SECURITY SUMMIT

Security Summit

Verona 15 ottobre 2025

Clusit 25th 2000-2025

ASTREA

ANSIA DA NIS2: PROVIAMO AD AFFRONTARLA SEMPLIFICANDO…

Alessio Pennasilico| CS Clusit
Bruno Giacometti | CEO & Founder, Axsym
Claudio Canepa | Information Security Advisor, *Axsym*

AXSYM
Compliance & Information Security

Alessio Pennasilico

Partner, Practice Leader Information & Cyber Security Advisory Team P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico Clusit

Membro del Comitato Direttivo di Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema. kiwa intertek

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano osservatori.net digital innovation

Bruno Giacometti
CEO & Founder, Axsym

Bruno Giacometti è attivo nel settore della sicurezza informatica dal **1996**.

Dopo aver fondato e guidato IFInet, uno dei **primi Managed Security Provider** in Italia, nel 2017 ha creato **Axsym**, società specializzata in **consulenza e formazione sulla governance e compliance della sicurezza IT**.

Oggi è **CEO** e **responsabile dello sviluppo della piattaforma GRC ATENA Governance**, tra le principali soluzioni italiane per la gestione di rischio, compliance e sicurezza.

Con una lunga esperienza manageriale, affianca le aziende nella **definizione e implementazione di strategie per il miglioramento continuo della loro postura di sicurezza**, sia dal punto di vista tecnico sia organizzativo.

Claudio Canepa

Senior IT & Information Security Advisor, ISO/IEC 27001 Auditor, Axsym

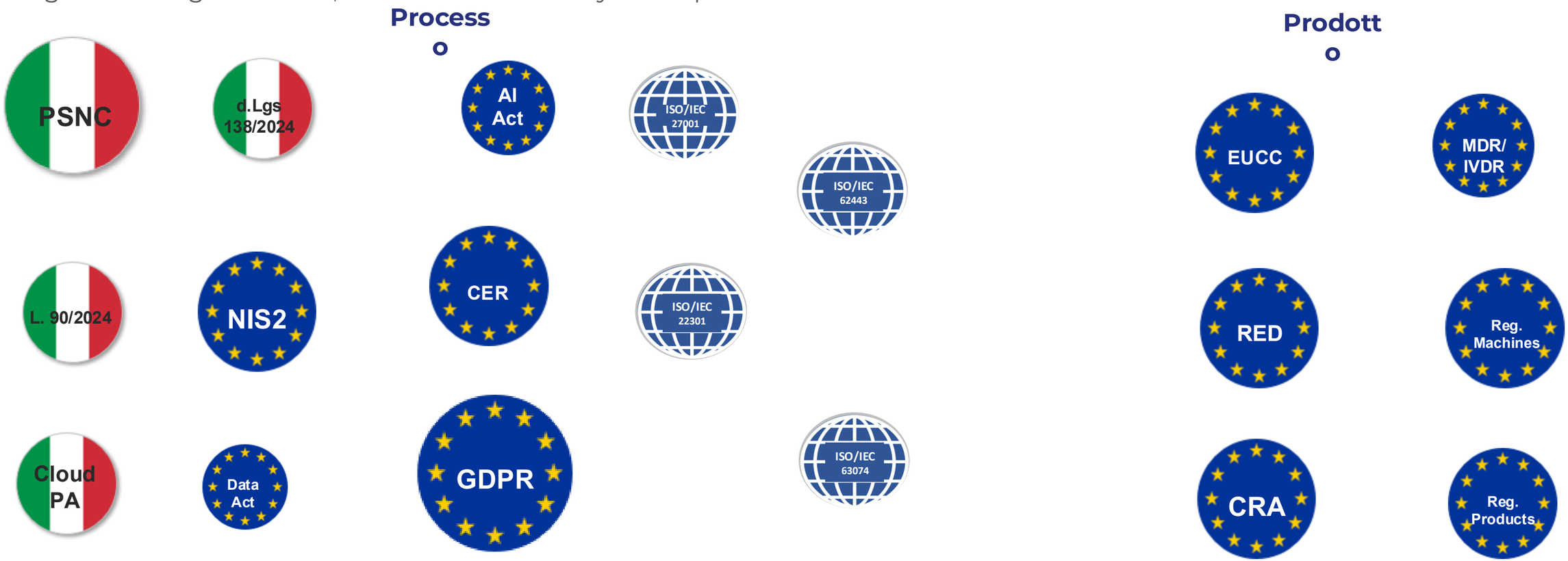
Professionista certificato in ambito **Information Security, Audit dei sistemi informativi e Governance IT**. Le sue competenze in tali ambiti sono ampiamente dimostrate nella sua più che trentennale esperienza come **Chief Information Officer** in una realtà produttiva italiana leader mondiale nel proprio settore.
Negli ultimi 8 anni ha ricoperto anche il ruolo di CISO, ottenendo la certificazione **ISO27001** per una Business Unit rilevante dell'azienda.

È **Lead Auditor** qualificato per la norma ISO/IEC 27001:2022.

Dal 2023 è **Senior Information Technology & Security Advisor presso Axsym**, azienda specializzata in attività di consulenza e formazione in tema Information Security Governance e Compliance (Standard ISO es. 27001, 20000, 22301 e GDPR).

Evoluzione normativa

Queste normative e standard presentano dei fattori comuni come la conduzione di valutazioni del rischio, la formazione interna in materia di cybersecurity,
la gestione degli incidenti, la business continuity e la supervisione dei fornitori.



Clusit 25 2000-2025
SECURITY SUMMIT
AXSYM Compliance & Information Security

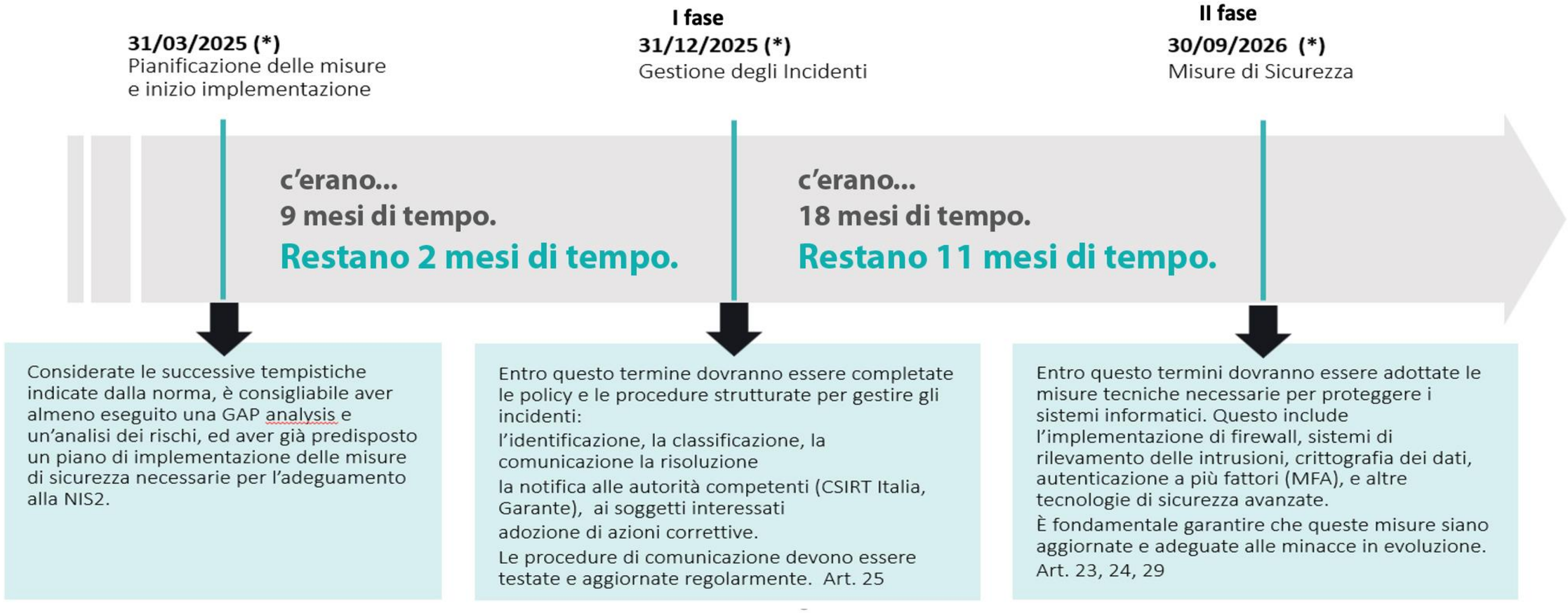
Cosa chiede il mercato?

