Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Direttiva NIS2:
quali sono le Novità e Come gestire in modo ottimale i nuovi Obblighi di audit e sicurezza della Supply Chain

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

20 marzo 2024 orario 12.20 - 13.00

Claudio Canepa

SENIOR IT E 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.

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

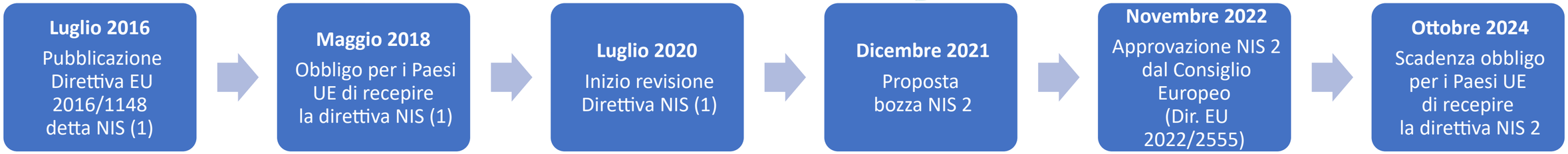
ATENA GOVERNANCE

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.

<u>Conseguenza</u>:
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.

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 informatica.

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 **piando di continuità aziendale** (Business Continuity)

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

MAPPATURA ARTICOLI NIS2 E FRAMEWORK

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

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

MAPPATURA ARTICOLI NIS2 E FRAMEWORK

NIS2	ISO 27001:2022	NIST v1.1 / FNCS v2.0 (Framework Nazionale di Cyber Security)	CIS v8
• 21.2 j) The use of multifactor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications system within the entity, where appropriate	• A.5.14 Information transfer • A.5.16 Identity management • A.5.17 Authentication information	• PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes • PR.AC-6 Identities are proofed and bound to credentials and asserted in interactions • PR.AC-7 Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	• 17.6 Define Mechanisms for Communicating During Incident Response • 6.3 Require MFA for Externally-Exposed Applications • 6.4 Require MFA for Remote Network Access • 6.5 Require MFA for Administrative Access • 6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems • 6.7 Centralize Access Control

MAPPATURA ARTICOLI NIS2 E FRAMEWORK

NIS2	ISO 27001:2022	NIST v1.1 / FNCS v2.0 (Framework Nazionale di Cyber Security)	CIS v8
• 21.4) Appropriate and proportionate corrective measures (if not comply)	•10.1 Non conformity and corrective actions •10.2 Non conformity and corrective actions		

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**

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

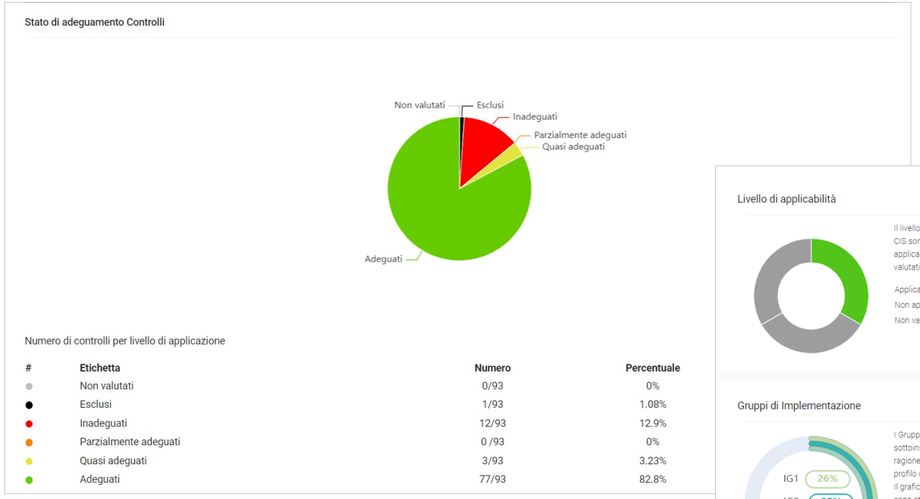
COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLA DIRETTIVA NIS2

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)

