Linee Guida per l'Audit CPF

Versione 1.0

Auditing dei Sistemi di Gestione delle Vulnerabilità Psicologiche

Giuseppe Canale, CISSP
Ricercatore Indipendente
g.canale@cpf3.org
ORCID: 0009-0007-3263-6897

Gennaio 2025

Sommario

Questo documento fornisce una guida pratica per condurre audit di conformità rispetto ai requisiti CPF-27001:2025. A differenza degli audit di sicurezza tecnica tradizionali, gli audit CPF richiedono competenze specializzate che spaziano dalla cybersecurity, alla psicologia, al diritto della privacy e alla metodologia di audit. La guida stabilisce tecniche di audit che preservano la privacy e verificano la gestione delle vulnerabilità psicologiche organizzative senza profilazione individuale. I principali elementi distintivi includono la raccolta di evidenze aggregate (minimo n=10), la verifica della privacy differenziale ($\varepsilon \leq 0.1$), protocolli di intervista trauma-informed e framework etici che trattano le vulnerabilità psicologiche come questioni organizzative sistemiche piuttosto che come fallimenti individuali. La metodologia si integra con ISO 19011:2018 affrontando al contempo le sfide uniche dell'auditing di processi pre-cognitivi e dinamiche di gruppo inconsce.

Indice

1 Introduzione

1.1 Scopo e Ambito

Le Linee Guida per l'Audit CPF forniscono una metodologia sistematica per valutare la conformità organizzativa ai requisiti CPF-27001:2025 del Sistema di Gestione delle Vulnerabilità Psicologiche (PVMS). Questo documento affronta le sfide uniche dell'auditing dei fattori umani nella cybersecurity mantenendo rigorose protezioni della privacy e standard etici.

Pubblico di Riferimento:

- Auditor di certificazione terza parte che conducono audit CPF-27001
- Auditor interni che implementano programmi di assurance PVMS
- Manager di programmi di audit che progettano metodologie di audit CPF
- Organizzazioni che si preparano per la certificazione CPF-27001

Confini dell'Ambito:

Nell'Ambito:

- Valutazione di conformità rispetto ai requisiti CPF-27001:2025
- Tecniche di raccolta evidenze che preservano la privacy
- Verifica degli indicatori di vulnerabilità psicologica
- Integrazione PVMS con ISMS esistente (ISO 27001)
- Valutazione del livello di maturità organizzativa

Fuori dall'Ambito:

- Valutazione psicologica individuale o valutazione clinica
- Processi di valutazione delle prestazioni o disciplinari dei dipendenti
- Test di efficacia dei controlli di sicurezza tecnici
- Penetration testing o vulnerability scanning
- Progettazione di simulazioni di social engineering

1.2 Relazione con Altri Standard

Integrazione ISO 19011:2018:

Gli audit CPF seguono le Linee Guida ISO 19011:2018 per l'Auditing dei Sistemi di Gestione come metodologia fondamentale, con miglioramenti specifici CPF per l'auditing delle vulnerabilità psicologiche.

Ecosistema Documentale CPF:

- **CPF-27001:2025 Requirements**: Standard normativo (Clausole 4-10)
- **CPF Scoring and Maturity Model**: Framework di verifica matematica

- **CPF Field Kits**: Strumenti operativi di valutazione degli indicatori
- **The Cybersecurity Psychology Framework**: Fondamento teorico

Standard Complementari:

- **ISO/IEC 27001:2022**: Punti di integrazione ISMS
- **ISO/IEC 27006:2015**: Requisiti per gli enti di certificazione
- **GDPR/Regolamenti sulla Privacy**: Framework di conformità legale

1.3 Come Utilizzare Questo Documento

Per Lead Auditor:

1. Rivedere la Sezione 1 per i differenziatori degli audit CPF
2. Applicare la Sezione 2 per la pianificazione degli audit basata sul rischio
3. Utilizzare la Sezione 3 per la raccolta di evidenze che preservano la privacy
4. Riferirsi alla Sezione 4 per la verifica dello scoring
5. Seguire la Sezione 6 per il reporting conforme

Per le Organizzazioni:

- Comprendere le aspettative degli auditor e i requisiti delle evidenze
- Preparare la documentazione secondo la guida della Sezione 2
- Assicurare che i controlli sulla privacy soddisfino gli standard della Sezione 3
- Auto-valutarsi utilizzando i metodi di verifica della Sezione 4

Navigazione del Documento:

- **Riferimento Rapido**: Checklist in Appendice per valutazione rapida
- **Metodologia Dettagliata**: Sezioni principali per comprensione completa
- **Esempi**: Casi studio nel testo per applicazione pratica

2 Differenziatori degli Audit CPF

2.1 Requisiti di Competenza Unici

L'auditing CPF richiede competenze interdisciplinari che vanno oltre l'auditing di sicurezza tradizionale. Gli auditor devono integrare conoscenze da quattro domini distinti:

2.1.1 Fondamenti di Cybersecurity

Conoscenze Richieste:

- Requisiti ISMS ISO/IEC 27001:2022 e metodologia di audit
- Vettori di attacco comuni (phishing, social engineering, minacce interne)
- Tecniche di valutazione dei programmi di security awareness
- Concetti di incident response e operazioni di sicurezza
- Metodologie di risk assessment e trattamento

Background Tipico: Certificazione CISSP, CISM, ISO 27001 Lead Auditor

2.1.2 Teoria e Pratica Psicologica

Conoscenze Richieste:

- **Concetti Psicoanalitici**: Assunti di base di Bion, relazioni oggettuali di Klein, ombra/inconscio collettivo di Jung
- **Psicologia Cognitiva**: Teoria del doppio processo di Kahneman, bias cognitivi, euristiche
- **Psicologia Sociale**: Principi di influenza di Cialdini, studi su conformità e obbedienza
- **Dinamiche di Gruppo**: Groupthink, risky shift, diffusione di responsabilità
- **Fisiologia dello Stress**: Risposte fight/flight/freeze/fawn, effetti del cortisolo

Background Tipico: Laurea in psicologia, formazione psicanalitica o formazione strutturata equivalente (minimo 40 ore di training specifico CPF)

2.1.3 Diritto della Privacy ed Etica

Conoscenze Richieste:

- Articoli GDPR 5 (minimizzazione dei dati), 9 (categorie speciali), 32 (sicurezza)
- Principi matematici della privacy differenziale (ε-privacy)
- Tecniche di aggregazione e anonimizzazione
- Requisiti di consenso informato per dati psicologici
- Metodologia di valutazione d'impatto sulla protezione dei dati (DPIA)

Background Tipico: Certificazione CIPP/E, formazione legale o esperienza come privacy officer

2.1.4 Metodologia di Audit

Conoscenze Richieste:

- Principi e pratiche di auditing ISO 19011:2018
- Teoria del campionamento e validità statistica
- Valutazione delle evidenze e classificazione dei finding
- Tecniche di intervista e metodi di osservazione
- Redazione di report e documentazione delle non conformità

Background Tipico: Certificazione ISO 27001 Lead Auditor o equivalente certificazione di auditor di sistemi di gestione

2.2 Framework Etico per l'Auditing Psicologico

Gli audit CPF operano secondo un framework etico distinto che differisce fondamentalmente dagli audit di sicurezza tecnica.

2.2.1 Principio del Focus Organizzativo

Principio Fondamentale: Le vulnerabilità psicologiche sono caratteristiche organizzative sistemiche, NON deficienze individuali.

Implicazioni Pratiche:

- I finding descrivono pattern organizzativi, mai comportamenti individuali
- I dati delle interviste aggregati a minimo n=10 prima dell'analisi
- Nessun collegamento tra risultati della valutazione e gestione delle prestazioni
- Stati vulnerabili inquadrati come normali risposte umane alle condizioni

Pratiche Vietate:

- Identificare individui specifici come "ad alto rischio" o "vulnerabili"
- Fornire feedback o raccomandazioni individuali
- Condividere dati disaggregati con il management
- Utilizzare la valutazione psicologica per decisioni di assunzione/promozione

2.2.2 Principio di Non Maleficenza

Principio Fondamentale: Il processo di audit non deve danneggiare la sicurezza psicologica o la fiducia organizzativa.

Implicazioni Pratiche:

- Interviste trauma-informed (vedere Sezione 3.3)

- Gestione dell'ansia organizzativa riguardo alla valutazione psicologica
- Comunicazione trasparente sullo scopo dell'audit e l'uso dei dati
- Rispetto delle differenze culturali nelle norme psicologiche

Comunicazione Pre-Audit:

- Spiegazione chiara che l'audit valuta i sistemi organizzativi, non gli individui
- Garanzia di anonimato e aggregazione
- Diritto di rifiutare la partecipazione senza conseguenze
- Risorse di supporto psicologico disponibili se l'audit scatena disagio

2.2.3 Principio di Giustizia ed Equità

Principio Fondamentale: La metodologia di audit non deve discriminare o creare impatti disparati.

Implicazioni Pratiche:

- Sensibilità culturale nell'interpretare gli indicatori psicologici
- Evitare la patologizzazione di pattern psicologici non occidentali
- Riconoscere che la "vulnerabilità" può riflettere fallimenti organizzativi, non debolezza individuale
- Garantire rappresentanza diversificata nel campionamento

2.3 Approccio Trauma-Informed

Gli audit CPF adottano principi trauma-informed riconoscendo che gli incidenti di sicurezza e lo stress organizzativo creano risposte traumatiche.

2.3.1 Sicurezza Prima di Tutto

Sicurezza Fisica e Psicologica:

- Spazi di intervista privati senza sorveglianza
- Confini chiari sulla confidenzialità
- L'auditor si presenta e spiega il suo ruolo
- L'intervistato controlla il ritmo e la profondità della discussione

2.3.2 Affidabilità e Trasparenza

Costruire Fiducia:

- Spiegare il processo di audit e la timeline in anticipo
- Chiarire come i dati saranno e NON saranno utilizzati
- Condividere domande di esempio in anticipo
- Fornire un riepilogo scritto della discussione

2.3.3 Supporto tra Pari

Riconoscere l'Esperienza Condivisa:

- Inquadrare le vulnerabilità come caratteristiche umane universali
- Riconoscere che l'auditor risponderebbe in modo simile nelle stesse condizioni
- Evitare la dinamica "esperto-vittima"
- Validare le risposte emotive ai fattori di stress di sicurezza

2.3.4 Collaborazione e Mutualità

Approccio Collaborativo:

- Invitare l'input organizzativo sul piano di audit
- Risoluzione collaborativa dei problemi per le lacune identificate
- Riconoscere l'expertise dell'organizzazione nella propria cultura
- Sviluppo congiunto di piani di azione correttiva

2.3.5 Empowerment e Scelta

Rispettare l'Autonomia:

- I partecipanti possono saltare domande o terminare l'intervista
- L'organizzazione sceglie tempistiche e approccio di campionamento (entro gli standard)
- I finding presentati come opportunità, non giudizi
- L'organizzazione controlla l'implementazione delle raccomandazioni

2.4 Integrazione con ISO 19011:2018

Gli audit CPF estendono i principi ISO 19011 con linee guida specifiche psicologiche:

Tabella 1: Estensioni ISO 19011 per Audit CPF

Principio ISO 19011	**Applicazione Standard**	**Estensione CPF**
Integrità	Reporting onesto, veritiero	Nessuna profilazione individuale, enforcement dell'aggregazione
Presentazione Equa	Finding accurati	Linguaggio trauma-informed, non patologizzante
Due Professional Care	Diligenza e giudizio	Protezione della privacy, sicurezza psicologica
Confidenzialità	Informazioni sicure	Anonimizzazione migliorata, privacy differenziale
Indipendenza	Imparzialità	Nessun doppio ruolo come terapeuta/counselor
Basato su Evidenze	Informazioni verificabili	Dati triangolati, validità statistica
Basato sul Rischio	Focus sui rischi significativi	Convergence Index, scoring del rischio psicologico

2.5 Gestione dell'Ansia Organizzativa

Il processo di audit stesso può innescare ansia organizzativa e risposte difensive. Gli auditor esperti riconoscono e affrontano queste dinamiche.

2.5.1 Manifestazioni Comuni dell'Ansia

Fase Pre-Audit:

- Preparazione eccessiva e "messa in scena" delle evidenze
- Coaching dei dipendenti su risposte "corrette"
- Tentativi di controllare l'accesso o il programma dell'auditor
- Razionalizzazione che "siamo diversi" o "questo non si applica"

Durante l'Audit:

- Reazioni difensive alle domande
- Minimizzazione delle vulnerabilità identificate
- Proiezione della colpa su fattori esterni
- Over-compliance ed eccessiva voglia di compiacere

2.5.2 Tecniche di Gestione dell'Ansia

Normalizzazione:

- "Ogni organizzazione ha vulnerabilità psicologiche"
- "Stiamo esaminando i sistemi, non giudicando le persone"
- "Queste sono risposte normali a condizioni stressanti"

Reframing:

- "Identificare le vulnerabilità è il primo passo verso il miglioramento"
- "La vostra apertura ci consente di fornire intuizioni preziose"
- "Questa valutazione protegge la vostra organizzazione e i dipendenti"

Contenimento dell'Ansia:

- Programma prevedibile e milestone chiari
- Brief-back regolari per ridurre l'incertezza
- Comportamento calmo e professionale come modello
- Riconoscere i finding positivi insieme alle lacune

3 Pianificazione dell'Audit

3.1 Attività Pre-Audit

3.1.1 Revisione Documentale

Documenti Richiesti (Richiesta Minimo 14 Giorni Prima del Sopralluogo):

Documentazione PVMS:

- Policy CPF (impegno del management, definizione dell'ambito)
- Dichiarazione di Ambito CPF (confini, esclusioni, unità organizzative)
- Metodologia di Risk Assessment (approccio valutazione 100 indicatori)
- Fogli di Calcolo CPF Score (valutazione più recente)
- Procedure di Protezione della Privacy (aggregazione, privacy differenziale, ritardo temporale)
- Piani di Trattamento del Rischio (interventi per indicatori Yellow/Red)

Documentazione di Integrazione:

- Policy e Ambito ISMS (ISO 27001 se applicabile)
- Organigramma (strutture di reporting, dimensioni dei team)
- Report di Incidenti (ultimi 12 mesi, incidenti con fattore umano)
- Materiali del Programma di Security Awareness (contenuti formativi, registri presenze)

Evidenza di Operatività:

- Verbali del Riesame di Direzione (ultimi 2 riesami)
- Report di Audit Interni (se condotto audit interno PVMS)

- Registri di Azioni Correttive (tracciamento non conformità)
- Registri di Monitoraggio e Misurazione (tracciamento KPI)

Checklist Revisione Documentale:

☐ Calcolo CPF Score matematicamente corretto (verificare per Scoring Model)

☐ Tutti i 10 domini valutati con metodologia documentata

☐ Protezioni privacy documentate (n≥10, $\varepsilon \leq 0.1$, ritardo 72h)

☐ Integrazione con ISMS chiaramente definita

☐ Impegno del management evidenziato (risorse, approvazione policy)

☐ Requisiti di competenza definiti per ruoli CPF

☐ Piani di trattamento del rischio affrontano vulnerabilità identificate

3.1.2 Allocazione Risorse

Composizione Team di Audit:

Team minimo per audit CPF-27001 completo:

- **Lead Auditor**: Certificato CPF Lead Auditor, preferibilmente con background psicologico
- **Auditor Tecnico**: Expertise cybersecurity (livello CISSP/CISM)
- **Specialista Privacy**: Expertise legale GDPR/privacy (può essere il Lead se qualificato)

Allocazione Tempo (Organizzazione Media Tipica, 250-500 dipendenti):

Tabella 2: Budget Tempo di Audit

Attività	**Giorni**	**Giorni-Auditor**
Revisione Documenti (fuori sede)	-	1.5
Riunione di Apertura	0.5	1.5
Interviste Management	0.5	1.5
Verifica Documentazione	1.0	3.0
Interviste Staff (aggregate)	1.0	3.0
Osservazione Sistema/Processi	1.0	3.0
Ricalcolo Score	0.5	1.5
Test Controlli Privacy	0.5	1.5
Deliberazione Team	0.5	1.5
Riunione di Chiusura	0.5	1.5
Totale In Loco	**5.0**	**19.0**
Redazione Report (fuori sede)	-	2.0
Totale Audit	-	**22.5**

Fattori di Scala:

- Piccola (¡100 dipendenti): moltiplicatore 0.6x → 13.5 giorni-auditor
- Grande (500-2000 dipendenti): moltiplicatore 1.5x → 33.8 giorni-auditor
- Molto Grande (¿2000 dipendenti): moltiplicatore 2.0x → 45 giorni-auditor
- Multi-sito: +0.5 giorni per sito aggiuntivo
- Audit di crisi: +1.0 giorno per analisi incidente

3.1.3 Protocollo di Comunicazione

Comunicazione Pre-Audit (3-4 Settimane Prima):

Al Management Esecutivo:

- Scopo dell'audit: Valutare conformità PVMS a CPF-27001:2025
- Panoramica ambito e metodologia
- Risorse richieste (sale riunioni, disponibilità staff)
- Protezioni privacy: Nessuna profilazione individuale, reporting solo aggregato
- Deliverable attesi e timeline

A Tutto lo Staff (tramite organizzazione):

- Annuncio audit imminente
- Enfasi su valutazione organizzativa, NON valutazione individuale
- Partecipazione volontaria alle interviste
- Garanzie di confidenzialità e anonimizzazione
- Informazioni di contatto per domande/preoccupazioni

Esempio Comunicazione Staff:

> *"La nostra organizzazione sta sottoponendosi a un audit CPF-27001 per valutare quanto bene gestiamo i fattori psicologici nella cybersecurity. Questa NON è una valutazione dei singoli dipendenti. Gli auditor analizzeranno pattern organizzativi utilizzando dati aggregati e anonimi. Se selezionati per un'intervista, la partecipazione è volontaria. Tutte le risposte sono confidenziali e saranno combinate con almeno altre 10 prima dell'analisi. Questa valutazione ci aiuta a creare un ambiente di sicurezza più sicuro e meno stressante per tutti."*

3.2 Approccio Basato sul Rischio

3.2.1 Determinazione Focus dell'Audit

Gli audit CPF danno priorità ai domini con rischio più elevato basandosi su:

1. **Analisi CPF Score**: Focus su domini con indicatori Red (score 14-20/20)

2. **Convergence Index**: Investigare domini che contribuiscono a valori CI elevati (>5)
3. **Storico Incidenti**: Domini correlati con incidenti di sicurezza passati
4. **Contesto Organizzativo**: Vulnerabilità specifiche del settore (es. dominio Authority nel healthcare)

Esempio Pianificazione Basata sul Rischio:

Profilo Organizzazione:

- Settore servizi finanziari (vulnerabilità Authority/Temporal intrinseche)
- Recente incidente CEO fraud (debolezza dominio Authority confermata)
- CPF Score: 58/100 (rating Fair)
- Domini: Authority [1.x] = 16/20 (Red), Temporal [2.x] = 14/20 (Red)

Aggiustamenti Piano Audit:

- Allocare 40% del tempo di audit ai domini Authority e Temporal
- Approfondimento su indicatori 1.1 (conformità acritica) e 2.1 (bypass urgenza)
- Intervistare specificamente staff finance (vulnerabilità CEO fraud)
- Testare protocolli di verifica per richieste di authority
- Verificare efficacia dei trattamenti del rischio implementati

3.2.2 Strategia di Campionamento

Principi di Campionamento che Preservano la Privacy:

- **Dimensione Minima Campione**: n $\geq$ 10 per qualsiasi gruppo analizzato
- **Campionamento Rappresentativo**: Proporzionale ai dati demografici organizzativi
- **Stratificazione per Ruolo**: Campionare attraverso aree funzionali
- **Selezione Casuale**: Evitare bias di selezione (organizzazione fornisce roster, auditor seleziona)

Calcolo Dimensione Campione:

Per livello di confidenza 95%, margine errore ±10%:

$$n = \frac{Z^2 \times p \times (1-p)}{E^2} = \frac{1.96^2 \times 0.5 \times 0.5}{0.10^2} = 96 \tag{1}$$

Linee Guida Pratiche Campionamento:

Esempio Stratificazione (organizzazione 500 dipendenti):

- Management Esecutivo: 3 interviste (5% del campione)

Tabella 3: Dimensioni Campione per Dimensione Organizzazione

Dimensione Organizzazione	Campione Minimo	Campione Raccomandato
¡100 dipendenti	20	30
100-500 dipendenti	30	50
500-2000 dipendenti	50	80
¿2000 dipendenti	80	100+

- Middle Management: 8 interviste (15%)
- Staff Tecnico: 15 interviste (30%)
- Staff Amministrativo: 12 interviste (24%)
- Staff Operativo: 12 interviste (26%)
- **Totale: 50 interviste**

3.3 Privacy Impact Assessment per l'Audit

Prima di iniziare qualsiasi audit CPF, gli auditor devono condurre un Privacy Impact Assessment (PIA) per il processo di audit stesso.

3.3.1 Confini della Raccolta Dati

Raccolta Dati Consentita:

- Pattern comportamentali aggregati (n≥10)
- Log di sistema che mostrano comportamento collettivo (pattern autenticazione, tempi risposta alert)
- Risposte anonime a survey
- Dati di osservazione di gruppo (riunioni team, esercitazioni incident response)
- Analisi a livello di ruolo (es. "dipartimento finance" non "Jane Doe")

Raccolta Dati Vietata:

- Profili o valutazioni psicologiche individuali
- Informazioni personalmente identificabili oltre ruolo/dipartimento
- Registrazioni video/audio di individui
- Monitoraggio real-time di individui specifici
- Informazioni mediche o sanitarie
- Dati di valutazione delle prestazioni

3.3.2 Gestione Consenso

Requisiti Consenso Informato:

- **Modulo Consenso Scritto** per partecipanti interviste che copre:
  - Scopo raccolta dati (audit conformità PVMS)
  - Tipi di dati raccolti (risposte, osservazioni)
  - Metodi anonimizzazione e aggregazione (n≥10, ritardo 72h)
  - Periodo conservazione dati (distruzione post-audit o max 3 anni)
  - Diritto di ritirare la partecipazione
  - Contatto per domande/preoccupazioni
- **Partecipazione Volontaria**: Nessuna penalità per rifiuto
- **Ri-consenso** se ambito audit cambia

