WORKSHOP GARR 2024

NET MAKERS

Sopravvivere alla bulimia normativa sulla sicurezza informatica: la NIS2 e la legge 90 nell'INFN

Luca G. Carbone

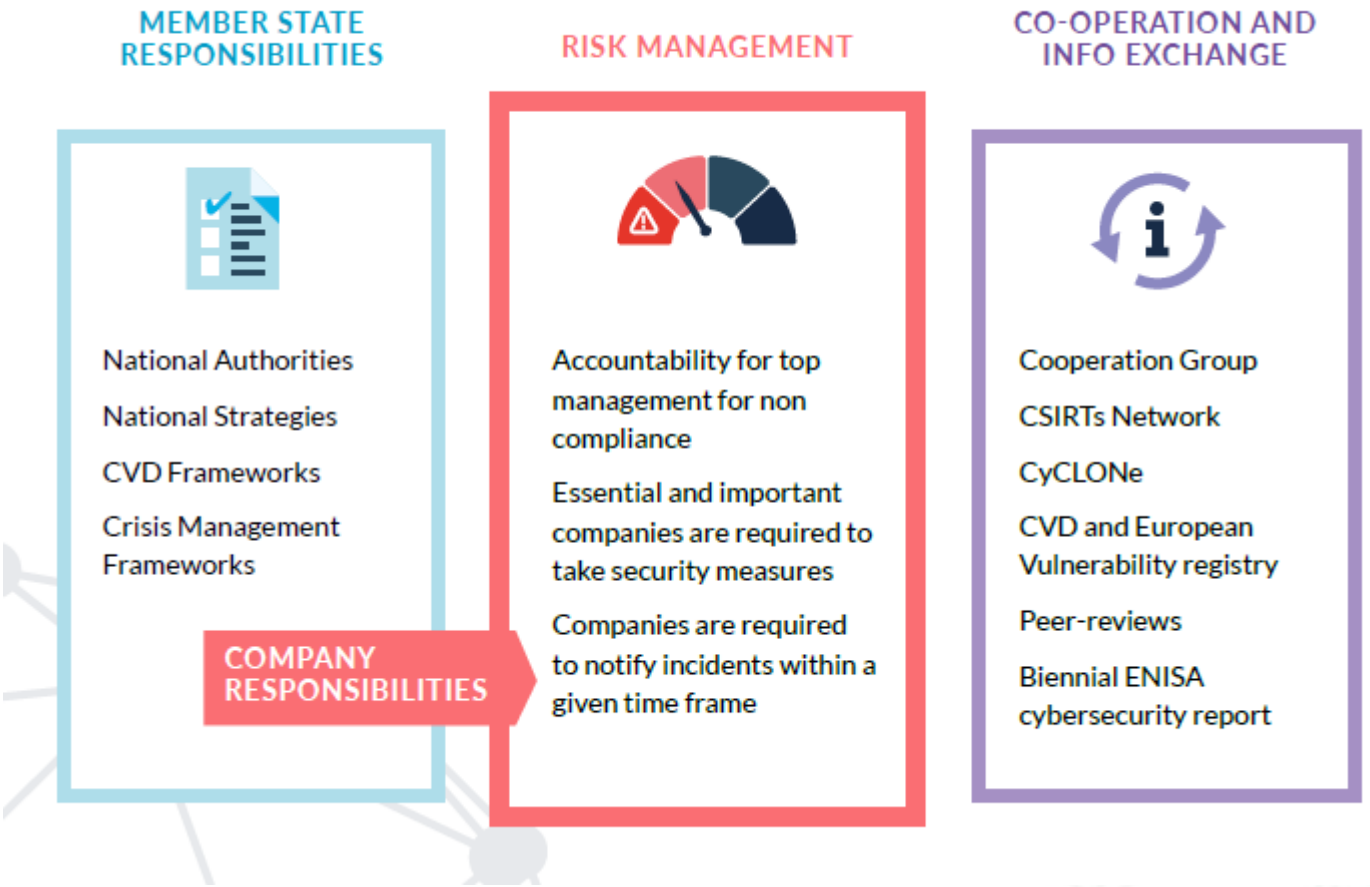
INFN – NUCS

INFN NUCS Istituto Nazionale di Fisica Nucleare NUcleo CyberSecurity

Domande a: wooclap.com e codice WSGARR24

La NIS2

- This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union; to that end, this Directive lays down:
  - obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
  - cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
  - rules and obligations on cybersecurity information sharing;
  - supervisory and enforcement obligations on Member States