#iosonopreoccupato

Direttiva (UE) 2022/2555 – NIS 2

D.Lgs. n.138 del 4 settembre 2024
(Recepimento Direttiva NIS2)
pubblicato in Gazzetta Ufficiale il 1 ottobre 2024

Tempi di implementazione e adeguamento



Clusit 25 2000-2025
SECURITY SUMMIT
AXSYM Compliance & Information Security

Determina ACN n.333017 del 19.09.2025: istituisce la figura del «Referente CSIRT» (+ «n» sostituti) da designare a cura del Punto di Contatto nella Piattaforma ACN fra il 20 novembre e il 31 dicembre 2025. Il Referente CSIRT e i sostituti saranno gli interlocutori del CSIRT per la notifica degli incidenti e dovranno possedere almeno competenze di base in materia di sicurezza informatica e di gestione di incidenti informatici, nonché una conoscenza approfondita dei sistemi informativi e di rete del soggetto per conto del quale operano

Obbligo di notifica degli incidenti

Un nuovo adempimento essenziale previsto dalla Direttiva NIS2 è **l'obbligo di notifica degli incidenti** all'autorità competente interessata o al CSIRT (Computer Security Incident Response Team) secondo le [illegible]mpi di svolgimento.

1ª fase: Entro 24 ore

Allerta precoce (o "preallarme") entro 24 ore dalla conoscenza dell'incidente

2ª fase: Entro 72 ore

Notifica ufficiale dell'incidente entro 72 ore dalla conoscenza dell'incidente, aggiornando le informazioni del preallarme. La segnalazione deve prevedere una **valutazione dell'incidente, della gravità, dell'impatto e indicatori di compromissione**

3ª fase: A richiesta

Se richiesto dal CSIRT o dall'autorità competente interessata, sarà necessario fornire a richiesta e nei tempi indicati un rapporto sullo stato intermedio di gestione dell'incidente

4ª fase: Entro 1 mese

Entro 1 mese dalla conoscenza dell'incidente sarà necessario trasmettere un **rapporto finale** completo del **contenuto minimo** indicato dal legislatore.

Misure di sicurezza e requisiti definiti da ACN

Nel dichiarare i requisiti minimi la direttiva NIS2 non dice alle aziende come implementarli ma sottolinea l'importanza di adottare le best practice e standard riconosciuti sviluppati proprio ai fini della sicurezza delle informazioni e cybersecurity.

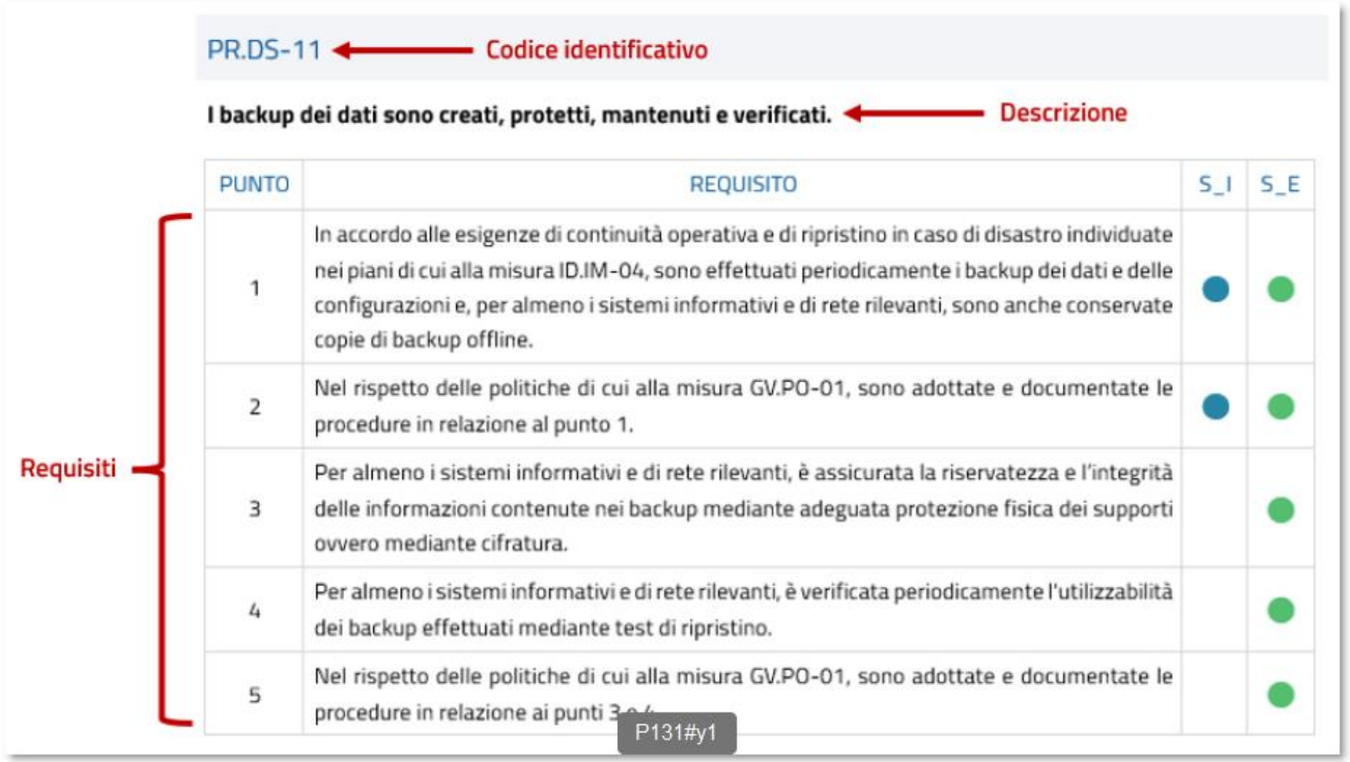
In Italia, ACN ha definito una serie di misure di sicurezza «di base» da adottare entro il 30.09.2026 e collegate al **Framework Nazionale per la Cybersecurity e Data Protection v2.1** (Edizione 2025) costituite da:

116 requisiti per i soggetti Essenziali (87 per i soggetti Importanti)
43 misure di sicurezza per i soggetti Essenziali (37 per i soggetti Importanti)

Il Framework Nazionale (**FNCDP v2.1**) è una rielaborazione del NIST CSF v2.0 costituito da 115 subcategorie (controlli)
Le misure di sicurezza definite da ACN corrispondono ad altrettanti controlli del FNCDP (quindi fanno riferimento a circa 1/3 dei controlli previsti dal framework completo)

In caso di verifiche, ACN fa riferimento allo schema FNCDP v2.1
Nel 2026 è prevista la definizione di ulteriori misure di sicurezza / requisiti

Esempio di misura di sicurezza (= controllo FNCDP v2.1) e requisiti per soggetti Essenziali e Importanti)



PR.DS-11 ← Codice identificativo

I backup dei dati sono creati, protetti, mantenuti e verificati. ← Descrizione

Requisiti

PUNTO	REQUISITO	S_I	S_E
1	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●

P131#y1

Il cerchio pieno di colore blu nella colona S_I indica che il corrispondente requisito si applica ai soggetti importanti e Il cerchio pieno di colore verde nella colona S_E indica che il corrispondente requisito si applica ai soggetti essenziali.

Fonte:
ACN
Linee Guida NIS
Specifiche di base
Guida alla lettura
Settembre 2025

Clusit 25 2000-2025
SECURITY SUMMIT
AXSYM Compliance & Information Security

Corrispondenza fra misure di sicurezza ACN (= Controlli FNCDP v2.1) e misure di sicurezza indicate dalla Direttiva NIS2 (rif. art. 24 c.2 D.Lgs.138/2024)

Appendice A – corrispondenza elementi misure

La seguente tabella riporta la mappatura tra le misure di sicurezza di base e gli elementi di cui all'articolo 24, comma 2 del decreto NIS.

Elemento decreto NIS	Codice misura di sicurezza
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;	GV.OC-04, GV.RM-03, GV.RR-02, GV.PO-01, GV.PO-02, ID.RA-05, ID.RA-06.
b) Gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26.	PR.PS-04, DE.CM-01, DE.CM-09, RS.MA-01, RS.CO-02.
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi.	ID.IM-04, PR.DS-11, RC.RP-01, RC.CO-03.
d) Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.	GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07.
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità.	GV.SC-05, ID.RA-01, ID.RA-08, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-06.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica.	ID.IM-01.
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica.	PR.AT-01, PR.AT-02.
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura.	PR.DS-01, PR.DS-02.
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti.	GV.RR-04, ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-4, PR.AA-01, PR.AA-03, PR.AA-05, PR.AA-06, PR.IR-01.
l) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.	PR.AA-03, PR.DS-02, PR.IR-03.

Fonte:
ACN
Linee Guida NIS
Specifiche di base
Guida alla lettura
Settembre 2025

Clusit 25 2000-2025
SECURITY SUMMIT
AXSYM Compliance & Information Security

Evidenze da fornire, secondo ACN

I soggetti, ai fini dell'attuazione delle misure di sicurezza e dell'attestazione dell'effettiva implementazione delle stesse, devono essere in possesso o provvedere all'elaborazione di una serie di documenti.

A seguire sono riportati i principali documenti richiesti (in corsivo quelli relativi ai soli soggetti essenziali) raggruppati per tipologie:

- **elenchi**: personale dell'organizzazione di sicurezza informatica, configurazioni di riferimento, sistemi ai quali è possibile accedere da remoto;
- **inventari**: apparati fisici, servizi, sistemi e applicazioni software, flussi di rete, servizi erogati dai fornitori, fornitori;
- **piani**: gestione dei rischi, business continuity e disaster recovery, trattamento dei rischi, gestione delle vulnerabilità, adeguamento, valutazione dell'efficacia delle misure di gestione del rischio, formazione in materia di sicurezza informatica, risposta agli incidenti;
- **politiche di sicurezza informatica**: per almeno i requisiti riportati nella tabella 1 in appendice all'Allegato 1, per i soggetti importanti, e all'allegato 2, per i soggetti essenziali, della determina 164179/2025;
- **procedure**: in relazione agli specifici requisiti per i quali sono richieste;
- **registri**: esiti del riesame delle politiche, attività formazione dei dipendenti, manutenzioni effettuate.

Fonte: **ACN**
Linee Guida NIS
Specifiche di base
Guida alla lettura
Settembre 2025

Direttiva NIS2 e standard: ISO 27001 & FNCDP v2.1

Nel dichiarare i requisiti minimi la direttiva NIS2 non dice alle aziende come implementarli ma sottolinea l'importanza di adottare le best practice e standard riconosciuti sviluppati proprio ai fini della sicurezza delle

Lo Standard che copre nel modo più completo i requisiti di sicurezza indicati dalla NIS2 è lo

Standard ISO/IEC 27001:2022

Questo perché lo standard ISO 27001, in linea con quanto richiesto dalla NIS2 prevede:

- Un approccio basato sul rischio
- Lo sviluppo di un **piano di continuità aziendale** (Business Continuity)
- E' l'unico standard certificabile da una terza parte indipendente

Tuttavia, l'Agenzia per la CyberSicurezza Nazionale (ACN) utilizza e riconosce esclusivamente il

Framework Nazionale per la CyberSecurity e la Data Protection (FNCDP) nella versione v2.1 rilasciata ad Aprile 2025

Ne consegue, per le aziende certificate o che hanno comunque adottato il modello ISO27001, la necessità di rimappare i controlli ISO27001 con quelli previsti dal FNCDP v2.1.

Collegamento fra FNCDP v2.1 e ISO/IEC 27001:2022

Per facilitare l'abbinamento fra i controlli/requisiti dei due schemi, è stata pubblicata la
Prassi di Riferimento UNI/PdR 174 del 30/04/2025

«Sistema di gestione per la cybersicurezza e la sicurezza delle informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001 e al Framework NIST CSF 2.0»

approvato anche da ACN (NIST CSF 2.0 -> FNCDP v2.1)

In pratica, le aziende già certificate ISO27001 (o che pensano di certificarsi o quantomeno di adottare tale modello per la gestione dell'Information Security) potranno implementare gli adempimenti NIS2 nei processi e documentazione già presenti nell'ambito dello schema ISO27001, pur con la necessità di abbinarli ai controlli previsti da FNCDP v2.1

Come gestire questo incrocio fra norme e controlli diversificati
e in buona parte sovrapponibili ?

Le grandi aziende sono probabilmente strutturate per gestire molteplici norme e le relative conformità.

La maggior parte delle aziende, tuttavia sono PMI, con ridotte risorse e competenze interne, parzialmente compensate dal ricorso a risorse esterne.

Per tali realtà soggette alla normativa NIS2, questo mix fra:
- misure sicurezza NIS2
- specifiche ACN
- controlli FNCDP v2.1
- requisiti e controlli ISO/IEC 27001:2022
ed in generale il tema della compliance NIS2 si sta rivelando molto ostico e laborioso, spesso accompagnato più dalla preoccupazione di «essere a posto» con gli aspetti formali perdendo di vista l'effettiva implementazione di adeguate misure di sicurezza che rafforzino l'effettiva capacità di gestire i rischi derivanti dalla cybersecurity

I) Semplificando l’approccio alla NIS2 con la metodologia Axsym

L’esperienza sul campo dei consulenti Axsym ha portato alla formulazione di un approccio strutturato alla NIS2 che coniuga i framework standard ISO27001 e FNCDP con i requisiti e le evidenze richiesta da ACN.

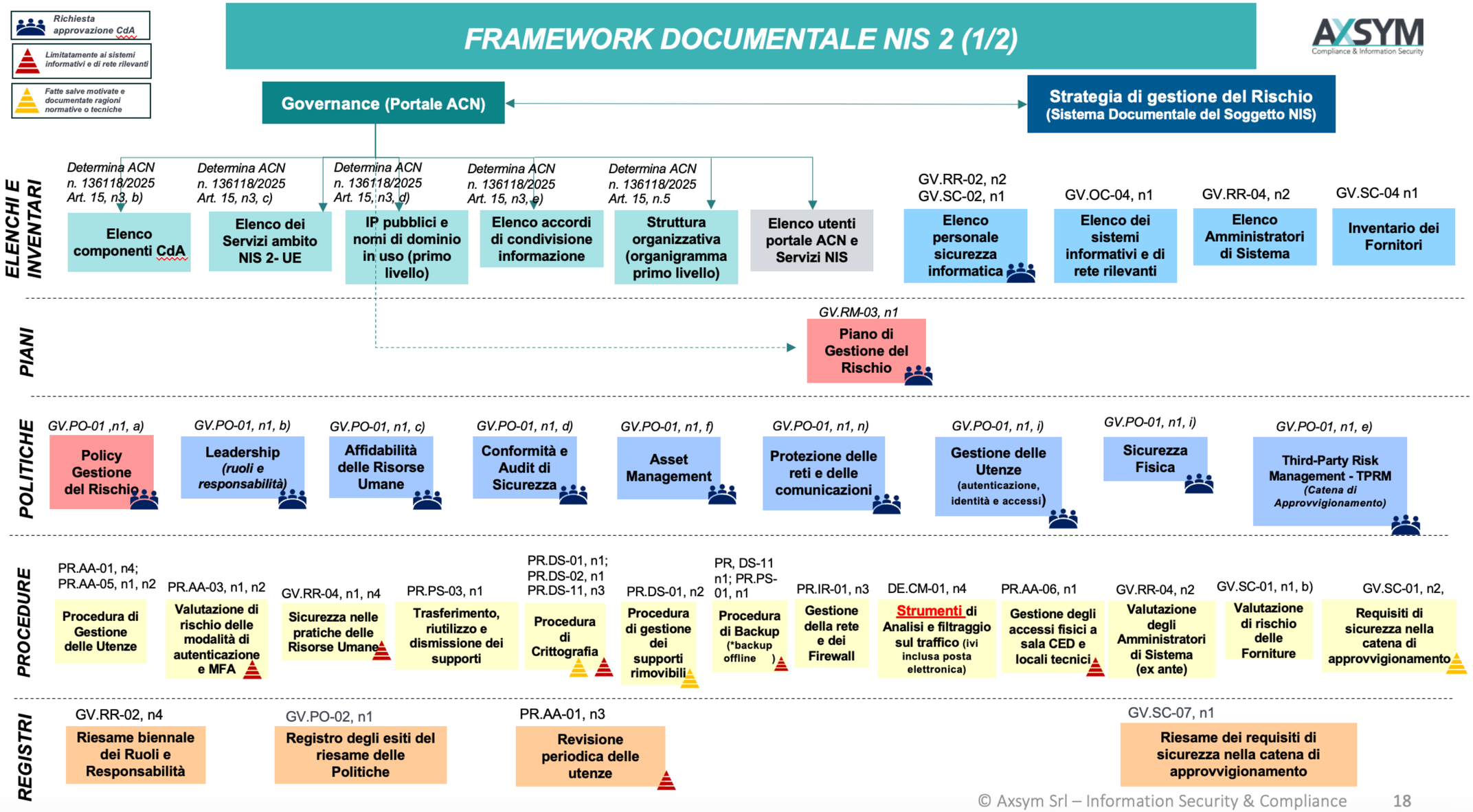
Tale metodologia è stata schematizzata in un «quadro sinottico» che offre una rappresentazione schematica e comprensibile agli adempimenti necessari per gestire la compliance alla normativa NIS2.

Definizione:

Un quadro sinottico (detto anche tavola sinottica o diagramma di classificazione) è una rappresentazione schematica e sintetica di un argomento complesso, organizzato in base a una gerarchia logica, che offre una visione d'insieme degli aspetti fondamentali e delle relazioni tra le varie parti. Si utilizza per rendere comprensibili argomenti difficili, per un confronto rapido e per la gestione efficiente di informazioni in diversi contesti.

L’impianto metodologico è accompagnato dalla fornitura di templates per le varie tipologie di documenti richiesti,
con fornitura di servizi consulenziali a vari livelli e personalizzati sulla base delle esigenze dei Clienti.

FRAMEWORK DOCUMENTALE NIS 2 (1/2)



© Axsym Srl – Information Security & Compliance

Richiesta approvazione CdA

Limitatamente ai sistemi informativi e di rete rilevanti

Fatte salve motivate e documentate ragioni normative o tecniche

FRAMEWORK DOCUMENTALE NIS 2 (2/2)

AXSYM Compliance & Information Security

Strategia di gestione del Rischio
(Sistema Documentale del Soggetto NIS)

ELENCHI E INVENTARI

- ID.AM-01,n1 — **Inventario Apparati Fisici (Hw, inclusi IoT, OT, mobile)**
- ID.AM-02,n1 — **Inventario dei servizi, sistemi e applicazioni (Sw, inclusi open-source)**
- ID.AM-03,n1 — **Inventario dei flussi di rete tra sistemi interni ed esterni**
- ID.AM-04,n1 — **Inventario dei servizi erogati dai fornitori, inclusi cloud**
- PR.AA-01,n1 — **Inventario delle utenze, incluse quelle con privilegi**
- PR.IR-01, n2 — **Elenco dei sistemi e reti con accesso da remoto**

PIANI

- ID.RA-01, n3; ID.RA-08 — **Piano di Gestione delle Vulnerabilità**
- ID.RA-06, n1 — **Piano di Trattamento del Rischio**
- ID.IM-01, n1 — **Piano di Adeguamento degli Interventi**
- ID.IM-01, n3, n1 — **Piano di Valutazione efficacia misure di gestione del rischio** *(KPI e metodi di valutazione)*
- ID.IM-04, n1 — **Piano di Continuità Operativa**
- ID.IM-04, n2 — **Piano di Ripristino dal Disastro**
- ID.IM-04, n3 — **Piano di Gestione della Crisi**
- RS.MA-01, n1; RS.CO-02, n1 RC.CO-03, n1 — **Piano di Gestione degli Incidenti** *(e notifica CSIRT)*
- PR.AT-01, n1 — **Piano di Formazione** *(ivi inclusi CdA)*

POLITICHE

- *GV.PO-01, n1, g)* — **Gestione delle vulnerabilità e patch**
- ID.RA-05,n1 — **Valutazione del Rischio** *(biennale)*
- *GV.PO-01, n1, l)* — **Sicurezza dei dati e dei sistemi**
- *GV.PO-01, n1, m)* — **Sviluppo, Configurazione, Manutenzione e Dismissione dei sistemi**
- *GV.PO-01, n1, 0)* — **Monitoraggio degli eventi di Sicurezza**
- *GV.PO-01, n1, h)* — **Continuità Operativa, Disastro e Gestione delle Crisi**
- *GV.PO-01, n1, 0)* — **Risposta agli incidenti e ripristino**
- *GV.PO-01, n1, k)* — **Formazione del Personale e Consapevolezza**

PROCEDURE

- **Metodologia valutazione dei rischi ????**
- ID.RA-08, n1 — **Monitoraggio canali CSIRT, CERT, ISAC**
- ID.RA-08, n5 — **Monitoraggio delle vulnerabilità (vendor software critico)**
- PR.PS-02, n1, n2, n4 PR.PS-06, n1 — **Gestione sicura del software (sviluppo e acquisto)**
- PR.PS-04, n1, n2, n3 — **Gestione e conservazione dei LOG** (compresi accessi da remoto)
- PR.IR-01, n1 — **Gestione degli accessi da remoto**
- PR.IR-03, n3 — **Gestione dei sistemi di comunicazione e di emergenza**
- DE.CM-01, n1 — **Strumenti di rilevamento degli incidenti (Siem)**
- RS.CO-01, n2 — **Comunicazione degli incidenti al pubblico e gli stakeholder**
- RC.RP-01, n1 — **Risposta e ripristino agli incidenti**
- PR.AT-02, n1; — **Formazione dedicata al personale specializzati**

REGISTRI

- ID.RA-01,n4 — **Relazione attività di Gestione delle Vulnerabilità**
- ID.IM-01, n4 — **Relazione Periodica sul piano di valutazione KPI**
- ID.IM-04, n5 — **Riesame dei piani di continuità, ripristino e gestione della crisi**
- PR.PS-03, n2 — **Registro delle manutenzione HW**
- DE.CM-01, n2 — **Livelli di Servizi Attesi (SL) dei servizi in ambito NIS**
- RS.MA-01, n3 — **Riesame del Piano di Gestione degli Incidenti**
- PR.AT-02, n2 — **Registro formazione** (elenco dipendenti e verifiche svolte

© Axsym Srl – Information Security & Compliance

Clusit 25 2000-2025 SECURITY SUMMIT AXSYM Compliance & Information Security

II) Semplificando l’approccio alla NIS2 con lo strumento: ATENA Governance

La piattaforma GRC:

1. Progettata e realizzata grazie alle **elevate competenze** dei propri consulenti, per affiancare i clienti nelle attività di implementazione e gestione di sistemi di compliance e governance della sicurezza IT
2. Strutturata con una metodologia che consente di **superare il tradizionale approccio basato sull’utilizzo di files Excel e documenti archiviati in modo non strutturato**
3. Pensata come **strumento semplice ed efficace** per supportare tutte le organizzazione nella **gestione della sicurezza delle informazioni**

Cos’è Atena Governance

ATENA Governance è la **piattaforma GRC integrata** che permette di **gestire con un unico strumento** i diversi ambiti di **Governance e Compliance** attraverso i seguenti moduli:

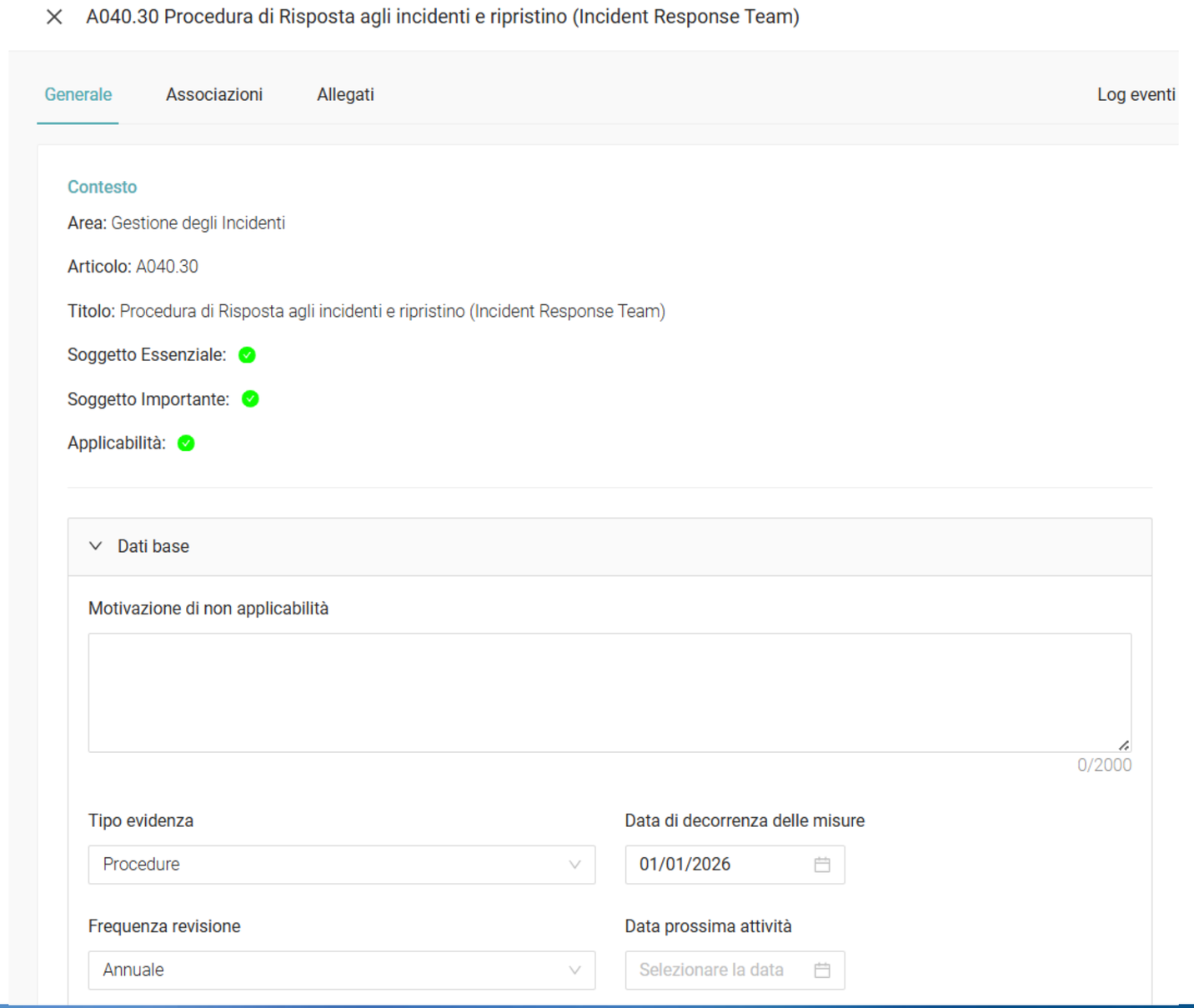
- GDPR
- NIS 2
- Business Impact Analysis
- Risk Assessment
- ISO 27001
- Cyber Security Framework FNCDP, NIST, CIS
- Incidenti di Sicurezza, Evidenze, KPI
- Audit e Action Plan

