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*

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

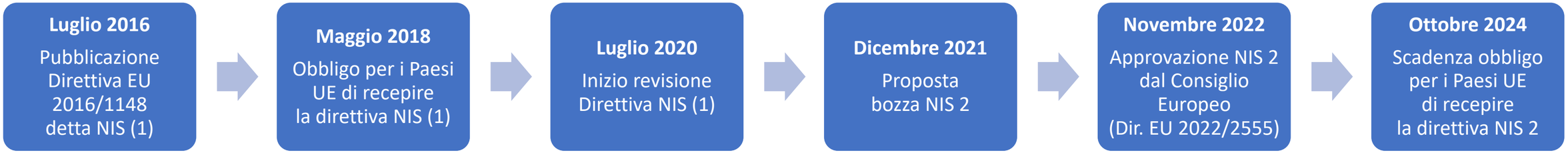
Gli ambiti della consulenza Axsym

- 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

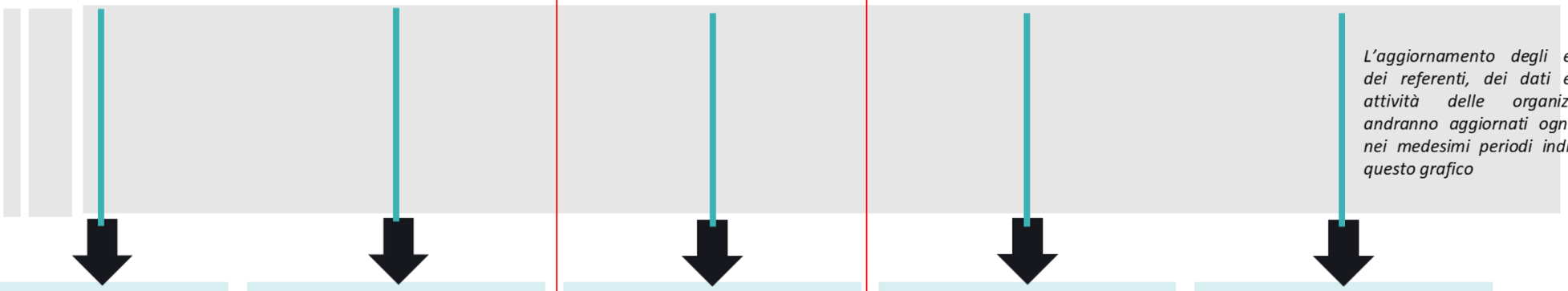
Dal 18/10/2024: portale iscrizioni (in attesa di pubblicazione)

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

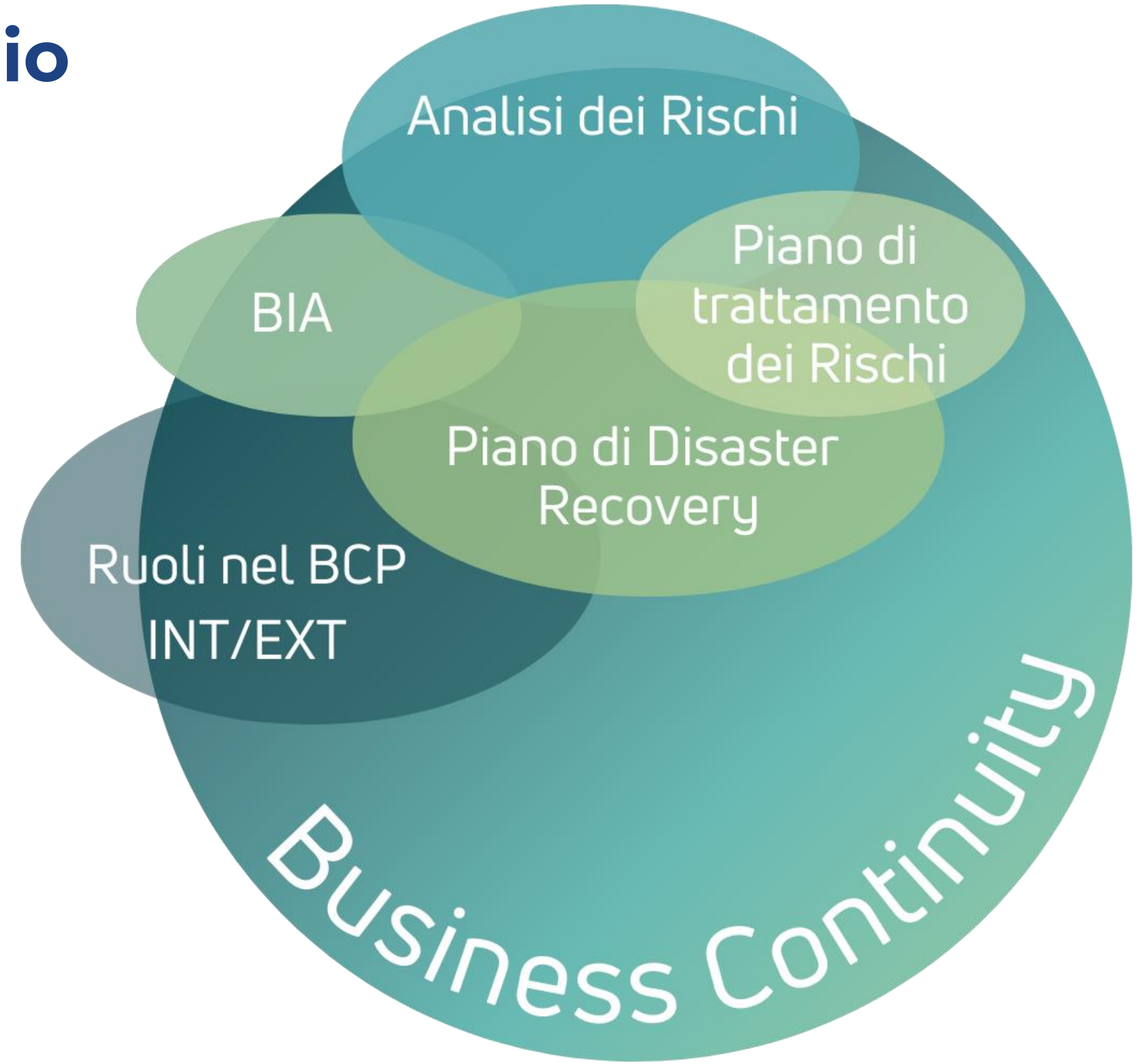
L’art. 2 (Definizioni) alla lettera dd) specifica:

«**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:

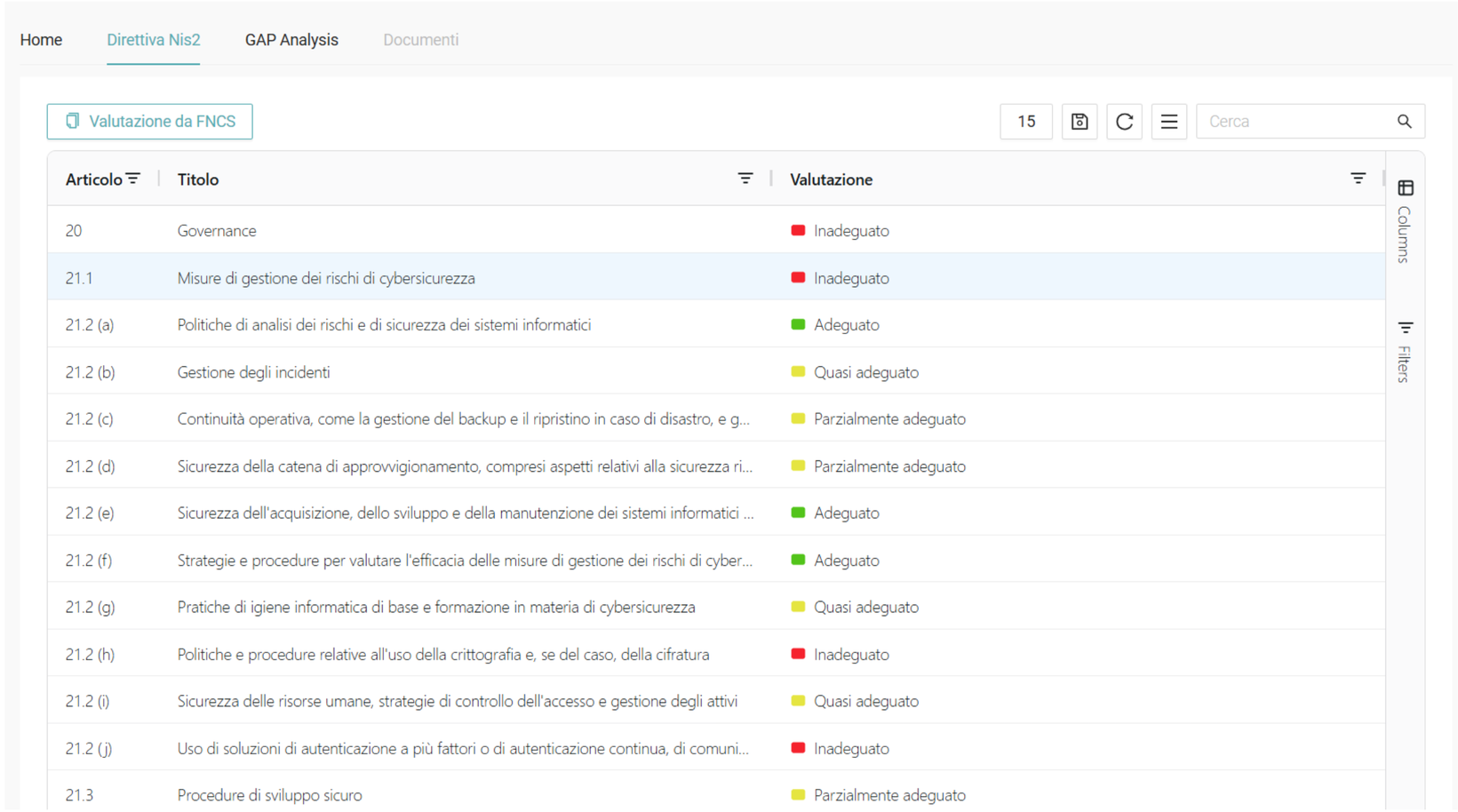
- GDPR
- NIS 2
- Business Impact Analysis
- Risk Assessment
- ISO 27001
- Cyber Security Framework FNCS, NIST, CIS
- Incidenti di Sicurezza, Evidenze, KPI
- Audit e Action Plan

Come Atena Governance semplifica la gestione della Direttiva NIS2?

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

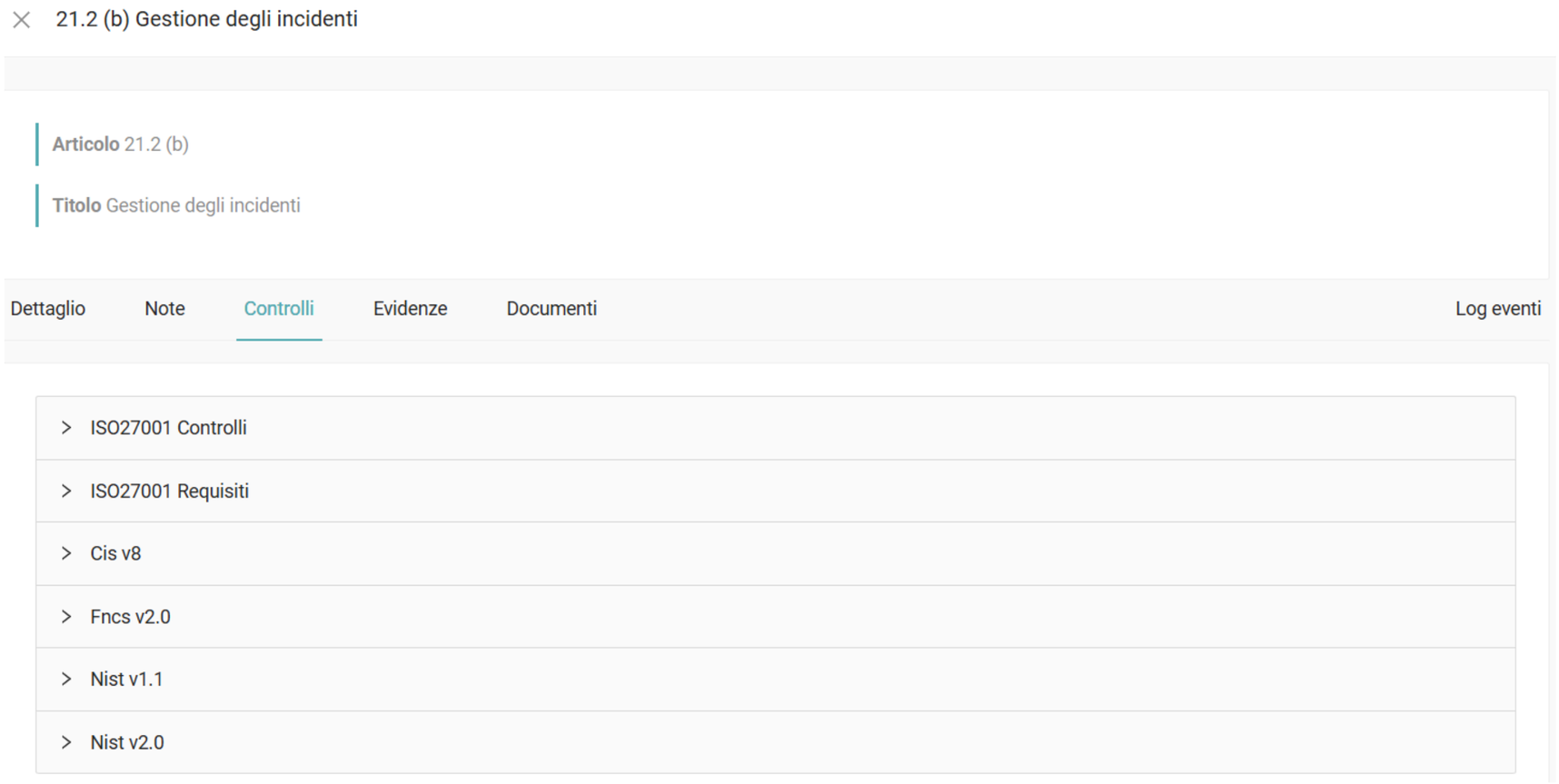
Gestire con un'**unica piattaforma web centralizzata in cloud** tutta la documentazione e le **attività richieste dallo standard e della Direttiva NIS2 a 360°** (anche per più aziende).

Come Atena Governance semplifica la gestione della Direttiva NIS2?



Valutazione adeguatezza requisiti richiesti dalla NIS2

Come Atena Governance semplifica la gestione della Direttiva NIS2?



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 | Cerca

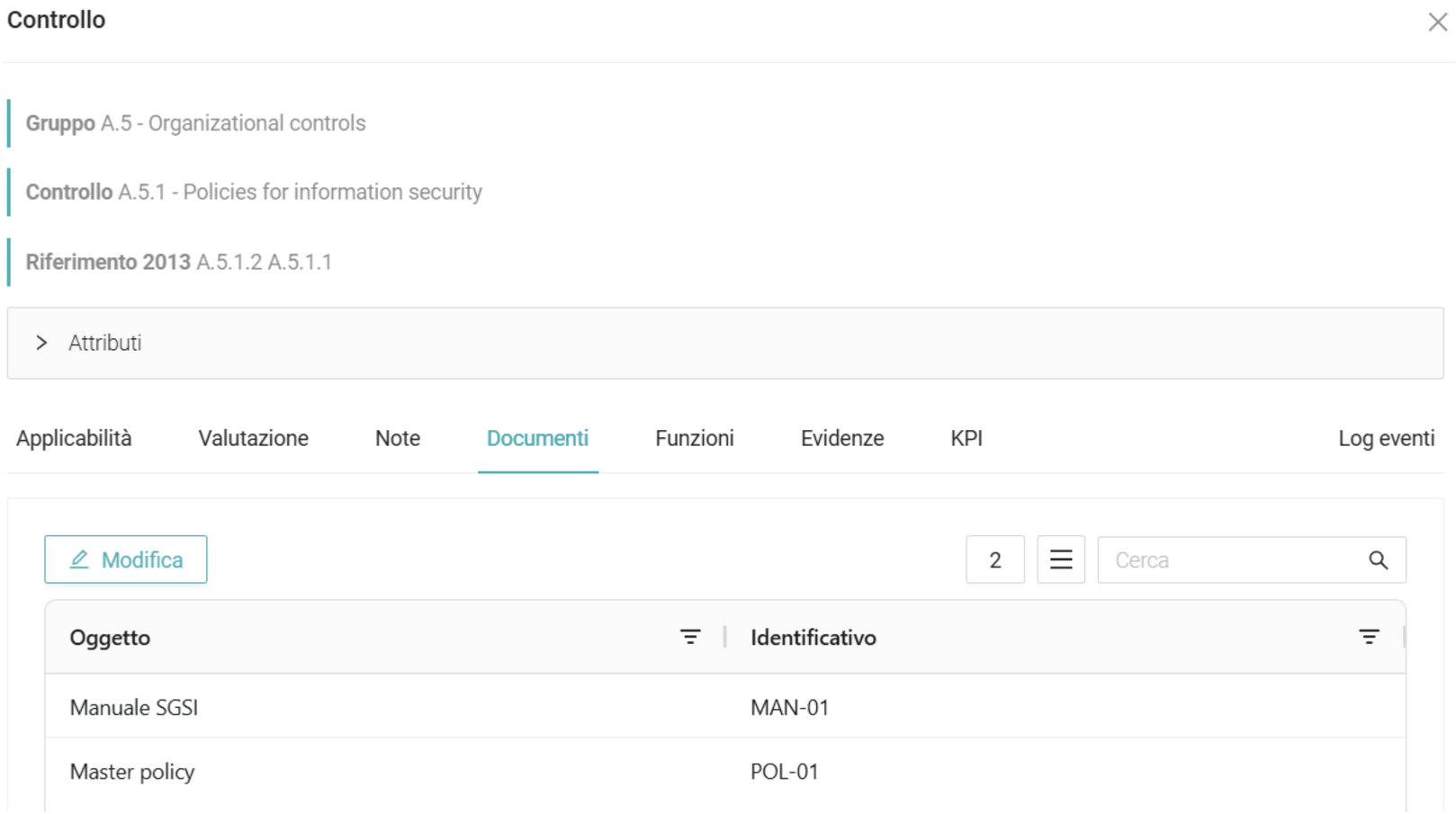
Titolo gruppo	ID	Ref.2013	Descrizione	Incluso	Valutazione	Valutazione target
Organizational controls	A.5.1	A.5.1.2 A.5.1.1	Policies for infor...	✓	Inadeguato	Quasi adeguato
Organizational controls	A.5.2	A.6.1.1	Information secu...	✓	Adeguato	Adeguato
Organizational controls	A.5.3	A.6.1.2	Segregation 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

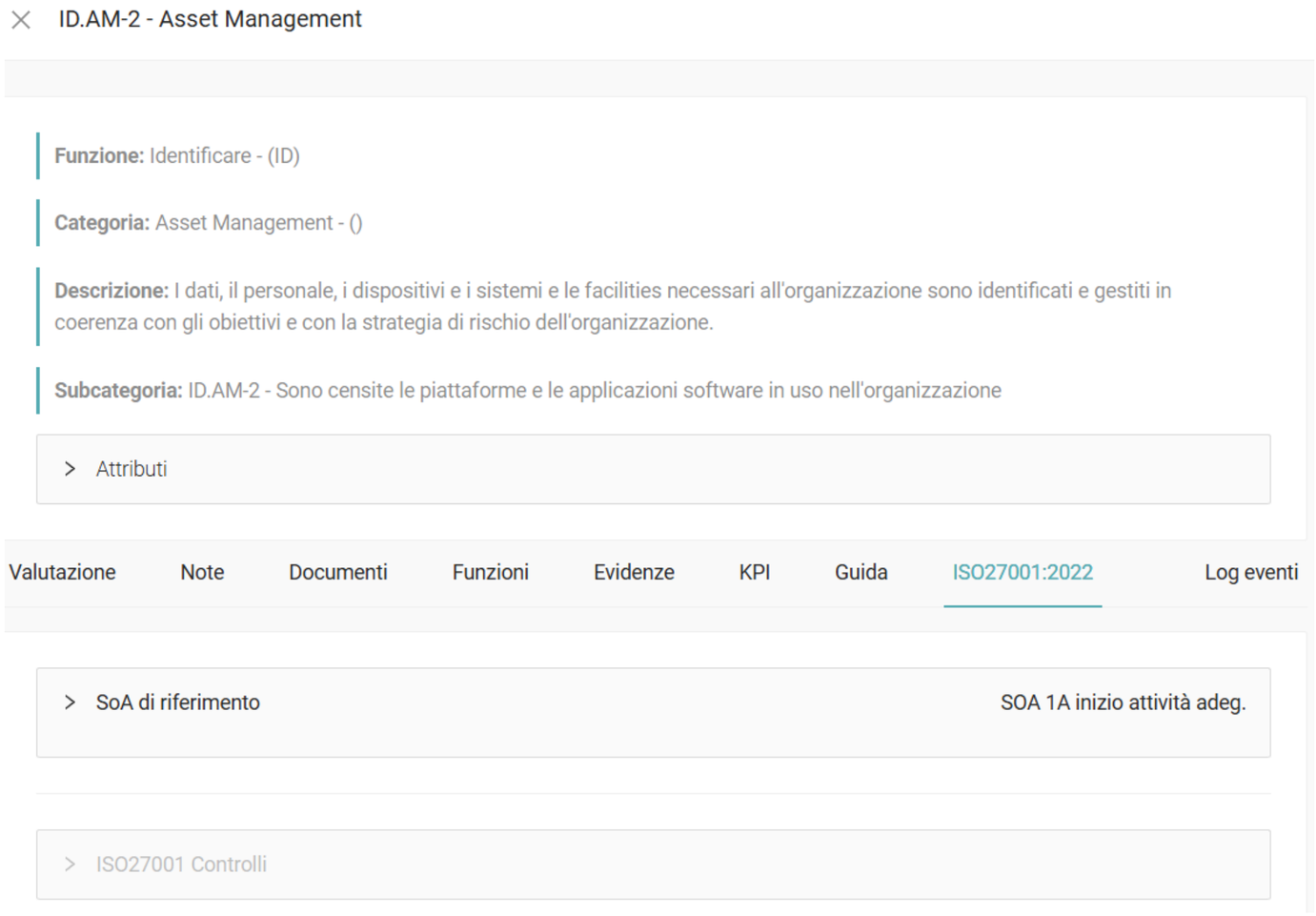
Come Atena Governance semplifica la gestione della Direttiva NIS2?



Inoltre:

- Note
- Documenti
- Funzioni
- Evidenze
- KPI

Come Atena Governance semplifica la gestione della Direttiva NIS2?



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

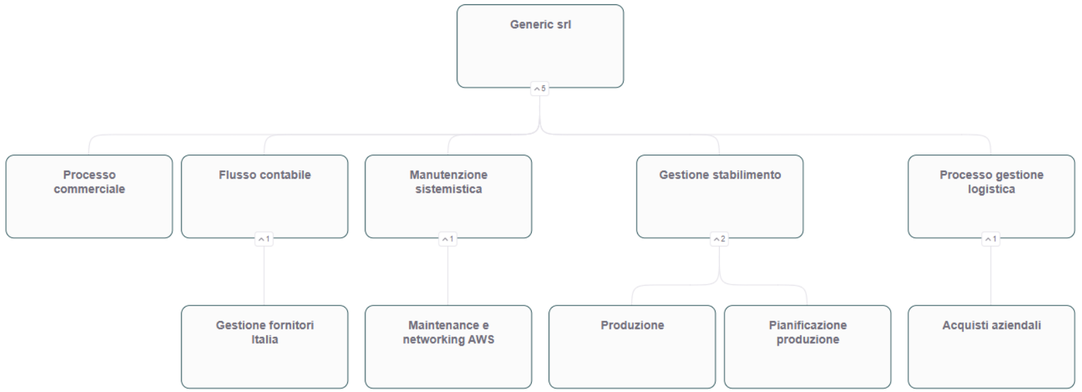
Identificativo	Attivo	Assegnato	Descrizione tecnica	Descrizione funzionale
0123	✓			
Ambiente esterno	✓		Ambiente esterno	
Data center	✓		Sala macchine	
Domain Controller	✓		Server Dell	
Edificio uffici	✓		Edificio uffici	
File Server	✓		File Server primario	
Firewall	✓			
Laptop		✓	intel i5 8gb RAM 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 Disegni	✓		File server dedicato ai disegni CAD	

Home Società Funzioni aziendali Processi Settings

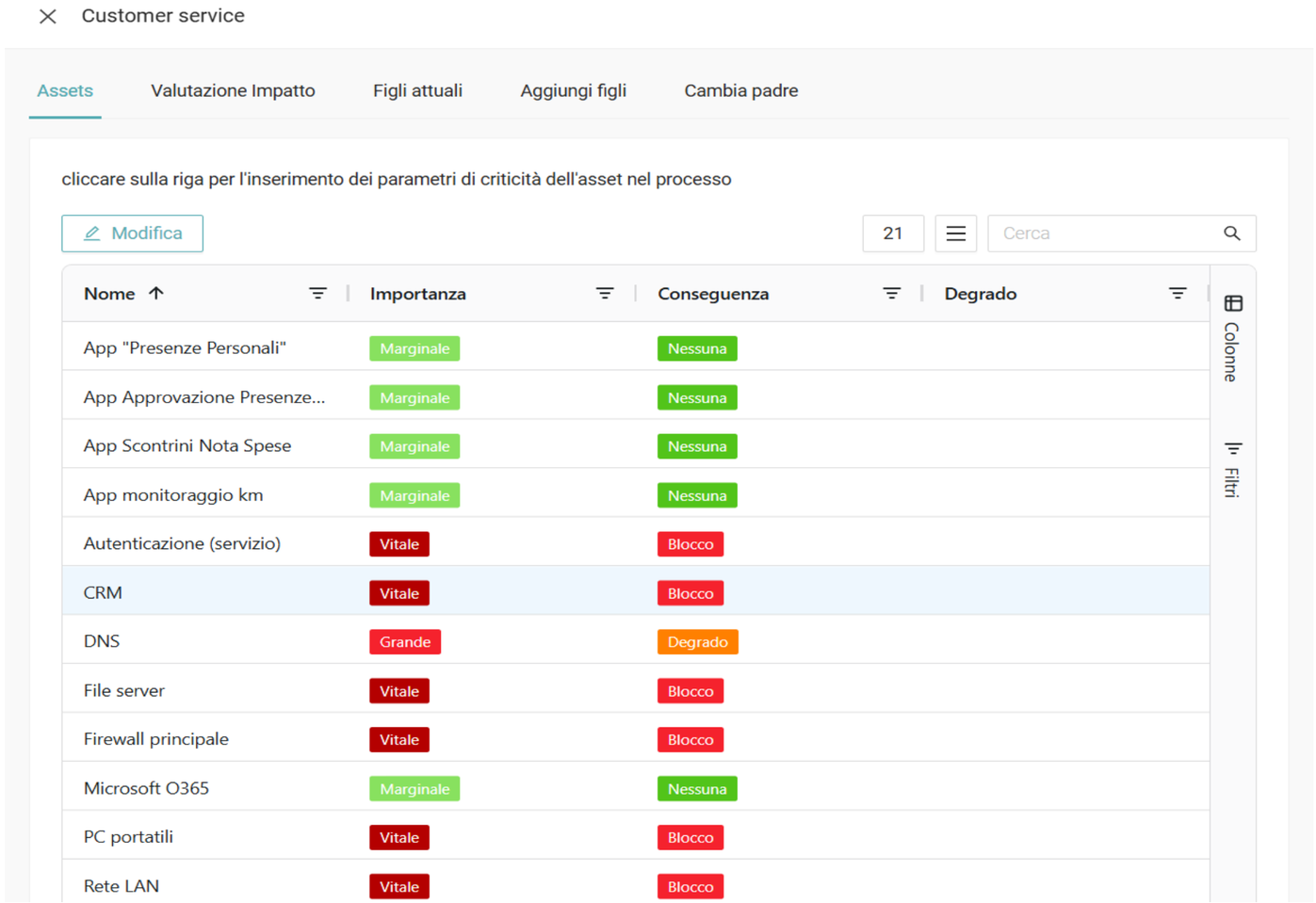
Generic srl | Tutte i processi

Tutte i processi

Orientamento

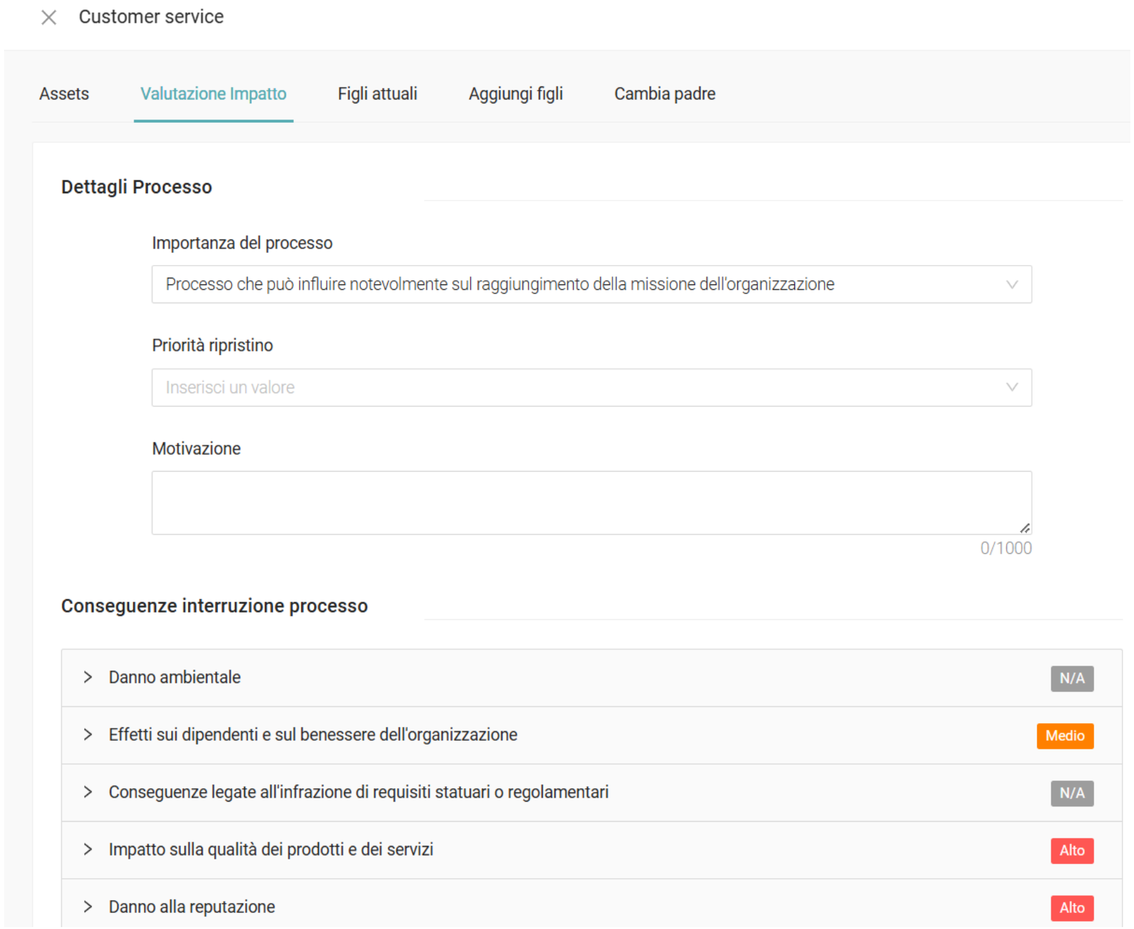


