



# Security Summit

Milano 11-12-13 marzo 2025



## **Risk Assessment e Business Impact Analysis. Metodologie e strumenti operativi per semplificare l'adeguamento alla Direttiva NIS2**

**Caludio Canepa** | Senior IT & Information Security Advisor, ISO/IEC 27001 Auditor, *Axsym*

1



## 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).

# 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



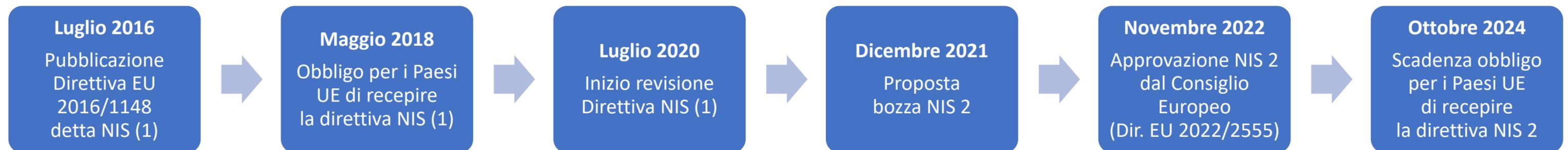
# Gli ambiti della consulenza Axsym

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



# NIS 2: 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:
  1. 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
  2. **Aumentare la resilienza informatica** attraverso requisiti di sicurezza più rigorosi e sanzioni per le violazioni
  3. Migliorare la **preparazione e resilienza delle organizzazioni essenziali e importanti dell'Unione**, e dei loro fornitori, ad affrontare gli attacchi informatici



# Tempi di recepimento e scadenze

**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

**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

# 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.

# Misure di gestione dei rischi di cybersecurity

La Direttiva NIS2 stabilisce 10 misure di gestione dei rischi di sicurezza che devono essere applicate da tutte le organizzazioni soggette alla normativa.

- Politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
- Gestione degli incidenti;
- Continuità operativa, come la gestione del backup e il ripristino in caso di disastro la gestione delle crisi;
- 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;
- Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
- Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cyber sicurezza;
- Pratiche di igiene informatica di igiene informatica e formazione in materia di cyber sicurezza;
- Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
- Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
- L'uso dei Multi-Factor Authentication (MFA) e comunicazioni di emergenza protette.

# Direttiva NIS2 e standard: ISO 27001 & FNCS

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.

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)

Tuttavia, l'Agenzia per la CyberSicurezza Nazionale (ACN) utilizza e riconosce esclusivamente il  
**Framework Nazionale per la CyberSecurity e la Data Protection (FNCS)**

Ne consegue la necessità di rimappare i controlli ISO27001 con quelli previsti dal FNCS.

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

# NIS2 e Analisi multi-rischio

L'art. 2 (Definizioni) alla lettera dd) specifica:

«**approccio multi-rischio**»: cosiddetto approccio all-hazards, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché' al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati.

L'art. 24 (Obblighi in materia di misure di gestione dei rischi per la sicurezza Informatica) c.1 recita:

«I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate ... alla **gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete** che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per **prevenire o ridurre al minimo l'impatto degli incidenti** per i destinatari dei loro servizi e per altri servizi.»

# NIS2 e Analisi multi-rischio



# Elementi di un'analisi multi-rischio

1. **Processo strutturato:** riduzione della soggettività delle valutazioni e ripetibilità del metodo
2. **Non limitarsi ai rischi di tipo informatico** (es. malware)
3. Identificare correttamente gli **asset aziendali** e le **minacce** che vi incombono (verosimiglianza-impatto)
4. Valutare l'**efficacia** delle **contromisure** adottate
5. Definire le modalità di **trattamento** dei **rischi residui** (mitigare, trasferire, accettare, evitare)
6. Predisporre un adeguato **piano di trattamento dei rischi**

