Security Summit

Verona, 24 ottobre 2024

NIS2:
un approccio strutturato alla compliance ed alla valutazione della Supply Chain

Alessio Pennasilico, CS Clusit

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

Alessio Pennasilico

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

Membro del Comitato Scientifico

Membro del Comitato Direttivo di Informatici Professionisti

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità

Membro del Comitato di schema

Direttore Scientifico della testata

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano

Claudio Canepa

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

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).

AXSYM, AL TUO SERVIZIO

- Azienda di **consulenza altamente specializzata** in Information Security Governance e Compliance
- Servizi progettati e implementati **su misura** delle necessità del singolo cliente
- Obiettivo: guidare e accompagnare le organizzazioni verso una **gestione più efficiente, sicura e consapevole delle informazioni** e dei sistemi informatici che si traduce anche in una maggiore affidabilità per i tuoi clienti e partner.

I NOSTRI SERVIZI SU MISURA

CONSULENZA SPECIALIZZATA

FORMAZIONE IN CYBERSECURITY

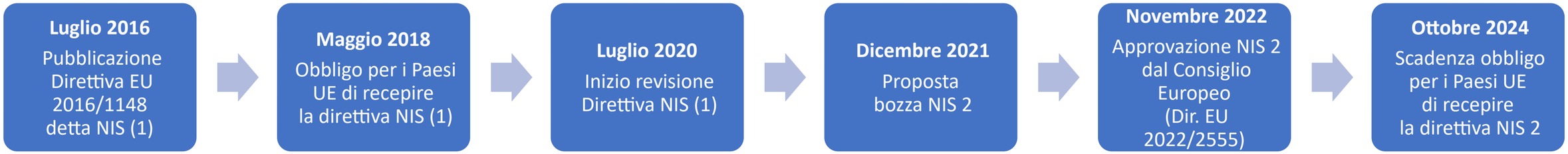
ATENA GOVERNANCE

GLI AMBITI DELLA CONSULENZA AXSYM

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

NIS2: INTRODUZIONE

- NIS2 (o NIS 2), acronimo di "**Network and Information Security 2**" è il termine con cui viene indicata la **Direttiva Europea 2022/2555** pubblicata in sostituzione della Direttiva 2016/1148 (comunemente indicata come NIS) sulla sicurezza informatica e la resilienza a livello dell'UE
- NIS 2 ha 3 obiettivi principali:
  - Portare tutti gli Stati Membri ad adottare **specifiche misure comuni e strategiche** al fine di **uniformare il livello e le modalità di sicurezza** in tali ambiti, incluse misure minime di sicurezza
  - **Aumentare la resilienza informatica** attraverso requisiti di sicurezza più rigorosi e sanzioni per le violazioni
  - **Migliorare la preparazione e resilienza delle organizzazioni essenziali e importanti dell'Unione**, e dei loro **fornitori**, ad affrontare gli attacchi informatici



PRINCIPALI NOVITÀ DELLA DIRETTIVA NIS2

- **Ampliamento dei soggetti interessati** alla normativa: non più “Operatori di servizi essenziali” e “Fornitori di servizi digitali” ma "Soggetti essenziali" e "Soggetti importanti" (10 settori in più) + **fornitori** aziende essenziali e importanti
- Introduzione dell'importanza della **sicurezza della supply chain e relativi controlli**
- **Nuovi requisiti di sicurezza obbligatori**, inclusi quelli per la gestione del rischio e la prevenzione degli incidenti
- **Obblighi di segnalazione degli incidenti più severi e in tempi minori** (24 ore vs. 72 ore della NIS1)
- **Responsabilizzazione dei membri della direzione**, responsabili della non conformità e personalmente responsabili per negligenza grave in caso di incidente di sicurezza informatica
- Obbligo di **registrazione dei fornitori digitali** presso ENISA
- Possibilità per le **autorità di vigilanza di emettere ordini, avvertimenti e multe** fino al 2% del fatturato mondiale totale di un'organizzazione per le organizzazioni essenziali e fino all'1,4% per le organizzazioni importanti

SETTORI INTERESSATI ALLA DIRETTIVA NIS2

Settori essenziali Settori importanti

PRESENTI GIÀ NELLA NIS1

- Energia
- Trasporti
- Settore bancario
- Infrastrutture e mercati finanziari
- Settore sanitario
- Infrastrutture digitali
- Fornitura acqua potabile
- Fornitori di servizi digitali

AGGIUNTI NELLA NIS2

- Pubblica Amministrazione
- Gestione acque reflue
- Gestione dei servizi TIC
- Spazio
- Servizi postali e di corriere
- Gestione dei rifiuti
- Sostanze chimiche
- Alimenti
- Fabbricazione
- Ricerca

MISURE DI GESTIONE DEI RISCHI DI CYBERSECURITY

La Direttiva NIS2 (art. 21.2) stabilisce 10 misure di gestione dei rischi di sicurezza che devono essere applicate da tutte le organizzazioni soggette alla normativa. Queste 10 misure sono:

a) **Politiche di analisi dei rischi e di sicurezza** dei sistemi informatici;

b) **Gestione degli incidenti;**

c) **Continuità operativa**, come la gestione del **backup** e il ripristino in caso di disastro **l**a gestione delle crisi;

d) **Sicurezza della catena di approvvigionamento**, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) **Sicurezza dell'acquisizione, dello sviluppo e della manutenzione** dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) **Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi** di cyber sicurezza;

g) **Pratiche** di igiene informatica di igiene informatica e **formazione** in materia di cyber sicurezza;

h) **Politiche e procedure** relative all'uso della **crittografia** e, se del caso, della **cifratura**;

i) **Sicurezza delle risorse umane**, strategie di **controllo dell'accesso** e **gestione degli attivi**;

j) **L’uso dei Multi-Factor Authentication (MFA) e comunicazioni di emergenza protette**.

SUPPLY CHAIN (ART. 21.3)

Gli Stati membri provvedono affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), del presente articolo, siano adeguate, **i soggetti tengano conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cyber sicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro**. Gli Stati membri provvedono inoltre affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), siano adeguate, i soggetti siano tenuti a tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22, paragrafo 1.

Conseguenza:
significativo allargamento della platea delle aziende interessate alla conformità alla NIS 2, al di là della diretta appartenenza ai soggetti definiti come essenziali o importanti

NON CONFORMITÀ (ART. 21.4)

Gli Stati membri provvedono affinché, **qualora un soggetto constati di non essere conforme** alle misure di cui al paragrafo 2, esso **adotti, senza indebito ritardo, tutte le misure correttive necessarie, appropriate e proporzionate.**

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 seguenti fasi e tempi 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.