Semplificare l’approccio alla NIS2: sinottico – vista globale

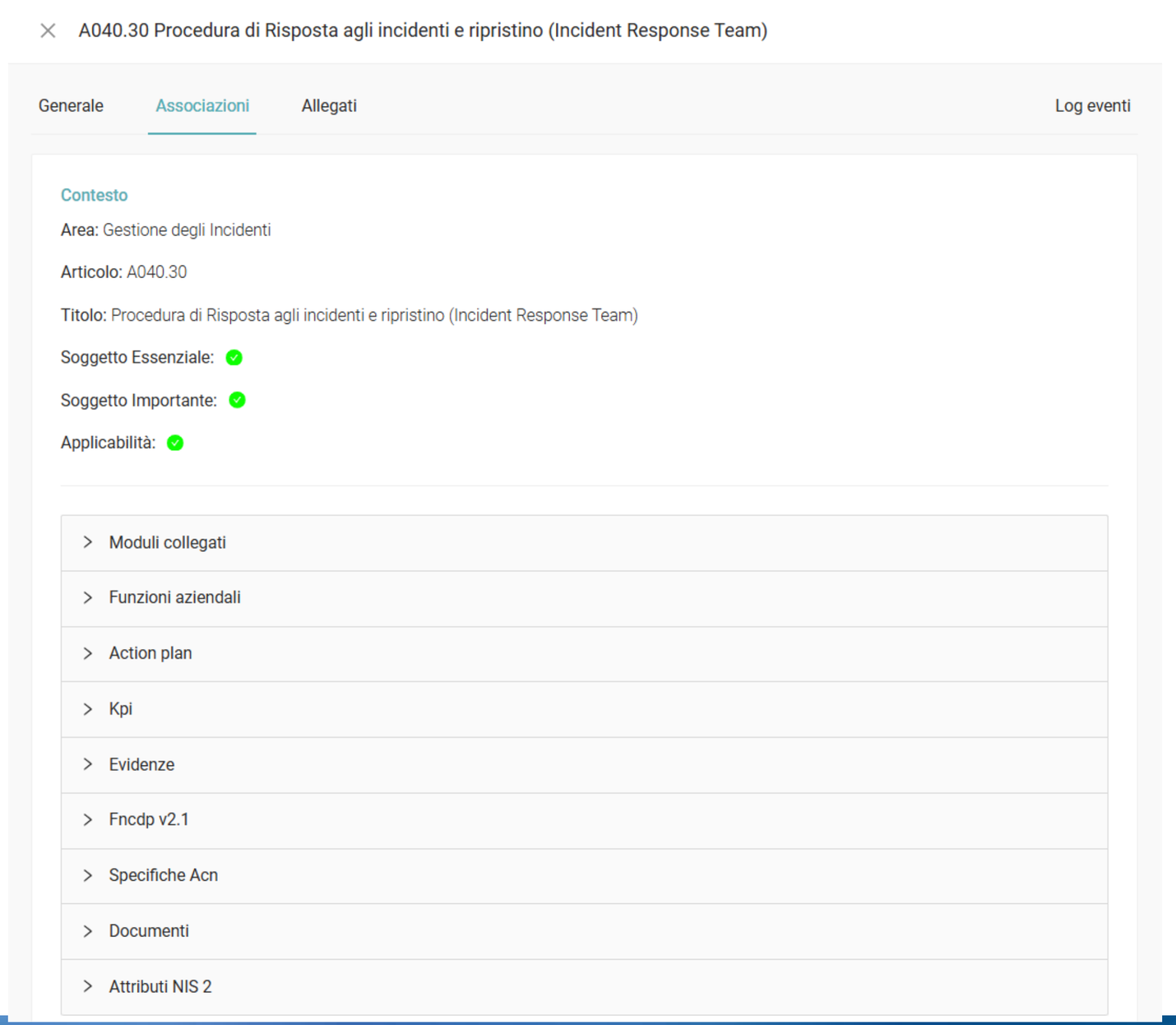
Home | Direttiva Nis2 | GAP Analysis | Sinottico

Società	ID	Elemento	s. Essenziale	s. Importante	Applicabilità
> Organizzazione e ruoli (5)					
> BIA - Business Impact Analysis (4)					
> Gestione del Monitoraggio Eventi (3)					
v Gestione degli Incidenti (6)					
Generic srl	A040.10	Policy Risposta e Ripristino degli Incidenti di Sicurezza Informatica	✓	✓	✓
Generic srl	A040.20	Piano di Gestione degli Incidenti (e notifica CSIRT)	✓	✓	✓
Generic srl	A040.30	Procedura di Risposta agli incidenti e ripristino (Incident Response Team)	✓	✓	✓
Generic srl	A040.40	Procedura comunicazione degli incidenti al pubblico e gli stakeholder	✓	✓	✓
Generic srl	A040.50	Riesame del Piano di Gestione degli Incidenti	✓	✓	✓
Generic srl	A040.60	Registro incidenti di sicurezza	✓	✓	✓
v Gestione delle Terze Parti (6)					
Generic srl	A050.10	Policy Sicurezza nella Catena di Approvvigionamento	✓	✓	✓
Generic srl	A050.20	Procedura Valutazione di rischio delle Forniture	✓	✓	✓
Generic srl	A050.30	Requisiti di sicurezza nella catena di approvvigionamento	✓	✓	✓
Generic srl	A050.40	Inventario dei Fornitori ICT e/o forniture con potenziali impatti sulla sicurezza dei...	✓	✓	✓
Generic srl	A050.50	Inventario dei servizi erogati dai fornitori, inclusi cloud	✓	✓	✓
Generic srl	A050.60	Riesame dei requisiti di sicurezza nella catena di approvvigionamento	✓	✓	✓

Semplificare l’approccio alla NIS2: sinottico – dettaglio di un elemento



Semplificare l’approccio alla NIS2: sinottico – collegamento con altri moduli



Semplificare l’approccio alla NIS2: gli archivi di base

Tabelle di base presenti nel modulo «Organizzazione» di Atena:

- Dati societari per NIS2 (es. tipo soggetto, punto di contatto e sostituto)
- Funzioni aziendali
- Processi
- Persone
- Asset
- Terze parti (es. fornitori)

Sono a disposizione di tutti i moduli Atena e da essi possono essere estratti vari **Inventari** e **Registri** richiesti da ACN

La documentazione di base (politiche, procedure, piani, istruzioni, etc.) può essere archiviata in modo strutturato nel **Repository Documentale** di Atena, e messa a disposizione di tutti i moduli della piattaforma

I documenti, senza necessità di replicarli, possono essere collegati sia ai singoli controlli dei vari framework (ISO27001, FNCDP, etc.) ma anche direttamente ai singoli elementi del Sinottico per un approccio «fast start»

Conclusioni

- La **Direttiva NIS 2** sta dimostrando di avere un impatto rilevante e crescente su molte aziende, in particolare sulle **PMI**, che spesso faticano a gestirne la complessità operativa e normativa.

- Un'implementazione basata esclusivamente su un approccio **top-down** dei controlli previsti dal FNCDP risulta difficile da applicare e da mantenere nel tempo.

- La nostra metodologia adotta invece un **approccio pragmatico e bottom-up**, che parte dalle azioni concrete da intraprendere per poi collegarle ai relativi schemi di riferimento. Questo consente di rendere la norma più comprensibile e attuabile, pur nel pieno rispetto dei requisiti normativi.

- Tale metodologia è supportata dalla funzionalità **"Sinottico"** integrata nel modulo **NIS2** della piattaforma GRC **ATENA Governance**, che consente di mappare, monitorare e gestire in modo strutturato gli adempimenti previsti.

Q&A

Clusit 25 2000-2025
SECURITY SUMMIT
AXSYM Compliance & Information Security

Contatti:
Tel. 0455118570
info@axsym.it
www.axsym.it

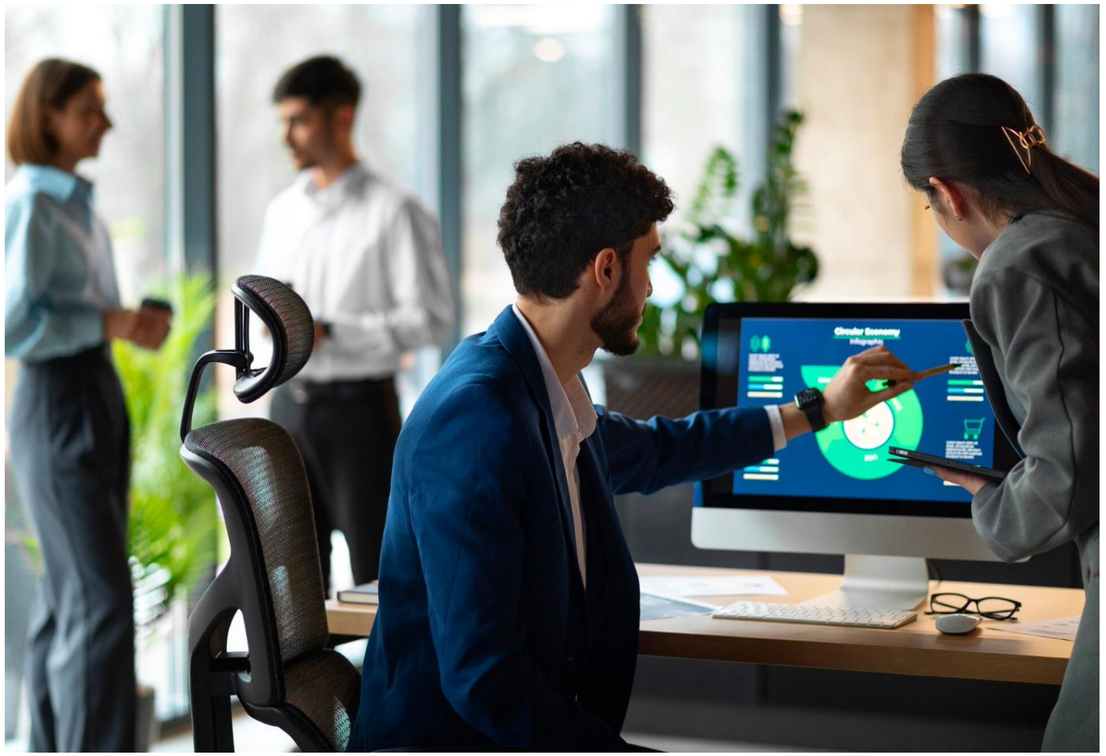
Per informazioni e demo gratuite del software ATENA Governance, vieni a trovarci al nostro desk!