# Metodologia di un'analisi dei rischi

- ✓ Sono generalmente previsti due approcci:
  - «**ad evento**»: considera globalmente i rischi, senza entrare nel dettaglio degli asset
  - «**per asset**»: vengono considerate le minacce che incombono sugli assets (anche raggruppati per categorie omogenee)
- ✓ La nostra metodologia prevede un'analisi «per asset» che consente:
  - Evidenza di quali **rischi** incombono sui diversi tipi di asset
  - Identificazione della **criticità** dei diversi asset
  - **Valutazione** se le **misure di sicurezza** sono implementate coerentemente con la criticità degli asset
  - L'approccio per asset risulta funzionale alla realizzazione della **Business Impact Analysis**
- ✓ Valutazione dei **rischi** relativi ai **Fornitori (Supply Chain)**: la NIS 2 obbliga i soggetti in perimetro a valutare i fornitori critici, che possono rappresentare un loro elemento di rischio
- ✓ Per le imprese industriali: **indispensabile** includere nell'**analisi** dei **rischi** anche la parte **OT**

# Relazione fra analisi dei rischi e Business Impact Analysis

- Per essere maggiormente aderente al contesto, un'analisi dei rischi dovrebbe essere preceduta da una BIA (Business Impact Analysis).
- La BIA prevede il **coinvolgimento** diretto delle **principali funzioni di Business**, per identificare:
  - I **processi critici** dell'organizzazione
  - Gli **impatti** che può avere un'interruzione dei servizi, sotto diversi aspetti (es. economico, reputazionale, normativo, etc)
  - Il massimo tempo tollerabile del blocco del processo (**MTPD**)
  - Il tempo di ripristino desiderato per il processo (**RTO**)
  - Le **risorse** necessarie per un ripristino graduale del processo
- Mappando gli **asset** necessari al funzionamento dei processi, si ottiene l'**evidenza del loro grado di criticità, priorità e tempi di ripristino**.

# Relazione fra analisi dei rischi e Business Impact Analysis

- L'esecuzione di una BIA rappresenta una base fondamentale per:
  1. Analisi dei Rischi
  2. Business Continuity Plan
- L'effettuazione di una BIA assicura che le valutazioni dei rischi, il loro trattamento ed i piani di ripristino vengano predisposti in linea con le **effettive necessità del Business**, e non solo secondo il punto di vista della funzione IT.
- Permette anche di identificare eventuali **incoerenze fra i tempi di ripristino richiesti dal Business ed i tempi tecnici di ripristino** che l'IT è in grado di garantire e di intraprendere le opportune azioni di allineamento (tecnologiche e/o organizzative).

# Axsym rivoluziona la GRC con 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 FNCS, NIST, CIS
- Incidenti di Sicurezza, Evidenze, KPI
- Audit e Action Plan

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

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

The screenshot shows the ATENA Governance web application interface. On the left is a dark sidebar with the ATENA logo and a navigation menu including: Home, Organizzazione, GDPR, Risk assessment, ISO 27001, Framework (with sub-items NIST, FNCS, CIS), Incidenti sicurezza, Audit, Evidenze, KPI, Remediation, and Manager. The main content area is titled "Benvenuto in ATENA Governance" and contains a welcome message, a description of the platform as an integrated system for Governance and Compliance, and links to "Manuali operativi e istruzioni per il primo utilizzo" and "Struttura della piattaforma". Below the text is a circular diagram illustrating the platform's structure, divided into segments for RISK ASSESSMENT, AUDIT, and REMEDIATION, with sub-segments like ANALISI DEI RISCHI, VALUTAZIONE DELLE MINACCE, BUSINESS IMPACT ANALYSIS, GAP ANALYSIS, DOMANDE PERSONALIZZABILI, and VERIFICHE PERIODICHE O SINGOLE.

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?

Home [Direttiva Nis2](#) GAP Analysis Documenti

Valutazione da FNCS 15 [Icona] [Icona] [Icona] Cerca

Articolo	Titolo	Valutazione
20	Governance	Inadeguato
21.1	Misure di gestione dei rischi di cybersicurezza	Inadeguato
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 g...	Parzialmente adeguato
21.2 (d)	Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza ri...	Parzialmente adeguato
21.2 (e)	Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici ...	Adeguato
21.2 (f)	Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cyber...	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	Inadeguato
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 comuni...	Inadeguato
21.3	Procedure di sviluppo sicuro	Parzialmente adeguato

Valutazione  
adeguatezza  
requisiti richiesti  
dalla NIS2

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

× 21.2 (b) Gestione degli incidenti

Articolo 21.2 (b)

Titolo Gestione degli incidenti

Dettaglio

Note

Controlli

Evidenze

Documenti

Log eventi

> ISO27001 Controlli

> ISO27001 Requisiti

> Cis v8

> Fncs v2.0

> Nist v1.1

> Nist v2.0

Mappatura misure  
di sicurezza NIS2  
con i vari  
framework  
(ISO27001, FNCS,  
etc.)

