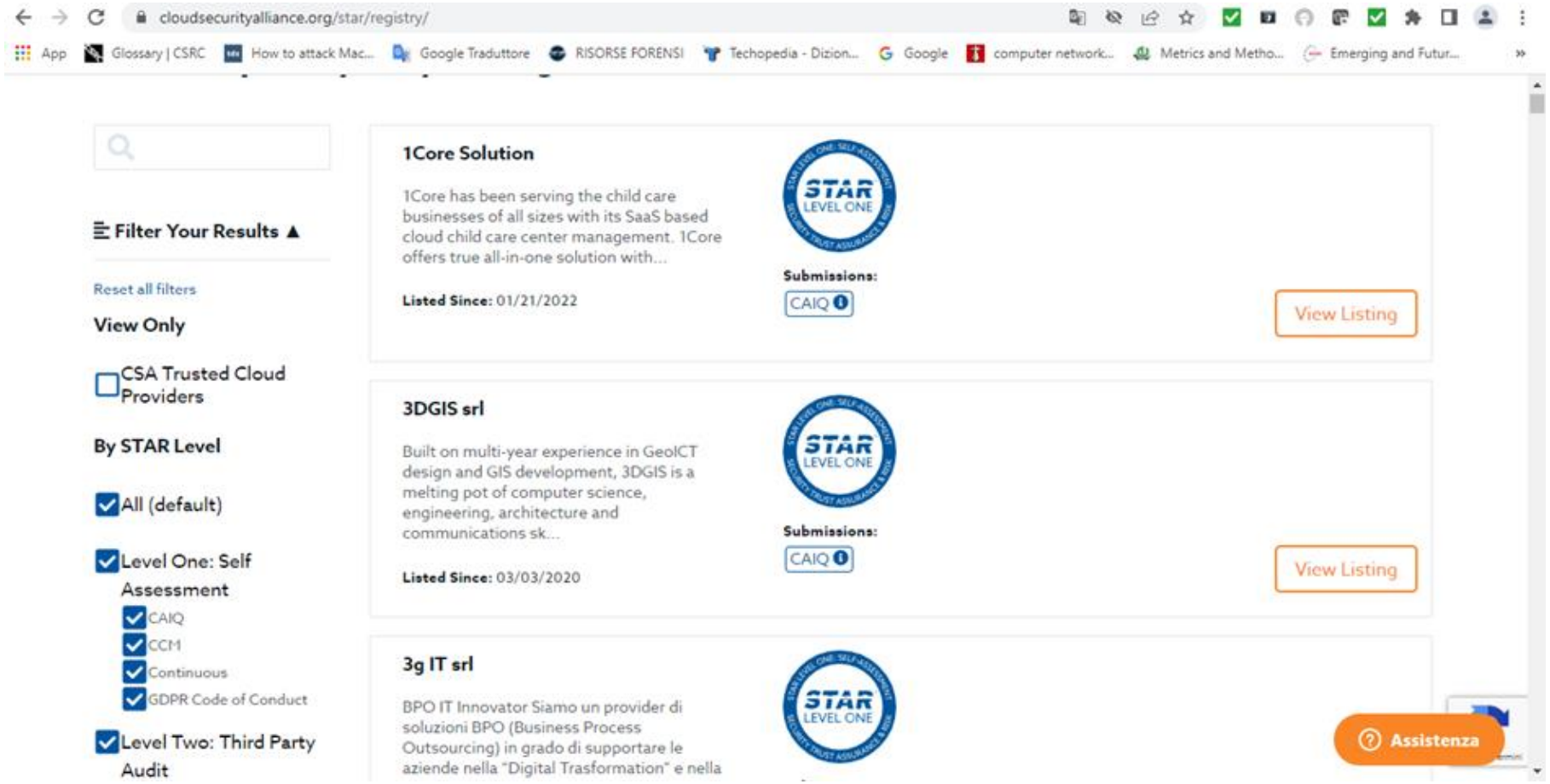
IS Audit/Assurance Program
Cloud Computing

Process Sub-area	Ref. Risk	Control Objectives	Controls	Control Type	Control Class	Control Frequency	Testing Step	Ref. COBIT 5	Ref. Framework/ Standar	Ref. Workpape	Pass / Fail	Comments
Incident Response, Notification and Remediation		**CO1**. Incident notifications, responses and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed.	**C1**. The contract SLAs describe specific definitions of incidents (data breaches, security violations) and events (suspicious activities) and the actions to be initiated by and the responsibilities of both parties.				**1**. Obtain and review the SLAs per the contract to determine that incidents and events are clearly defined and responsibilities assigned. **2**. Review cooperation agreements, and evaluate the responsibilities for the investigation of incidents. **3**. Notification procedures according to local laws are incorporated into the incident and event process.	APO09; APO10; APO13; DSS02;				
			C2. Issue monitoring processes are implemented and actively used by the service provider to document and report all defined incidents.				**1**. Obtain and review the service provider's issue monitoring procedures. **2**. Determine if the monitored reporting requirements are aligned with the customer's incident reporting policy. **3**. Obtain the incident monitoring reports for a representative period of time. **4**. Determine that the: - Customer was notified of the incident within the SLA requirements - Remediation was timely based on the scope and risk of the incident - Remediation was appropriate - Issue was escalated, if appropriate - Issue was closed and the customer notified in a timely manner	APO09; APO10; APO13; DSS02				
			C3. The customer has established an issue monitoring process to track internal and service provider incidents.				**1**. Obtain the customer incident monitoring procedure. **2**. Determine if the incident monitoring procedure tracks both internal and service provider incidents. **3**. Select a sample of incidents, and determine that: - The service provider notified the customer on a timely basis within scope of the contract. - The remediation was timely based on the scope and risk of the incident. - The remediation was appropriate. - The issue was escalated within the service provider's hierarchy. - The issue was closed by the service provider. - The issue was monitored and reported to customer management. - Customer procedures were modified to recognize the increased risk.	DSS02; MEA02				