3.3.3 Verifica Anonimizzazione

Checklist Auditor per Protezione Privacy:

☐ Note interviste non contengono nomi (usare codici: INT-001, INT-002)

☐ Citazioni in report sanitizzate da dettagli identificativi

☐ Dati piccoli gruppi ($n < 10$) non riportati separatamente

☐ Dettagli demografici generalizzati ("senior manager" non "VP of Finance")

☐ Log di sistema aggregati con rumore privacy differenziale

☐ Report rivisto per rischi di re-identificazione prima della consegna

3.4 Timeline Programma Audit

Programma Tipico Audit Certificazione Iniziale:

Tabella 4: Timeline Audit

Settimana	Attività	Responsabile
-4	Richiesta documenti inviata	Lead Auditor
-3	Documenti ricevuti	Organizzazione
-2	Revisione documenti completata	Team Audit
-1	Chiamata pre-audit, comunicazione staff	Entrambi
1	Audit in loco (5 giorni)	Team Audit
2	Redazione report	Lead Auditor
3	Report consegnato a organizzazione	Lead Auditor
4-6	Azioni correttive (se necessarie)	Organizzazione
7	Verifica azioni correttive	Lead Auditor
8	Decisione emissione certificato	Ente Certificazione

4 Tecniche di Audit che Preservano la Privacy

4.1 Analisi Dati Aggregati

4.1.1 Enforcement Unità Minima di Aggregazione

La Regola n≥10:

Nessun dato di valutazione psicologica può essere riportato o analizzato per gruppi più piccoli di 10 individui. Questa è la protezione privacy fondamentale nell'auditing CPF.

Passi di Verifica Audit:

1. **Rivedere Report Valutazione**: Controllare che tutte le metriche riportate mostrino n≥10
2. **Test Calcolo**: Richiedere all'organizzazione di dimostrare calcolo score con dati oscurati
3. **Query Database**: Se usato sistema digitale, verificare che i vincoli database impediscano query n<10
4. **Intervistare Privacy Officer**: Confermare comprensione e meccanismi di enforcement

Non Conformità Comuni:

- Piccolo dipartimento (n=7) analizzato separatamente → **MAJOR**: Violazione privacy
- Team esecutivo (n=5) profilato come gruppo → **MAJOR**: Violazione privacy
- Dashboard consente filtraggio a livello individuale → **CRITICAL**: Difetto progettazione sistema
- Risultati survey "anonimi" con n=3 rispondenti → **MAJOR**: Rischio re-identificazione

Esempio Approccio Conforme:

Scenario: Organizzazione ha team IT security di 8 persone (sotto soglia n=10)

Vietato: Riportare indicatori "Team IT Security" separatamente

Opzioni Conformi:

- Combinare con categoria più ampia "Staff Tecnico" (n=45)
- Riportare solo a "Livello Organizzativo" (n=250)
- Escludere team IT security dalla valutazione con giustificazione documentata

4.1.2 Requisiti Validità Statistica

Verifica Intervallo di Confidenza:

Per i CPF score riportati, gli auditor dovrebbero verificare la validità statistica:

$$\text{Margine di Errore} = Z \times \sqrt{\frac{p(1-p)}{n}} \tag{2}$$

Dove:

- Z = 1.96 (livello confidenza 95%)
- p = proporzione osservata
- n = dimensione campione

Test Audit:

Selezionare uno score di dominio riportato dall'organizzazione. Verificare:

- Dimensione campione documentata
- Intervallo confidenza calcolato (se dichiarato)
- Margine errore accettabile per decision-making

Esempio Verifica:

Organizzazione riporta: "Dominio Authority [1.x] score: 14/20 (Red), n=32"

Auditor calcola: MoE $= 1.96 \times \sqrt{\frac{0.7 \times 0.3}{32}} = \pm 15.8\%$

Interpretazione: Con confidenza 95%, lo score vero è 14 ± 3.2 punti (range 10.8-17.2). Ancora saldamente in zona Red (14-20), quindi il finding è statisticamente robusto.

4.1.3 Test Chi-Quadrato per Indipendenza

Quando l'organizzazione afferma nessuna correlazione tra domini, gli auditor possono verificare usando test chi-quadrato.

Ipotesi Nulla: Gli score dei domini sono indipendenti (nessuna correlazione)

$$\chi^2 = \sum \frac{(O - E)^2}{E} \tag{3}$$

Dove O = frequenza osservata, E = frequenza attesa

Applicazione Audit:

Testare se gli indicatori Red si raggruppano in domini specifici vs. distribuzione casuale.

4.2 Metodi di Osservazione

4.2.1 Principi Osservazione Non Invasiva

Gli audit CPF si basano sull'osservazione di pattern organizzativi, NON sorveglianza di individui.

Osservazione Consentita:

- Sessioni training security awareness (dinamiche gruppo)
- Esercitazioni tabletop incident response (pattern risposta stress)
- Workflow security operations center (carico cognitivo, alert fatigue)
- Riunioni all-hands (gradiente authority, pattern comunicazione)

- Postura sicurezza fisica (conformità controllo accessi, tailgating)

Osservazione Vietata:

- Monitoraggio postazione lavoro individuale
- Revisione contenuto email (solo analisi metadata, aggregata)
- Videosorveglianza di individui specifici
- Tracciamento real-time movimenti dipendenti
- Osservazione nascosta senza consenso informato

Protocollo Osservazione:

1. **Annunciare Presenza**: Auditor si presenta e spiega lo scopo
2. **Ottenere Consenso**: Consenso di gruppo per osservazione
3. **Registrare Pattern**: Notare comportamenti organizzativi, non individuali
4. **Debrief**: Condividere osservazioni generali con il gruppo

4.2.2 Log Sistema vs. Monitoraggio Individuale

Analisi Log Conforme:

- **Pattern Autenticazione Aggregati**: "30% dei login avviene fuori orario lavorativo" (n=250)
- **Risposta Alert Collettiva**: "Tempo medio risposta alert alta gravità: 47 minuti" (n=12 analisti)
- **Pattern Ora del Giorno**: "Tasso click phishing: 8% mattina, 19% pomeriggio" (n=500 destinatari test)

Analisi Log Non Conforme:

- "Utente JDoe ha cliccato link phishing 3 volte in 6 mesi" → Profilazione individuale
- "Dipartimento finance (n=7) ha tasso click 45%" → Sotto soglia n=10
- "Top 5 utenti per tentativi login falliti" → Ranking individuale

Verifica Audit:

Richiedere campione report analisi log. Controllare per:

☐ Nessun username individuale o identificatore

☐ Tutti i gruppi riportati soddisfano requisito n≥10

☐ Livello aggregazione appropriato (dipartimento, ruolo, periodo tempo)

☐ Nessuna "classifica" o ranking individuale

4.2.3 Valutazione Comportamentale in Gruppi

Metodologia Focus Group:

Gli audit CPF possono usare focus group facilitati per valutare vulnerabilità psicologiche a livello aggregato.

Protocollo Focus Group:

- **Dimensione**: 8-12 partecipanti (soddisfa n≥10, consente discussione)
- **Composizione**: Eterogenea (cross-funzionale) o omogenea (singolo ruolo)
- **Facilitatore**: Formato su dinamiche gruppo e tecniche trauma-informed
- **Registrazione**: Note su temi/pattern, NON attribuzione a individui
- **Consenso**: Consenso scritto da tutti i partecipanti

Esempio Domande Focus Group (Dominio Authority):

- "In generale, quanto si sentono a proprio agio le persone nel mettere in discussione richieste insolite dai dirigenti?"
- "Cosa succede tipicamente quando qualcuno solleva preoccupazioni sulla richiesta di una figura di autorità?"
- "Potete descrivere la cultura organizzativa riguardo alle eccezioni di sicurezza per la leadership?"

Approccio Analisi:

- Identificare temi ricorrenti attraverso più partecipanti
- Notare dinamiche gruppo (consenso, conflitto, voci dominanti)
- Citare anonimamente: "Diversi partecipanti hanno notato..." o "Un tema comune era..."
- Mai attribuire dichiarazioni a individui specifici nel report

4.2.4 Verifica Ritardo Temporale

CPF-27001 richiede ritardo minimo 72 ore tra raccolta dati e reporting per prevenire sorveglianza real-time.

Verifica Audit:

1. **Rivedere Timestamp**: Controllare date report valutazione vs. date raccolta dati
2. **Intervistare Team Valutazione**: "Come assicurate il ritardo di 72 ore?"
3. **Testare Controlli Sistema**: Se automatizzato, verificare che sistema imponga ritardo
4. **Rivedere Incident Response**: Controllare che alert real-time non bypassino controlli privacy

Non Conformità Comuni:

- Dashboard mostra metriche vulnerabilità psicologica "live" → **MAJOR**
- Incident response usa indicatori stress real-time → **MAJOR**
- Report mensile generato stesso giorno raccolta dati → **MINOR**

Eccezione Accettabile:

Vere emergenze (incidente sicurezza attivo, crisi stato convergente) possono richiedere valutazione real-time, ma richiede:

- Autorizzazione esecutiva
- Giustificazione documentata
- Revisione privacy immediata post-incidente
- Distruzione dati dopo risoluzione incidente

4.3 Tecniche di Intervista

4.3.1 Raccolta Feedback Anonimizzato

Setup Intervista:

- **Spazio Privato**: Nessuna osservazione da management o colleghi
- **Modulo Consenso**: Firmato prima inizio intervista
- **Registrazione**: Solo note (no audio/video a meno di consenso specifico)
- **Sistema Codifica**: Assegnare codice (INT-001) invece di usare nomi
- **Durata**: 30-45 minuti tipico

Struttura Intervista:

1. **Apertura (5 min)**: Costruire rapport, spiegare scopo, confermare consenso
2. **Domande Generali (15 min)**: Cultura organizzativa, security awareness
3. **Specifiche Dominio (15 min)**: Domande mirate basate su risk assessment
4. **Chiusura (5 min)**: Eventuali preoccupazioni, ringraziare partecipante, prossimi passi

Guida Intervista Esempio (Focus Dominio Authority):

Apertura:

- "Grazie per partecipare. Questo è confidenziale e le vostre risposte saranno combinate con almeno altre 10."
- "Stiamo valutando pattern organizzativi, non valutando individui."

- "Potete saltare qualsiasi domanda o fermarvi in qualsiasi momento. Avete domande prima di iniziare?"

Domande Generali:

- "Come descriverebbe la cultura della sicurezza qui?"
- "Cosa aiuta le persone a seguire le procedure di sicurezza? Cosa lo rende difficile?"
- "Può pensare a un momento in cui le esigenze di sicurezza e business sono entrate in conflitto?"

Domande Specifiche Authority:

- "Se ricevesse una richiesta insolita da un dirigente, cosa farebbe tipicamente?"
- "Esiste un processo per verificare richieste che sembrano urgenti o fuori dal normale?"
- "Quanto comode pensate che le persone si sentano nel mettere in discussione figure di autorità sulla sicurezza?"