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

× SOA 1A inizio attività adeg.

Generale **Controlli**

Operazioni massive

? 93 C ☰ Cerca

Titolo gruppo	ID	Ref.2013	Descrizione	Incluso	Valutazione	Valutazione target
Organizational controls	A.5.1	A.5.1.2 A.5.1.1	Policies for infor...	✓	Inadeguato	Quasi adeguato
Organizational controls	A.5.2	A.6.1.1	Information secu...	✓	Adeguato	Adeguato
Organizational controls	A.5.3	A.6.1.2	Segregation of d...	✓	Quasi adeguato	Adeguato
Organizational controls	A.5.4	A.7.2.1	Management res...	✓	Quasi adeguato	Adeguato
Organizational controls	A.5.5	A.6.1.3	Contact with aut...	✓	Adeguato	Adeguato
Organizational controls	A.5.6	A.6.1.4	Contact with spe...	✓	Adeguato	Adeguato
Organizational controls	A.5.7	new	Threat intelligence	✓	Quasi adeguato	Adeguato
Organizational controls	A.5.8	A.6.1.5 A.14.1.1	Information secu...	✓	Quasi adeguato	Adeguato
Organizational controls	A.5.9	A.8.1.1 A.8.1.2	Inventory of infor...	✓	Adeguato	Adeguato
Organizational controls	A.5.10	A.8.2.3 A.8.1.3	Acceptable use o...	✓	Adeguato	Adeguato
Organizational controls	A.5.11	A.8.1.4	Return of assets	✓	Inadeguato	Adeguato
Organizational controls	A.5.12	A.8.2.1	Classification of i...	✓	Adeguato	Adeguato
Organizational controls	A.5.13	A.8.2.2	Labelling of infor...	✓	Adeguato	Adeguato

Colonne  
Filtri

Per ogni framework supportato:

- Applicabilità
- Maturità
- GAP analysis

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

Controllo



Gruppo A.5 - Organizational controls

Controllo A.5.1 - Policies for information security

Riferimento 2013 A.5.1.2 A.5.1.1

> Attributi

Applicabilità

Valutazione

Note

**Documenti**

Funzioni

Evidenze

KPI

Log eventi

Modifica

2



Cerca



Oggetto



Identificativo



Manuale SGSI

MAN-01

Master policy

POL-01

Inoltre:

- Note
- Documenti
- Funzioni
- Evidenze
- KPI

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

× ID.AM-2 - Asset Management

**Funzione:** Identificare - (ID)

**Categoria:** Asset Management - ()

**Descrizione:** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.

**Subcategoria:** ID.AM-2 - Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione

> Attributi

Valutazione   Note   Documenti   Funzioni   Evidenze   KPI   Guida   ISO27001:2022   Log eventi

> SoA di riferimento

SOA 1A inizio attività adeg.

> ISO27001 Controlli

Mappatura  
trasversale  
controlli FNCS  
con ISO27001

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

## Mappatura asset e processi (elenco / gerarchia)

Home **Asset** Modelli stampa Documenti

+ Aggiungi Cancella Importa

? 20

Identificativo ↑	Attivo	Assegnato	Descrizione tecnica	Descrizione funzionale
0123	✓			
Ambiente esterno	✓		Ambiente esterno	
Data center	✓		Sala macchine	
Domain Controller	✓		Server Dell	
Edificio uffici	✓		Edificio uffici	
File Server	✓		File Server primario	
Firewall	✓			
Laptop		✓	intel i5 8gb RAM 256gb HD	
Laptop pro		✓	intel i7 32GB ram 512gb HD	
PC 08281	✓	✓	Computer 22 pollici	
PC fisso basico			intel i3 4gb ram 128gb hd	
Proxy	✓		Proxy	
Server Diseani	✓		File server dedicato ai diseani CAD	