Axsym al tuo servizio

- Siamo un’azienda di **consulenza altamente specializzata** in Information Security Governance, Compliance e Formazione in Cyber Security;

- Proponiamo servizi progettati e implementati **a misura** delle necessità del singolo cliente;

- Il nostro obiettivo primario è accompagnare le organizzazioni nell’implementazione di una **gestione più efficiente, sicura e consapevole delle informazioni** e dei sistemi informatici e di raggiungere una maggiore resilienza a fronte di incidenti di sicurezza IT.



I nostri servizi su misura

CONSULENZA SPECIALIZZATA

FORMAZIONE IN CYBERSECURITY

PIATTAFORMA GRC ATENA GOVERNANCE

Gli ambiti di consulenza Axsym

- Compliance GDPR e Whistleblowing
- Information Security Governance
- Compliance Direttiva NIS 2
- Compliance standard ISO 27001, 22301, 20000
- Framework di Cyber Security CIS, FNCDP, NIST
- Compliance al Cloud ISO 27017, 27018, CSA
- Business Impact Analysis
- Risk Assessment
- Continuità operativa ICT
- Compliance IA ISO 42001

Semplificare l’approccio alla NIS2: Evidenze preconfigurate

Il modulo «Evidenze» fornisce adeguato supporto per documentare l’effettivo adempimento delle misure di sicurezza richieste, e può essere integrato a piacere.

ID elemento	Nome evidenza	Descrizione	Frequenza
A010.30	Segregazione dei ruoli	Matrice RACI Ruoli e Responsabilità (SOD) [NIS2 A010.30]	Biennale
A010.50	Riesame Ruoli e Responsabilità	Riesame periodico Ruoli e Responsabilità: Verbali CdA [NIS2 A010.50]	Biennale
A020.30	Elenco sistemi rilevantI NIS2	Elenco sistemi informativi e di rete rilevanti [NIS2 A020.30]	Annuale
A110.30	Piano Formazione	Piano di Formazione (incluso CdA) [NIS2 A110.30]	Annuale
A130.40	Relazione valutazione KPI	Relazione Periodica sul piano di valutazione KPI [NIS2 A130.40]	Annuale
A140.50	Report utenze inattive	Estrazione utenze inattive da oltre 90gg [NIS2 A140.50]	Trimestrale
A140.60	Revisione periodica utenze	Documentazione/email delle revisioni utenze effettuate [NIS2 A140.60]	Semestrale
A150.40	Verifica supporti rimovibili	Verifica implementazione procedura di gestione dei supporti rimovibili (es. schermate di blocco porte USB, etc.) [NIS2 A150.40]	Annuale
A170.20	Piano di VA/PT	Piano di VA/PT [NIS2 A170.20]	Annuale
A170.40	Relazione di VA/PT	Relazione finale Vulnerability Assessment / Penetration Test effettuati [NIS2 A170.40]	Annuale
A180.30	Elenco sistemi accessibili da remoto	Elenco dei sistemi e reti con accesso da remoto [NIS2 A180.30]	Annuale
A210.70	Riesame BCP/DRP/CMP	Verbali riesame dei piani di continuità, ripristino e gestione della crisi [NIS2 A210.70]	Annuale
A300.10	Riesame delle Politiche	Verbale riesame periodico delle Politiche [NIS2 A300-10]	Annuale

Semplificare l’approccio alla NIS2: ISO/IEC 27001:2022

Home | Requisiti | SoA | Gap analysis | Analisi rischi

Operazioni massive | 30 | Cerca

Capitolo	Titolo capitolo	Sezione	Titolo sezione	Descrizione	Valutazione
4	Context of the organisation	4.1	Organisational context	Determine the organizatio...	Inadeguato
4	Context of the organisation	4.1 (amd1)	Organisational context	The organization shall dete...	Parzialmente adeguato
4	Context of the organisation	4.2 (a)	Interested parties	Identify interested parties i...	Parzialmente adeguato
4	Context of the organisation	4.2 (b)	Interested parties	Determine their informatio...	Parzialmente adeguato
4	Context of the organisation	4.2 (c)	Context of the organization	Describe which of these re...	Inadeguato
4	Context of the organisation	4.3	ISMS scope	Determine and document t...	Parzialmente adeguato
4	Context of the organisation	4.4	ISMS	Establish, implement, main...	Quasi adeguato
5	Leadership	5.1	Leadership & commitment	Top management must de...	Inadeguato
5	Leadership	5.2	Policy	Establish the information s...	Quasi adeguato
5	Leadership	5.3	Organizational roles, responsibilities...	Assign and communicate i...	Inadeguato

Modulo ISO27001:2022: gestione completa dei requisiti e controlli

SOA 1A inizio attività adeg.

Generale | Controlli | Log ev

Stampa | 93 | Cerca

Titolo gruppo	ID	Ref.2013	Descrizione	Incluso	Valutazione
Organizational controls	A.5.1	A.5.1.2 A.5.1.1	Policies for information s...	✓	Inadeguato
Organizational controls	A.5.2	A.6.1.1	Information security roles...	✓	Adeguato
Organizational controls	A.5.3	A.6.1.2	Segregation of duties	✓	Quasi adeguato
Organizational controls	A.5.4	A.7.2.1	Management responsibili...	✓	Quasi adeguato
Organizational controls	A.5.5	A.6.1.3	Contact with authorities	✓	Adeguato
Organizational controls	A.5.6	A.6.1.4	Contact with special inter...	✓	Adeguato
Organizational controls	A.5.7	new	Threat intelligence	✓	Quasi adeguato
Organizational controls	A.5.8	A.6.1.5 A.14.1.1	Information security in pr...	✓	Quasi adeguato
Organizational controls	A.5.9	A.8.1.1 A.8.1.2	Inventory of information ...	✓	Adeguato
Organizational controls	A.5.10	A.8.2.3 A.8.1.3	Acceptable use of inform...	✓	Adeguato
Organizational controls	A.5.11	A.8.1.4	Return of assets	✓	Inadeguato