Risk Management Measures

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

All measures must:

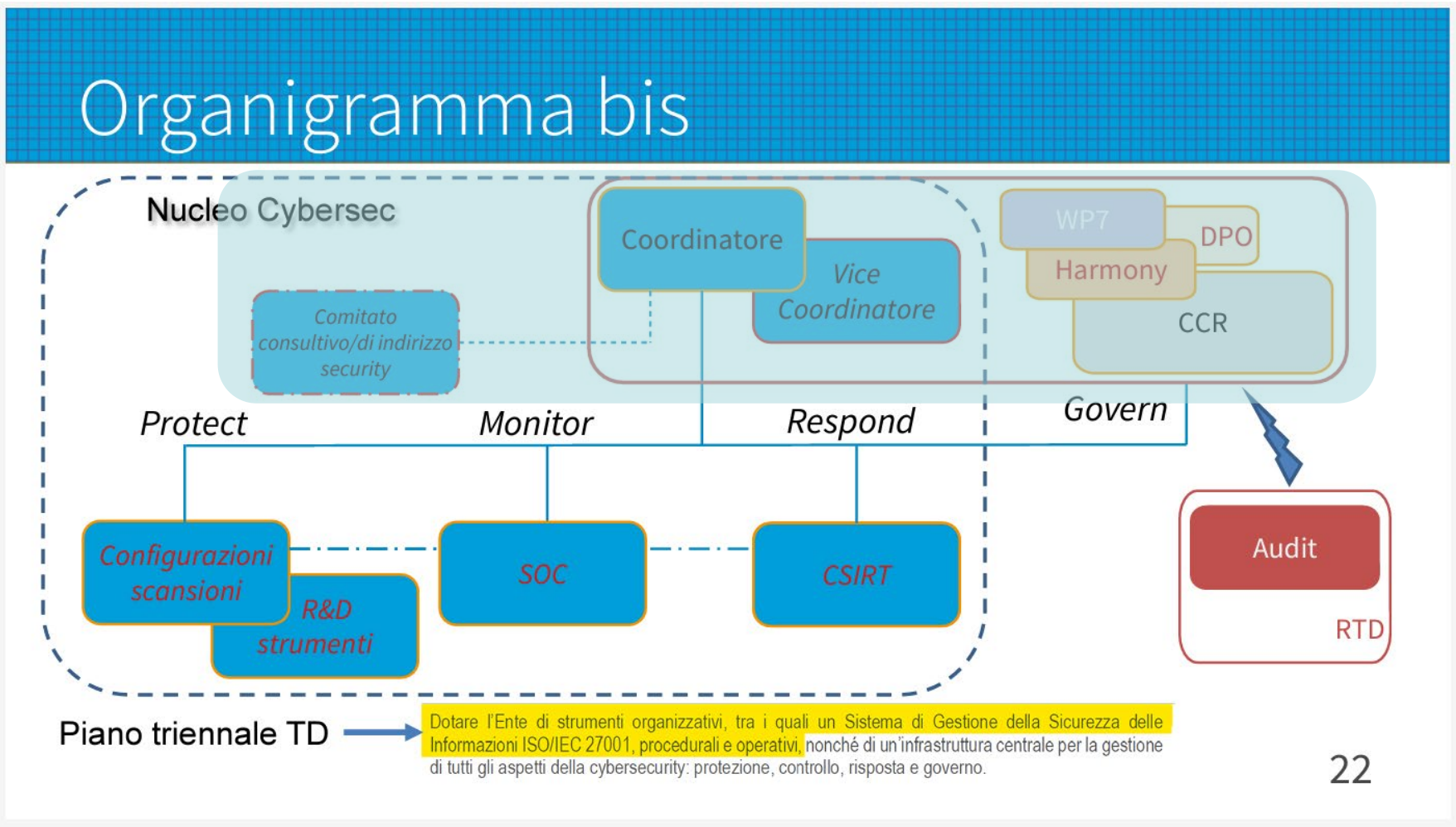
- be proportionate to risk, size, cost, and impact & severity of incidents
- take into account the state-of-the-art, and where applicable relevant European and international standards

EU can:

- carry out risk assessments of critical ICT services, systems or supply chains
- impose certification obligations
- adopt implementing acts laying down technical requirements

Quasi tutte queste misure sono mappabili su controlli della ISO 27001:2022 (c'è chi l'ha già fatto) o del Cybersecurity framework del NIST: l'occasione è propizia per valutarne l'adozione.

INFN NUCS (da kickoff WS 02/2023 – in corso d'opera…)



La funzione GOVERN (provvidenzialmente introdotta dalla II versione del framework del NIST) è prevista ma coinvolge solo figure tecniche e non è mai stata ufficialmente formalizzata: la NIS2 ci offre l'opportunità di implementarla allargandone la partecipazione, come richiesto, al management dell'ente.

Risk Management Measures nell'INFN

Piano di gestione del rischio informatico (da estendere con tool AGID/ACN – approccio multirischio) – WG Scansioni

INFN CSIRT (TI Listed), WG SOC & EDR

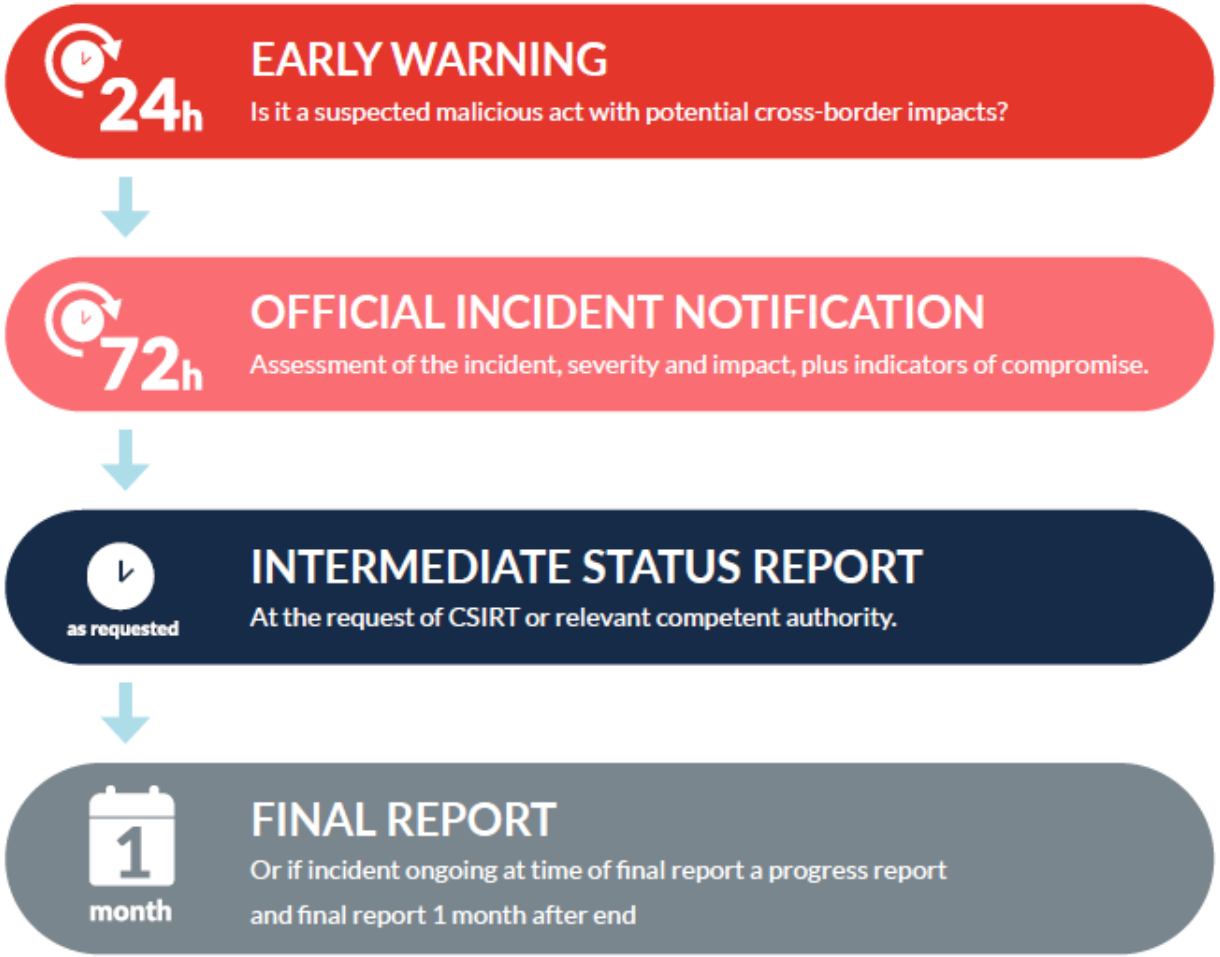
Misure Minime AGID (eventualmente adottando quelle di più alto livello); AUDIT interni