TEMPI DI RECEPIMENTO E SCADENZE

D.Lgs. n.138 del 4 settembre 2024 (Recepimento Direttiva NIS2)

pubblicato in Gazzetta Ufficiale il 1 ottobre 2024

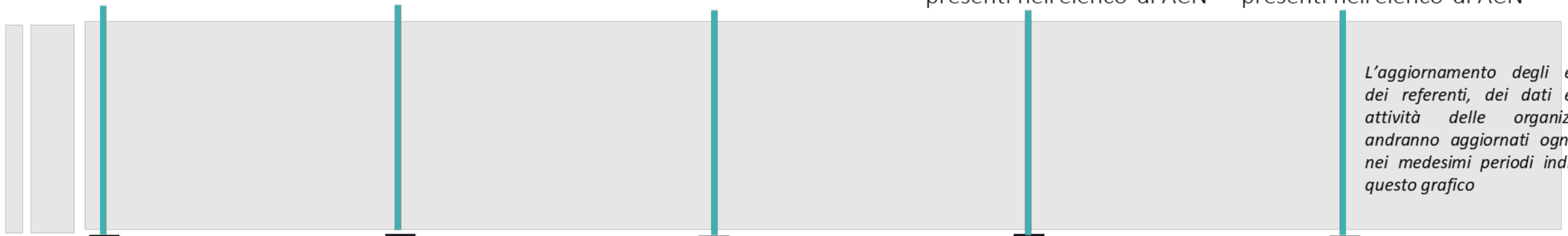
Dal 18/10/2024: portale iscrizioni (in attesa di pubblicazione)

Entro il 28/02/2025 Registrazione nel portale

31/03/2025 Redazione elenco dei Soggetti

15/04 – 31/05/2025 Completamento registrazione dei soggetti presenti nell'elenco di ACN

01/05 – 30/06/2026 Completamento registrazione dei soggetti presenti nell'elenco di ACN



L'aggiornamento degli elenchi, dei referenti, dei dati e delle attività delle organizzazioni andranno aggiornati ogni anno nei medesimi periodi indicati in questo grafico

ACN – Agenzia per la Cyber Sicurezza Nazionale mette a disposizione un portale per le iscrizioni

Art. 7 comma 1 – i *Soggetti* dovranno registrarsi o aggiornare
a) Ragione Sociale
b) Recapiti
c) Punto di contatto (referente)
d) Settore appartenenza

Art. 7 comma 2 – *ACN* Redige / Aggiorna l'elenco dei Soggetti
a) Inserimento nell'elenco
b) Permanenza nell'elenco
c) Espunzione dall'elenco

Art. 7 comma 4 – tramite la piattaforma i *Soggetti* forniscono
a) Spazio Indirizzamenti IP Pubblico e domini
b) Stati membri in cui forniscono servizi
c) Responsabili
d) Sostituto del punto di contatto

Art. 30 comma 1 – tramite la piattaforma i *Soggetti* forniscono Elenco delle proprie attività e dei propri servizi
L'obbligo decorre dal 1 gennaio 2026 (art. 42 c.2)

TEMPI DI IMPLEMENTAZIONE E ADEGUAMENTO

(*) Date indicative, in quanto fanno riferimento alla data della comunicazione che ACN invierà al soggetto interessato (art. 42 c.1 lett.c)

31/03/2025 (*)
Pianificazione delle misure
e inizio implementazione

31/12/2025 (*)
Gestione degli Incidenti

30/09/2026 (*)
Misure di Sicurezza

9 mesi di tempo

18 mesi di tempo

Considerate le successive tempistiche indicate dalla norma, è consigliabile aver almeno eseguito una GAP analysis e un'analisi dei rischi, ed aver già predisposto un piano di implementazione delle misure di sicurezza necessarie per l'adeguamento alla NIS2.

Entro questo termine dovranno essere completate le policy e le procedure strutturate per gestire gli incidenti:
l'identificazione, la classificazione, la comunicazione la risoluzione
la notifica alle autorità competenti (CSIRT Italia, Garante), ai soggetti interessati
adozione di azioni correttive.
Le procedure di comunicazione devono essere testate e aggiornate regolarmente. Art. 25

Entro questo termini dovranno essere adottate le misure tecniche necessarie per proteggere i sistemi informatici. Questo include l'implementazione di firewall, sistemi di rilevamento delle intrusioni, crittografia dei dati, autenticazione a più fattori (MFA), e altre tecnologie di sicurezza avanzate.
È fondamentale garantire che queste misure siano aggiornate e adeguate alle minacce in evoluzione.
Art. 23, 24, 29

Il D.Lgs. 138/2024 ha rinumerato gli articoli rispetto alla Direttiva UE 2022/2555

E’ pertanto necessario precisare, nella documentazione interna di applicazione della norma, se si fa riferimento agli articoli della Direttiva UE o del decreto di recepimento.

Si suggerisce comunque di inserire nella documentazione una tabella di corrispondenza, come nell’esempio che segue.

Art.NIS2	Titolo	Art.D.Lgs.138
20	Governance	23
21.1	Misure di gestione dei rischi di cibersicurezza	24.1
21.2 (a)	Politiche di analisi dei rischi e di sicurezza dei sistemi informatici	24.2 a)
21.2 (b)	Gestione degli incidenti	24.2 b)
21.2 (c)	Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi	24.2 c)
21.2 (d)	Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi	24.2 d)
21.2 (e)	Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità	24.2 e)
21.2 (f)	Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza	24.2 f)
21.2 (g)	Pratiche di igiene informatica di base e formazione in materia di cibersicurezza	24.2 g)
21.2 (h)	Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura	24.2 h)
21.2 (i)	Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi	24.2 i)
21.2 (j)	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, se del caso	24.2 l)
21.3	Procedure di sviluppo sicuro	24.3
21.4	Misure correttive appropriate e proporzionate (se non conformi)	24.4
23	Obblighi di segnalazione	25

PERCHÉ INIZIARE ORA L'ADEGUAMENTO ALLA NIS2

A prima vista si potrebbe pensare che è ancora lontana la scadenza che renderà obbligatoria l'applicazione della Direttiva NIS2. Tuttavia bisogna ricordarsi che:

- L'Italia ha recepito la Direttiva UE con **D.Lgs. n.138 del 4 settembre 2024** fissando l'entrata in vigore della norma al 18 ottobre 2024, pur diluendo nel tempo i termini per l'applicazione delle misure di sicurezza prescritte
- l'implementazione richiede **tempo** ed è necessaria una serie completa di misure per raggiungere il livello di adeguamento richiesto, a partire dalla situazione «as-is» (**necessario assessment iniziale**)
- dato il focus della NIS2 sulla sicurezza della supply chain, è richiesto il coinvolgimento e la collaborazione dei **fornitori**, condizione che allunga inevitabilmente i tempi di attuazione
- è necessario pianificare per tempo il **budget** necessario per l'implementazione delle attività/tecnologie di sicurezza necessarie

DIRETTIVA NIS2 E STANDARD ISO 27001

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.