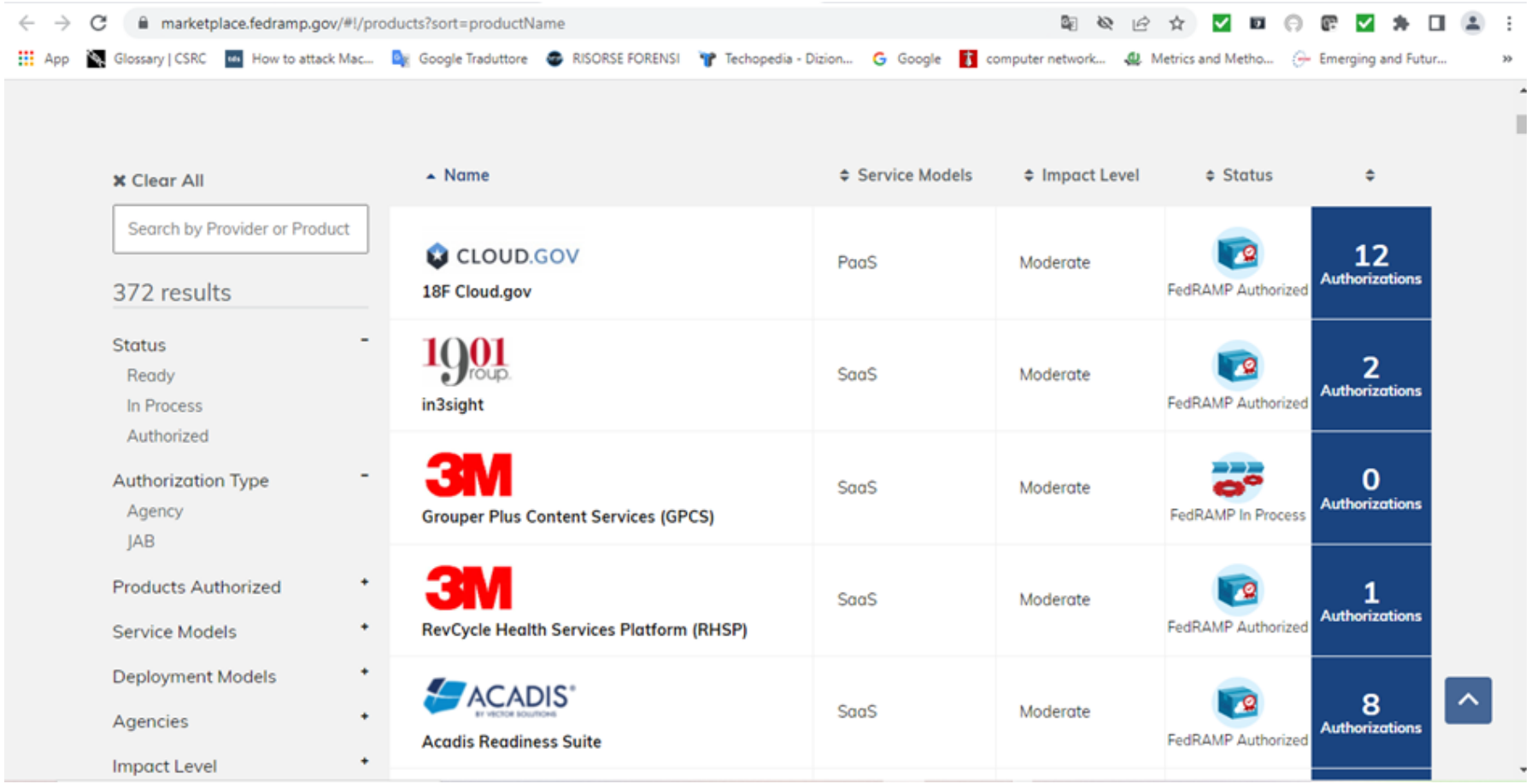
AGID Cloud marketplace



CSA STAR

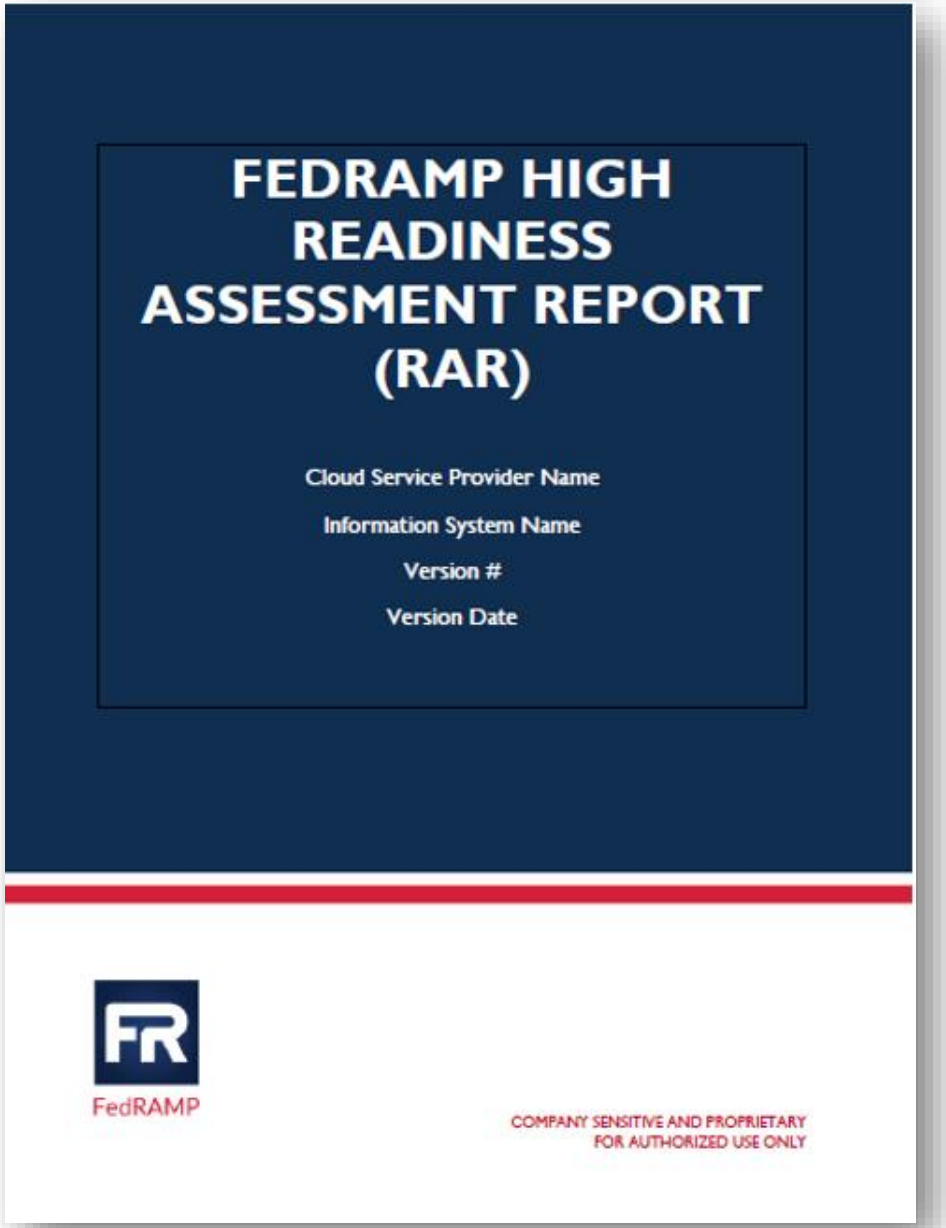

cloudsecurityalliance.org/star/registry/
App
Glossary | CSRC
How to attack Mac...
Google Traduttore
RISORSE FORENSI
Techopedia - Dizion...
Google
computer network...
Metrics and Metho...
Emerging and Futur...
Filter Your Results ▲
Reset all filters
View Only
CSA Trusted Cloud Providers
By STAR Level
All (default)
Level One: Self Assessment
CAIQ
CCM
Continuous
GDPR Code of Conduct
Level Two: Third Party Audit
1Core Solution
1Core has been serving the child care businesses of all sizes with its SaaS based cloud child care center management. 1Core offers true all-in-one solution with...
Listed Since: 01/21/2022
Submissions:
CAIQ
View Listing
3DGIS srl
Built on multi-year experience in GeoICT design and GIS development, 3DGIS is a melting pot of computer science, engineering, architecture and communications sk...
Listed Since: 03/03/2020
Submissions:
CAIQ
View Listing
3g IT srl
BPO IT Innovator Siamo un provider di soluzioni BPO (Business Process Outsourcing) in grado di supportare le aziende nella "Digital Trasformation" e nella
STAR LEVEL ONE
Assistenza