WG Scansioni: Linee guida AGID su SSL/TLS e HTTPS,SSH hardening. ***Crittografia MAIL?***

Dispiegamento 2FA iniziato (WG AAI); NUCS (CSIRT e SOC), DPO. AAI dispongono di canali di comunicazione OOB di emergenza

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

(significant) Incident Notification/Reporting

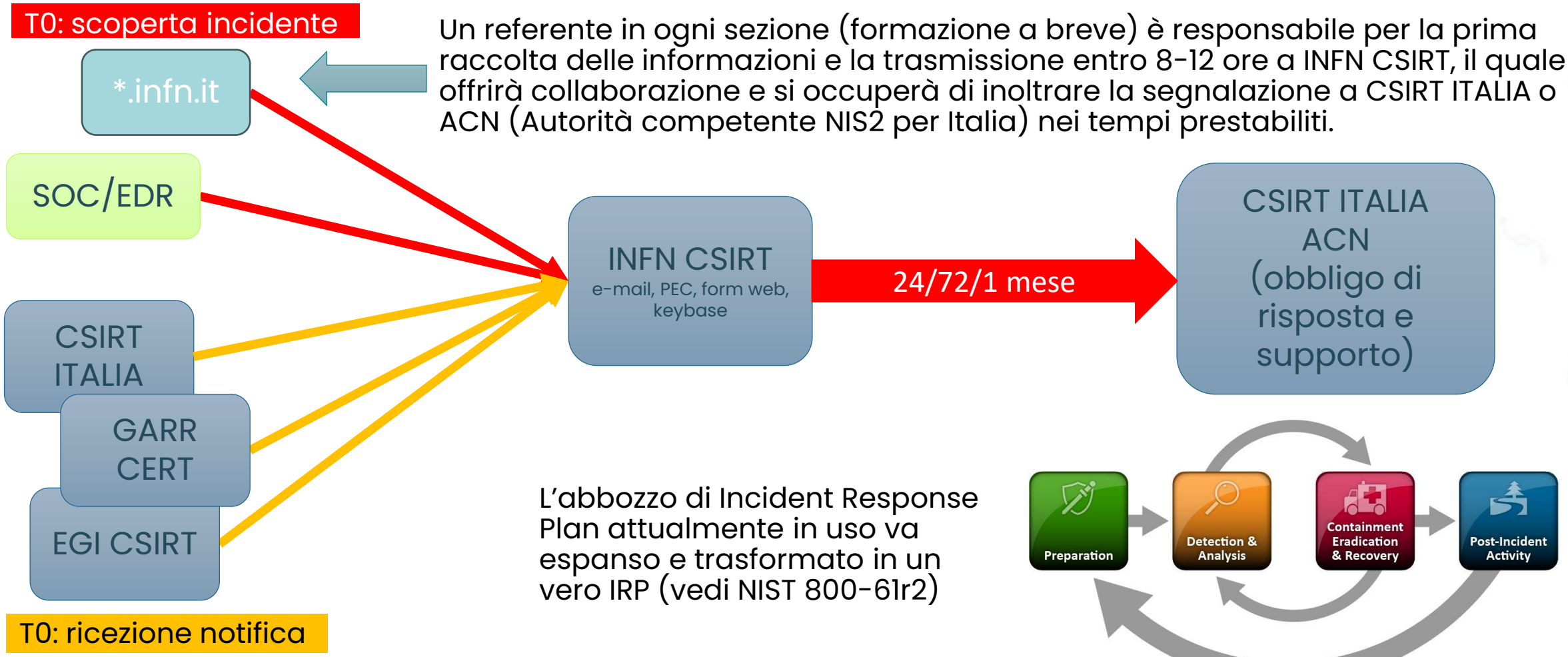


Article 23

...

3. An incident shall be considered to be **significant** if:
   a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
   b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Incident reporting nell'INFN



Un referente in ogni sezione (formazione a breve) è responsabile per la prima raccolta delle informazioni e la trasmissione entro 8-12 ore a INFN CSIRT, il quale offrirà collaborazione e si occuperà di inoltrare la segnalazione a CSIRT ITALIA o ACN (Autorità competente NIS2 per Italia) nei tempi prestabiliti.

L'abbozzo di Incident Response Plan attualmente in uso va espanso e trasformato in un vero IRP (vedi NIST 800-61r2)

Last but not least: Management responsibilities

Approve the adequacy of the cybersecurity risk management measures taken by the entity;

Supervise the implementation of the risk management measures;

Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity

Offer similar training to their employees on a regular basis;

Be accountable for the non-compliance

NIS2 porta la gestione della sicurezza informatica fuori dall'ambito più strettamente tecnico per farla entrare nella C-suite (CEO, …) e renderla quindi ***una funzione attiva e strategica*** dell'ente; la formazione specifica in ambito di gestione del rischio per il management diventa un obbligo.

Gli stati membri possono imputare responsabilità personali agli organismi di gestione e, in caso di palesi non conformità in entità essenziali, comminare sanzioni o imporre divieti temporanei all'esercizio delle funzioni dirigenziali.

Possibile scenario: mancata (o ritardata) somministrazione di formazione sulle minacce derivanti dal social engineering in presenza di un rischio conclamato di phishing.

Management responsibilities nell'INFN (*si parte da zero*)

Attività propedeutiche:

- Rapporto CLUSIT: presentazione ufficiale ad hoc
- The Trusted CI Framework

Four Pillars. Sixteen Musts. An Architecture for Cybersecurity Programs

Mission Alignment

Governance

Resources

11. Organizations must devote **adequate resources** to address unacceptable cybersecurity risk.
12. Organizations must establish and maintain a cybersecurity **budget**.
13. Organizations must allocate **personnel** resources to cybersecurity.
14. Organizations must identify **external cybersecurity resources** to support the cybersecurity programs.

Controls

15. Organizations must adopt and use a **baseline control set**.
16. Organizations must select and deploy **additional and alternate controls** as warranted.