Pur non essendo citata direttamente nel testo della Direttiva,
al momento lo Standard che copre nel modo più completo i requisiti di sicurezza
indicati dalla NIS2 è lo

Standard ISO 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)

È comunque possibile gestirlo efficacemente anche attraverso **altri standard es. NIST, FNCS, CIS**...

L'adozione di uno standard garantisce un approccio strutturato ed efficace alla compliance.

MAPPATURA ARTICOLI NIS2 E FRAMEWORK (ESEMPIO)

NIS2	ISO 27001:2022	NIST v1.1 / FNCS v2.0 (Framework Nazionale di Cyber Security)	CIS v8
• 21.2 b) Incident handling	• A.5.24 Information security incident management planning and preparation • A.5.25 Assessment and decision on information security events • A.5.26 Response to information security incidents • A.5.27 Learning from information security incidents • A.5.28 Collection of evidence • A.6.8 Information security event reporting	• ID.AM-5 Resources (e.g., hardware, devices, data, and software are prioritized based on their classification, criticality, and business value • RS.AN-4 Incidents are categorized consistent with response plans • RS.MI-1 Incidents are contained	• 13.1 Security Event Alerting • 13.11 Tune Security Event Alerting Thresholds • 17.1 Designate Personnel to Manage Incident Handling • 17.2 Establish and Maintain Contact Information for Reporting Security Incidents • 17.3 Establish and Maintain an Enterprise Process for Reporting Incidents • 17.4 Establish and Maintain an Incident Response Process • 17.5 Assign Key Roles and Responsibilities • 17.6 Define Mechanisms for Communicating During Incident Response • 17.7 Conduct Routine Incident Response Exercises • 17.8 Conduct Post-Incident Reviews • 17.9 Establish and Maintain Security Incident Thresholds • 8.10 Retain Audit Logs • 8.2 Collect Audit Logs • 8.5 Collect Detailed Audit Logs • 8.9 Centralize Audit Logs

MAPPATURA ARTICOLI NIS2 E FRAMEWORK (ESEMPIO)

NIS2	ISO 27001:2022	NIST v1.1 / FNCS v2.0 (Framework Nazionale di Cyber Security)	CIS v8
• 21.2 d) Supply chain security, including security related aspects concerning the relationship between each entity and its direct suppliers or service providers	• A.5.19 Information security in supplier relationship • A.5.20 Addressing information security within supplier agreements • A.5.21 Managing information security in ICT supply chain • A.5.22 Monitoring, review and change management of supplier services • A.5.23 Information security for use of cloud services	• DE.AE-4 Impact of events is determined • DE.CM-5 Unauthorized mobile code is detected • DE.CM-8 Vulnerability scans are performed • ID.AM-3 Organizational communication and data flows are mapped • ID.AM-5 Resources (e.g., hardware, devices, data, and software are prioritized based on their classification, criticality, and business value • ID.BE-4 Dependencies and critical functions for delivery of critical services are established • PR.AT-3 Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities • PR.AT-5 Physical and information security personnel understand roles & responsibilities • PR.DS-5 Protections against data leaks are implemented • PR.IP-1 A baseline configuration of information technology/industrial control systems is created and maintained • PR.IP-2 A System Development Life Cycle to manage systems is implemented • RC.CO-2 Reputation after an event is repaired • RS.AN-1 Notifications from detection systems are investigated	• 15.1 Establish and Maintain an Inventory of Service Providers • 15.2 Establish and Maintain a Service Provider Management Policy • 15.3 Classify Service Providers • 15.4 Ensure Service Provider Contracts Include Security Requirements • 15.5 Assess Service Providers • 15.6 Monitor Service Providers • 15.7 Securely Decommission Service Providers • 8.12 Collect Service Provider Logs

COME PREPARARSI ALLA NIS2

Per impostare una gestione della cyber security in linea con la NIS2 è necessario svolgere:

1. **Fin da subito la giusta pianificazione**: l'implementazione delle diverse misure **richiede tempo e budget**. Prima si entra nell'ottica dell'adeguamento, meglio lo si potrà gestire e programmare
2. Attività di **Gap analysis** per verificare quali dei requisiti minimi della NIS2 l'azienda deve implementare da zero o in modo più efficace
3. **Selezione di uno o più framework/standard di cyber security** per individuare come raggiungere i requisiti minimi fissati dalla Direttiva (es. ISO 27001)
4. Le **valutazioni necessarie** tra cui Risk Assessment, Business Impact Analysis, Vulnerability Assessment, valutazione delle misure di sicurezza in atto
5. **Aggiornare/realizzare il Sistema di Gestione Sicurezza delle Informazioni**, il piano di business continuity, di mitigazione dei rischi, di incident response ecc. in modo che questi soddisfino i requisiti previsti dalla NIS2
6. Svolgere **audit interni e sui fornitori**

SICUREZZA DELLA SUPPLY CHAIN: CONSIDERAZIONI

La NIS 2 introduce l'obbligo, a carico dei soggetti essenziali e importanti, di verificare la sicurezza della catena di approvvigionamento (supply chain)

Per poterla attuare, è necessario considerare alcuni aspetti:

1. Inserire nelle condizioni contrattuali le opportune clausole relative alle misure di sicurezza che i fornitori devono assicurare

2. Inserire nelle condizioni contrattuali l'obbligo di collaborare all'esecuzione delle verifiche

3. Identificare i fornitori critici da verificare, raggruppandoli in cluster omogenei (es. servizi IT, cloud, fornitori di componenti critici,…)

4. Rafforzare la partnership con i fornitori, volta ad assicurarsi la miglior collaborazione e lo scambio di informazioni relative alla sicurezza

SICUREZZA DELLA SUPPLY CHAIN: MODALITA' DI ESECUZIONE DEGLI AUDIT

1. Per ogni cluster di fornitori identificare il set di controlli di verificare

2. Predisporre i questionari di valutazione, diversificati per tipologia di fornitore, selezionando gli opportuni set di controlli

3. I questionari dovrebbero contenere delle metriche di valutazione

4. Definire la modalità di verifica, a seconda dei casi:
   - questionario da compilare a cura del fornitore
   - audit da remoto
   - audit in presenza

5. Un questionario ben costruito può supportare ciascuna delle modalità indicate

6. Necessaria una valutazione finale dell'audit per pianificare eventuali azioni correttive e/o verifiche successive *(non serve accumulare decine di questionari se poi nessuno li guarda…)*

COME AXSYM PUÒ AIUTARVI IN QUESTO PERCORSO?