Come Atena Governance semplifica la gestione della Direttiva NIS2?



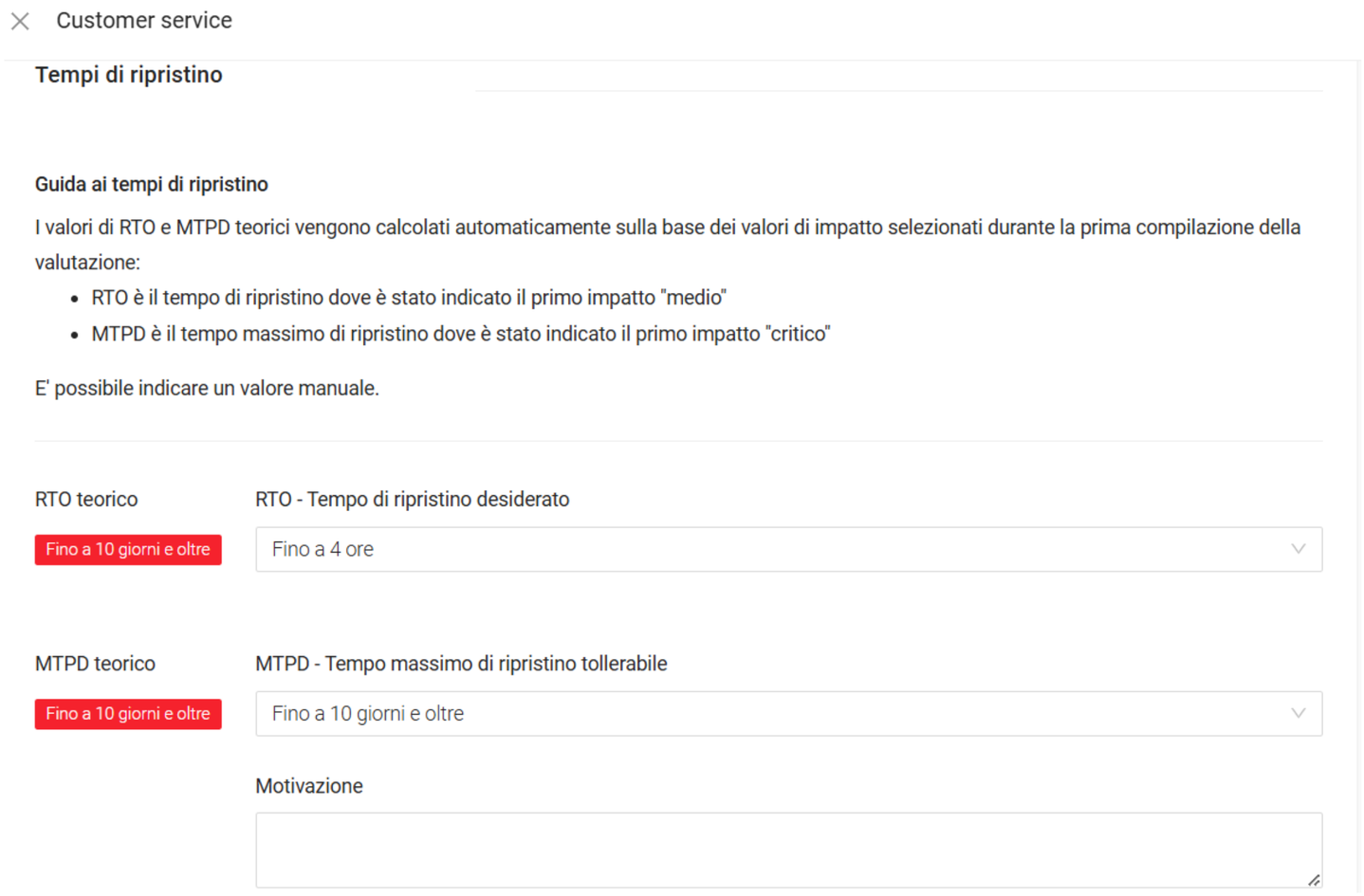
Modulo BIA & Risk Assessment: processi e criticità degli asset su cui poggiano

Come Atena Governance semplifica la gestione della Direttiva NIS2?



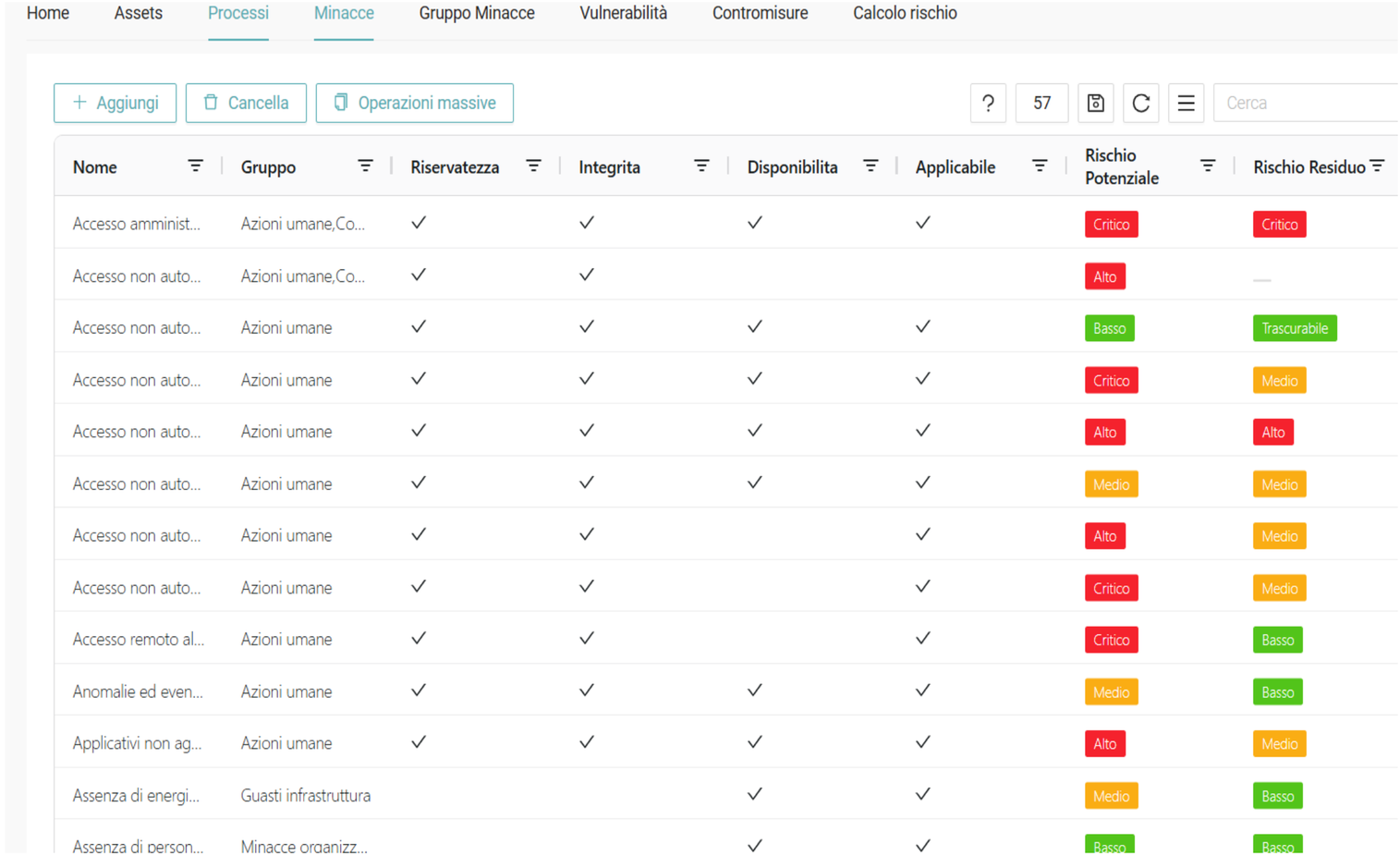
Modulo BIA & Risk Assessment: processi e conseguenze interruzione (sotto 6 aspetti)

Come Atena Governance semplifica la gestione della Direttiva NIS2?



Modulo BIA & Risk Assessment: processi e RTO / MTPD

Come Atena Governance semplifica la gestione della Direttiva NIS2?