FEDRAMP

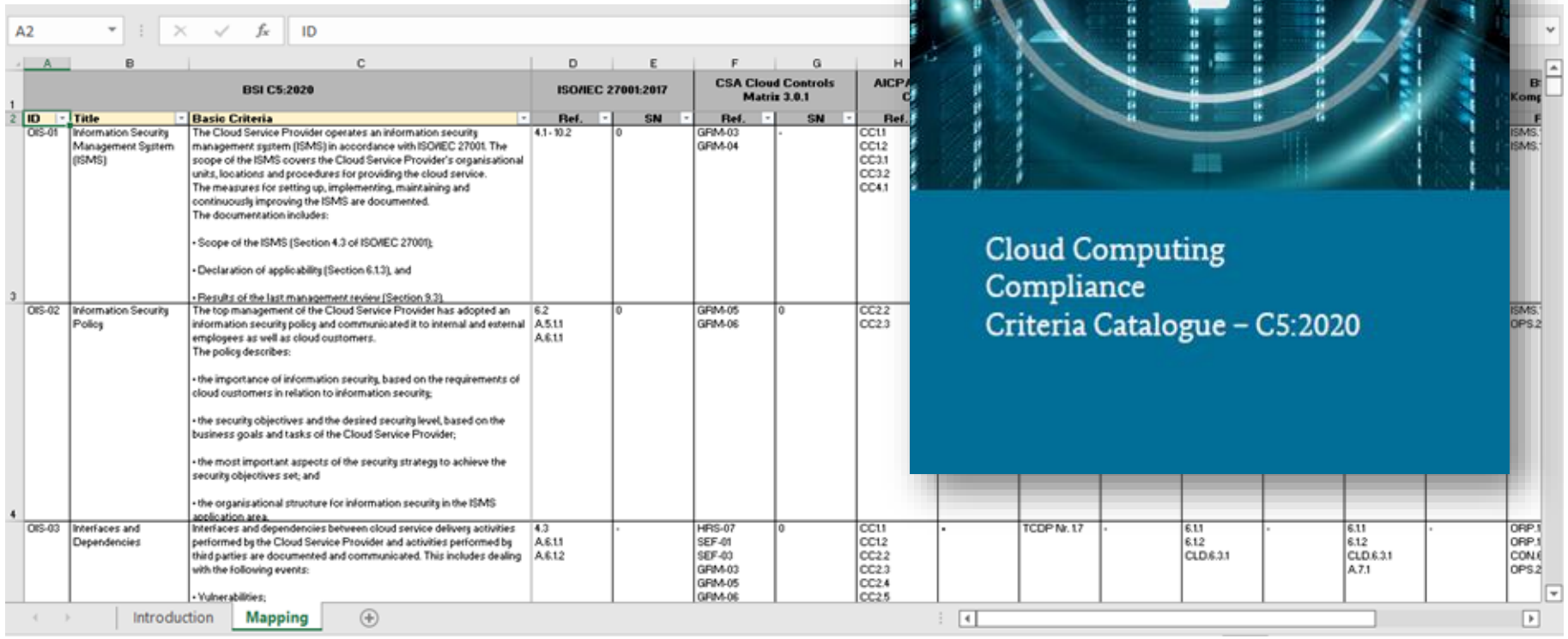

marketplace.fedramp.gov/#!/products?sort=productName
App
Glossary | CSRC
How to attack Mac...
Google Traduttore
RISORSE FORENSI
Techopedia - Dizion...
Google
computer network...
Metrics and Metho...
Emerging and Futur...
Clear All
Search by Provider or Product
372 results
Status
Ready
In Process
Authorized
Authorization Type
Agency
JAB
Products Authorized
Service Models
Deployment Models
Agencies
Impact Level
Name
Service Models
Impact Level
Status
CLOUD.GOV
18F Cloud.gov
PaaS
Moderate
FedRAMP Authorized
12 Authorizations
1901 Group
in3sight
SaaS
Moderate
FedRAMP Authorized
2 Authorizations
3M
Grouper Plus Content Services (GPCS)
SaaS
Moderate
FedRAMP In Process
0 Authorizations
3M
RevCycle Health Services Platform (RHSP)
SaaS
Moderate
FedRAMP Authorized
1 Authorizations
ACADIS
Acadis Readiness Suite
SaaS
Moderate
FedRAMP Authorized
8 Authorizations

CSA STARTM Level and Scheme Requirements

TYPE OF AUDIT	AUDIT FREQUENCY	Security	Privacy
●—●—●	STAR Level 3	Continuous Auditing	———
●—●—○	STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment	———
	STAR Level 2	3rd Party Certification	GDPR CoC Certification
●—○—○	STAR Level 1 Continuous	Continuous Self-Assessment	———
	STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment



BSI: C5



	BSI C5:2020			ISO/IEC 27001:2017		CSA Cloud Controls Matrix 3.0.1		AICPA
ID	Title	Basic Criteria		Ref.	SN	Ref.	SN	Ref.
OIS-01	Information Security Management System (ISMS)	The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organisational units, locations and procedures for providing the cloud service. The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3).		4.1 - 10.2	0	GRM-03 GRM-04	-	CC1.1 CC1.2 CC3.1 CC3.2 CC4.1
OIS-02	Information Security Policy	The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers. The policy describes: • the importance of information security, based on the requirements of cloud customers in relation to information security; • the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • the most important aspects of the security strategy to achieve the security objectives set; and • the organisational structure for information security in the ISMS application area.		6.2 A.5.1.1 A.6.1.1	0	GRM-05 GRM-06	0	CC2.2 CC2.3
OIS-03	Interfaces and Dependencies	Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third parties are documented and communicated. This includes dealing with the following events: • Vulnerabilities;		4.3 A.6.1.1 A.6.1.2	-	HRS-07 SEF-01 SEF-03 GRM-03 GRM-05 GRM-06	0	CC1.1 CC1.2 CC2.2 CC2.3 CC2.4 CC2.5

Introduction | Mapping

Federal Office for Information Security

Cloud Computing Compliance Criteria Catalogue – C5:2020

Verifiche di terze parti

Service Organization Control Reports® (AICPA)

- SOC 1® Report Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting This meets the needs of user entities' managements and auditorsas they evaluate the effect of a service organization's controls on a user entity's financial statement assertions. These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of compliance with laws and regulations and for when user entity auditors plan and perform financial statement audits.
- SOC 2® Report Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) For those who need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality or privacy. These reports can play an important role in oversight of the organization, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight. Stakeholders who may use these reports include management or those charged with governance of the user entities and of the service organization, customers, regulators, business partners and suppliers, among others.
- SOC 3® Report Trust Services Principles, Criteria, and Illustrations Designed to accommodate users who want assurance on a service organization's controls related to security, availability, processing integrity, confidentiality or privacy but do not have the need for the detailed and comprehensive SOC 2® Report. It can be used in a service organization's marketing efforts.

LogMeIn
Be Limitless.

MISURE DI SICUREZZA

L'impegno di LogMeIn è rivolto al monitoraggio e al costante miglioramento delle sue misure di sicurezza tecniche e organizzative al fine di garantire ai clienti una migliore protezione dei loro contenuti sensibili. Teniamo sempre in grande considerazione le pratiche conformi agli standard di settore relative alla sicurezza nonché alla riservatezza delle informazioni e dei dati tecnici, adoperandoci per soddisfare o superare tali standard. I nostri programmi dedicati alla sicurezza sono completi e ne coprono ogni aspetto.