1. **Axsym ha le giuste competenze per affiancarvi nelle attività di assessment e adeguamento**
2. **Axsym propone ai suoi clienti di superare il tradizionale approccio gestionale basato su files Excel e documenti sparsi nelle cartelle o anche in sistemi documentali non orientati ad una gestione strutturata e metodologicamente corretta della Governance e Compliance**
3. **Axsym propone una piattaforma progettata specificatamente per gestire gli ambiti GRC (Governance, Risk assessment, Compliance):**
   ATENA Governance

- Digitalizzazione dei documenti
- Database strutturato
- Collaboration
- Applicazioni progettate per l'ambito GRC

COS'È ATENA GOVERNANCE

ATENA Governance è il **software integrato** che permette di **gestire con un unico strumento** i diversi ambiti di **Governance e Compliance** attraverso moduli

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

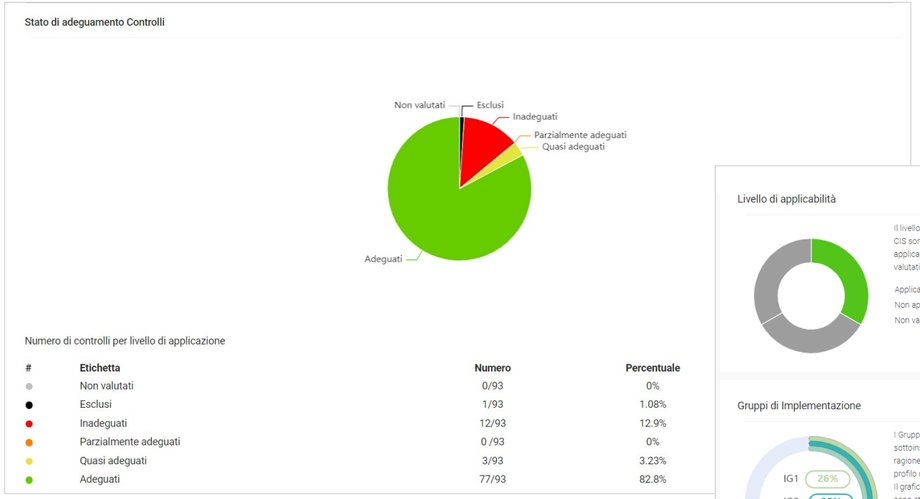
COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLA DIRETTIVA NIS2

Grazie alla struttura modulare e coerente di ATENA Governance la tua organizzazione può:

1. Gestire con **un'unica piattaforma web centralizzata in cloud** tutta la documentazione e **le attività richieste dallo standard e della Direttiva NIS2 a 360°**
(anche per più aziende)

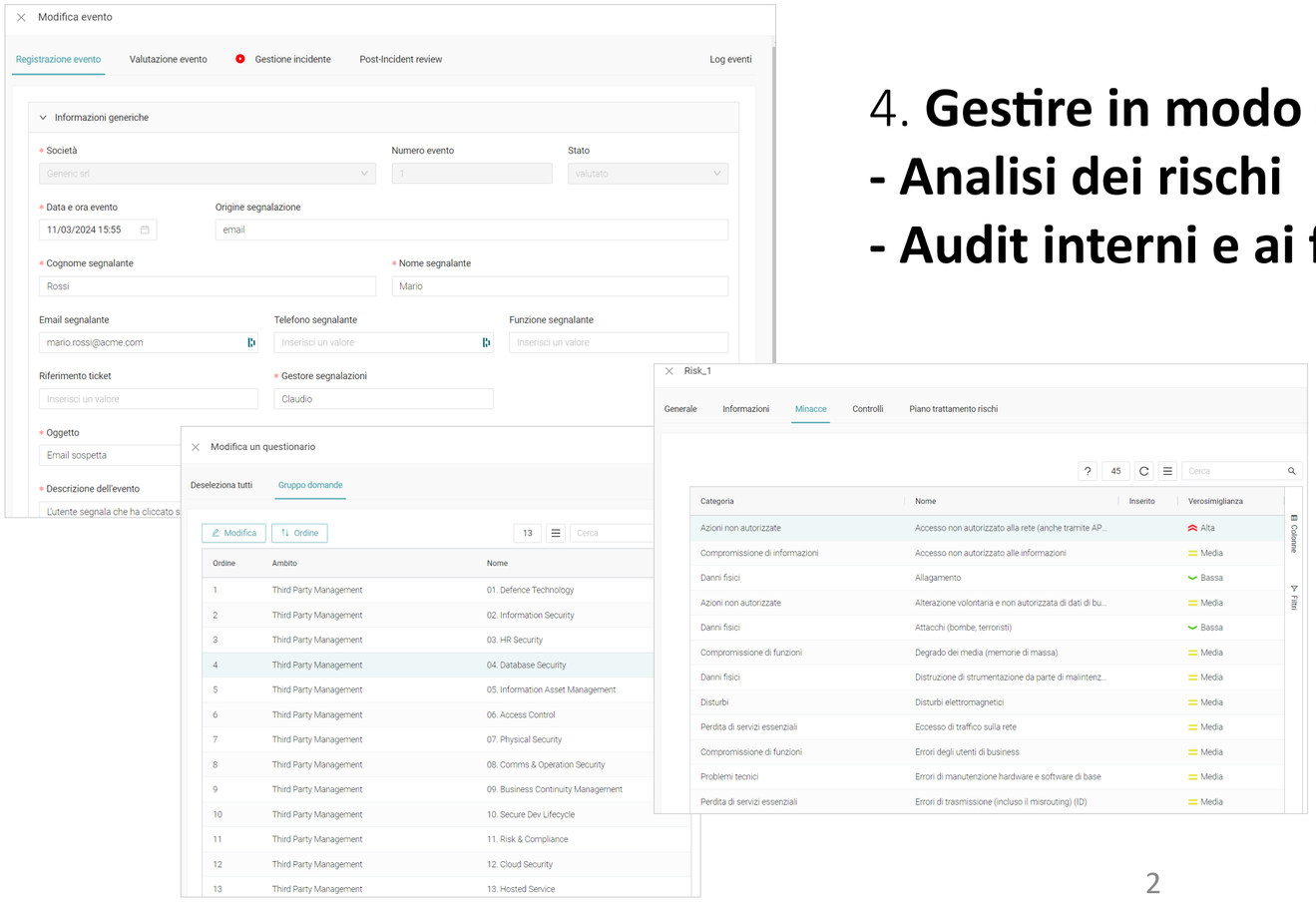
COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLA DIRETTIVA NIS2

