La nuova disciplina europea sulla cyber security: aspetti tecnico-giuridici a confronto.

Barbara Martelli CNAF

Nadina Foggetti INFN Bari

La nuova disciplina

- la Direttiva (UE) 2022/2555 (Direttiva NIS2), relativa a **misure per un livello comune elevato di cibersicurezza nell'Unione** che ha apportato modifiche a far data dal 18 Ottobre 2024 al Regolamento (UE) 2014/910 e alla Direttiva (UE) 2018/1972 e ha abrogato la Direttiva (UE) 2016/1148 c.d. NIS 1 che dovrà essere recepita dagli Stati membri entro **il 17 Ottobre 2024**;
- la Direttiva (UE) 2022/2556 , che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto **riguarda la resilienza operativa digitale per il settore finanziario** che dovrà essere recepita dagli Stati membri entro **il 17 Ottobre 2025**;
- la Direttiva (UE) 2022/2557 **, relativa alla resilienza dei soggetti critici che abroga, dal 18 Ottobre 2024**, la Direttiva 2008/114/CE che dovrà essere recepita dagli Stati membri entro il **17 Ottobre 2024**.

Cyber Resilience Act

Proposta di

REGOLAMENTO relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

Novità introdotte

1. Norme per l'immissione sul mercato di prodotti con elementi digitali per garantire la cibersicurezza di tali prodotti;

b) requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cibersicurezza;

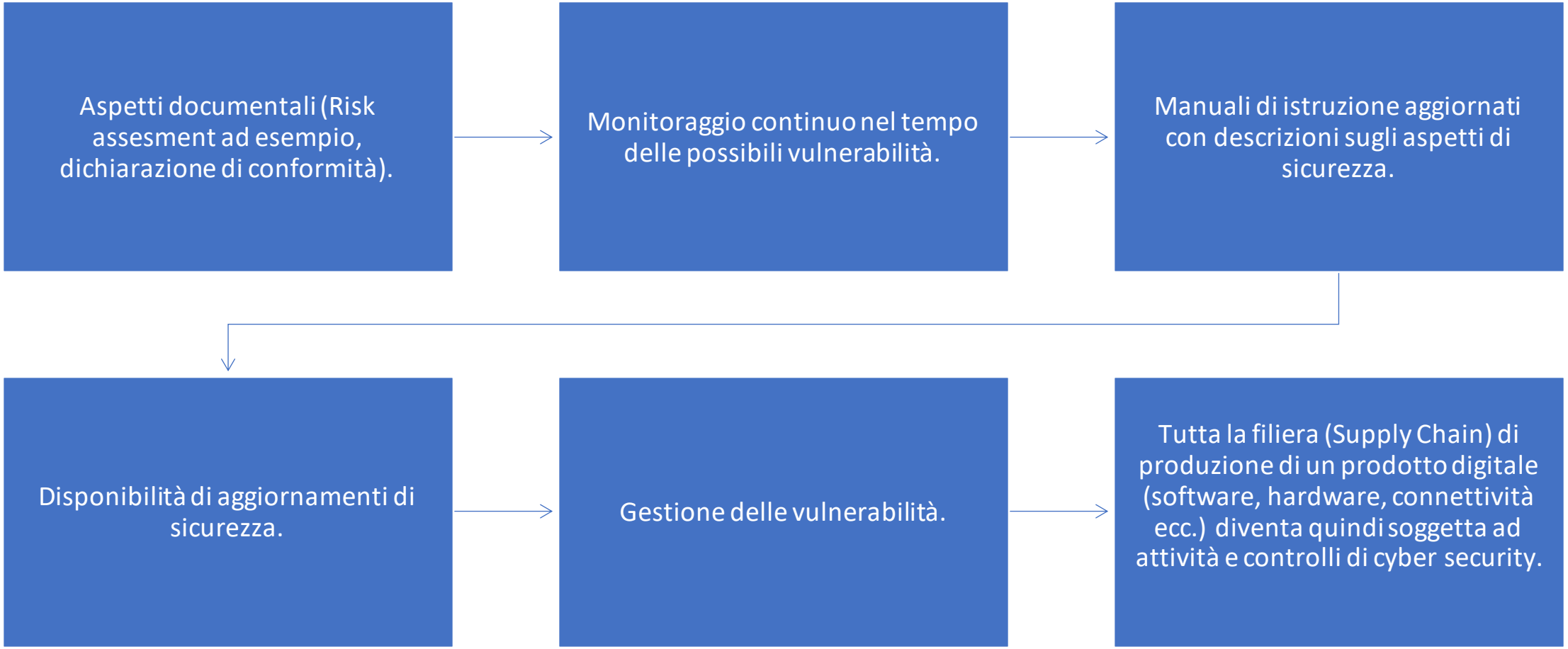
c) requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cibersicurezza dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi;

d) norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti di cui sopra.

2. si applica ai prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete

3. Si applica anche ai sistemi di Intelligenza artificiale

Il nuovo cyber resilient Act

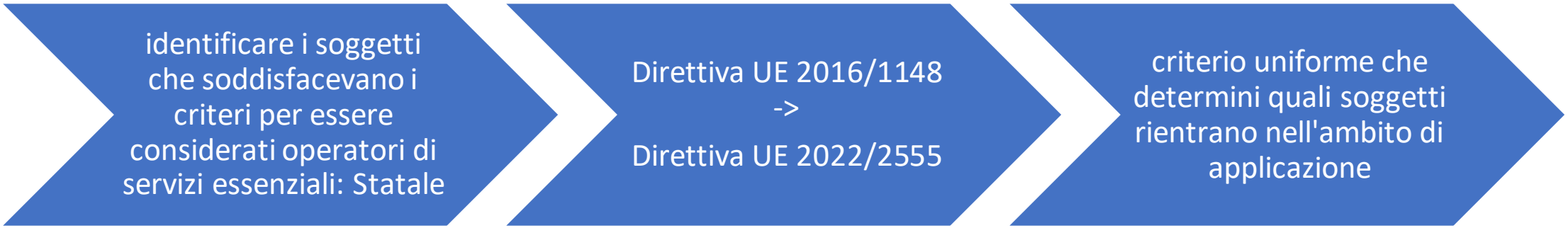


Punti di contatto con la direttiva NIS 2

- Saranno tre le categorie di prodotti coinvolti dal Cyber Resilience Act:

1. Categoria di Default, soggetta a Self-assessment (prodotti non critici)
2. Classe I (prodotti critici)
3. Classe II (prodotti critici)
    - La distinzione dalla prima classe a quelle successive si basa sui seguenti aspetti:
        - funzionali (ad esempio in ambito critical software);
        - modalità d'uso (ad esempio per il settore industrial control/NIS2);
        - altri criteri.

NIS 1 – NIS 2: ambito di applicazione



Data Center

- I servizi di cloud computing dovrebbero comprendere servizi digitali che consentono **l'amministrazione su richiesta** di un pool scalabile ed elastico di risorse di calcolo **condivisibili** e **l'ampio accesso remoto** a quest'ultimo, anche quando tali risorse sono distribuite in varie ubicazioni.
- Le risorse di calcolo comprendono risorse come reti, server o altre infrastrutture, sistemi operativi, software, archiviazione, applicazioni e servizi. I modelli di servizio del cloud computing comprendono, tra gli altri, il servizio a livello di infrastruttura (IaaS), il servizio a livello di piattaforma (PaaS), il servizio a livello di software (SaaS) e il servizio a livello di rete (NaaS).
- cloud privato, di comunità, pubblico e ibrido.
- I servizi di cloud computing e di distribuzione hanno lo stesso significato dei termini di servizio e dei modelli di distribuzione di cui alla norma ISO/IEC 17788:2014

Ampio accesso remoto

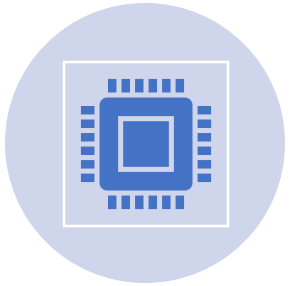
- (*broad network access*) è utilizzata per descrivere il fatto che le capacità cloud sono fornite sulla rete e accessibili attraverso meccanismi che promuovono l'uso di piattaforme client eterogenee leggere o pesanti (compresi telefoni cellulari, tablet, computer portatili e workstation.