Home Società Funzioni aziendali **Processi** Settings

Generic srl Tutte i processi

Orientamento

```
graph TD;
  Root[Generic srl ^5] --- P1[Processo commerciale];
  Root --- P2[Flusso contabile ^1];
  Root --- P3[Manutenzione sistemistica ^1];
  Root --- P4[Gestione stabilimento ^2];
  Root --- P5[Processo gestione logistica ^1];
  P2 --- P2_1[Gestione fornitori Italia];
  P3 --- P3_1[Maintenance e networking AWS];
  P4 --- P4_1[Produzione];
  P4 --- P4_2[Pianificazione produzione];
  P5 --- P5_1[Acquisti aziendali];
```

The diagram shows a hierarchical structure of processes for 'Generic srl'. The root node is 'Generic srl' with a cardinality of 5. It branches into five main categories: 'Processo commerciale', 'Flusso contabile' (cardinality 1), 'Manutenzione sistemistica' (cardinality 1), 'Gestione stabilimento' (cardinality 2), and 'Processo gestione logistica' (cardinality 1). Further sub-processes are shown: 'Gestione fornitori Italia' under 'Flusso contabile', 'Maintenance e networking AWS' under 'Manutenzione sistemistica', 'Produzione' and 'Pianificazione produzione' under 'Gestione stabilimento', and 'Acquisti aziendali' under 'Processo gestione logistica'.

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

Customer service

Assets Valutazione Impatto Figli attuali Aggiungi figli Cambia padre

cliccare sulla riga per l'inserimento dei parametri di criticità dell'asset nel processo

Modifica 21 Cerca

Nome ↑	Importanza	Conseguenza	Degrado
App "Presenze Personali"	Marginale	Nessuna	
App Approvazione Presenze...	Marginale	Nessuna	
App Scontrini Nota Spese	Marginale	Nessuna	
App monitoraggio km	Marginale	Nessuna	
Autenticazione (servizio)	Vitale	Blocco	
CRM	Vitale	Blocco	
DNS	Grande	Degrado	
File server	Vitale	Blocco	
Firewall principale	Vitale	Blocco	
Microsoft O365	Marginale	Nessuna	
PC portatili	Vitale	Blocco	
Rete LAN	Vitale	Blocco	

Modulo BIA & Risk Assessment: processi e criticità degli asset su cui poggiano

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

× Customer service

Assets Valutazione Impatto Figli attuali Aggiungi figli Cambia padre

### Dettagli Processo

Importanza del processo  
Processo che può influire notevolmente sul raggiungimento della missione dell'organizzazione

Priorità ripristino  
Inserisci un valore

Motivazione  
0/1000

### Conseguenze interruzione processo

> Danno ambientale	N/A
> Effetti sui dipendenti e sul benessere dell'organizzazione	Medio
> Conseguenze legate all'infrazione di requisiti statuari o regolamentari	N/A
> Impatto sulla qualità dei prodotti e dei servizi	Alto
> Danno alla reputazione	Alto

Modulo BIA & Risk Assessment: processi e conseguenze interruzione (sotto 6 aspetti)

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

× Customer service

## Tempi di ripristino

### Guida ai tempi di ripristino

I valori di RTO e MTPD teorici vengono calcolati automaticamente sulla base dei valori di impatto selezionati durante la prima compilazione della valutazione:

- RTO è il tempo di ripristino dove è stato indicato il primo impatto "medio"
- MTPD è il tempo massimo di ripristino dove è stato indicato il primo impatto "critico"

E' possibile indicare un valore manuale.