2. **Avere tutto sotto controllo** grazie a **dashboard riepilogative** con dati e indicatori in evidenza nonché grazie allo storico delle modifiche



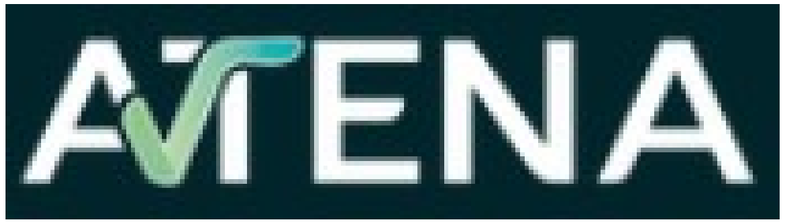
3. Svolgere le attività richieste dalla direttiva, <u>dimostrabili attraverso l'adozione di un framework standard</u> (ISO27001, NIST, FNS, CIS)

COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLA DIRETTIVA NIS2 E DELLO STANDARD ISO 27001



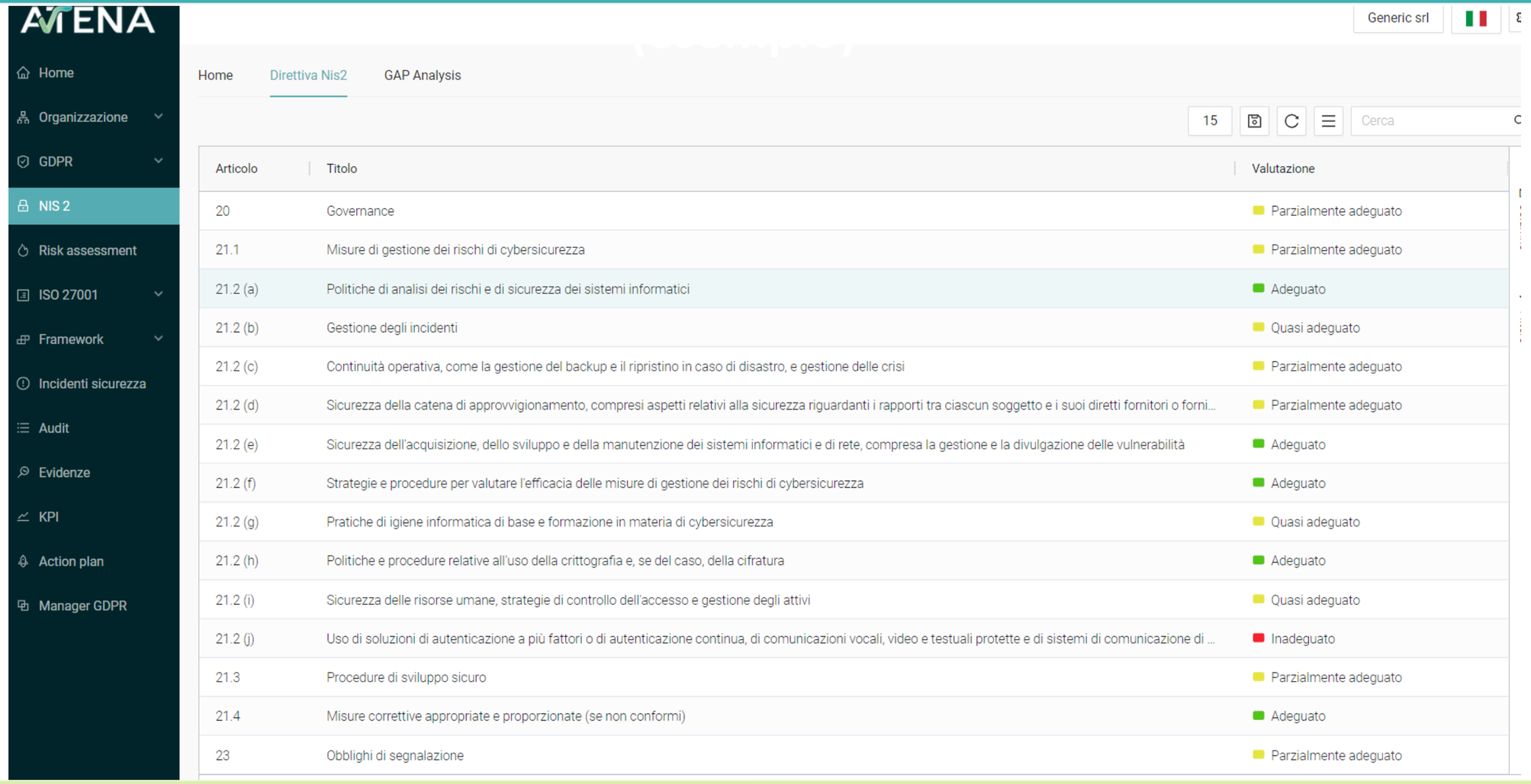
4. **Gestire in modo strutturato e integrato:**
- Analisi dei rischi
- Audit interni e ai fornitori

5. Compiere tutto ciò con **un'unica piattaforma estremamente intuitiva** e facile da utilizzare che permette di risparmiare tempo, denaro e fatica!