Semplificare l’approccio alla NIS2: FNCDP v2.1

Dashboard SoA GAP analysis

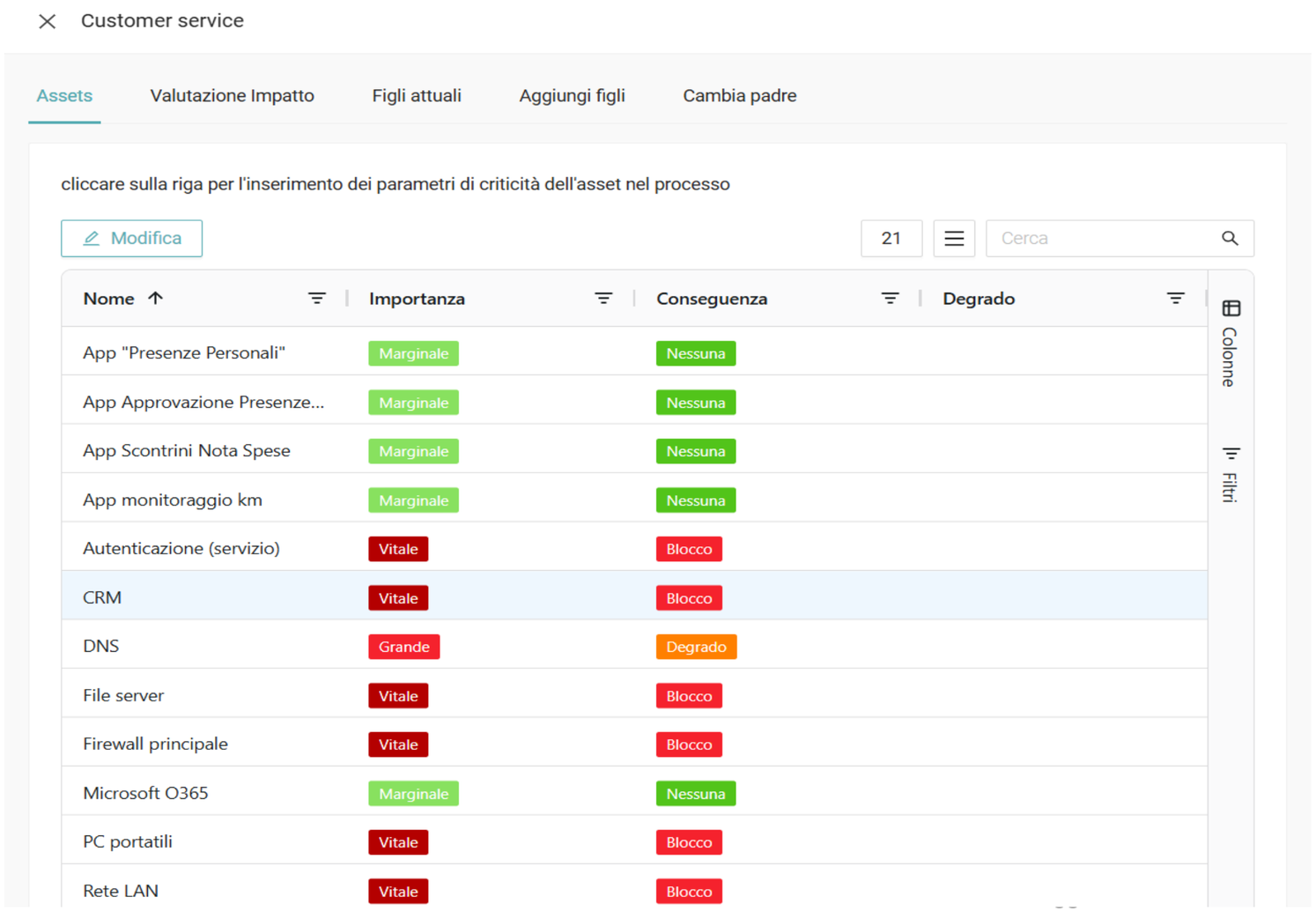
Operazioni massive

115 Cerca

Funzione	ce categ	e contr	Controllo	Maturità	Articolo NIS2
GOVERN	GV.OC	GV.OC-01	La missione dell'organizzazione è compresa e informa la ...	Adeguato	20 21.1
GOVERN	GV.OC	GV.OC-04	Gli obiettivi, le capacità e i servizi critici dai quali gli stake...	Inadeguato	21.2 (a)
GOVERN	GV.RM	GV.RM-01	Gli obiettivi di gestione del rischio sono stabiliti e accettat...	Inadeguato	21.1
GOVERN	GV.RM	GV.RM-03	Le attività e gli esiti della gestione del rischio di cybersec...	Inadeguato	21.2 (a)
GOVERN	GV.RR	GV.RR-02	I ruoli, le responsabilità e i correlati poteri relativi alla gest...	Inadeguato	21.2 (a)
GOVERN	GV.RR	GV.RR-04	La cybersecurity è inclusa nelle pratiche delle risorse uma...	Parzialmente adeguato	21.2 (i)
GOVERN	GV.PO	GV.PO-01	La politica per la gestione del rischio di cybersecurity è st...	Inadeguato	21.2 (a)
GOVERN	GV.PO	GV.PO-02	La politica per la gestione del rischio di cybersecurity è re...	Inadeguato	21.2 (a)
GOVERN	GV.SC	GV.SC-01	Sono stabiliti e accettati dagli stakeholder dell'organizzaz...	Inadeguato	21.2 (d)
GOVERN	GV.SC	GV.SC-02	I ruoli e le responsabilità in materia di cybersecurity per f...	Inadeguato	21.2 (d)
GOVERN	GV.SC	GV.SC-04	I fornitori sono noti e prioritizzati in base alla criticità.	Parzialmente adeguato	21.2 (d)

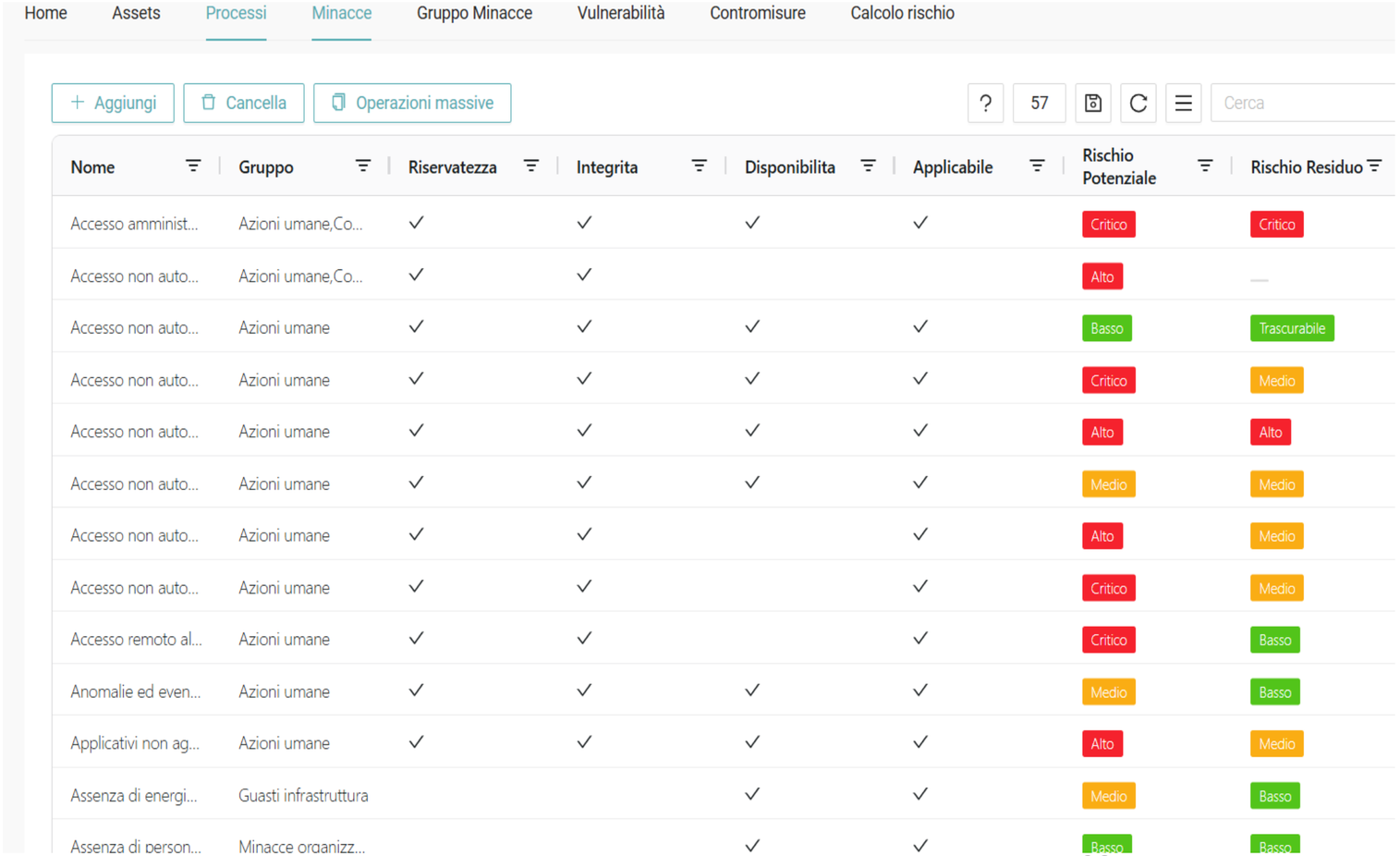
Modulo FNCDP v2.1: gestione completa dei controlli con/senza filtro riferimento NIS2

Semplificare l’approccio alla NIS2: Business Impact Analysis (BIA)



Modulo BIA: processi e criticità degli asset su cui poggiano

Semplificare l’approccio alla NIS2: Risk Assessment



Nome	Gruppo	Riservatezza	Integrita	Disponibilita	Applicabile	Rischio Potenziale	Rischio Residuo
Accesso amminist...	Azioni umane,Co...	✓	✓	✓	✓	Critico	Critico
Accesso non auto...	Azioni umane,Co...	✓	✓			Alto	—
Accesso non auto...	Azioni umane	✓	✓	✓	✓	Basso	Trascurabile
Accesso non auto...	Azioni umane	✓	✓	✓	✓	Critico	Medio
Accesso non auto...	Azioni umane	✓	✓	✓	✓	Alto	Alto
Accesso non auto...	Azioni umane	✓	✓	✓	✓	Medio	Medio
Accesso non auto...	Azioni umane	✓	✓		✓	Alto	Medio
Accesso non auto...	Azioni umane	✓	✓		✓	Critico	Medio
Accesso remoto al...	Azioni umane	✓	✓		✓	Critico	Basso
Anomalie ed even...	Azioni umane	✓	✓	✓	✓	Medio	Basso
Applicativi non ag...	Azioni umane	✓	✓	✓	✓	Alto	Medio
Assenza di energi...	Guasti infrastruttura			✓	✓	Medio	Basso
Assenza di person...	Minacce organizz...			✓	✓	Basso	Basso

Modulo Risk Assessment: minacce e valutazione del rischio

Clusit 25 2000-2025
SECURITY SUMMIT
ATENA

Semplificare l’approccio alla NIS2: modulo Audit

Questionari configurabili per l’audit della supply chain

Modifica gruppo domande

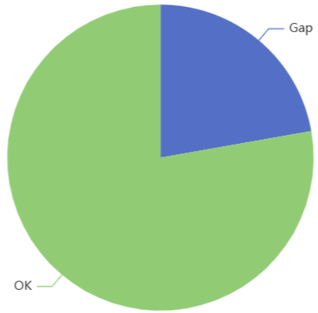
Informazioni generali | Domande | Log eventi

+ Aggiungi | Ordine | Cancella | 4 | Cerca

Ordine	Dipende da	Domanda	Tipologia risposta	Peso	Numero risposte
22		La continuità operativa è assicurata tra...	Singola		3
23		La continuità operativa è assicurata tra...	Singola		3
24		La continuità operativa è assicurata tra...	Singola		3
25		La continuità operativa è assicurata tra...	Singola		3

La continuità operativa è assicurata tramite la ridondanza geografica di tutti i sistemi critici in un sito remoto situato a più di 50 km dal sito primario?