Chiusura:

- "C'è qualcosa di importante che non abbiamo discusso?"
- "Ha preoccupazioni su questa intervista o il processo di audit?"
- "Il vostro contributo è prezioso per migliorare la sicurezza organizzativa. Grazie."

4.3.2 Sicurezza Psicologica nelle Interviste

Creare Ambiente Sicuro:

- **Posizione Non Giudicante**: Validare tutte le risposte come prospettive legittime
- **Normalizzare Vulnerabilità**: "Queste sono risposte umane universali"
- **Evitare Domande Tendenziose**: "Come fa..." non "Non pensa che..."
- **Rispettare Confini**: Se partecipante a disagio, passare al prossimo argomento
- **Gestire Dinamiche Potere**: Riconoscere ruolo auditor, ma enfatizzare partnership

Segnali di Allarme per Auto-Monitoraggio Auditor:

- Partecipante dà solo risposte "corrette" (eccessivamente compiacente)
- Partecipante difensivo o ostile (percependo giudizio)
- Partecipante timoroso sulla confidenzialità
- Partecipante incolpa individui vs. discutere sistemi

Tecniche di Recupero:

- **Rassicurare Privacy**: "Ricordi, nessun nome nel report, minimo 10 risposte combinate"
- **Riformulare Scopo**: "Stiamo esaminando il design organizzativo, non le persone"
- **Validare Preoccupazione**: "Apprezzo che l'abbia sollevato; la confidenzialità è critica"
- **Offrire Pausa**: "Vorrebbe qualche minuto prima di continuare?"

4.3.3 Domande Trauma-Informed

Le organizzazioni che hanno vissuto incidenti di sicurezza possono avere risposte traumatiche. Gli auditor devono riconoscere e accomodare queste.

Indicatori Trauma:

- Disagio visibile quando si discute di incidenti passati
- Evitamento di certi argomenti o periodi temporali
- Ipervigilanza o postura difensiva
- Espressione di colpa, vergogna o senso di colpa
- Disregolazione emotiva (rabbia, lacrime, shutdown)

Adattamenti Trauma-Informed:

- **Avvertimento**: "Vorrei chiedere di [incidente]. Va bene discuterne?"
- **Ritmo**: Permettere tempo extra, non affrettare contenuto emotivo
- **Controllo**: "Possiamo saltare questo o tornarci più tardi"
- **Grounding**: Se partecipante dissocia, reindirizzare al presente ("È al sicuro qui ora")
- **Supporto**: Avere risorse assistenza dipendenti disponibili

Esempio Progressione Domanda Trauma-Informed:

Invece di: "Mi parli dell'incidente ransomware dell'anno scorso."

Trauma-Informed:

1. "Ho capito che la vostra organizzazione ha vissuto un evento di sicurezza significativo. Va bene discuterne?"
2. (Se sì) "Non ci servono dettagli su cosa è successo. Sono interessato a come l'organizzazione ha risposto e cosa è cambiato da allora."
3. (Se evidente disagio) "Vedo che questo è difficile. Preferisce concentrarsi sulle procedure attuali invece?"

5 Verifica Scoring e Maturità

5.1 Ricalcolo CPF Score

Gli auditor devono verificare in modo indipendente il calcolo del CPF Score dell'organizzazione per assicurare accuratezza matematica e conformità metodologica.

5.1.1 Metodologia di Campionamento per Verifica

Approccio di Campionamento Audit:

Piuttosto che ri-valutare tutti i 100 indicatori (dispendioso in termini di tempo), gli auditor campionano strategicamente:

Campione Minimo: 20 indicatori (copertura 20%)

Campione Raccomandato: 30 indicatori (copertura 30%)

Strategia di Campionamento:

- **Selezione Basata sul Rischio**: Tutti gli indicatori Red (score 2) devono essere verificati
- **Proporzionale per Dominio**: Campionare proporzionalmente da ogni dominio
- **Componente Casuale**: 50% del campione selezionato casualmente
- **Indicatori Critici**: Includere indicatori con pesi più alti

Piano Campionamento Esempio (30 indicatori):

Tabella 5: Distribuzione Campionamento Indicatori

Dominio	Indicatori Totali	Conteggio Red	Dimensione Campione
Authority [1.x]	10	4	5 (tutti 4 Red + 1 casuale)
Temporal [2.x]	10	3	4 (tutti 3 Red + 1 casuale)
Social Influence [3.x]	10	1	3 (1 Red + 2 casuali)
Affective [4.x]	10	2	3 (2 Red + 1 casuale)
Cognitive Overload [5.x]	10	3	4 (tutti 3 Red + 1 casuale)
Group Dynamics [6.x]	10	1	3 (1 Red + 2 casuali)
Stress Response [7.x]	10	2	3 (2 Red + 1 casuale)
Unconscious [8.x]	10	0	2 (2 casuali)
AI-Specific [9.x]	10	1	2 (1 Red + 1 casuale)
Convergent [10.x]	10	1	1 (1 Red)
Totale	**100**	**18**	**30**

5.1.2 Processo Verifica Indicatori

Per ogni indicatore campionato, l'auditor esegue una valutazione indipendente:

Passo 1: Raccolta Evidenze

Richiedere evidenze dell'organizzazione per l'indicatore. Secondo metodologia Field Kit, minimo 3 fonti dati indipendenti richieste.

Esempio - Indicatore 1.1 (Conformità Acritica):

- Fonte Dati 1: Log gateway email (pattern richieste insolite)
- Fonte Dati 2: Osservazioni audit sicurezza (conformità verifica)
- Fonte Dati 3: Risultati survey anonimi (comfort nel questionare authority)

Passo 2: Verifica Triangolazione

Valutare se l'organizzazione ha raggiunto accordo minimo 67% delle fonti (2 su 3 fonti convergono).

