ISO 27001 e mitigazione preventiva dei rischi

Trasformare la sicurezza IT da adempimento a vantaggio operativo

Daniele Cerbarano

Lead Auditor ISO 27001



Giorgia Morettin

IT Specialist



Vincenzo Coppola

Pre Sales



factorial IT

Audit Service & Certification

Daniele Cerbarano

CISO & Lead Auditor ISO 27001 di AS&C

Daniele Cerbarano è un professionista specializzato in sistemi di gestione, compliance, cybersecurity e risk management. Vanta esperienza nelle attività di audit e nella gestione della sicurezza delle informazioni, con particolare riferimento allo standard ISO/IEC 27001 e ai temi della NIS2, GDPR e Business Continuity.



Chi è AS&C

Audit Service & Certification è un **Organismo di Certificazione accreditato** da IAS (*International Accreditation Service*) per i servizi di certificazione secondo le norme ISO a livello internazionale.

Oltre ai servizi di verifica e certificazione, AS&C progetta ed eroga corsi di formazione per Auditor e Lead Auditor, fornendo competenze teoriche e pratiche avanzate a risorse aziendali e professionisti che desiderano affacciarsi ai sistemi di gestione (*come ISO 27001, ISO 9001, ISO 14001, ISO 45001 e altri standard di settore*).

I nostri numeri

Valutazione media su google

4.9/5

Basata su 78 recensioni

+2000

Aziende certificate ISO

+500

Auditor formati

Contesto generale

Le minacce crescono in numero e gravità: ransomware con doppia estorsione, attacchi alla supply chain, PMI sempre più nel mirino — e il vettore d'ingresso più frequente resta il fattore umano.

Dati sui cyber attacchi in Italia nel 2025



227

media di
episodi mensili



38%

crescita delle
attività ostili



9,6%

percentuale rispetto agli
incidenti globali

**fonti: La Repubblica, ANSA*

CONTESTO

Contesto normativo

L'Europa ha reso la cybersecurity un obbligo di legge: NIS2, DORA e CRA impongono misure concrete, scadenze e sanzioni a chi resta indietro. Tre normative diverse, ma con requisiti che sul piano operativo si sovrappongono.



NIS2

Direttiva UE 2022/2555

Direttiva europea sulla sicurezza delle reti e dei sistemi informativi, che rafforza gli obblighi di cybersecurity per organizzazioni operanti in settori critici e importanti.

DORA

Regolamento UE 2022/2554

Regolamento europeo sulla resilienza operativa digitale del settore finanziario, volto a garantire che banche, assicurazioni e altre entità finanziarie sappiano prevenire, gestire e recuperare da incidenti ICT.

CRA

Regolamento UE 2024/2847

Regolamento europeo che introduce requisiti di cybersecurity per prodotti con elementi digitali, imponendo ai produttori di garantire sicurezza durante progettazione, sviluppo, distribuzione e ciclo di vita del prodotto.

CONTESTO

Cos’è la ISO 27001?

La ISO/IEC 27001 è lo standard internazionale che definisce i requisiti per stabilire, attuare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza dell'Informazione (SGSI).

Essa preserva la riservatezza, l'integrità e la disponibilità delle informazioni applicando un processo di gestione del rischio su misura per l'organizzazione.



CONTESTO

Il valore della ISO 27001

Un SGSI ben fatto è la base comune per la conformità alle recenti normative europee GDPR, NIS2, DORA e CRA.

La certificazione è quindi un asset commerciale:



Dà accesso a gare e bandi pubblici



Soddisfa i requisiti di qualifica dei fornitori



Riduce gli audit imposti dai clienti



Garantisce affidabilità a tutti gli stakeholders

RISK ASSESSMENT

Confini e Scopo

Prima di procedere al Risk Assessment, l'organizzazione deve determinare i confini e lo scopo (Campo di Applicazione) del SGSI, che deve essere conservato come informazione documentata.

I 4 componenti fondamentali:

- Perimetro Geografico e Fisico
- Processi e Servizi di Business
- Asset e Infrastrutture Tecnologiche
- Fattori Interni/Esterni e Dipendenze



1. Definizione dei Criteri

L’organizzazione deve stabilire i criteri per i rischi di sicurezza delle informazioni che includano:



Accettazione del rischio

qual è la soglia di rischio che l'organizzazione è disposta a tollerare senza dovere applicare ulteriori misure o contromisure.



Valutazione del rischio

I criteri per effettuare le **valutazioni dei rischi** relativi alla sicurezza delle informazioni.

Metodologia Ripetibile: Il processo deve garantire risultati consistenti, validi e comparabili nel tempo.

2. Identificazione del rischio

Si parte da un inventario degli asset aggiornato e si identificano i rischi sulla base di:



Perdita di riservatezza



Integrità delle informazioni



Disponibilità delle informazioni

Ogni rischio ha un risk owner che ne risponde e ne approva il trattamento

3. Analisi e Valutazione

La valutazione parte dai processi di business: per ogni attività ci si chiede cosa accadrebbe se venisse meno la riservatezza, l'integrità o la disponibilità delle informazioni che la alimentano.

1. Stima dell'impatto (conseguenze potenziali)
2. Stima della Probabilità
3. Calcolo del Livello di Rischio
4. Confronto con i criteri di accetazione per definire le priorità di trattamento

RISK ASSESSMENT

Il fattore umano

Il fattore umano è un rischio a tutti gli effetti: phishing, credenziali compromesse, errore involontario e insider threat entrano nel registro come qualunque minaccia tecnica.



Formazione e consapevolezza

Il personale deve ricevere formazione e aggiornamenti periodici sulla sicurezza delle informazioni, in relazione al proprio ruolo.

Segnalazione degli eventi

L’organizzazione deve garantire canali appropriati per segnalare tempestivamente eventi di sicurezza delle informazioni, anche sospetti.

RISK TREATMENT

Opzioni di trattamento



1
Modificare il rischio
(Mitigazione)

Applicare misure e controlli tecnici o organizzativi per ridurre la probabilità che l'evento si verifichi o l'impatto del danno.

2
Condividere il rischio
(Trasferimento)

Spostare parte dell'impatto economico o operativo su terzi, ad esempio stipulando un'assicurazione cyber o esternalizzando un servizio.

3
Accettare il rischio
(Accettazione)

Decidere di non implementare ulteriori contromisure e convivere con il rischio residuo, spesso perché il costo per mitigarlo sarebbe superiore al danno potenziale.

4
Evitare il rischio
(Evitamento)

Rinunciare del tutto all'attività, al processo o alla tecnologia che genera quel rischio per azzerare l'esposizione.

RISK TREATMENT

Dichiarazione di Applicabilità (SoA)

Il piano di trattamento è un progetto con **azioni dettagliate, responsabili, tempi e risorse.**

L'Allegato A conta 93 controlli, divisi in Controlli Organizzativi, sulle Persone, Fisici e Tecnologici: la SoA deve essere allineata.

La SoA dichiara per ogni controllo perché è incluso, se è implementato e perché eventuali controlli sono esclusi.

1
Controlli necessari

L'elenco dei controlli selezionati per gestire i rischi.

2
Giustificazione dell'inclusione

Perché il controllo è stato scelto.

3
Stato di implementazione

Se il controllo è attualmente implementato o meno.

4
Giustificazione dell'esclusione

La motivazione puntuale per qualsiasi controllo escluso

Le non conformità tipiche

Fornitori critici senza requisiti di sicurezza contrattualizzati e azioni correttive ferme alla correzione, senza analisi delle cause radice.

1

Rischio non aggiornato

Dopo cambiamenti significativi (migrazione cloud, nuovi servizi) la Clausola 8.2 esige il riesame del rischio.

2

SoA disallineata dalla realtà

Controlli dichiarati implementati senza evidenza operativa, o esclusi pur essendo pertinenti al contesto.

3

Diritti di accesso mai rivisti

account ancora attivi di dipendenti o fornitori usciti da tempo: una gestione degli accessi priva di riesami periodici.

4

Fornitori e azioni correttive

Fornitori critici senza requisiti di sicurezza contrattualizzati e azioni correttive ferme alla correzione, senza analisi delle cause.

Le evidenze



Il Lead Auditor verifica su tre canali che devono coincidere:

Documenti

Cosa l'organizzazione dichiara

Record

Cosa è realmente avvenuto

Interviste

Come le persone lavorano ogni giorno

Le evidenze credibili sono distribuite nel tempo.

Una non conformità gestita bene è un credito di maturità, non un fallimento.