SECURITY SUMMIT

Verona, 10 ottobre 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

# *ISO 27001:2022 vs 2013, quali sono le differenze e come gestire in modo ottimale l'adeguamento alla nuova versione dello Standard*

*Alessio L.R. Pennasilico, Comitato Scientifico CLUSIT*

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

10 ottobre Verona 2023 orario 12.20-13.00

# Alessio L.R. Pennasilico aka -=mayhem=-

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

Membro del Comitato Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Membro del Comitato Direttivo di Informatici Professionisti AIP Associazione Informatici Professionisti ITCS Italian Computer Society

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

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

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

# 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 DELLE CONSULENZE AXSYM

- **Information Security Governance**
- Framework di Cyber Security **CIS, NIS2, NIST**
- **Business Impact Analysis**
- **Risk Assessment**
- **Continuità operativa ICT**
- **Compliance GDPR** e **Whistleblowing**
- Compliance al Cloud **ISO 27017, 27018, CSA**
- Compliance standard **ISO 27001, 22301, 20000**

**Axsym è certificata**
**ISO/IEC 27001:2013**
Passaggio a versione 2022 pianificato per Aprile 2024

# PREMESSA: LO STANDARD NON È SOLO PER CHI VUOLE CERTIFICARSI

Erroneamente molti pensano che il passaggio alla nuova versione dello standard sia rilevante solo per le aziende certificate/che desiderano certificarsi ISO/IEC 27001.

In realtà lo standard risulta molto utile non solo per le organizzazioni effettivamente interessate a certificarsi ISO 27001, ma anche per tutte le organizzazioni che desiderano **rendere più efficiente ed efficace la gestione della sicurezza IT** prendendo come riferimento proprio lo standard ISO 27001 in quanto frutto delle **best practice internazionali** in ambito sicurezza delle informazioni.

In tal caso l'organizzazione può decidere a quali dei controlli ISO 27001:2022 adeguarsi e in quale misura, senza vincoli dettati dalla necessità di certificazione, ma solo con la volontà di fare ciò che è meglio per la propria organizzazione dal punto di vista della sicurezza IT restando comunque aggiornati sulle evoluzioni settoriali e, di conseguenza, della normativa.

# COSA CAMBIA CON LA NUOVA ISO 27001:2022

## NOVITÀ E DIFFERENZE DELLA NUOVA VERSIONE DELLO STANDARD ISO 27001:2022 RISPETTO ALLA ISO 27001:2013

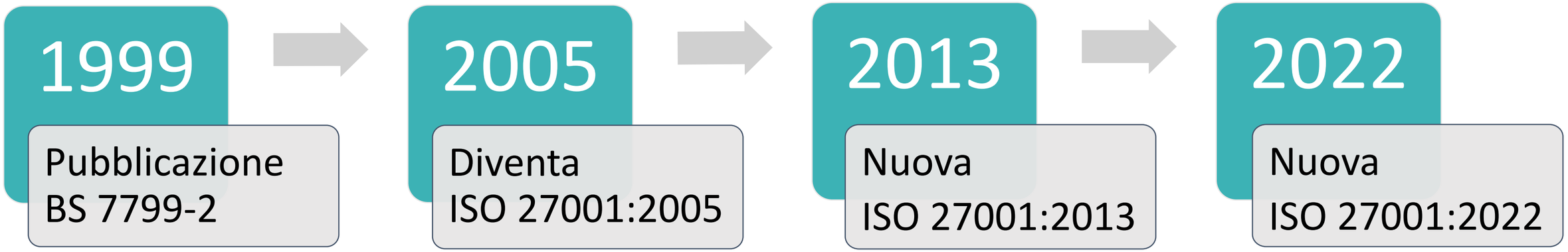
Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
VERONA

AXSYM
Compliance & Information Security

# LO STANDARD ISO 27001

A ottobre 2022 è stata pubblicata la **nuova versione** dello standard ISO/IEC 27001 relativo ai Sistemi di Gestione della Sicurezza delle Informazioni - riconducibile a una più ampia **revisione degli standard della famiglia ISO 27000**.



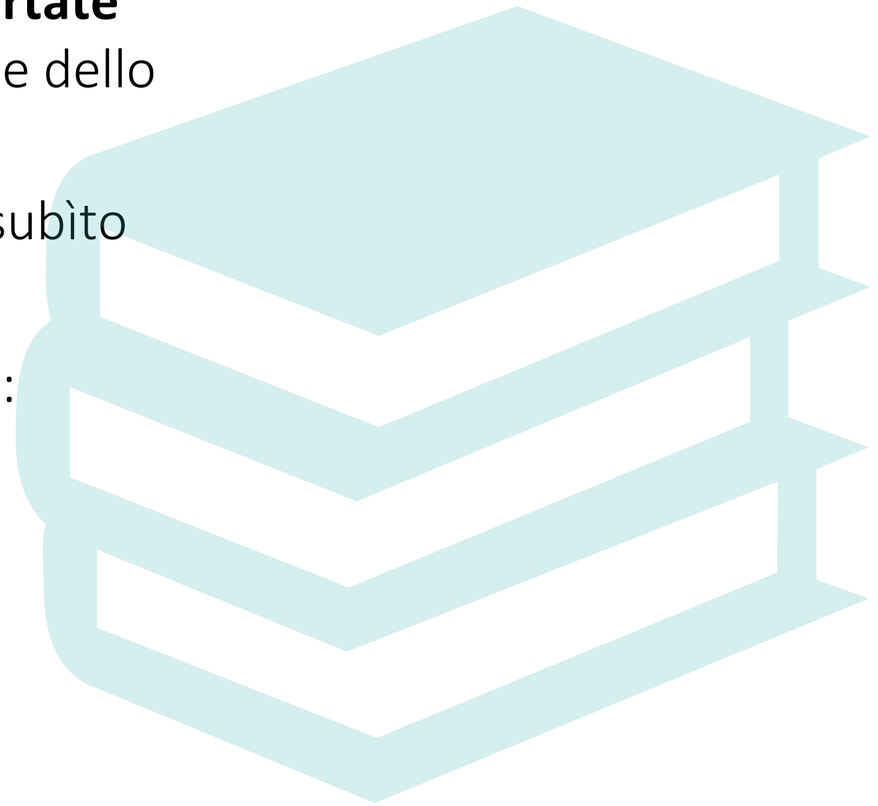
# MODIFICHE AL DOCUMENTO PRINCIPALE DELLO STANDARD

Nel complesso, rispetto alla revisione del 2013, le **modifiche apportate** dalla nuova versione della ISO 27001:2022 al documento principale dello standard **sono di piccola entità (minor release)**.

Di seguito vengono presentati i nuovi requisiti e quelli che hanno subìto delle modifiche.

Per completezza di informazione, si segnala che è cambiato anche:

- Il nome dello standard
- L'abstract
- Il punto 3 relativo alla terminologia



## NUOVO NOME

| ISO 27001:2013 | ISO 27001:2022 |
| --- | --- |
| Information **technology** — **Security techniques** — Information security management systems — Requirements | Information **security, cybersecurity and privacy protection** — Information security management systems — Requirements |

# ABSTRACT E TERMINOLOGIA

Nell'abstract è stata aggiunta la seguente dicitura: "Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document."
È stato quindi specificato che per poter dichiarare che la propria organizzazione è conforme allo standard ISO 27001 questa **deve applicare necessariamente tutti i requisiti dal punto 4 al punto 10**.

Nel punto 3 relativo alla terminologia viene indicato di applicare le definizione della norma ISO/IEC 27000 + di consultare la terminologia data sui rispettivi siti web dell'Organizzazione ISO e di IEC Electropedia.

# NUOVI REQUISITI

- Nessun requisito significativo è stato cancellato
- Il numero di requisiti rimane pari a 11
- I nuovi requisiti sono i seguenti:
  - **4.2 c)** Requisiti delle parti interessate da soddisfare attraverso l'ISMS
  - **6.4** Pianificazione dei cambiamenti
  - **8.1** Stabilire criteri per i processi e attuare il controllo su di essi
  - **9.3.2. c)** Input del riesame della direzione
    - cambiamenti nei bisogni e
    nelle aspettative delle parti interessate

## NUOVO REQUISITO: 4.2 C)

# COMPRENDERE I BISOGNI E LE ASPETTATIVE DELLE PARTI INTERESSATE

Rispetto alla versione precedente, la versione 2022 prevede un nuovo elemento c) al punto 4.2 dei requisiti (Comprendere i bisogni e le aspettative delle parti interessate).

Il nuovo punto (c) richiede di effettuare un'analisi di quali dei requisiti delle parti interessate devono essere affrontati attraverso l'ISMS.

## NUOVO REQUISITO: 6.3

# PIANIFICAZIONE DEI CAMBIAMENTI

Secondo il punto 6.3, quando l'organizzazione decide di effettuare dei cambiamenti a livello di Sistema di Gestione della Sicurezza delle Informazioni, questi devono essere svolti in modo pianificato, non improvvisato.

## NUOVO REQUISITO: 8.1

# PIANIFICAZIONE E CONTROLLO

Sono stati aggiunti nuovi requisiti per stabilire criteri per i processi di sicurezza e per implementare processi secondo tali criteri.

Tra questi, l'organizzazione deve garantire che i processi, i prodotti o i servizi forniti esternamente che sono rilevanti per il sistema di gestione della sicurezza delle informazioni siano controllati.

## NUOVO REQUISITO: 9.3.2

# RIESAME DELLA GESTIONE

Nella clausola 9.3 è stato aggiunto il nuovo punto 9.3.2 c)
che chiarisce che gli input delle parti interessate devono riguardare
le loro esigenze e aspettative e devono essere rilevanti per l'ISMS.

# REQUISITI CON MODIFICHE

- Al punto **4.4** (Sistema di gestione della sicurezza delle informazioni) è stata aggiunta una frase che specifica che il ISMS deve essere realizzato tenendo conto dei processi aziendali e delle loro interazioni.
- Al punto **5.3** (Ruoli organizzativi, responsabilità e autorità) è stato specificato che la comunicazione dei ruoli avviene internamente all'organizzazione.
- Al punto **6.2** (Obiettivi di sicurezza dell'informazione e pianificazione per raggiungerli), sono stati aggiunti due elementi relativi ai requisiti degli obiettivi che devono quindi essere 1) monitorabili e 2) disponibili in forma documentata.

# REQUISITI CON MODIFICHE

- Al punto **7.4** (Comunicazione), in merito a cosa, quando e a chi trasmettere comunicazioni relative all'ISMS, i punti relativi a "chi deve comunicare" (punto d) e "attraverso quale processo" (punto e) sono stati sintetizzati in un semplice "come".
- Al punto **9.2 e 9.3** è cambiata la struttura con l'aggiunta di sotto-punti.
- Al punto **10** (Miglioramento), è stato invertito l'ordine dei sotto-punti.
  Quindi la prima è Miglioramento continuo (10.1), e la seconda è Non conformità e azioni correttive (10.2). Il testo di tali clausole non è cambiato.

# MODIFICHE ALL'ALLEGATO A (ANNEX A)

A prima vista, l'allegato A è molto cambiato: il numero dei controlli è sceso da 114 a 93 ed è organizzato in sole quattro sezioni rispetto alle 14 della revisione del 2013. Tuttavia, dopo uno sguardo più attento, diventa evidente che **le modifiche nell'allegato A sono abbastanza moderate**, essendo molte più le variazioni a livello di forma che di sostanza come controlli accorpati o rinominati.

**I nuovi controlli invece sono stati aggiunti in modo da rispondere alle nuove tendenze dell'IT e della sicurezza.**

Di seguito, uno schema riassuntivo delle principali modifiche.

# APPLICABILITÀ DEI CONTROLLI

La nuova ISO 27001:2022 incorpora i precedenti *technical corrigendum* che prevedono un'applicazione più flessibile dei controlli.

Questo perché **i controlli della SoA** (*Statement of Applicability* o Dichiarazione di Applicabilità) **non devono essere necessariamente quelli dell'Allegato A dello standard ma si possono usare anche quelli di altri controlli.**

È comunque necessario effettuare una **verifica rispetto ai controlli dell'Allegato A** in quanto è necessario indicare quali di questi controlli sono stati esclusi.

# LE MODIFICHE DELL'ALLEGATO A IN NUMERI

| ISO 27001:2013 | | ISO 27001:2022 |
|---|---|---|
| 114 | Numero di controlli di sicurezza nell'Allegato A | 93 |
| 14 | Numero di sezioni nell'Allegato A | 4 |
| 33 | Categorie di controllo | Eliminate |

# CATEGORIZZAZIONE DEI CONTROLLI

## ISO 27001:2013

14 aree:

- A.5 Information security policies
- A.6 Organisation of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development, and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

## ISO 27001:2022

4 aree:

- **Organizzativi** (37 controlli)
- **Persone** (8 controlli)
- **Fisici** (14 controlli)
- **Tecnologici** (34 controlli)

# ENTITÀ DELLE MODIFICHE AI CONTROLLI

| | |
|---|---|
| **Modifiche importanti** | 11 nuovi controlli |
| **Modifiche moderate** | 57 controlli accorpati<br>1 controllo diviso |
| **Modifiche lievi** | 23 controlli rinominati ma hanno mantenuto lo scopo |
| **Nessuna modifica** | 35 controlli non hanno subito modifiche ma solo ricodificati |

# CONTROLLI RINOMINATI CON MODIFICHE SIGNIFICATIVE (ESEMPIO)

| ISO 27001:2013 | ISO 27001:2022 |
| --- | --- |
| A.6.2.1 Politica per i dispositivi portatili | A.8.1 User endpoint devices |
| A.9.2.1 Registrazione e de-registrazione degli utenti | A.5.16 Identity manager |
| A.17.1.2. Pianificazione della continuità della sicurezza delle informazioni | A.5.29. Information security during disruption |

# ELENCO DEI NUOVI CONTROLLI

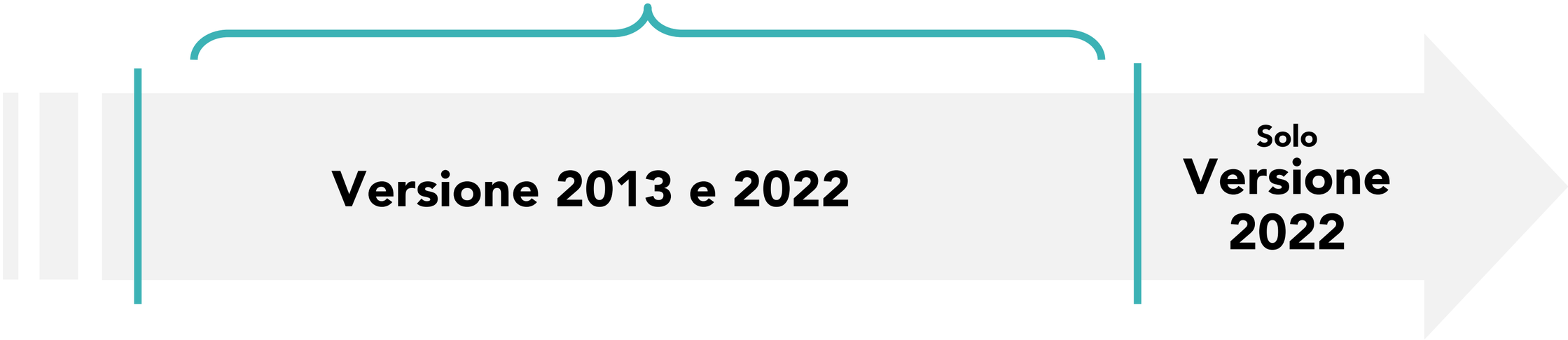
- A.5.7 Threat intelligence
- A.5.23 Information security for use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding

# TEMPI DI TRANSIZIONE

25 ottobre 2022:
Pubblicazione versione ISO27001:2022

**Periodo di transizione**:
le organizzazioni possono scegliere quale versione adottare per la certificazione

31 ottobre 2025:
Scadono tutte le certificazioni basate sulla versione 2013
Sono valide solo le certificazioni svolte sulla versione 2022



# ATTIVITÀ DI TRANSIZIONE: ALCUNE SPECIFICHE

Il termine entro il quale effettuare la transizione è stato definito **nell'IAF MD 26:2022**, documento che ha l'obiettivo di fornire regole uniformi per l'accreditamento degli Organismi di Certificazione.

Secondo tale documento l'audit di transizione:

- **Può essere svolto durante un audit di sorveglianza o ricertificazione** già programmato o in un audit diverso
- **Non può essere documentale**: dovrà prevedere un riesame sul campo dei controlli tecnologici nuovi o modificati scelti dall'organizzazione.

IAF = *International Accreditation Forum*, l'associazione mondiale che raggruppa gli organismi che svolgono l'accreditamento della valutazione di conformità e altri organismi interessati alla valutazione di conformità per quanto riguarda sistemi di gestione ecc.

# ENTRATA IN VIGORE ISO/IEC 27001:2022 COSA FARE?

## INDICAZIONI PER GESTIRE AL MEGLIO IL PASSAGGIO O L'ADEGUAMENTO ALLA NUOVA VERSIONE DELLE NORMA

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
VERONA

AXSYM
Compliance & Information Security

# COSA FARE PER CHI HA GIÀ UN SGSI SECONDO L'ISO 27001:2013

1. Rivedere il **Risk Assessment per allinearlo alla nuova struttura e ricodifica dei controlli**
2. Rivedere e aggiornare la Dichiarazione di applicabilità (**SoA**)
3. Rivedere e aggiornare la **procedura di revisione della gestione ISMS**
4. Rivedere e aggiornare gli **obiettivi di Information Security** e la procedura di monitoraggio, misurazione, analisi e valutazione
5. Rivedere e aggiornare il **piano di comunicazione ISMS**

# COSA FARE SE SI HA UN SGSI

6. Rivedere e aggiornare se necessario altre **politiche, standard e procedure**
7. Rivedere e aggiornare le checklist e i questionari utilizzati per gli **audit** (interni ed esterni)
8. Valutare ed eventualmente adattare **strumenti e servizi di sicurezza di terze parti** (ad es. GRC, SIEM, Threat Intelligence, ecc.) per garantire il supporto dei nuovi punti di controllo.

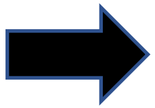
# APPROCCIO COMUNEMENTE UTILIZZATO NELLE AZIENDE ITALIANE

"Metodologie":

- "Abbiamo sempre fatto così"
- "Navigazione a vista"
- "Tutto urgente"
- "Finché non lo chiede, io non lo faccio"

Strumenti:

- Faldoni di documenti cartacei
- Cartelle di file su computer/altri dispositivi
- Condivisione file su tecnologie cloud
- File Excel



Manca sia una solida metodologia alla base sia uno strumento in grado di implementarla correttamente

# APPROCCIO CORRETTO PER LA GESTIONE DELLE ATTIVITÀ DI GOVERNANCE

Metodologie:

- Adozione delle corrette metodologie
- Pianificazione attività
- Tempistiche coerenti con gli obiettivi
- Proattività

Strumenti:

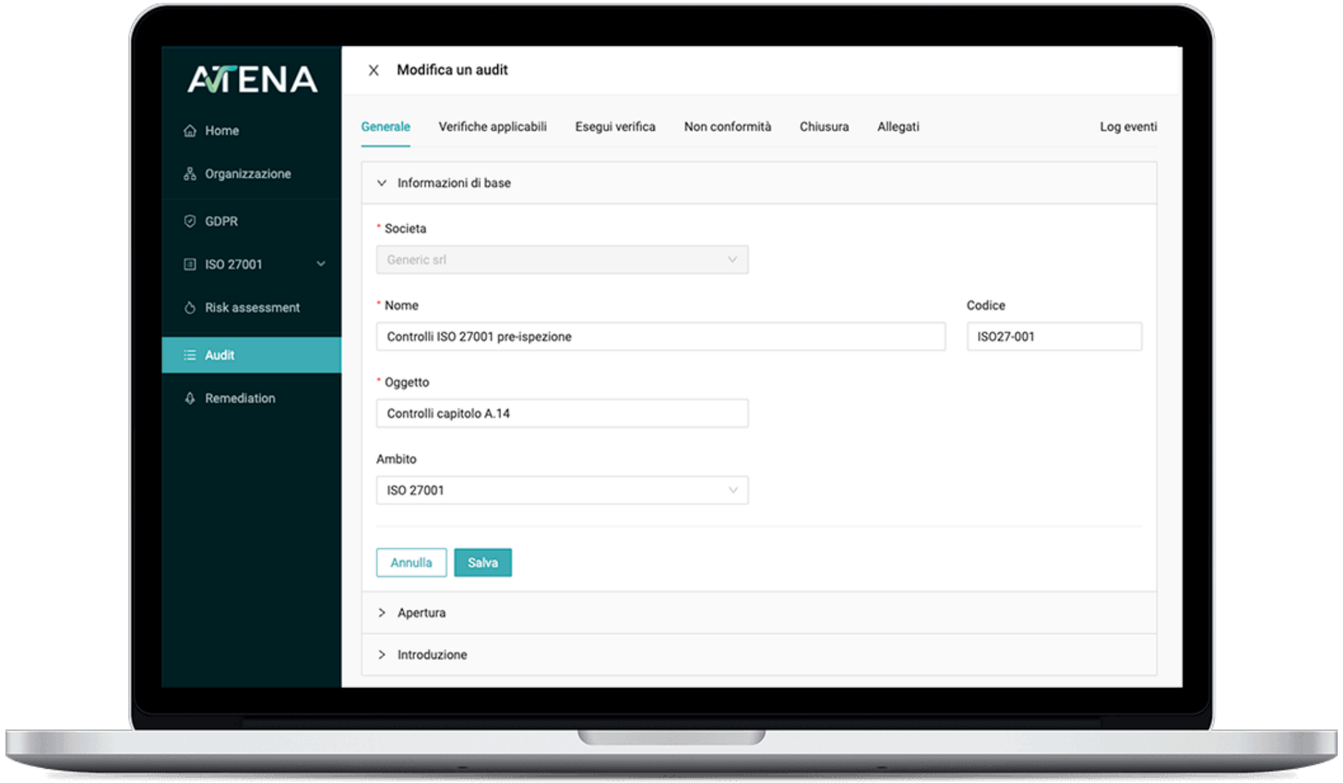
- Digitalizzazione dei documenti
- Database strutturato
- Collaboration
- Piattaforme applicative adeguate

# 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
- Risk Assessment
- Business Impact Analsys
- Cyber Security Framework NIST, NIS, CIS
- Audit e Action Plan
- GDPR

# COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLO STANDARD ISO 27001




Grazie al modulo ISO 27001 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 a 360°** (anche per più aziende)

# COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLO STANDARD ISO 27001

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

3. Svolgere le attività richieste dallo standard come la **dichiarazione di applicabilità, gli audit periodici, l'analisi del rischio e il piano di trattamento dei rischi**

# COME ATENA GOVERNANCE SEMPLIFICA LA GESTIONE DELLO STANDARD ISO 27001


4. **Gestire le non-conformità rilevate**, con indicazione dello stato di avanzamento delle attività, programmazione, scadenze e compiti assegnati

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

# CONCLUSIONI

L'adozione dello standard ISO/IEC 27001 diventa sempre più necessaria per i seguenti motivi:

- Gestire in modo organizzato ed efficace l'Information Security
- Qualificare la propria cyber security posture come elemento di differenziazione e competitività
- Requisito di valutazione della supply chain



**L'adozione di uno strumento ad hoc** come **ATENA Governance** migliorerà la transizione da una versione all'altra o l'implementazione del sistema di gestione, permettendo di ottenere un importante risparmio di tempo, denaro e fatica nella gestione dei processi e delle informazioni richiesti dallo standard.

# 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