In aggiunta ai nostri rigorosi controlli di sicurezza interni, siamo in possesso delle seguenti certificazioni di sicurezza rilasciate da società terze affidabili. Nel quadro della nostra dedizione ai clienti, effettuiamo verifiche convalidate dalla certificazione SOC 2 (tipo II) e ne mettiamo a loro disposizione una versione condivisibile: il rapporto SOC 3. Le certificazioni applicabili di tutti i prodotti sono disponibili nella pagina delle relative risorse, da dove è possibile scaricarne una copia.

SOC 2
Controlli di sicurezza, disponibilità e riservatezza.

SOC 3
Rapporto pubblico sui controlli di sicurezza, disponibilità e riservatezza.

C5
Attestato C5 (Cloud Computing Compliance Controls Catalog) del BSI.

otherwise undergo on-site assessments by LogMeIn which are reviewed by the LogMeIn Governance, Risk, & Compliance (GRC) Team to ensure consistency with LogMeIn's vendor risk management requirements/policies.

LogMeIn's service architecture is designed to perform replication in near-real-time to geo-diverse locations.

LogMeIn's Technology Operations Department (TechOps) manages production servers, monitors systems, performs backups, upgrades operating systems, and manages production firewalls and system updates. The LogMeIn Security and Information Technology (IT) teams manage the configuration of corporate firewalls, network system security, and endpoint devices (desktops, laptops, and mobile devices).

Authentication and Access

Physical and logical access controls are implemented to restrict access to the UCC Services' production systems, internal support tools, and customer data (referred to as Content in the LogMeIn Terms of Service). These control procedures are designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. LogMeIn follows a formal process to grant or revoke employee access to LogMeIn resources (corporate systems, applications, and production environments). This process is designed to grant access rights to systems and data only to authorized users. Both user and internal access to customer data is restricted by using unique user account IDs, where technically feasible. Access to sensitive systems and applications requires multi-factor authentication in the form of a unique user account ID, strong passwords, security keys, and/or specialized security tokens. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices, and support tools is managed via an access management procedure and access is reviewed as needed on at least a quarterly basis.

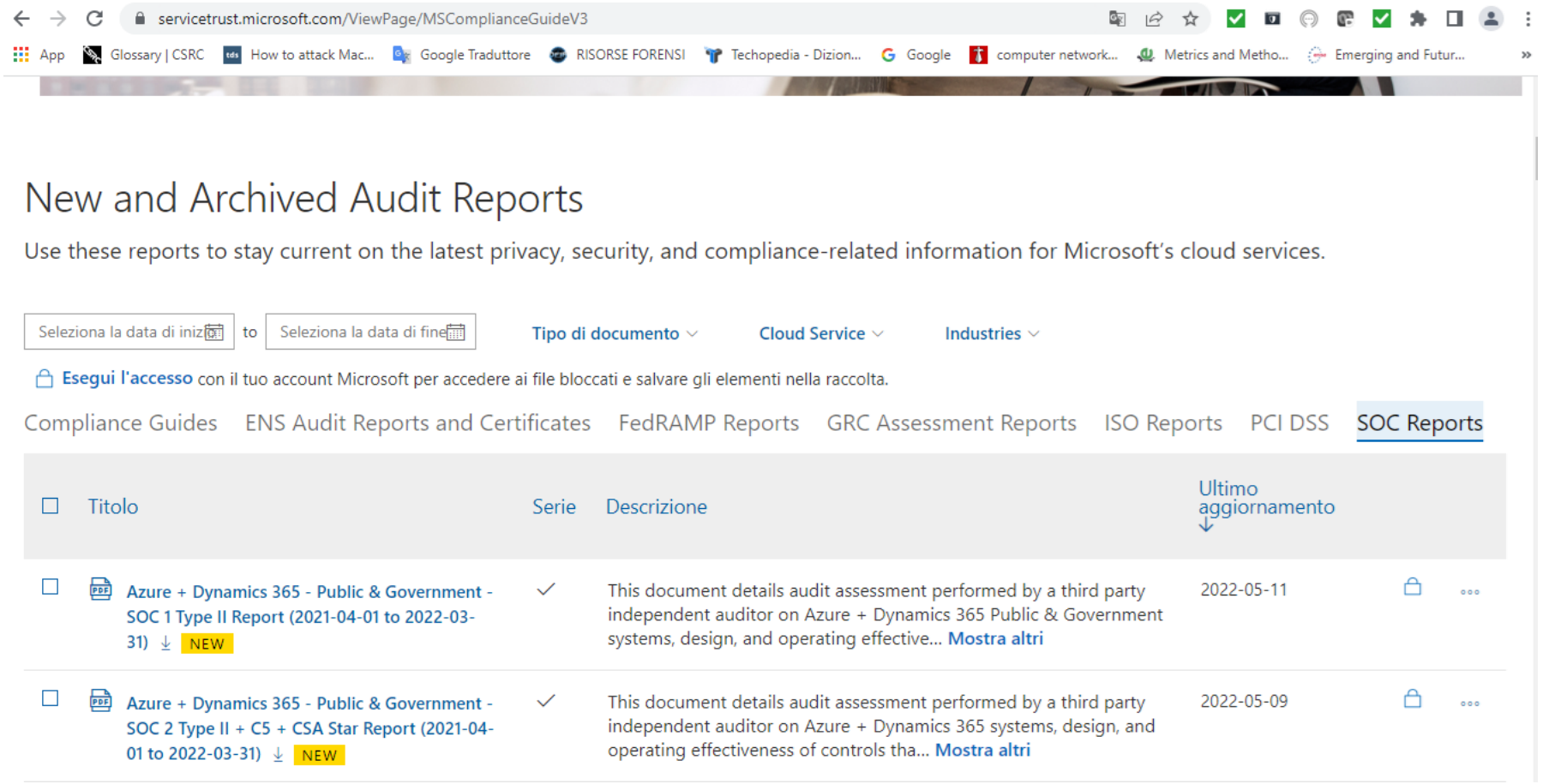
Software

The UCC Services are developed by the LogMeIn software development staff and run on shared multi-tier architectures with network segmentation and server role assignments.

People and Organization

LogMeIn has implemented a process-based system and environment designed to deliver the UCC Services to customers. In order to deliver consistent and quality services, LogMeIn has invested in developing a highly skilled team of resources and has adopted standardized, repeatable processes. LogMeIn has established internal teams to efficiently manage core infrastructure and product related security, availability, and confidentiality controls.

Esempi
Audit di terzi per prodotti Microsoft



Exit strategy

The EBA Guidelines (GL) on outsourcing arrangements require institutions to have a documented exit strategy when outsourcing critical or important functions which are in line with their outsourcing policy and business continuity. Institutions have to take into account the possibility of unintentional or unplanned termination of services.

These will include:

- the termination of outsourcing arrangements;
- the failure of the service provider;
- the deterioration of the quality of the function
- provided and actual or potential business
- disruptions caused by the inappropriate or failed provision of the function;
- material risks arising for the appropriate and continuous application of the function.

Fornitori critici

ARTICOLO *31*

Designazione dei fornitori terzi critici di servizi TIC

1.Le AEV, tramite il comitato congiunto e su raccomandazione del forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1:

a) designano i fornitori terzi di servizi TIC che sono critici per le entità finanziarie, a seguito di una valutazione che tiene conto dei criteri di cui al paragrafo 2;

b) nominano quale autorità di sorveglianza capofila di ciascun fornitore terzo critico di servizi TIC la AEV che è responsabile, a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, delle entità finanziarie che possiedono complessivamente la quota maggiore delle attività totali rispetto al valore delle attività totali di tutte le entità finanziarie che utilizzano i servizi del pertinente fornitore terzo critico di servizi TIC, secondo quanto risulta dalla somma dei singoli bilanci di quelle entità finanziarie.

2. La designazione di cui al paragrafo 1, lettera a), si fonda su tutti i criteri indicati di seguito in relazione ai servizi TIC prestati da un fornitore terzo di servizi TIC:

a) *l'impatto sistemico sulla stabilità, la continuità o la qualità della fornitura di servizi finanziari qualora il fornitore terzo di servizi TIC pertinente sia interessato da una disfunzione operativa su vasta scala che gli impedisca di fornire i suoi servizi, tenendo conto del numero di entità finanziarie e del valore totale delle attività delle entità finanziarie cui quel fornitore terzo di servizi TIC presta servizi;*

b) il carattere sistemico o ***l'importanza delle entità finanziarie che dipendono da quel fornitore terzo di servizi TIC***, valutati in conformità dei parametri seguenti:

i) ***il numero di enti a rilevanza sistemica a livello globale (G-SII) o di altri enti a rilevanza sistemica (O-SII) che dipendono dal rispettivo fornitore terzo di servizi TIC;***

ii) ***l'interdipendenza tra i G-SII o gli O-SII di cui al punto i) e altre entità finanziarie, comprese le situazioni in cui i G-SII o gli O-SII prestano servizi finanziari infrastrutturali ad altre entità finanziarie;***

c) la dipendenza delle entità finanziarie dai servizi prestati dal pertinente fornitore terzo di servizi TIC in rapporto alle funzioni essenziali o importanti delle entità finanziarie che in ultima analisi coinvolgono quel ***medesimo fornitore terzo di servizi TIC, indipendentemente dal fatto che le entità finanziarie dipendano da tali servizi direttamente o indirettamente, mediante accordi di subappalto;***

d) ***il grado di sostituibilità*** del fornitore terzo di servizi TIC, prendendo in considerazione i parametri seguenti:

i) la ***mancanza di alternative reali, anche parziali,*** dovuta al ***limitato numero di fornitori*** terzi di servizi TIC attivi su un mercato specifico, alla ***quota di mercato del fornitore*** terzo di servizi TIC in questione, o ancora alla ***complessità tecnica o al grado di sofisticazione,*** anche in relazione a ***eventuali tecnologie proprietarie***, o alle ***caratteristiche specifiche dell'organizzazione*** o dell'attività del fornitore terzo di servizi TIC;

ii) ***difficoltà inerenti alla migrazione, totale o parziale, dei dati e dei carichi di lavoro*** dal fornitore terzo di servizi TIC pertinente a un altro, ***a causa dei cospicui costi finanziari, del tempo o di altre risorse*** che possono essere necessarie per

il processo di migrazione, ***oppure dei maggiori rischi informatici o di altri rischi operativi cui l'entità finanziaria può esporsi a causa di tale migrazione***.

3. Laddove il fornitore terzo di servizi TIC appartenga a un ***gruppo***, i criteri di cui al paragrafo 2 sono presi in considerazione in relazione ai servizi TIC prestati dal gruppo nel suo insieme.

4. I fornitori terzi critici di servizi TIC che fanno parte di un gruppo designano una persona giuridica come punto di coordinamento per garantire un'adeguata rappresentanza e la comunicazione con l'autorità di sorveglianza capofila.

5. ***L'autorità di sorveglianza capofila informa il fornitore terzo di servizi TIC in merito all'esito della valutazione*** che ha portato alla designazione di cui al paragrafo 1, lettera a). ***Entro sei settimane dalla data della notifica, il fornitore terzo di servizi TIC può presentare all'autorità di sorveglianza capofila una dichiarazione motivata*** contenente tutte le informazioni pertinenti ai fini della valutazione. L'autorità di sorveglianza capofila esamina la dichiarazione motivata e può richiedere ulteriori informazioni da presentare entro 30 giorni di calendario dal ricevimento di detta dichiarazione.

Dopo aver designato un fornitore terzo di servizi TIC come critico, ***le AEV, tramite il comitato congiunto, notificano al fornitore terzo di servizi TIC tale designazione e la data di inizio a partire dalla quale sarà effettivamente soggetto ad attività di sorveglianza***. ***La data di inizio è fissata a non più di un mese dall'avvenuta notifica***. ***Il fornitore terzo di servizi TIC notifica alle entità finanziarie a cui presta servizi la propria designazione come critico***.

6. *Alla Commissione è conferito il potere di adottare un atto delegato, conformemente all'articolo 57, per integrare il presente regolamento specificando ulteriormente i criteri di cui al paragrafo 2 del presente articolo, entro il 17 luglio 2024.*

7. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non è utilizzato fino a quando la Commissione non abbia adottato un atto delegato in conformità del paragrafo 6.

8. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non si applica:

i) alle entità finanziarie che forniscono servizi TIC ad altre entità finanziarie;

ii) ai fornitori terzi di servizi TIC che sono soggetti a quadri di sorveglianza istituiti a supporto dei compiti di cui all'articolo 127, paragrafo 2, del trattato sul funzionamento dell'Unione europea;

iii) ai fornitori intragruppo di servizi TIC;

iv) ai fornitori terzi di servizi TIC che prestano servizi TIC unicamente in uno Stato membro a entità finanziarie attive solo in tale Stato membro.

9. ***Le AEV, tramite il comitato congiunto, redigono, pubblicano e aggiornano ogni anno l'elenco dei fornitori terzi critici di servizi TIC a livello di Unione.***

10. Ai fini del paragrafo 1, lettera a), ***le autorità competenti, con cadenza annuale e in forma aggregata***, trasmettono le relazioni di cui all'articolo 28, paragrafo 3, terzo comma, al forum di sorveglianza istituito ai sensi dell'articolo 32. Il forum di sorveglianza valuta la dipendenza delle entità finanziarie da terzi nel settore delle TIC sulla base delle informazioni ricevute dalle autorità competenti.

11. I fornitori terzi di servizi TIC che non sono inseriti nell'elenco di cui al paragrafo 9 possono chiedere di essere designati come critici conformemente al paragrafo 1, lettera a).

Ai fini del primo comma, il fornitore terzo di servizi TIC ***presenta una domanda motivata all'ABE, all'ESMA o all'EIOPA***; queste ultime, tramite il comitato congiunto, decidono se designare tale fornitore terzo di servizi TIC come critico conformemente al paragrafo 1, lettera a).

La ***decisione di cui al secondo comma è adottata e notificata al fornitore terzo di servizi TIC entro sei mesi*** dalla data in cui è stata ricevuta la domanda.

12.**Le entità finanziarie ricorrono ai servizi di un fornitore terzo di servizi TIC stabilito in un paese terzo e che è stato designato come critico** conformemente al paragrafo 1, lettera a), **soltanto se detto fornitore ha istituito un'impresa figlia nell'Unione entro 12 mesi dalla designazione**.

13.Il fornitore terzo critico di servizi TIC di cui al paragrafo 12 **notifica all'autorità di sorveglianza capofila eventuali cambiamenti nella struttura gestionale dell'impresa figlia istituita nell'Unione.**

Sanzioni

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.*

3. *Fatto salvo il diritto degli Stati membri di imporre sanzioni penali in conformità dell'articolo 52, gli Stati membri stabiliscono norme che prevedano adeguate sanzioni amministrative e misure di riparazione per le violazioni del presente regolamento e ne garantiscono l'effettiva applicazione.*

Tali sanzioni e misure sono efficaci, proporzionate e dissuasive.

4. *Gli Stati membri conferiscono alle autorità competenti il potere di applicare almeno le sanzioni amministrative o misure di riparazione seguenti per le violazioni del presente regolamento:*

a) emanare un ordine che imponga alla persona fisica o giuridica di porre termine al comportamento in violazione del presente regolamento e di astenersi dal ripeterlo;

b) richiedere la cessazione temporanea o permanente di qualsiasi pratica o comportamento che le autorità competenti considerino contrari alle disposizioni del presente regolamento e prevenirne la reiterazione;

c) adottare qualsiasi tipo di misura, anche di natura pecuniaria, per assicurare che le entità finanziarie continuino a rispettare i requisiti di legge;

d) chiedere, nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti di traffico dati detenute dagli operatori di telecomunicazioni, qualora vi sia il ragionevole sospetto di violazioni del presente regolamento e qualora si ritenga che le registrazioni possano essere pertinenti ai fini delle rispettive indagini; nonché

e) pubblicare comunicazioni pubbliche, comprese dichiarazioni pubbliche, indicanti l'identità della persona fisica o giuridica e la natura della violazione.

5. Qualora il paragrafo 2, lettera c), e il paragrafo 4 si applichino a persone giuridiche, gli Stati membri conferiscono alle autorità competenti il potere di imporre sanzioni amministrative e misure di riparazione, alle condizioni previste dal diritto nazionale, nei confronti di membri dell'organo di gestione e di altre persone che, ai sensi del diritto nazionale, siano responsabili della violazione.

6. Gli Stati membri garantiscono che qualsiasi decisione di imporre sanzioni amministrative o misure di riparazione adottata ai sensi del paragrafo 2, lettera c), sia adeguatamente motivata e preveda il diritto di ricorso.