Valutazione audit

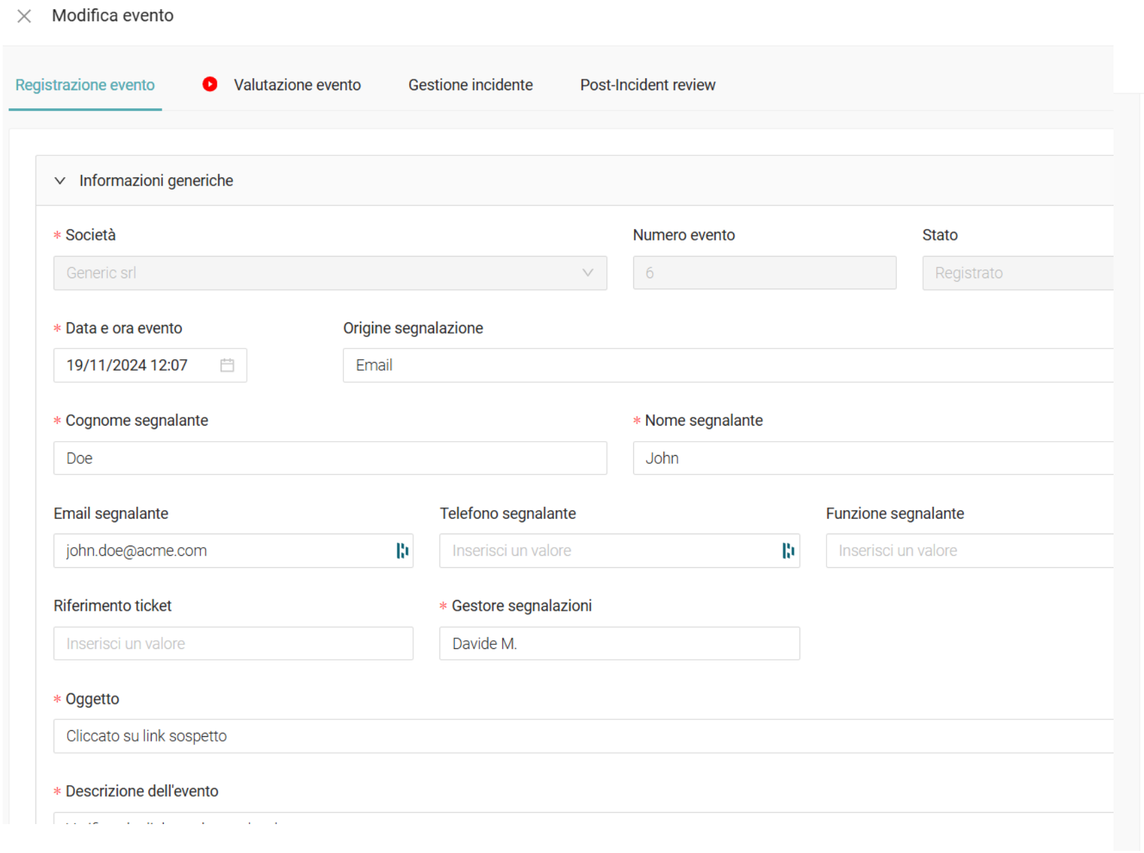


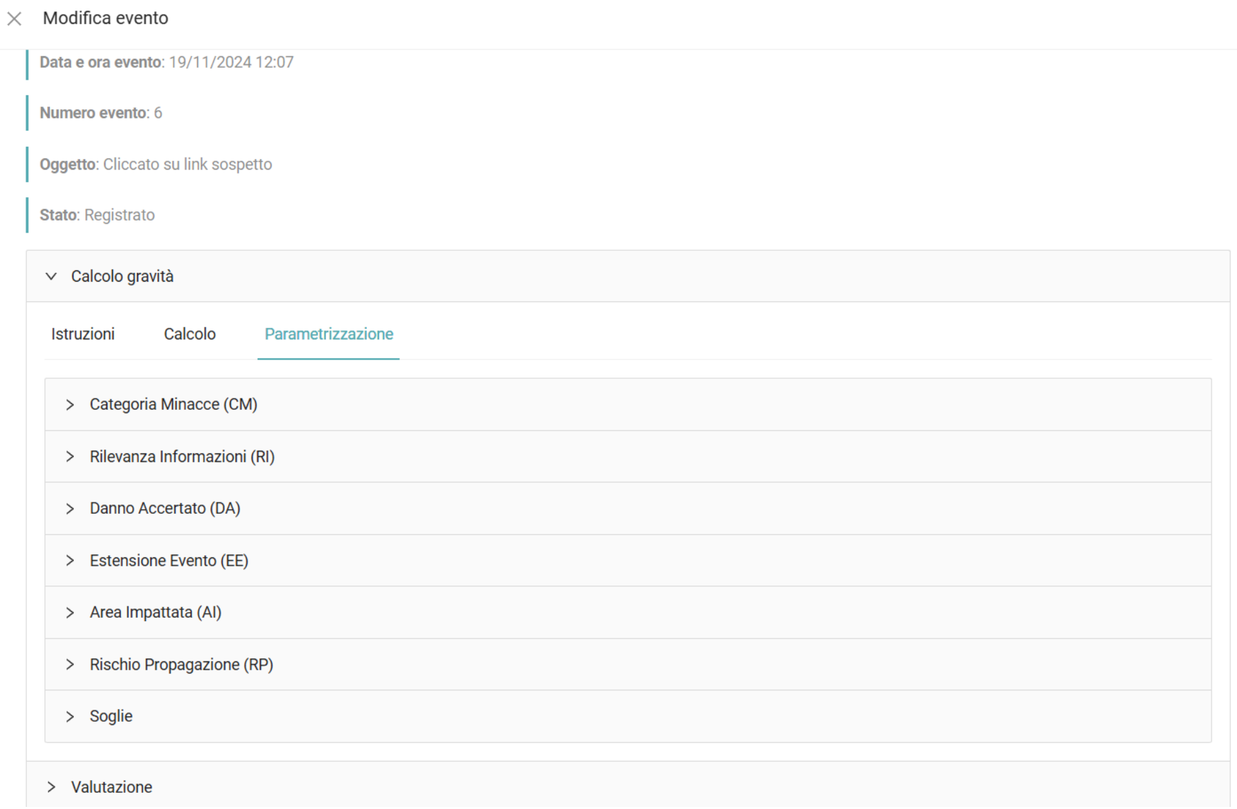
Risultati audit - Audit fornitore Acme Inc. 2024	
Totale punteggio ideale	900
Totale punteggio ottenuto	700
% raggiunta	77,78%
Totale punteggio ideale pesato	90.000
Totale punteggio ottenuto pesato	70.000
% raggiunta	77,78%

Clusit 25 2000-2025
SECURITY SUMMIT
ATENA

Semplificare l’approccio alla NIS2: modulo Gestione Incidenti

Gestione incidenti con calcolo gravità parametrizzabile





Semplificare l’approccio alla NIS2: modulo Action Plan

Action plan: pianificazione e gestione delle remediations

Home | Richieste | Progetti | Task

+ Aggiungi | Cancella | Visualizza tutti | 6 | Cerca

Progetto	Descrizione	Tipologia	Data inizio prevista	Data fine prevista	Stato
Progetto 1 (4)					
Progetto 1	Primo task	Formazione	24/02/2025	28/02/2025	In corso
Progetto 1	Quarto task	Documento di pro...	27/02/2025	28/02/2025	Da fare
Progetto 1	Secondo task	Remediation N.C.	03/03/2025	07/02/2025	Da fare
Progetto 1	Terzo task	Manutenzione ev...	10/03/2025	14/02/2025	Da fare
Progetto 2 (1)					
Progetto 2	Kick-off	Formazione	27/02/2025	28/02/2025	In corso
Progetto 3 (1)					

Colonne | Filtri

Grazie per l’attenzione!