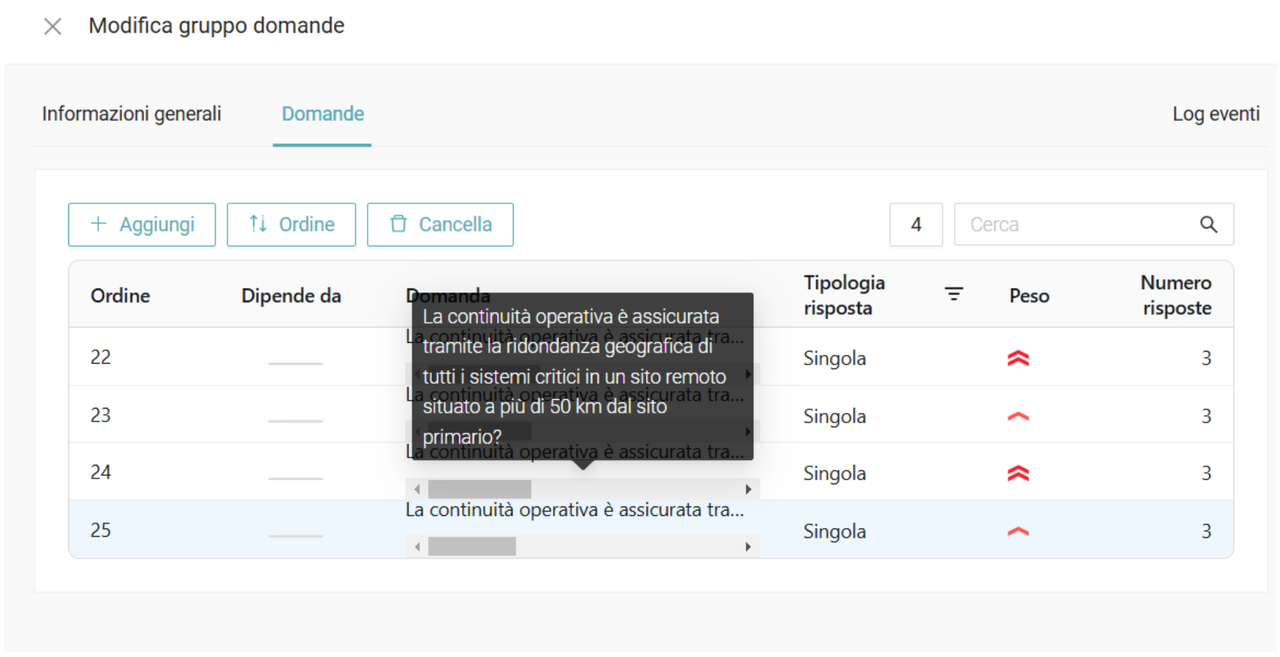


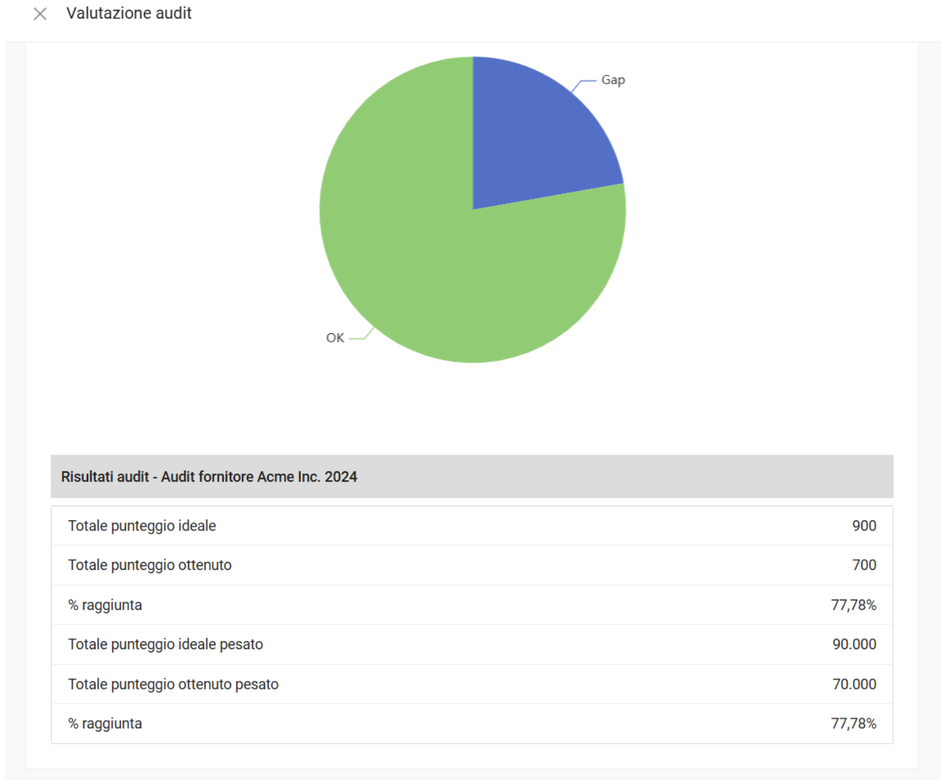
Nome	Gruppo	Riservatezza	Integrità	Disponibilità	Applicabile	Rischio Potenziale	Rischio Residuo
Accesso amminist...	Azioni umane,Co...	✓	✓	✓	✓	Critico	Critico
Accesso non auto...	Azioni umane,Co...	✓	✓			Alto	—
Accesso non auto...	Azioni umane	✓	✓	✓	✓	Basso	Trascurabile
Accesso non auto...	Azioni umane	✓	✓	✓	✓	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 BIA & Risk Assessment: minacce e valutazione del rischio

Come Atena Governance semplifica la gestione della Direttiva NIS2?

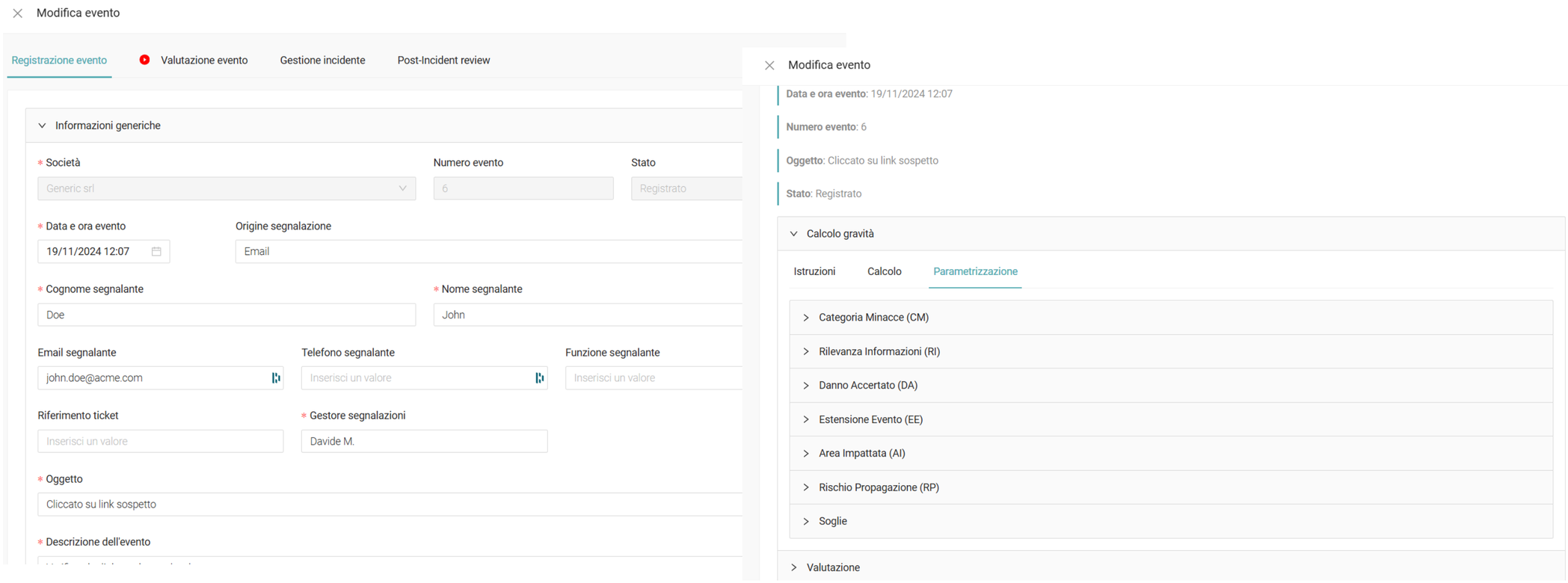
Questionari configurabili per l'audit della supply chain





Come Atena Governance semplifica la gestione della Direttiva NIS2?

Gestione incidenti con calcolo gravità parametrizzabile



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 | 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 fatto 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

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

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

Grazie per l’attenzione!