ARTICOLO *51*

Esercizio del potere di imporre sanzioni amministrative e misure di riparazione

1.Le autorità competenti esercitano il potere di imporre sanzioni amministrative e misure di riparazione di cui all'articolo 50 in conformità del proprio quadro giuridico nazionale, a seconda dei casi:

a) direttamente;

b) in collaborazione con altre autorità;

c) sotto la propria responsabilità mediante delega ad altre autorità; oppure

d) rivolgendosi alle competenti autorità giudiziarie.

2.Per stabilire il tipo e il livello della sanzione amministrativa o della misura di riparazione da imporre a norma dell'articolo 50, le autorità competenti tengono conto della misura in cui la violazione è intenzionale o è dovuta a negligenza e di tutte le altre circostanze pertinenti, tra cui, secondo il caso:

a) la rilevanza, la gravità e la durata della violazione;

b) il grado di responsabilità della persona fisica o giuridica responsabile della violazione;

c) la solidità finanziaria della persona fisica o giuridica responsabile;

d) *l'importanza degli utili realizzati o delle perdite evitate da parte della persona fisica o giuridica responsabile, nella misura in cui possano essere determinati;*

e) *le perdite subite da terzi a causa della violazione, nella misura in cui possano essere determinate;*

f) *il livello di cooperazione che la persona fisica o giuridica responsabile ha dimostrato nei confronti dell'autorità competente, ferma restando la necessità di garantire la restituzione degli utili realizzati o delle perdite evitate da tale persona fisica o giuridica;*

g) *le precedenti violazioni commesse dalla persona fisica o giuridica responsabile.*

ARTICOLO 52

Sanzioni penali

1. *Gli Stati membri possono decidere di non emanare norme relative a sanzioni amministrative o misure di riparazione per violazioni che, ai sensi del rispettivo diritto nazionale, siano passibili di sanzioni penali.*

2. *Qualora abbiano deciso di imporre sanzioni penali per violazioni del presente regolamento, gli Stati membri provvedono affinché siano messe in atto misure adeguate per far sì che le autorità competenti dispongano di tutti i poteri necessari per stabilire contatti con le autorità giudiziarie, le autorità inquirenti o le autorità di giustizia penale della loro giurisdizione, al fine di ricevere informazioni specifiche sulle indagini o i procedimenti penali avviati per violazioni del presente regolamento, e di trasmetterle alle altre autorità competenti, nonché all'ABE, all'ESMA o all'EIOPA in modo tale che possano adempiere l'obbligo di cooperazione ai fini del presente regolamento.*

ARTICOLO 53

Obblighi di notifica

Gli Stati membri notificano alla Commissione, all'ESMA, all'ABE e all'EIOPA le disposizioni legislative, regolamentari e amministrative adottate in attuazione del presente capo, incluse le eventuali norme di diritto penale pertinenti, entro il 17 gennaio 2025. Gli Stati membri notificano senza indebito ritardo alla Commissione, all'ESMA, all'ABE e all'EIOPA tutte le successive modifiche.

ARTICOLO *54*

Pubblicazione delle sanzioni amministrative

1. *Le autorità competenti pubblicano senza indebito ritardo sul proprio sito web ufficiale qualsiasi decisione di imporre sanzioni amministrative contro la quale non vi sia diritto di ricorso, dopo la notifica al destinatario.*

2. *La pubblicazione di cui al paragrafo 1 comprende informazioni sul tipo e la natura della violazione, l'identità delle persone responsabili e le sanzioni imposte.*

3. Qualora, in seguito a una valutazione caso per caso, ritenga che la pubblicazione dell'identità, nel caso di persone giuridiche, o dell'identità e dei dati personali, nel caso di persone fisiche, sarebbe sproporzionata, ivi compresi rischi inerenti alla protezione dei dati personali, metterebbe a repentaglio la stabilità dei mercati finanziari o lo svolgimento di un'indagine penale in corso, oppure provocherebbe, nella misura in cui possano essere determinati, danni sproporzionati alla persona coinvolta, l'autorità competente adotta una delle soluzioni seguenti in merito alla decisione di imporre una sanzione amministrativa:

a) rinvia la pubblicazione fino al momento in cui cesseranno di esistere tutti i motivi che giustificano la non pubblicazione;

b) pubblica la sanzione in forma anonima in maniera conforme al diritto nazionale; oppure

c) si astiene dalla pubblicazione, qualora le opzioni di cui alle lettere a) e b) siano ritenute insufficienti per scongiurare ogni pericolo per la stabilità dei mercati finanziari, oppure quando tale pubblicazione non sarebbe proporzionata alla mitezza della sanzione imposta.

4. Qualora si decida di pubblicare una sanzione amministrativa in forma anonima, ai sensi del paragrafo 3, lettera b), la pubblicazione dei dati pertinenti può essere rinviata.

5. Qualora l'autorità competente pubblichi una decisione che impone una sanzione amministrativa che è oggetto di ricorso dinanzi alle pertinenti autorità giudiziarie, le autorità competenti aggiungono immediatamente sul proprio sito web ufficiale tale informazione e, nelle fasi successive, eventuali informazioni correlate all'esito del ricorso. È pubblicata anche ogni decisione giudiziaria che annulli una decisione di imporre una sanzione amministrativa.

6. Le autorità competenti provvedono affinché le informazioni pubblicate ai sensi dei paragrafi da 1 a 4 restino sul loro sito web ufficiale unicamente per il periodo necessario ai fini dell'applicazione del presente articolo. Tale periodo non è superiore ai cinque anni dalla sua pubblicazione.

Grazie per l’attenzione

giancarlo.butti@promo.it

gbutti@clusit.it

338 9230742