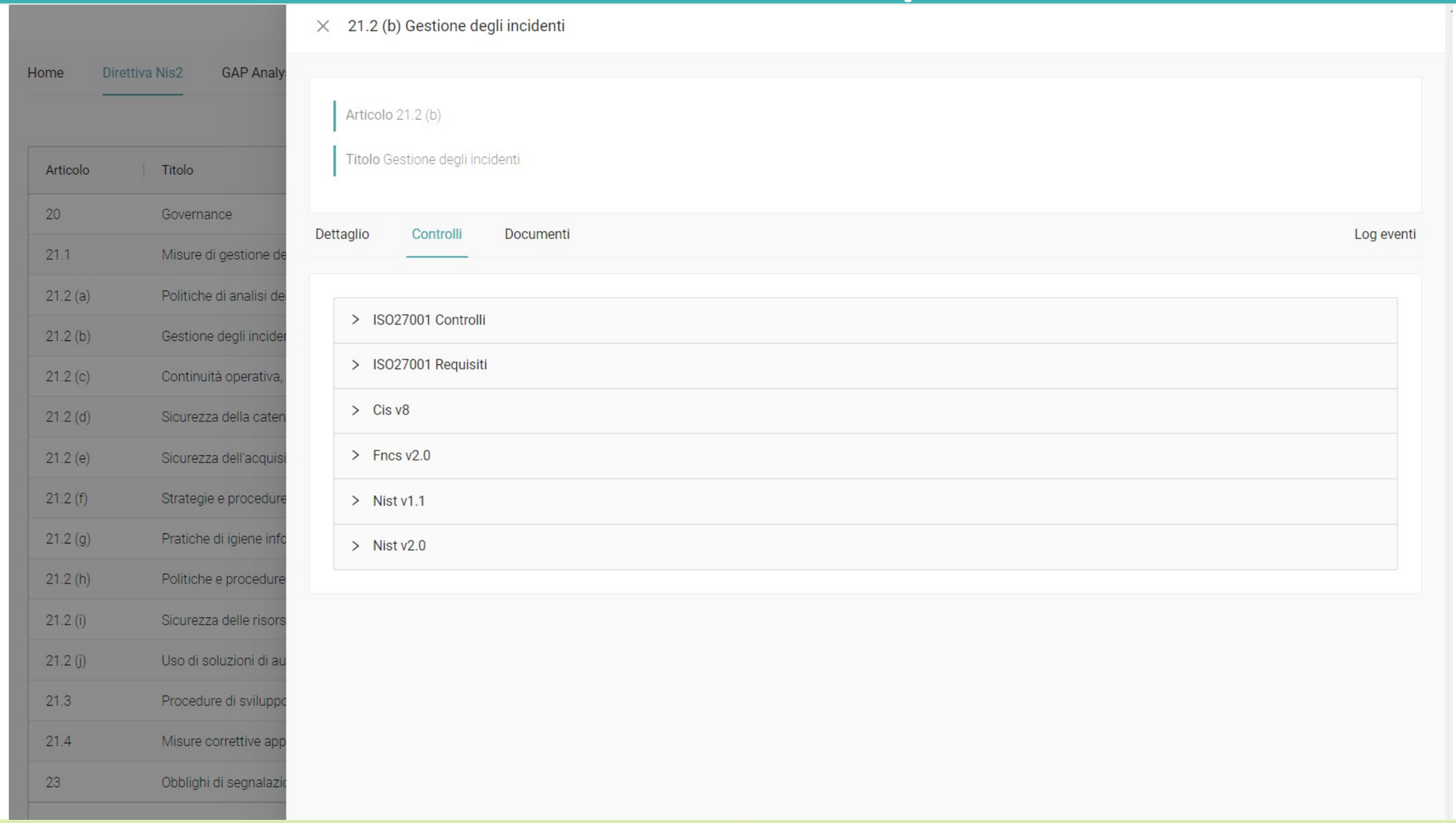
ESEMPI

Valutazione dello stato di adeguamento complessivo delle misure di sicurezza della Direttiva NIS2



Articolo	Titolo	Valutazione
20	Governance	Parzialmente adeguato
21.1	Misure di gestione dei rischi di cybersicurezza	Parzialmente adeguato
21.2 (a)	Politiche di analisi dei rischi e di sicurezza dei sistemi informatici	Adeguato
21.2 (b)	Gestione degli incidenti	Quasi adeguato
21.2 (c)	Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi	Parzialmente adeguato
21.2 (d)	Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o forni...	Parzialmente adeguato
21.2 (e)	Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità	Adeguato
21.2 (f)	Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza	Adeguato
21.2 (g)	Pratiche di igiene informatica di base e formazione in materia di cybersicurezza	Quasi adeguato
21.2 (h)	Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura	Adeguato
21.2 (i)	Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi	Quasi adeguato
21.2 (j)	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 ...	Inadeguato
21.3	Procedure di sviluppo sicuro	Parzialmente adeguato
21.4	Misure correttive appropriate e proporzionate (se non conformi)	Adeguato
23	Obblighi di segnalazione	Parzialmente adeguato

Associazione fra le misure di sicurezza NIS 2 ed i controlli di tutti i framework disponibili



Visualizzazione immediata dello stato di adeguamento dei controlli del framework selezionato