Altri aspetti definitori

«scalabile» si riferisce alle risorse informatiche che sono assegnate in modo flessibile dal fornitore di servizi nel cloud, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda.

«pool elastico» è usata per descrivere le risorse di calcolo fornite e rilasciate in base alla domanda, al fine di aumentare e diminuire rapidamente le risorse disponibili in base al carico di lavoro.

«condivisibile» è usato per descrivere le risorse di calcolo che sono fornite a una molteplicità di utenti che condividono un accesso comune al servizio, mentre l'elaborazione è effettuata separatamente per ciascun utente anche se il servizio è fornito a partire dalla stessa apparecchiatura elettronica.



«distribuito» è usato per descrivere le risorse di calcolo che si trovano su diversi computer o dispositivi collegati in rete e che comunicano e si coordinano tra di loro mediante il passaggio di messaggi.

Obiettivi della nuova disciplina

b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557;

c) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza;

d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

In dettaglio

- **aumentare il livello di resilienza informatica di un insieme completo di imprese** che operano nell'Unione europea in tutti i settori pertinenti, mediante l'adozione di norme e adeguate misure di sicurezza informatica;
- **ridurre le incoerenze nella resilienza nel mercato interno nei settori già contemplati dalla direttiva**, allineando ulteriormente l'ambito di applicazione (de facto) i requisiti di sicurezza e di segnalazione degli incidenti, le disposizioni che disciplinano la vigilanza e l'esecuzione nazionali e le capacità delle autorità competenti pertinenti degli Stati membri;
- **migliorare il livello di consapevolezza comune (situational awareness) e la capacità collettiva di prepararsi e rispondere** adottando misure per aumentare il livello di fiducia tra le autorità competenti condividendo maggiori informazioni e stabilendo regole e procedure in caso di incidente o crisi su vasta scala.