The Trusted CI Framework is structured around **4 Pillars** which make up the foundation of a competent cybersecurity program: **Mission Alignment, Governance, Resources, and Controls**.
Composing these pillars are **16 Musts** that identify the concrete, critical requirements for establishing and running a competent cybersecurity program.

TODO: Formazione su Risk Assessment

Timeline

FEBBRAIO 23 - METÀ OTTOBRE 24

Recepimento

Avvio di alcuni tavoli settoriali
7 agosto 2024: adozione definitiva in CDM
1° ottobre 2024: pubblicazione in Gazzetta Ufficiale
16 ottobre 2024: entrata in vigore

METÀ OTTOBRE 24 – METÀ APRILE 25

Prima fase attuativa

Avvio formale di tutti i tavoli settoriali
Entro febbraio 2025: censimento e registrazione dei soggetti
Entro marzo 2025: adozione dell'elenco dei soggetti NIS
Entro aprile 2025: notifica ai soggetti NIS
Entro aprile 2025: elaborazione e adozione obblighi di base

METÀ APRILE 25 – METÀ APRILE 26

Seconda fase attuativa

Monitoraggio e supporto
A partire da gennaio 2026: obbligo di notifica di base
Entro aprile 2026: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
Entro aprile 2026: elaborazione e adozione degli obblighi a lungo termine
Entro settembre 2026: completa implementazione delle misure di sicurezza di base

DA METÀ APRILE 26

Terza fase attuativa

Categorizzazione delle attività e dei servizi
Implementazione degli obblighi a lungo termine

Legge 28/6/2024, n. 90

Art. 1

Obblighi di notifica di incidenti

1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le citta' metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonche' le societa' di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le societa' di trasporto pubblico extraurbano operanti nell'ambito delle citta' metropolitane e le aziende sanitarie locali segnalano e notificano, con le modalita' e nei termini di cui al comma 2 del presente articolo, gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresi' comprese le rispettive societa' in house che

Introduce in forma assai poco leggibile (*comme d'habitude*) requisiti per le PA molto simili a quelli della NIS2, e non si lascia sfuggire l'occasione per inasprire alcune pene. A prima vista tradisce un po' lo spirito della NIS2, ma a una lettura più attenta si rivela quasi complementare a essa - sembra pensata essenzialmente per inquadrare le attività di cybersecurity in un contesto organizzativo compiutamente definito.

Ci riguarda?

L' art.1, comma 3, legge 31/12/2009, n. 196 rimanda alla *ricognizione delle amministrazioni pubbliche (...) operata annualmente dall'ISTAT con proprio provvedimento e pubblicata nella Gazzetta Ufficiale entro il 30 settembre* (di ogni anno).

Enti e Istituzioni di ricerca

Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile – ENEA
Agenzia spaziale italiana – ASI
Area di Ricerca Scientifica e Tecnologica di Trieste – Area Science Park
Consiglio nazionale delle ricerche – CNR
Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria – CREA[17]
Elettra Sincrotrone Trieste S.c.p.a.
Fondazione Centro ricerche marine
Fondazione Human Technopole
Fondazione Istituto italiano di tecnologia – IIT
Istituto italiano di studi germanici
Istituto nazionale di alta matematica "Francesco Severi" – INDAM
Istituto nazionale di astrofisica – INAF
Istituto nazionale di documentazione, innovazione e ricerca educativa – INDIRE
Istituto nazionale di fisica nucleare – INFN
Istituto nazionale di geofisica e vulcanologia – INGV
Istituto nazionale di oceanografia e di geofisica sperimentale – OGS
Istituto nazionale di ricerca metrologica – INRIM
Istituto nazionale di statistica – ISTAT
Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione – INVALSI
Istituto nazionale per l'analisi delle politiche pubbliche – INAPP
Istituto Pasteur Italia – Fondazione Cenci Bolognetti
Istituto superiore di sanità – ISS
Istituto superiore per la protezione e la ricerca ambientale – ISPRA
Museo storico della fisica e Centro studi e ricerche Enrico Fermi
Stazione zoologica Anton Dohrn di Napoli