21.2 (b) Gestione degli incidenti

ISO27001 Controlli

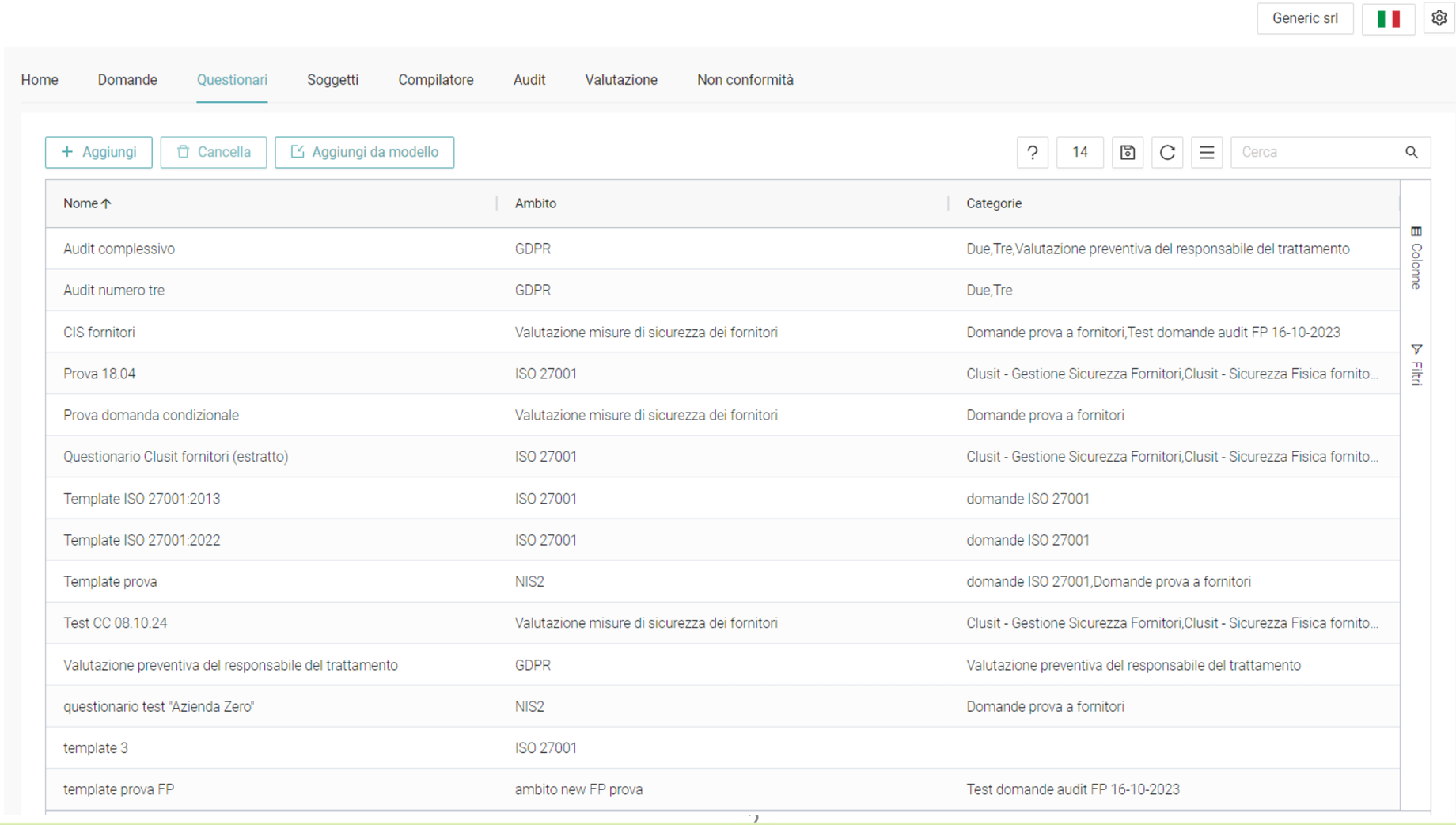
9 | Cerca

Nome SoA	Sezione	ID controllo	Descrizione controllo	Valutazione	Valutazione target
SOA 4A	CONTROLLI	A.5.24	Information security incident management planning and preparation	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.25	Assessment and decision on information security events	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.26	Response to information security incidents	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.27	Learning from information security incidents	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.28	Collection of evidence	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.29	Information security during disruption	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.5	Contact with authorities	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.5.7	Threat intelligence	Adeguato	Adeguato
SOA 4A	CONTROLLI	A.6.8	Information security event reporting	Adeguato	Adeguato