Estensioni operate dalla direttiva

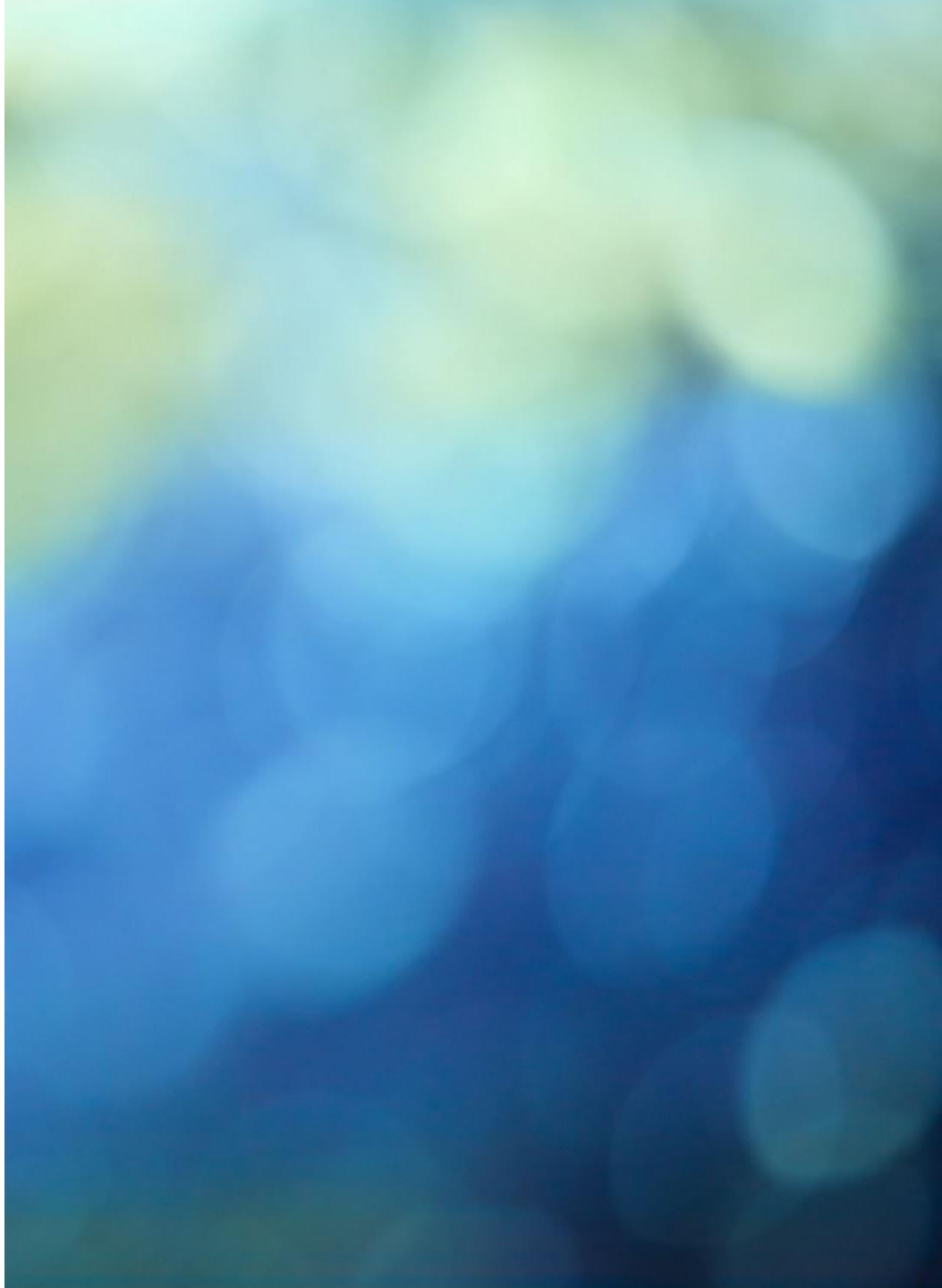
Effetto

- **sono stati limitati gli elementi di discrezionalità** che nella Direttiva NIS2 erano lasciati ai singoli Stati nella determinazione dell’appartenenza alla categoria.

enti “essenziali” e “importanti”

con differenti regimi di vigilanza e applicazione per quelli non essenziali.

a nuova direttiva NIS2 introduce una regola del massimale dimensionale (Size-cap) come regola generale per l’identificazione delle entità regolamentate.



Cybersecurity

- Ogni Stato membro definisce gli obiettivi strategici e le risorse necessarie per conseguirli
- Notifica entro 3 mesi alla commissione
- Valuta le proprie strategie nazionali per la cibersicurezza periodicamente e almeno ogni cinque anni sulla base di indicatori chiave di prestazione e, se necessario, le aggiornano. L'ENISA assiste gli Stati membri,

- **la NIS 2 istituisce formalmente la rete europea di organizzazioni di collegamento per le crisi informatiche** (EU-CyCLONe), per supportare la gestione coordinata degli incidenti di sicurezza informatica su larga scala.
- Un meccanismo volontario di apprendimento tra pari è finalizzato ad aumentare la fiducia reciproca e l'apprendimento dalle buone pratiche e dalle esperienze nell'Unione, contribuendo così al raggiungimento di un elevato livello comune di cybersicurezza.
-

Quali domande farci

- valutare se INFN(e in particolare Data Cloud) operi in uno dei settori di applicazione della direttiva
- monitorare e verificare l'attuazione nazionale della disciplina (2025)
- avviare o rivedere e aggiornare la governance e le procedure di sicurezza
- valutare la conformità dei fornitori dal punto di vista della sicurezza e, se necessario, rafforzare le misure contrattuali per ottenere il livello di efficacia concordato
- Formazione

Cosa cambia in materia di sicurezza dei dati?

imporre un cambiamento a livello di mentalità nei confronti della sicurezza informatica, capace di andare oltre i concetti legati alla protezione dei dati, già ben noti per via della normativa GDPR.

Rideterminazione e ampliamento dell'ambito di applicazione delle norme in materia di sicurezza dei dati

Potenziamento degli organi e delle attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale, grazie alla condivisione delle esperienze tra gli stati membri

Razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria degli incidenti informatici

Estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità a tutta la supply chain, coinvolgendo tutti o un maggior numero di stakeholder coinvolti

I requisiti minimi in materia di sicurezza dei dati previsti dalla Direttiva NIS2

Analizzare e valutare i rischi di sicurezza dei sistemi informativi con operazioni di vulnerability assessment, penetration test, ecc.

Gestire gli incidenti di sicurezza informatici con un piano e un'attività di incident response

Dotarsi di un piano di continuità di business e gestione delle crisi

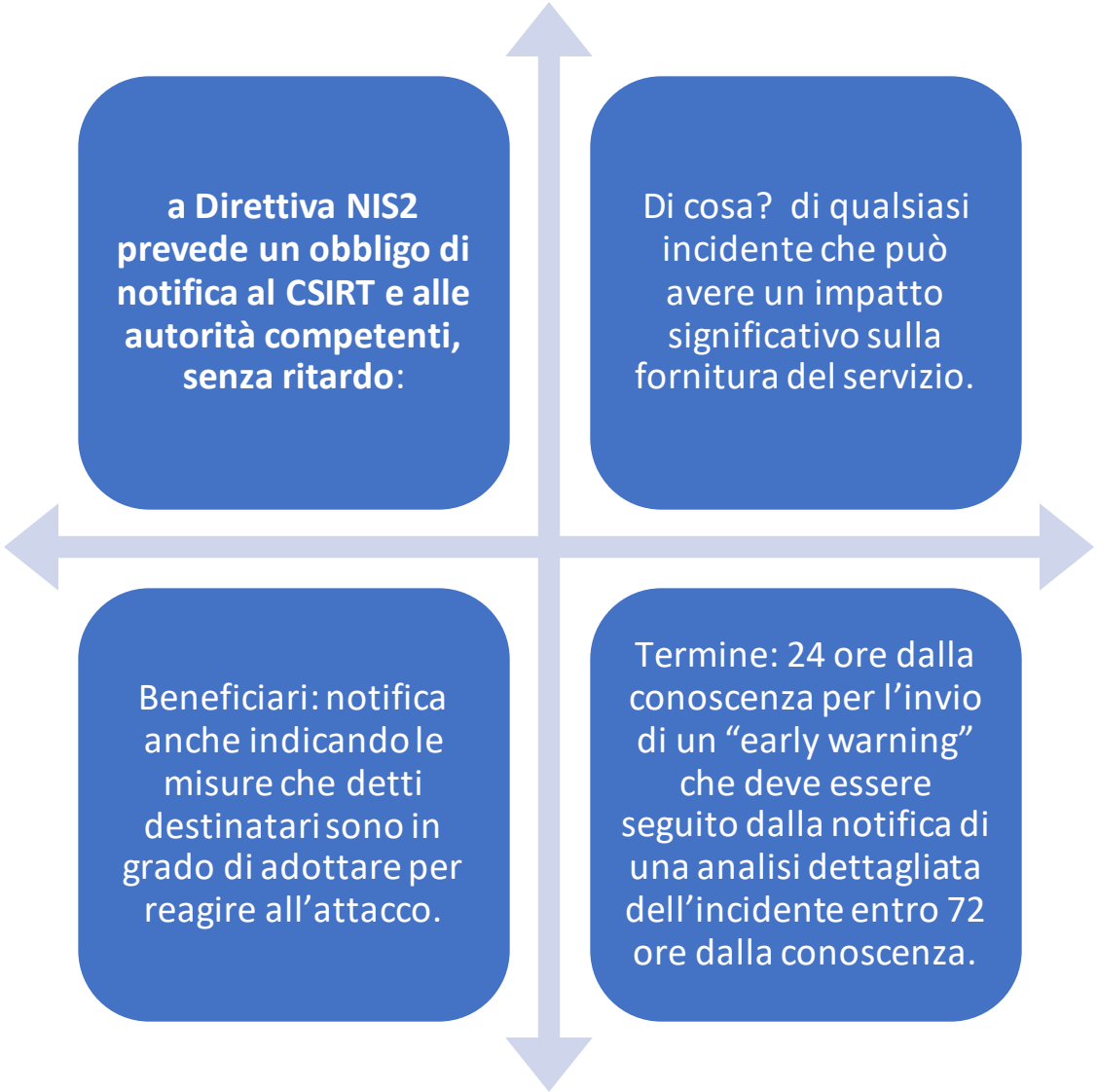
Testare regolarmente la sicurezza dell'infrastruttura IT e l'efficacia delle misure di gestione del rischio adottate

Assicurare la sicurezza delle supply chain, controllando che i propri fornitori dispongano di adeguati requisiti in termini di sicurezza.

Gli Stati dovranno imporre misure tecniche volte a:

1. policy sull'**analisi dei rischi** e sulla **sicurezza dei sistemi informativi;**
2. sistemi di **gestione degli incidenti**;
3. sistemi di **business continuity**, come la gestione dei backup e il disaster recovery, e la gestione delle crisi;
4. misure di gestione della **sicurezza della supply chain**;
5. la sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi, compresa la gestione e la **divulgazione delle vulnerabilità**;
6. policy e procedure per **valutare l'efficacia delle misure di gestione del rischio di cybersecurity**;
7. pratiche di **igiene informatica di base** [i.e., regole fondamentali per garantire la cybersecurity] e formazione in materia di sicurezza informatica;
8. policy e procedure relative all'uso della **crittografia** e, se del caso, della cifratura crittografia;
9. misure sulla sicurezza delle **risorse umane**, le politiche di controllo degli accessi e la gestione degli asset; e
10. l'uso di **soluzioni di autenticazione a più fattori** [i.e., la c.d. multi-factor authentication] o di autenticazione continua, di comunicazioni vocali, video e di testo protette e di sistemi di comunicazione di emergenza protetti all'interno dell'entità.

Obblighi di notifica dei cyber attacchi ai sensi della Direttiva NIS2



La notifica

- la Direttiva NIS2 prevede l'obbligo di notificare l'incidente a un "*Team di risposta agli incidenti di sicurezza informatica*" che dovrà essere appositamente istituito (c.d. CSIRT), nonché alle autorità competenti e in taluni casi ai destinatari del servizio, qualsiasi incidente che possa impattare in modo significativo sulla fornitura del servizio, senza ritardo.

NIS2 Art. 21
Cybersecurity risk-management measures

Essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems

Taking into account the "**state-of-the-art**" and, where applicable, **relevant European and international standards**, as well as **the cost of implementation**

The measures shall be based on an "all-hazards approach" […] and shall include "**at least**" the following:

a) policies on **risk analysis and information system security**;

b) **incident handling**;

c) **business continuity**, such as backup management and disaster recovery, and crisis management;

d) **supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

e) security in network and information systems **acquisition**, **development and maintenance**, including vulnerability handling and disclosure;

f) policies and procedures to assess the **effectiveness of cybersecurity risk-management measures**;

g) basic cyber hygiene practices and **cybersecurity training**;