Definizione di incidente

- **Legge 28 giugno 2024, n. 90, art. 1**: *(…) incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge, aventi impatto su reti, sistemi informativi e servizi informatici.*
  - **Decreto-legge [illegible] settembre 2019, n. 105, art. 1, comma 3-bis**: *[illegible]ti di cui al comma 2-bis notificano gli incidenti di cui all'articolo 1, comma 1, lettera h), del [illegible]to di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, aventi impatto su reti, (…)*
    - ~~**Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, art. 1, comma 1, lettera h):** *[Ai fini del presente decreto si intende per:] incidente, ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici;*~~

Abrogato da art. 43, comma 2 del DL applicativo della NIS2 per assicurare la coerenza con gli obblighi da essa imposti (*fondamentale il confronto con Ufficio Legale INFN*) – è lecito attendersi che anche ACN elabori prima o poi un criterio di significatività per gli incidenti informatici (da NCSC IE):

Significant Incidents

- *'incident' means an event compromising the **availability**, **authenticity**, **integrity** or **confidentiality** of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;*
- *Guidance on how to determine a significant incident will be provided (e.g a total outage of the service for >10 mins, or more than 5% of users cannot access the service for more than an hour etc.).*
- *Sector and organisation specific context is very important. If in doubt – report.*
- *"Initial Assessment: Importance of system affected to service, severity and technical characteristics of the cyber threat and underlying vulnerabilities that are exploited."*

Obblighi di notifica e sanzioni

- Una prima segnalazione deve avvenire senza ritardo e comunque entro il termine massimo di **ventiquattro ore** dal momento in cui ne sono venuti a conoscenza;
- entro **settantadue ore** dal medesimo momento dovrà avvenire la notifica completa di tutti gli elementi informativi disponibili.

Sia la segnalazione sia la notifica completa dovranno avvenire utilizzando le procedure disponibili sul sito internet dell'Agenzia per la cybersicurezza nazionale.

In caso di inosservanza degli obblighi di segnalazione sono previste sanzioni (da 25k a 125k) e ispezioni volte a verificare l'attuazione degli interventi di rafforzamento della loro resilienza rispetto al rischio di incidenti, siano detti interventi direttamente indicati dall'Agenzia ovvero previsti da apposite linee guida adottate dall'Agenzia.

La violazione può comunque anche costituire causa di responsabilità disciplinare e amministrativo-contabile nei confronti dei funzionari e dei dirigenti responsabili.

Il management non viene esplicitamente coinvolto nella gestione della cybersecurity ma può essere ritenuto responsabile di violazioni e inadempienze.

Rafforzamento della resilienza delle PA e referente unico per la cybersicurezza

Le PA tenute alle segnalazioni, ove già non presente, individuano una **struttura**, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede:

a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;
b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;
d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;
e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);
f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

All'interno di tale struttura opera un **referente** (NdA: ***FISICO***), individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza, che svolge la funzione di **punto di contatto unico dell'amministrazione con l'ACN** alla quale deve essere riferito il relativo nominativo.

La struttura per la cybersicurezza e il referente per la cybersicurezza possono essere individuati nell'ufficio e nel responsabile per la transizione al digitale.

CF, estremi CI, contatti etc.

WORKSHOP GARR 2024

NET MAKERS

La legge 90 è già in vigore ed è parzialmente sovrapponibile alla NIS2: orientarsi in questa selva di norme sta iniziando a diventare impegnativo, per la qual cosa, e per evitare che l'entropia cresca a dismisura, è fondamentale il confronto costante con gli Uffici Legali. Fare rete (e massa critica) per elaborare soluzioni standard, comuni e condivise (e magari offrire spunti in merito ad ACN) potrebbe diventare molto importante.

Riferimenti: *ENISA, NCSC IE, ACN IT, Portale NORMATTIVA, TRUSTED CI*

Luca G. Carbone <carbone@infn.it>