RTO teorico

Fino a 10 giorni e oltre

RTO - Tempo di ripristino desiderato

Fino a 4 ore

MTPD teorico

Fino a 10 giorni e oltre

MTPD - Tempo massimo di ripristino tollerabile

Fino a 10 giorni e oltre

Motivazione

Modulo BIA & Risk  
Assessment:  
processi e  
RTO / MTPD

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

Home Assets **Processi** Minacce Gruppo Minacce Vulnerabilità Contromisure Calcolo rischio

+ Aggiungi Cancella Operazioni massive ? 57 Cerca

Nome	Gruppo	Riservatezza	Integrità	Disponibilità	Applicabile	Rischio Potenziale	Rischio Residuo
Accesso amministr...	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 oranzizz...			✓	✓	Basso	Basso

Modulo BIA & Risk Assessment: minacce e valutazione del rischio

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

Questionari configurabili per l'audit della supply chain

✕ Modifica gruppo domande

Informazioni generali

Domande

Log eventi

+ Aggiungi

↑↓ Ordine

🗑 Cancelli

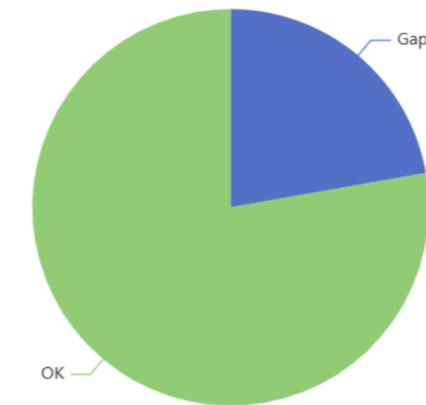
4

Cerca



Ordine	Dipende da	Domanda	Tipologia risposta	Peso	Numero risposte
22	—	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?	Singola	⬆	3
23	—	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?	Singola	⬆	3
24	—	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?	Singola	⬆	3
25	—	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?	Singola	⬆	3

✕ 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%

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

Gestione incidenti con calcolo gravità parametrizzabile

× Modifica evento

Registrazione evento ● Valutazione evento Gestione incidente Post-Incident review

× Modifica evento

Data e ora evento: 19/11/2024 12:07

Numero evento: 6

Oggetto: Cliccato su link sospetto

Stato: Registrato

× Modifica evento

▼ Informazioni generiche

\* Società: Generic srl | Numero evento: 6 | Stato: Registrato

\* Data e ora evento: 19/11/2024 12:07 | Origine segnalazione: Email

\* Cognome segnalante: Doe | \* Nome segnalante: John

Email segnalante: john.doe@acme.com | Telefono segnalante: Inserisci un valore | Funzione segnalante: Inserisci un valore

Riferimento ticket: Inserisci un valore | \* Gestore segnalazioni: Davide M.

\* Oggetto: Cliccato su link sospetto

\* Descrizione dell'evento:

▼ Calcolo gravità

Istruzioni | Calcolo | Parametrizzazione

- > Categoria Minacce (CM)
- > Rilevanza Informazioni (RI)
- > Danno Accertato (DA)
- > Estensione Evento (EE)
- > Area Impattata (AI)
- > Rischio Propagazione (RP)
- > Soglie
- > Valutazione

# Come Atena Governance semplifica la gestione della Direttiva NIS2?

Action plan: pianificazione e gestione delle remediations

Home Richieste Progetti **Task**

+ Aggiungi Cancella Visualizza tutti

6 [Icona] [Icona] [Icona] 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

# Conclusioni

- La **Direttiva NIS 2 impatterà un gran numero di aziende**, ben oltre il perimetro dei soggetti essenziali e importanti (si stimano circa 15.000 soggetti, oltre alla supply chain)
- La **gestione strutturata della cyber-security** sarà un requisito fondamentale per le aziende per poter continuare ad operare con i propri clienti, ovvero diventa un **elemento abilitante del business** (inclusa la possibilità di ricevere credito dal sistema bancario)
- La **compliance** alle prescrizioni della NIS 2 dovrà essere adeguatamente dimostrabile: possibile di farlo con l'**adesione a framework standard** (ISO27001 / FNCS)
- Un'**adeguata analisi multi-rischio** ne è un **requisito fondamentale**

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

# Q&A



# Security Summit

Milano 11-12-13 marzo 2025



## Contatti:

**Tel. 0455118570**

**[info@axsym.it](mailto:info@axsym.it)**

**[www.axsym.it](http://www.axsym.it)**

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

**Grazie per l'attenzione!**