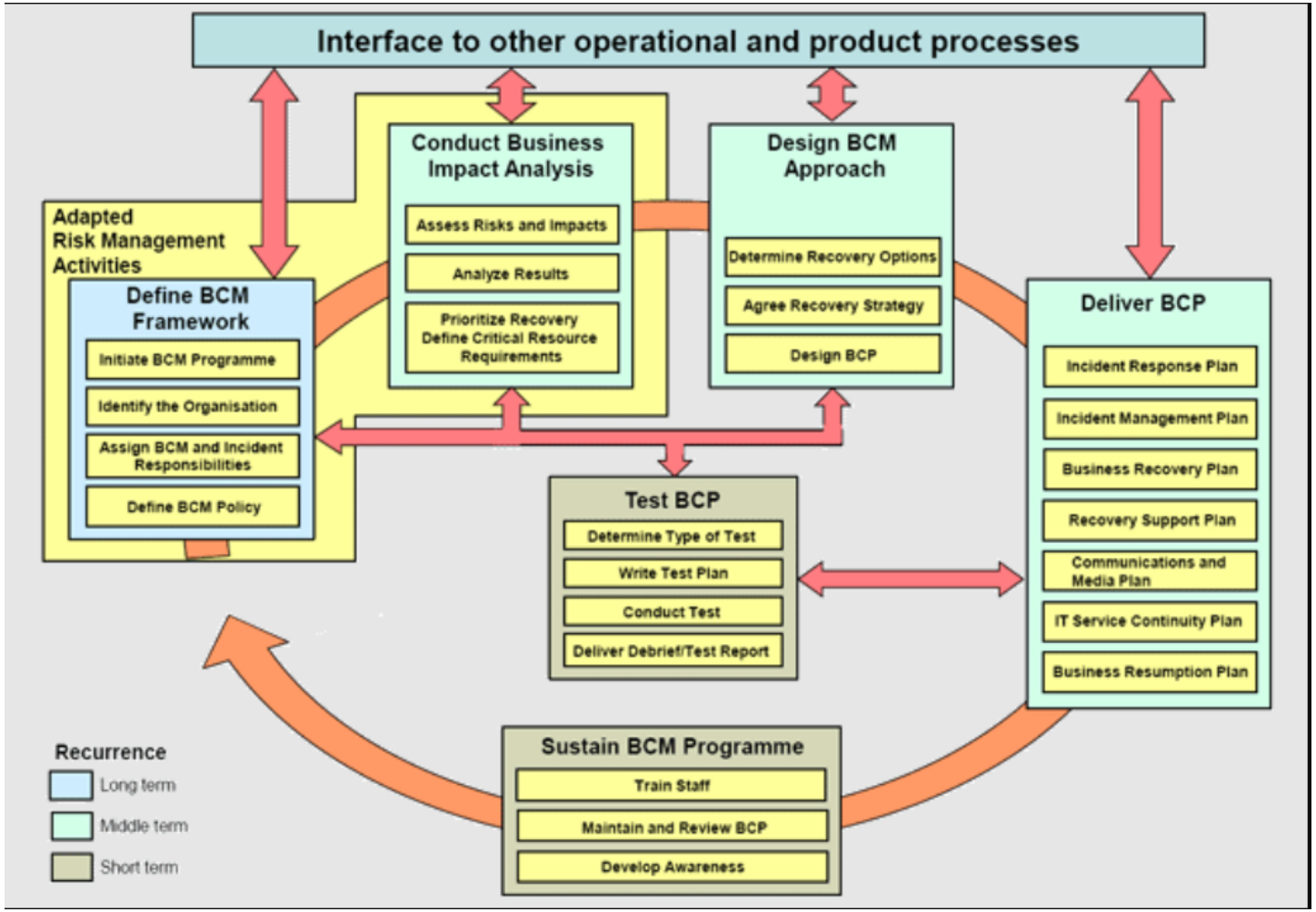
h) **policies and procedures regarding the use of cryptography** and, where appropriate, encryption;

i) **human resources security**, **access control policies** and **asset management**;

j) the use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Business continuity

1. Definire il framework di Business Continuity Management -> in EPIC usiamo ISO 22301
2. Definire il processo di Business Continuity -> in EPIC P02-BCP
3. Condurre la Business Impact Analysis -> in EPIC R02-BIA
4. Redigere un Business Continuity Plan -> in EPIC R36-BCP
5. Effettuare i test ad intervalli regolari -> in EPIC documentati su Jira con label BCTest



https://www.enisa.europa.eu/

Supply Chain Security

- Policy:
  - Classificare I fornitori che possono aver impatto sulla sicurezza delle informazionio
  - Stabilire i criteri con i quali valutare e selezionare i fornitori in base alla sensibilita' delle informazioni/prodotti/servizi da essi gestiti
  - Valutare i controlli che i fornitori effettuano sui loro processi e l'accuratezza e completezza della loro applicazione
  - Monitorare la compliance con i requisiti di sicurezza richiesti
  - Mitigare i casi di non-compliance dei fornitori
  - Gestire gli incidenti connessi a prodotti/servizi acquistati all'esterno e gestire nei contratti le responsabilita' delle parti
- Link a Information Security in Supplier Relationships Policy di EPIC (versione pubblica)

Policy “Security in Supplier Relationships”

- Basata su linee guida AGID per la sicurezza del procurement ICT
- Necessario espanderla per includere servizi cloud esterni (in corso attivita’ in Harmony)
- Catalogo dei servizi cloud qualificati, passato da AGID ad AC N, ad oggi non visibile https://catalogocloud.agid.gov.it/
- Idea di costruire una policy che ricalchi quella per la qualificazione dei servizi cloud per la PA
- Ma prima di tutto e’ necessario classificare i dati -> Data classification policy