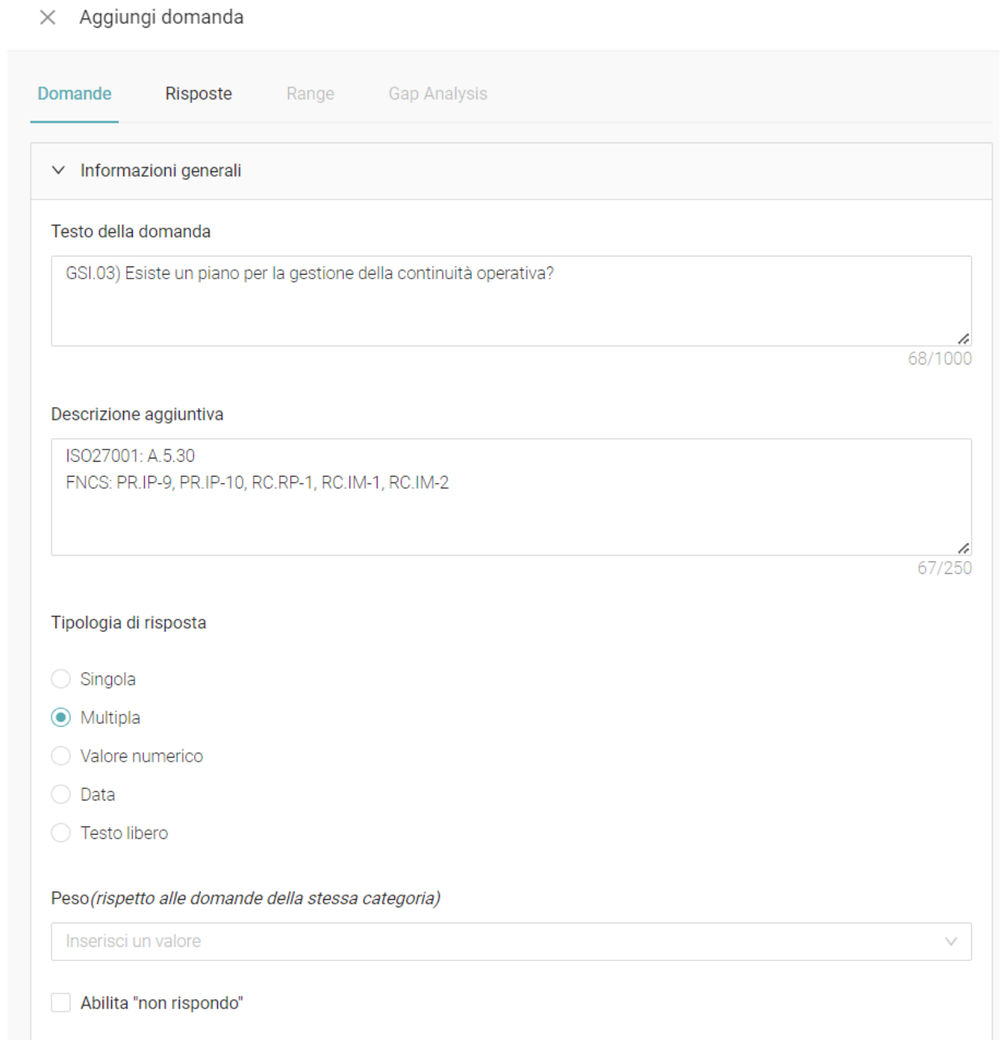
Columns

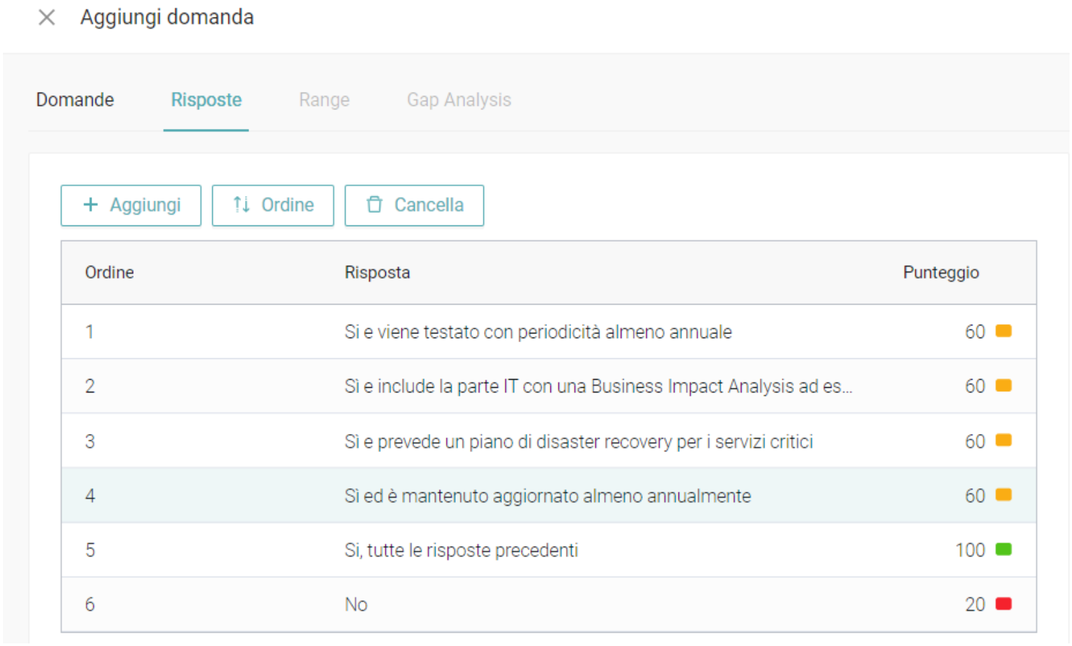
Filters

Modulo di Audit: questionari configurabili per ogni esigenza

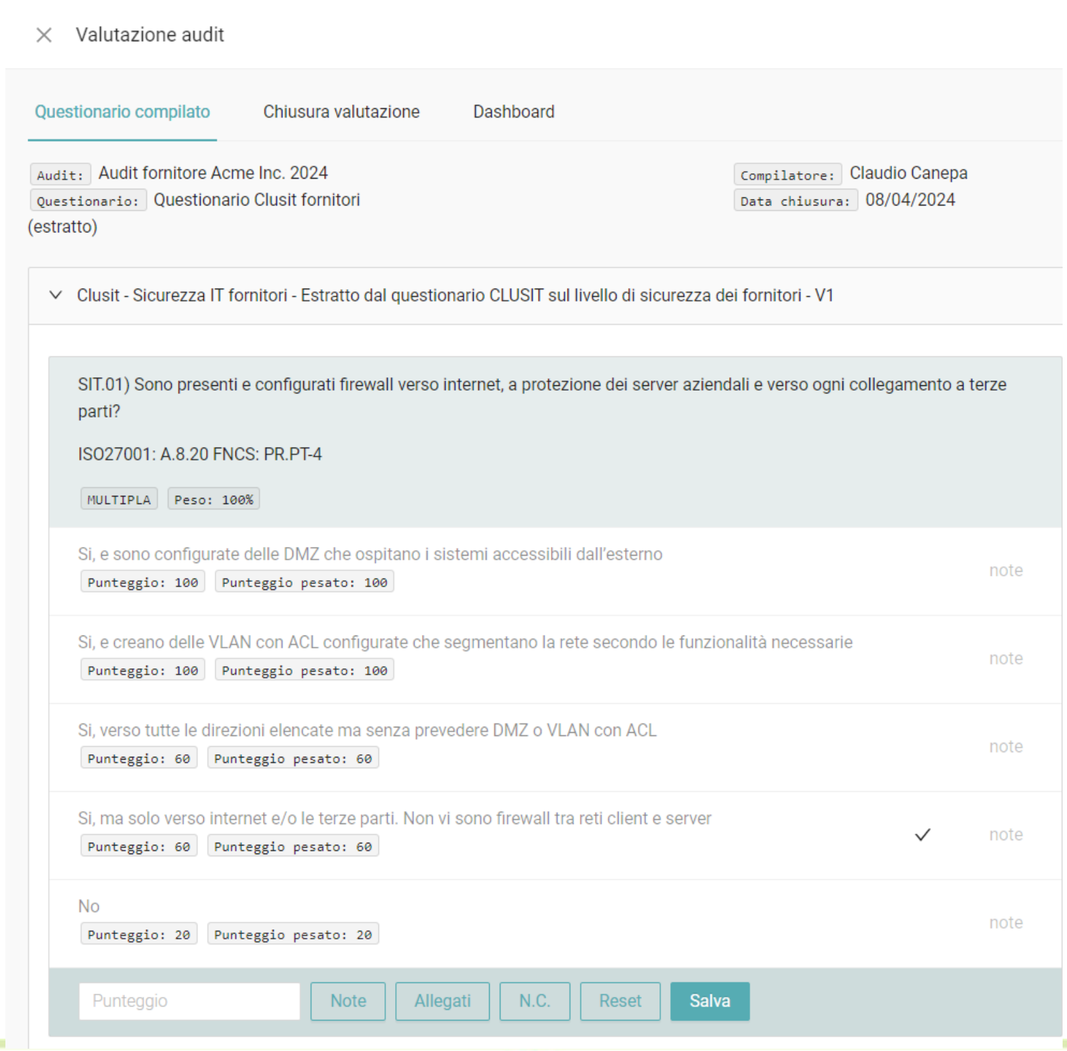


Modulo di Audit: domande e risposte configurabili





Modulo di Audit: valutazione degli audit compilati



CONCLUSIONI

- La Direttiva NIS 2 impatterà un gran numero di aziende, ben oltre il perimetro dei soggetti essenziali e importanti (già più ampio della NIS 1)
- La gestione strutturata della cyber-security sarà un requisito fondamentale per le aziende per poter continuare ad operare con i propri clienti, molto di più di quanto avviene oggi
- La compliance alle prescrizioni della NIS 2 dovrà essere adeguatamente dimostrabile: possibile di fatto con l'adesione a framework standard
- La valutazione della supply chain ne sarà parte integrante

L'adozione di uno strumento ad hoc come **ATENA Governance** renderà più semplice ed efficace tutto ciò, permettendo di ottenere un importante risparmio di tempo, denaro e fatica nella gestione dei processi e delle informazioni richiesti dalla Direttiva e dallo standard adottato.

Q&A

CONTATTI

AXSYM
Compliance & Information Security

Per informazioni e demo gratuite del software ATENA Governance, veniteci a trovare al desk!

Tel. 045 5118570
info@axsym.it – www.axsym.it

Grazie per l’attenzione

AXSYM
Compliance & Information Security