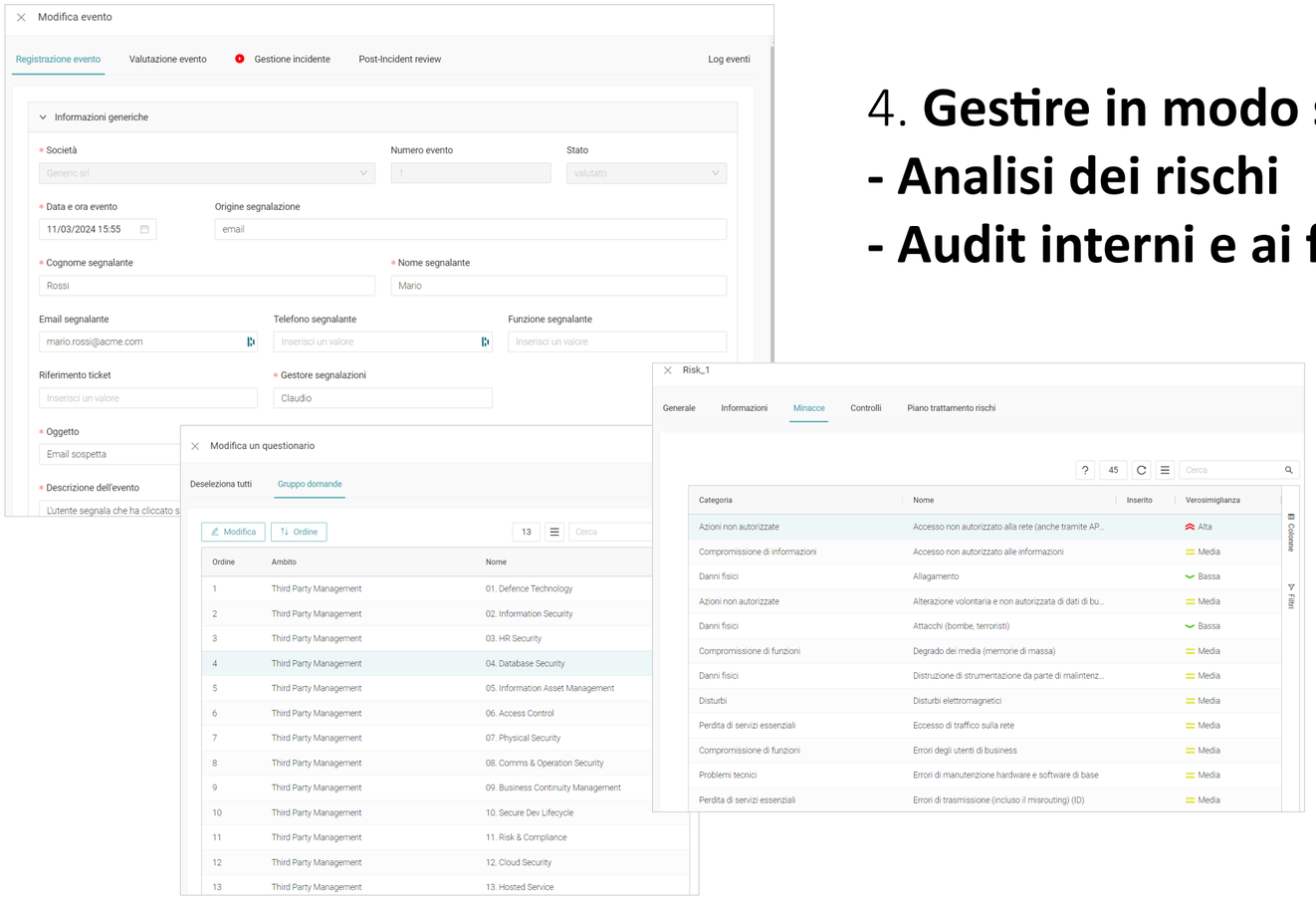
COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLA DIRETTIVA NIS2

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**
- **Incidenti**
- **KPI**
- **Evidenze**
- **Action Plan**

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

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

AXSYM Compliance & Information Security

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

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT