REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere SICURI?

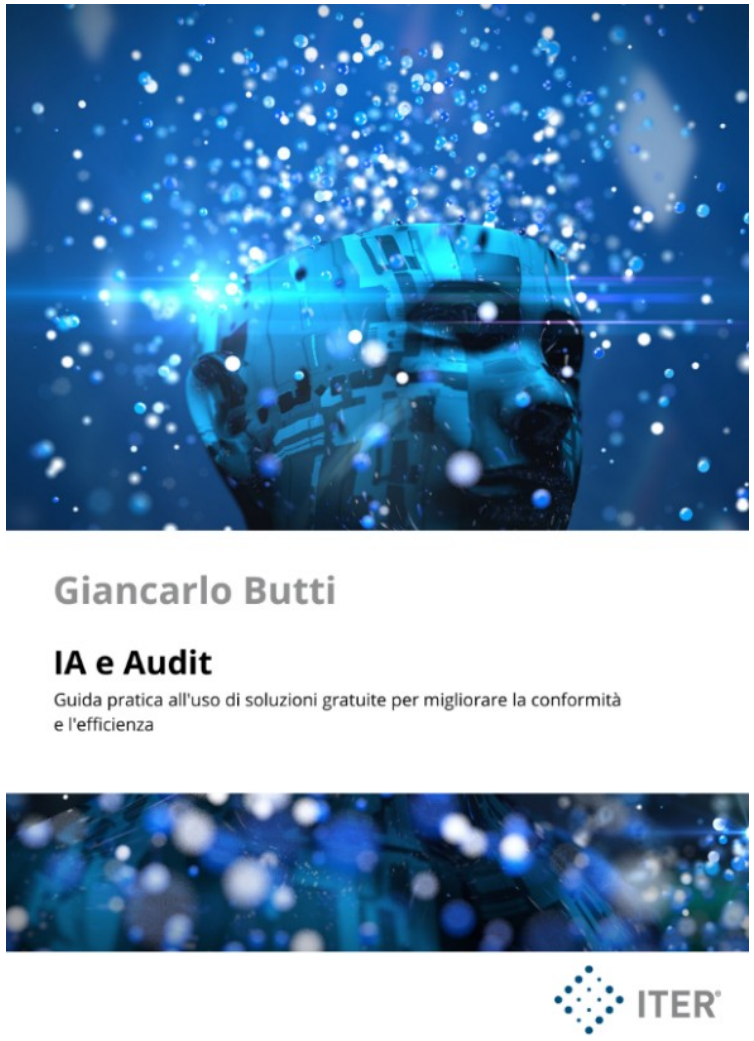
NIS2: le misure di sicurezza

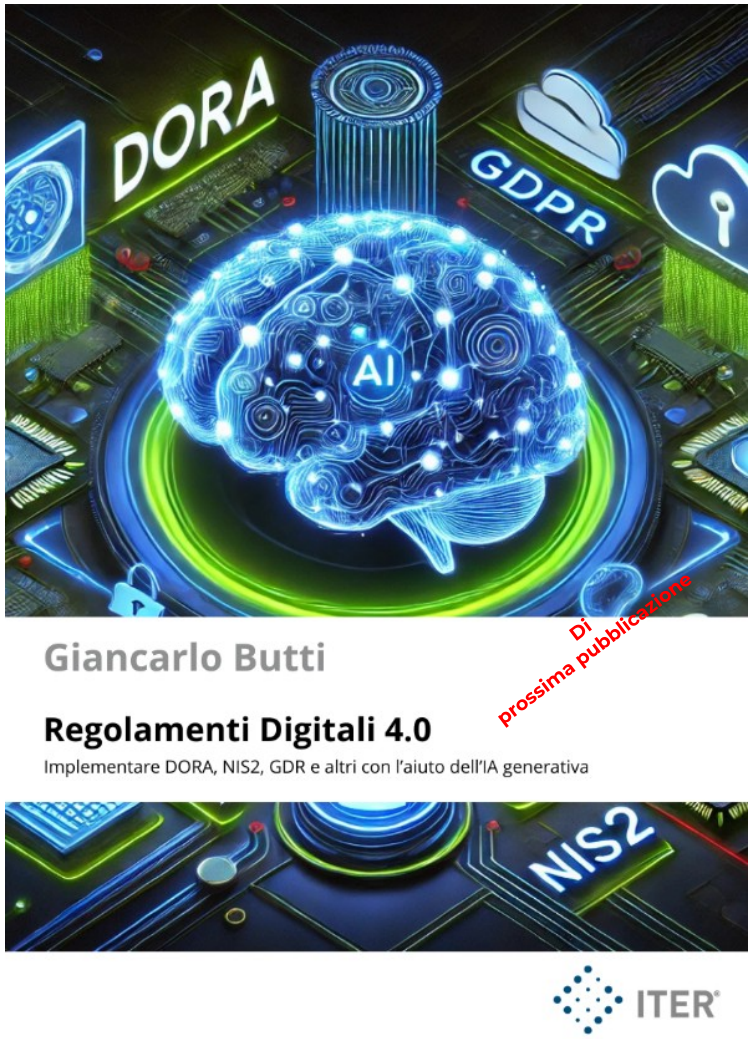
L’uso dell’IA nelle attività di audit

Giancarlo Butti CLUSIT

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Referente Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT.
Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 170 corsi e seminari presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CA FOSCARI, CEFRIEL, ABI…
Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.
Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate.
Ha pubblicato 28 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 31 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di AIEA è socio del CLUSIT, di DFA, di ACFE e del BCI.
Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.blog.europrivacy.info .
Ha inoltre acquisito le certificazioni/qualificazioni (LA BS 7799, LA ISO IEC 27001:2005/2013/2022, LA ISO 20000-1, LA ISO 22301, LA ISO IEC 42001), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI





Alcuni testi derivano da queste mie pubblicazioni

Possibili impieghi dell’AI generativa nelle attività di audit

1. Preparazione e pianificazione degli audit

Identificazione dei rischi: ChatGPT può aiutare a identificare i principali rischi legati a specifici processi o settori. Può fornire una base di conoscenze sui rischi comuni e sulle migliori pratiche per la mitigazione.

Creazione di check-list: Basandosi su normative, standard di settore e best practice, ChatGPT può generare check-list personalizzate per l’audit.

Definizione degli obiettivi: Può supportare la definizione degli obiettivi di audit, aiutando a chiarire le aree chiave di interesse e i criteri di valutazione.

2. Supporto nelle fasi di esecuzione

Analisi documentale: ChatGPT può aiutare a esaminare documenti, contratti e report, evidenziando potenziali aree di criticità o non conformità.

Automazione di risposte a domande frequenti: Durante le interviste o i controlli, ChatGPT può rispondere a domande comuni o fornire chiarimenti su termini tecnici, normativa e standard di audit.

Interpretazione di normative e standard: In caso di dubbi sull'applicazione di determinati requisiti, ChatGPT può fornire un'interpretazione di standard, regolamenti e policy, aiutando a garantire la conformità.

3. Analisi e sintesi dei dati

Riepilogo dei risultati: ChatGPT può generare riassunti delle osservazioni e delle conclusioni delle verifiche di audit, facilitando la sintesi dei dati.

Analisi delle deviazioni: Aiuta ad analizzare deviazioni nei processi e nelle procedure rispetto agli standard di riferimento, suggerendo possibili cause e impatti.

Identificazione di tendenze: Attraverso l'analisi di report storici e dati di audit, può aiutare a individuare pattern di rischio e suggerire aree da approfondire nelle revisioni future.

4. Supporto alla redazione del report di audit

Stesura di sezioni del report: ChatGPT può redigere parti del report di audit, come la descrizione del processo, i punti critici e i rischi identificati, accelerando il processo di scrittura.

Suggerimento di raccomandazioni: In base alle osservazioni, ChatGPT può suggerire raccomandazioni o misure correttive da includere nel report finale, basate sulle best practice.

Verifica della conformità alle linee guida: Può aiutare a controllare che il report sia in linea con le linee guida e gli standard di reportistica dell’azienda.

5. Formazione e supporto continuo

Formazione degli auditor: ChatGPT può fungere da assistente virtuale per la formazione di nuovi auditor, fornendo spiegazioni su metodologie di audit, standard e normative.

Aggiornamenti normativi: Fornisce aggiornamenti su normative e regolamenti rilevanti per l’audit, mantenendo il team informato sulle nuove leggi e standard di settore.

6. Gestione delle comunicazioni

Risposte alle richieste dei dipendenti: ChatGPT può rispondere a richieste di chiarimenti o informazioni da parte dei dipendenti sui processi di audit, facilitando la trasparenza e la comprensione dei controlli.

Feedback ai team: Durante il processo di audit, ChatGPT può essere usato per generare feedback su specifiche osservazioni in tempo reale, facilitando la comunicazione con i team responsabili.

La NIS2 introduce una maggiore responsabilità diretta per i vertici aziendali, che devono dimostrare consapevolezza e controllo delle misure adottate. La governance della cybersecurity deve essere chiaramente definita con ruoli, responsabilità e processi decisionali appropriati.

- Leadership e Responsabilità Esecutiva
- 11. Il management ha formalmente approvato le politiche di cybersecurity?
- 12. Sono stati designati ruoli specifici per la cybersecurity a livello dirigenziale?
- 13. Esiste un budget dedicato alla cybersecurity approvato dalla direzione?
- 14. La direzione riceve report regolari sullo stato della cybersecurity?
- 15. Sono definite le responsabilità legali del CEO e del rappresentante legale in materia di cybersecurity?
- 16. Esiste un processo formale per l'approvazione delle decisioni relative alla sicurezza informatica?
- 17. La direzione partecipa attivamente alle decisioni di risk management?
- 18. È documentata la competenza della direzione in materia di cybersecurity?

- ### 5. **Monitoraggio e rilevamento delle minacce**
- - L’organizzazione dispone di un Security Operations Center (SOC)?
- - Sono attivi sistemi di rilevamento delle intrusioni (IDS/IPS)?
- - Esiste un piano di gestione degli incidenti informatici?
- - Vengono effettuate simulazioni di attacchi per testare la resilienza dell’organizzazione?
- - I log di sicurezza vengono raccolti e analizzati regolarmente?

- ### 6. **Risposta agli incidenti**
- - L’organizzazione ha un piano documentato di risposta agli incidenti?
- - Il piano di risposta agli incidenti è stato testato di recente?
- - Esiste un processo definito per il contenimento e la mitigazione degli attacchi?
- - I dipendenti sanno come segnalare un incidente informatico?
- - Sono previste notifiche agli stakeholder in caso di violazione dei dati?

Sezione 1: Governance e Organizzazione (Min. 15 domande)

- 1. È stata designata una figura o un team responsabile della conformità NIS2 all'interno dell'organizzazione?
- 2. Esiste una chiara definizione dei ruoli e delle responsabilità per la sicurezza delle informazioni a tutti i livelli (Board, C-level, IT, Operazioni)?
- 3. Il Consiglio di Amministrazione (o organo equivalente) è regolarmente informato sui rischi cyber e sullo stato della sicurezza?
- 4. Sono stati stanziati budget adeguati per l'implementazione e il mantenimento delle misure di sicurezza NIS2?
- 5. Esiste una politica di gestione del rischio cyber approvata dalla direzione?
- 6. Sono state condotte analisi del divario (gap analysis) rispetto ai requisiti NIS2?
- 7. È stato redatto un piano d'azione per colmare eventuali lacune identificate?
- 8. Esiste un programma di formazione e sensibilizzazione sulla sicurezza informatica per tutto il personale?
- 9. La formazione include temi specifici legati alla NIS2 e alle minacce attuali?
- 10. La frequenza della formazione è adeguata e documentata?
- 11. Vengono svolte esercitazioni di risposta agli incidenti che coinvolgono la direzione?
- 12. Esistono procedure per la revisione periodica della politica di sicurezza?
- 13. È stata designata una persona di contatto per le autorità competenti NIS2?
- 14. Sono stati identificati i servizi essenziali o importanti che rientrano nel campo di applicazione NIS2?
- 15. L'organizzazione è registrata o ha notificato la propria inclusione nel registro degli enti NIS2 alle autorità competenti?

2. Risk Management

- 11. È stata effettuata un’analisi dei rischi informatici per l’intera organizzazione?
- 12. Sono stati identificati asset critici?
- 13. È adottata una metodologia di risk assessment riconosciuta (es. ISO 27005)?
- 14. L’analisi dei rischi è aggiornata almeno annualmente?
- 15. I risultati del risk assessment sono condivisi con il top management?
- 16. L’organizzazione ha definito una soglia di accettabilità del rischio?
- 17. È prevista la gestione del rischio legato alla supply chain?
- 18. Sono stati presi in considerazione i rischi legati ai fornitori cloud?
- 19. È documentato l’impatto potenziale su altri soggetti in caso di incidente?
- 20. Il piano di trattamento dei rischi è stato approvato?

5. BUSINESS CONTINUITY E DISASTER RECOVERY

5.1 Pianificazione della Continuità

- 59. Esiste un Business Continuity Plan (BCP) aggiornato?
- 60. Sono stati identificati i processi business critici?
- 61. Sono definiti i Recovery Time Objective (RTO) e Recovery Point Objective (RPO)?
- 62. Esistono siti alternativi per il disaster recovery?
- 63. Il BCP viene testato regolarmente?
- 64. Sono identificate le dipendenze critiche esterne?
- 65. Esistono accordi con fornitori per il supporto in emergenza?

5.Gestione dei Rischi (Allegato Reg. Esecuzione Sec 2.1, Allegato 1 & 2 ACN GV.RM-03, ID.RA-05, ID.RA-06, ID.RA-08):

- Verificare che esista un piano di gestione dei rischi per identificare, analizzare, valutare, trattare e monitorare i rischi.
- Verificare che la valutazione del rischio sia eseguita e documentata (identificazione, analisi, ponderazione).
- Verificare che la valutazione del rischio sia eseguita a intervalli pianificati (almeno ogni due anni) e dopo incidenti significativi, variazioni organizzative, mutamenti esposizione al rischio.
- Verificare che la valutazione del rischio sia approvata dagli organi di amministrazione e direttivi.
- Per soggetti essenziali: Verificare che la valutazione del rischio consideri minacce interne/esterne, vulnerabilità non risolte e impatti.
- Verificare che sia definito, documentato, eseguito e monitorato un piano di trattamento del rischio.
- Verificare che il piano di trattamento includa opzioni/misure, responsabili/tempistiche, descrizione/ragioni accettazione rischi residui.
- Verificare che, in caso di non attuazione di requisiti specifici (Tabella 2 Appendice Allegati ACN), siano adottate/descritte misure compensative.

3.1.2 Identificazione e Catalogazione dei Rischi

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Inventario completo dei rischi	Identificazione sistematica di tutti i rischi cyber rilevanti per l'organizzazione	🔍 Registro dei rischi 🔍 Tassonomie delle minacce 🔍 Scenari di rischio	🔴 CRITICO
Categorizzazione per fonte	I rischi sono categorizzati per fonte (interna, esterna, tecnologica, umana, ambientale)	🔍 Matrice di categorizzazione 🔍 Analisi delle fonti di rischio 🔍 Mappatura delle minacce	🟠 ALTO
Valutazione dell'impatto	Ogni rischio è valutato in termini di impatto potenziale sui servizi essenziali	🔍 Analisi di impatto business 🔍 Scenari di worst-case 🔍 Quantificazione	🔴 CRITICO

Esempio di check list generata da strumenti di IA

Tratto da (in fase di pubblicazione):

Il contenuto della check list non è stato verificato dall'autore e quindi deve essere considerata solo come esemplificativa dei possibili risultati dell'uso di strumenti di AI nella loro versione gratuita.

L'uso della check list per reale finalità di audit sulla NIS2 deve essere preceduto pertanto da una verifica puntuale dei contenuti ed al loro adattamento alla situazione reale.

Checklist per un audit mirato al rispetto del **Decreto Legislativo 4 settembre 2024, n. 138** (il "Decreto NIS"), del **Regolamento di Esecuzione (UE) 2024/2690**, e delle misure di base previste dalla **Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale** ("Determinazione ACN") per la fase di prima applicazione.

Questa checklist si basa sui requisiti tecnici e metodologici, sulle misure di sicurezza di base e sugli incidenti significativi di base descritti nelle fonti fornite. **È fondamentale distinguere tra i requisiti applicabili ai "soggetti essenziali" e quelli per i "soggetti importanti"**. L'Allegato 2 (per i soggetti essenziali) include o espande spesso i requisiti dell'Allegato 1 (per i soggetti importanti). La checklist evidenzia le differenze dove esplicite.

Checklist di Audit per la Conformità al Decreto NIS e Misure di Base ACN (Fase di Prima Applicazione)

Ambito: Verifica del rispetto degli obblighi in materia di gestione dei rischi per la sicurezza informatica e di notifica degli incidenti da parte di un Soggetto NIS (essenziale o importante).

Periodo di Riferimento: Dalla data di ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS (o dalla data di entrata in vigore della Determinazione ACN per specifiche tipologie di soggetti in regime transitorio) fino alla data dell'audit.

Parte 1: Obblighi Generali e Governo (GOVERN)

1. **Registrazione e Informazioni (Art. 7 Decreto NIS):**
    - Verificare che il soggetto NIS si sia registrato o abbia aggiornato la propria registrazione sulla piattaforma digitale ACN entro i termini previsti.
    - Verificare che la registrazione includa: ragione sociale, indirizzo, recapiti aggiornati (email, telefono).
    - Verificare che sia designato un punto di contatto (ruolo e recapiti).
    - Verificare che siano indicati i pertinenti settori, sottosettori e tipologie (Allegati I-IV).
    - Verificare che siano fornite/aggiornate le informazioni richieste annualmente: spazio di indirizzamento IP pubblico, nomi di dominio in uso, elenco Stati membri dove si forniscono servizi NIS, recapiti responsabili, recapiti sostituto punto di contatto.
    - **Per specifiche tipologie di soggetti (es. fornitori servizi digitali, gestiti, ecc.):** Verificare che siano fornite l'indirizzo della sede principale/altre sedi nell'UE e, se non stabilito nell'UE, i contatti del rappresentante designato.
    - Verificare che le modifiche alle informazioni registrate siano notificate ad ACN entro 14 giorni.
2. **Organi di Amministrazione e Direttivi (Art. 23 Decreto NIS, Allegato 1 & 2 ACN):**
    - Verificare che gli organi di amministrazione e direttivi abbiano approvato le modalità di implementazione delle misure di gestione dei rischi di sicurezza informatica.
    - Verificare che sovrintendano all'implementazione degli obblighi (Art. 7 e Capo IV Decreto NIS).
    - Verificare che abbiano seguito una formazione in materia di sicurezza informatica.
    - Verificare che promuovano la formazione periodica dei dipendenti.
    - Verificare che siano informati periodicamente o tempestivamente sugli incidenti e le notifiche.
    - Verificare che la politica di sicurezza sia approvata dagli organi di amministrazione e direttivi.
    - Verificare che la valutazione del rischio sia approvata dagli organi di amministrazione e direttivi.
    - Verificare che il piano di trattamento del rischio sia approvato dagli organi di amministrazione e direttivi.
    - Verificare che il piano di adeguamento (in esito alle valutazioni) sia approvato dagli organi di amministrazione e direttivi.
    - Verificare che gli organi di amministrazione/direttivi siano informati sugli esiti dei piani di adeguamento.
    - **Per soggetti essenziali:** Verificare che gli organi di amministrazione/direttivi siano informati sul piano di valutazione dell'efficacia delle misure di gestione del rischio.

- Verificare che i piani di continuità operativa, ripristino disastro e gestione crisi siano approvati dagli organi di amministrazione e direttivi.
- Verificare che il piano di gestione degli incidenti e notifica al CSIRT Italia sia approvato dagli organi di amministrazione e direttivi.
- Verificare che il piano di formazione del personale sia approvato dagli organi di amministrazione e direttivi.
- **Per gestori TLD e fornitori di servizi di registrazione nomi di dominio:** Verificare che le modalità di adeguamento all'Art. 29.1-2 e le politiche/procedure Art. 29.3 siano approvate dagli organi di amministrazione e direttivi. Verificare che le politiche di sicurezza informatica (coerenti con Allegato 1 ACN) siano approvate dagli organi di amministrazione e direttivi.

3. **Politica di Sicurezza dei Sistemi Informativi e di Rete (Allegato Reg. Esecuzione Sec 1.1, Allegato 1 & 2 ACN GV.PO-01, GV.PO-02):**
   - Verificare che esista una politica di sicurezza che definisca l'approccio alla gestione della sicurezza dei sistemi.
   - Verificare che la politica sia adeguata e complementare alla strategia e obiettivi aziendali.
   - Verificare che stabilisca obiettivi di sicurezza.
   - Verificare che includa impegno al miglioramento continuo e a fornire risorse adeguate (personale, finanziarie, processi, strumenti, tecnologie).
   - Verificare che sia comunicata e riconosciuta da dipendenti e parti esterne.
   - Verificare che definisca ruoli e responsabilità (punto 1.2 Allegato Reg. Esecuzione).
   - Verificare che elenchi la documentazione da conservare e la durata.
   - Verificare che elenchi le politiche specifiche per tematica.
   - Verificare che stabilisca indicatori e misure per monitorare l'attuazione e il livello di maturità.
   - Verificare che sia stata formalmente approvata dagli organi di gestione.
   - Verificare che sia riesaminata e aggiornata (almeno annualmente) e dopo incidenti significativi o cambiamenti operativi/di rischio, con esito documentato.
   - Verificare che siano adottate e documentate politiche per almeno gli ambiti specifici elencati (gestione rischio, ruoli/resp, affidabilità RU, conformità/audit, catena approvvigionamento, asset, vulnerabilità, continuità/ripristino/crisi, autenticazione/accessi, sicurezza fisica, formazione, sicurezza dati, sviluppo/config/manutenzione, protezione reti/com, monitoraggio eventi, risposta/ripristino incidenti).
   - Verificare che le politiche specifiche per tematica includano i requisiti indicati nella Tabella 1 degli Allegati ACN.
   - **Per soggetti essenziali:** Verificare che sia mantenuto un registro aggiornato degli esiti del riesame delle politiche.
4. **Ruoli, Responsabilità e Autorità (Allegato Reg. Esecuzione Sec 1.2, Allegato 1 & 2 ACN GV.RR-02):**

- Verificare che siano stabilite e assegnate responsabilità e autorità in materia di sicurezza informatica, comunicate agli organi di gestione.
- Verificare che sia definita l'organizzazione per la sicurezza informatica, approvata dagli organi di amministrazione/direttivi e resa nota.
- Verificare che sia mantenuto un elenco aggiornato del personale con ruoli specifici in sicurezza informatica.
- Verificare che il punto di contatto NIS e almeno un suo sostituto siano inclusi nell'organizzazione di sicurezza informatica.
- Verificare che tutti i dipendenti e terzi siano tenuti ad applicare le politiche e procedure di sicurezza.
- Verificare che almeno una persona riporti direttamente agli organi di gestione sulla sicurezza informatica.
- Verificare che vi siano ruoli o compiti specifici per la sicurezza informatica.
- Verificare che funzioni e aree di responsabilità contrastanti siano separate (se applicabile).
- Verificare che ruoli, responsabilità e autorità siano riesaminati e aggiornati periodicamente (almeno ogni due anni per ACN Allegati) e in seguito a incidenti significativi o cambiamenti operativi/di rischio.

5. **Gestione dei Rischi (Allegato Reg. Esecuzione Sec 2.1, Allegato 1 & 2 ACN GV.RM-03, ID.RA-05, ID.RA-06, ID.RA-08):**
   - Verificare che esista un piano di gestione dei rischi per identificare, analizzare, valutare, trattare e monitorare i rischi.
   - Verificare che la valutazione del rischio sia eseguita e documentata (identificazione, analisi, ponderazione).
   - Verificare che la valutazione del rischio sia eseguita a intervalli pianificati (almeno ogni due anni) e dopo incidenti significativi, variazioni organizzative, mutamenti esposizione al rischio.
   - Verificare che la valutazione del rischio sia approvata dagli organi di amministrazione e direttivi.
   - **Per soggetti essenziali:** Verificare che la valutazione del rischio consideri minacce interne/esterne, vulnerabilità non risolte e impatti.
   - Verificare che sia definito, documentato, eseguito e monitorato un piano di trattamento del rischio.
   - Verificare che il piano di trattamento includa opzioni/misure, responsabili/tempistiche, descrizione/ragioni accettazione rischi residui.
   - Verificare che, in caso di non attuazione di requisiti specifici (Tabella 2 Appendice Allegati ACN), siano adottate/descritte misure compensative.
   - Verificare che il piano di trattamento del rischio (incl. accettazione rischi residui) sia approvato dagli organi di amministrazione e direttivi.

Struttura del Documento

La checklist è organizzata in 10 sezioni principali che coprono tutti gli aspetti della conformità NIS2:

1. **Identificazione e Classificazione dell'Entità**
2. **Governance e Responsabilità**
3. **Gestione del Rischio di Cybersecurity**
4. **Misure Tecniche di Sicurezza**
5. **Gestione degli Incidenti**
6. **Formazione e Sensibilizzazione**
7. **Supply Chain Security**
8. **Reporting e Notifiche**
9. **Continuità Operativa e Resilienza**
10. **Compliance e Documentazione**

Modalità di Utilizzo

Per ogni elemento della checklist sono previste le seguenti informazioni:

- **Riferimento normativo**: Articolo specifico della Direttiva o del Regolamento
- **Descrizione del requisito**: Spiegazione dettagliata dell'obbligo normativo
- **Criteri di verifica**: Elementi specifici da controllare durante l'audit
- **Evidenze richieste**: Documentazione e prove necessarie per dimostrare la conformità
- **Livello di criticità**: Classificazione dell'importanza del requisito (Critico/Alto/Medio/Basso)
- **Note per l'auditor**: Suggerimenti pratici per la verifica

Settori di Applicazione

La presente checklist si applica alle entità operanti nei seguenti settori critici identificati dalla Direttiva NIS2:

Settori ad alta criticità (Allegato I): - Energia (elettricità, petrolio, gas, idrogeno) - Trasporti (aereo, ferroviario, per vie navigabili, stradale) - Servizi bancari - Infrastrutture dei mercati finanziari - Sanità - Acqua potabile - Acque reflue - Infrastrutture digitali - Gestione dei servizi ICT (B2B) - Pubblica amministrazione - Spazio

Settori critici (Allegato II): - Servizi postali e di corriere - Gestione dei rifiuti - Fabbricazione, produzione e distribuzione di sostanze chimiche - Produzione, trasformazione e distribuzione di alimenti - Fabbricazione di dispositivi medici, dispositivi medico-diagnostici in vitro, medicinali - Apparecchiature informatiche,

elettroniche e ottiche - Macchinari e apparecchiature - Veicoli a motore, rimorchi, semirimorchi - Altri mezzi di trasporto - Fornitori di servizi digitali - Ricerca

---

LEGENDA E ISTRUZIONI

Simboli Utilizzati

- ✅ **Conforme**: Il requisito è completamente soddisfatto
- ⚠️ **Parzialmente conforme**: Il requisito è parzialmente soddisfatto, necessita miglioramenti
- ❌ **Non conforme**: Il requisito non è soddisfatto
- 📋 **Da verificare**: Richiede ulteriore analisi o documentazione
- 🔍 **Evidenza richiesta**: Documentazione specifica necessaria

Livelli di Criticità

- 🔴 **CRITICO**: Requisito obbligatorio, non conformità comporta violazione normativa grave
- 🟠 **ALTO**: Requisito importante, non conformità comporta rischi significativi
- 🟡 **MEDIO**: Requisito raccomandato, non conformità comporta rischi moderati
- 🟢 **BASSO**: Requisito di best practice, non conformità comporta rischi limitati

Istruzioni per l'Auditor

1. **Preparazione**: Rivedere la documentazione dell'organizzazione prima dell'audit
2. **Interviste**: Condurre colloqui con il personale chiave identificato
3. **Verifica tecnica**: Esaminare sistemi, configurazioni e controlli implementati
4. **Documentazione**: Raccogliere evidenze documentali per ogni requisito
5. **Valutazione**: Assegnare un punteggio di conformità per ogni elemento
6. **Reporting**: Compilare il rapporto finale con raccomandazioni specifiche

---

SEZIONE 1: IDENTIFICAZIONE E CLASSIFICAZIONE DELL'ENTITÀ

1.1 Determinazione dell'Applicabilità della Direttiva NIS2

Riferimento normativo: Art. 2, 3 e Allegati I-II Direttiva (UE) 2022/2555

La prima fase di qualsiasi audit NIS2 deve stabilire con certezza se l'organizzazione rientra nell'ambito di applicazione della direttiva. Questa determinazione è fondamentale poiché influenza tutti gli obblighi successivi e le misure di sicurezza da implementare.

1.1.1 Verifica del Settore di Attività

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Identificazione settore principale	L'organizzazione opera in uno dei settori elencati negli Allegati **I** o **II** della Direttiva	🔍 Codice ATECO principale 🔍 Statuto societario 🔍 Licenze/ autorizzazioni settoriali	🔴 CRITICO
Classificazione alta criticità vs critica	Determinazione se l'entità appartiene all'Allegato **I** (alta criticità) o **II** (critica)	🔍 Analisi delle attività principali 🔍 Documentazione dei servizi offerti	🔴 CRITICO
Verifica soglie dimensionali	Per settori Allegato **II**: verifica se l'entità supera le soglie di medie imprese (⩾50 dipendenti e ⩾10M€ fatturato)	🔍 Bilancio degli ultimi 3 anni 🔍 Registro dipendenti 🔍 Dichiarazioni fiscali	🔴 CRITICO

Criteri di verifica dettagliati:

L'auditor deve verificare che l'organizzazione abbia correttamente identificato il proprio settore di appartenenza secondo la classificazione NIS2. Per le entità dell'Allegato **I** (alta criticità), l'applicazione della direttiva è automatica indipendentemente dalle dimensioni. Per quelle dell'Allegato **II** (critica), è necessario verificare il superamento delle soglie dimensionali stabilite dalla Raccomandazione 2003/361/CE della Commissione.

La verifica deve includere un'analisi delle attività secondarie dell'organizzazione, poiché un'entità potrebbe operare in più settori. In tal caso, si applica il principio dell'attività principale, determinata in base al fatturato o al numero di dipendenti dedicati.

1.1.2 Analisi dell'Importanza dei Servizi

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Criticità dei servizi offerti	I servizi dell'entità sono essenziali per il mantenimento di attività economiche e sociali critiche	🔍 Analisi di impatto dei servizi 🔍 Mappatura dei clienti critici 🔍 Valutazione delle dipendenze	🟠 ALTO
Interconnessioni settoriali	Identificazione delle dipendenze con altri settori critici	🔍 Mappa delle interconnessioni 🔍 Contratti con entità critiche 🔍 Analisi della supply chain	🟠 ALTO
Impatto geografico	Estensione territoriale dei servizi e potenziale impatto su scala nazionale/europea	🔍 Copertura geografica dei servizi 🔍 Analisi del bacino di utenza 🔍 Valutazione dell'impatto territoriale	🟡 MEDIO

1.2 Registrazione presso le Autorità Competenti

Riferimento normativo: Art. 24 Direttiva (UE) 2022/2555

1.2.1 Identificazione dell'Autorità Competente

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Autorità nazionale competente	Identificazione corretta dell'autorità competente per il settore di appartenenza	🔍 Comunicazioni ufficiali con l'autorità 🔍 Documentazione di registrazione	🔴 CRITICO

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
		🔍 Corrispondenza formale	
Autorità di vigilanza settoriale	Per settori regolamentati, identificazione dell'autorità di vigilanza specifica	🔍 Licenze e autorizzazioni 🔍 Rapporti di vigilanza 🔍 Comunicazioni con regolatori	🟠 ALTO
Punto di contatto unico	Designazione di un punto di contatto per le comunicazioni con le autorità	🔍 Nomina formale del responsabile 🔍 Comunicazione all'autorità 🔍 Procedure di escalation	🟠 ALTO

1.2.2 Processo di Registrazione e Notifica

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Registrazione iniziale	L'entità si è registrata presso l'autorità competente entro i termini previsti	🔍 Certificato di registrazione 🔍 Comunicazione di avvenuta registrazione 🔍 Timestamp delle comunicazioni	🔴 CRITICO
Aggiornamenti informativi	Comunicazione tempestiva di modifiche significative (fusioni, acquisizioni, cambi di controllo)	🔍 Comunicazioni di variazione 🔍 Documentazione societaria 🔍 Cronologia degli aggiornamenti	🟠 ALTO
Mantenimento dello status	Verifica periodica del mantenimento dei requisiti	🔍 Autovalutazioni periodiche 🔍 Monitoraggio delle	🟡 MEDIO

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
	per l'inclusione nell'ambito NIS2	soglie 🔍 Procedure di verifica interna	

1.3 Mappatura delle Reti e Sistemi Informativi Critici

Riferimento normativo: Art. 21 Direttiva (UE) 2022/2555, Art. 5 Regolamento (UE) 2024/2690

1.3.1 Inventario delle Risorse Critiche

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Inventario completo delle risorse	Esistenza di un inventario aggiornato di tutte le reti e sistemi informativi	🔍 Database degli asset 🔍 Diagrammi di rete 🔍 Documentazione tecnica	🔴 CRITICO
Classificazione per criticità	Le risorse sono classificate in base alla loro importanza per i servizi essenziali	🔍 Matrice di criticità 🔍 Analisi di impatto business 🔍 Procedure di classificazione	🔴 CRITICO
Identificazione delle dipendenze	Mappatura delle interdipendenze tra sistemi e servizi	🔍 Diagrammi delle dipendenze 🔍 Analisi dei flussi dati 🔍 Documentazione delle interconnessioni	🟠 ALTO

1.3.2 Perimetro di Sicurezza

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Definizione del perimetro		🔍 Diagrammi del perimetro	

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
	Il perimetro di sicurezza è chiaramente definito e documentato	🔍 Politiche di segmentazione 🔍 Documentazione architetturale	🔴 CRITICO
Controlli di accesso perimetrali	Implementazione di controlli di accesso ai confini del perimetro	🔍 Configurazioni firewall 🔍 Politiche di accesso 🔍 Log di monitoraggio	🔴 CRITICO
Monitoraggio del perimetro	Sistemi di monitoraggio continuo del perimetro di sicurezza	🔍 Sistemi SIEM/SOC 🔍 Procedure di monitoraggio 🔍 Report di sicurezza	🟠 ALTO

1.4 Valutazione dell'Ecosistema Digitale

Riferimento normativo: Art. 21 Direttiva (UE) 2022/2555

1.4.1 Analisi dei Fornitori di Servizi Digitali

Elemento di Verifica	Criteri di Controllo	Evidenze Richieste	Criticità
Inventario fornitori critici	Identificazione di tutti i fornitori di servizi digitali critici	🔍 Registro fornitori 🔍 Contratti di servizio 🔍 Valutazioni di criticità	🟠 ALTO
Valutazione della conformità fornitori	I fornitori critici sono conformi agli standard di sicurezza richiesti	🔍 Certificazioni di sicurezza 🔍 Audit di terze parti 🔍 Clausole	🟠 ALTO