Passo 3: Scoring Indipendente

Applicare logica scoring ternaria (Green/Yellow/Red) basata su soglie evidenze:

- **Green (0)**: Tasso eccezioni $< 5\%$, controlli efficaci
- **Yellow (1)**: Tasso eccezioni 5-15%, monitoraggio necessario
- **Red (2)**: Tasso eccezioni $> 15\%$, intervento immediato richiesto

Passo 4: Confronto con Score Organizzazione

- **Accordo**: Passare al prossimo indicatore
- **Differenza Un Livello**: Documentare razionale, accettare con nota
- **Differenza Due Livelli**: Segnalare come potenziale non conformità, investigare ulteriormente

Varianza Accettabile:

- $\leq$ **20% tasso disaccordo**: Metodologia valutazione conforme
- **20-30% disaccordo**: Non conformità minore (raffinamento metodologia necessario)
- $>$ **30% disaccordo**: Non conformità maggiore (fallimento sistemico valutazione)

5.1.3 Controllo Accuratezza Calcolo

Verifica Score Dominio:

Selezionare 2-3 domini per verifica completa calcolo:

$$\text{Domain\_Score}_d = \sum_{i=1}^{10} \text{Indicator}_i \tag{4}$$

Test Audit:

Organizzazione Riporta: Dominio Authority [1.x] = 16/20

Auditor Verifica:

- Sommare score indicatori individuali: 1.1(2) + 1.2(1) + 1.3(2) + 1.4(2) + 1.5(1) + 1.6(2) + 1.7(2) + 1.8(1) + 1.9(2) + 1.10(1) = 16 ✓
- Controllare: Range 0-20? Sì ✓
- Classificazione: 14-20 = Red? Sì ✓

Verifica CPF Score Complessivo:

$$\text{CPF\_Score} = 100 - \left(\sum_{d=1}^{10} w_d \times \text{Domain\_Score}_d \right) \times 2.5 \tag{5}$$

Procedura Audit:

1. Ottenere score domini dall'organizzazione
2. Verificare pesi domini utilizzati (riferimento: CPF Scoring Model, Sezione 4.2)
3. Ricalcolare somma pesata
4. Applicare moltiplicatore 2.5
5. Verificare che score finale corrisponda allo score riportato dall'organizzazione

Esempio Verifica Calcolo:

$$\begin{aligned}\text{Somma Pesata} &= (16 \times 0.15) + (14 \times 0.12) + (5 \times 0.11) + (11 \times 0.10) \\ &\quad + (16 \times 0.11) + (7 \times 0.09) + (12 \times 0.10) \\ &\quad + (4 \times 0.08) + (9 \times 0.07) + (6 \times 0.07) \\ &= 2.40 + 1.68 + 0.55 + 1.10 + 1.76 + 0.63 + 1.20 + 0.32 + 0.63 + 0.42 \\ &= 10.69\end{aligned}$$

$$\text{CPF\_Score} = 100 - (10.69 \times 2.5) = 100 - 26.73 = 73.27 \tag{6}$$

Errori Calcolo Comuni:

- Pesi domini errati applicati → Non conformità **MAJOR**
- Errori aritmetici nella somma → Non conformità **MINOR**
- Moltiplicatore errato (non 2.5) → Non conformità **MAJOR**
- Errori arrotondamento > 2 punti → Non conformità **MINOR**

5.1.4 Validazione Convergence Index

Verifica Formula CI:

$$\text{CI} = \prod_{i=1}^{n}(1 + v_i) \tag{7}$$

dove v_i = score vulnerabilità normalizzato (Red=1.0, Yellow=0.5), n = conteggio indicatori Yellow/Red

Passi Audit:

1. **Identificare Indicatori Vulnerabili**: Contare tutti gli indicatori Yellow (1) e Red (2)
2. **Normalizzare Score**: Yellow → 0.5, Red → 1.0
3. **Calcolare Prodotto**: $(1 + v_1) \times (1 + v_2) \times ... \times (1 + v_n)$
4. **Verificare Classificazione Soglia**:
   - CI < 2: Rischio basso

- $2 \leq \text{CI} < 5$: Rischio moderato
- $5 \leq \text{CI} < 10$: Rischio alto
- $\text{CI} \geq 10$: Rischio critico

Esempio Verifica CI:

Dati Organizzazione:

- 18 indicatori Red (score 2)
- 27 indicatori Yellow (score 1)
- 55 indicatori Green (score 0)

Calcolo Auditor:

$$\begin{aligned}\text{CI} &= (1 + 1.0)^{18} \times (1 + 0.5)^{27} \\ &= 2^{18} \times 1.5^{27} \\ &= 262,144 \times 14,551.9 \\ &= 3.81 \times 10^{9} \quad \text{(Convergenza critica)}\end{aligned}$$

Finding: $\text{CI} \gg 10$, indicando stato convergenza catastrofica che richiede risposta emergenza.

5.2 Valutazione Livello Maturità

5.2.1 Requisiti Evidenze per Livello

Gli auditor verificano le dichiarazioni del livello di maturità rispetto ai criteri CPF Maturity Model.

Livello 1 (Initial) - Checklist Verifica:

☐ Briefing consapevolezza esecutiva documentato (verbali riunione, presentazione)

☐ Valutazione iniziale condotta (minimo 20 indicatori, non 100 completi)

☐ Fattori psicologici in report incidenti (rivedere 3+ incidenti recenti)

☐ Psicologia base in programma awareness (materiali formativi riferiscono concetti CPF)

☐ CPF Score > 20/100 (verificare calcolo)

☐ Minimo 3 su 10 categorie valutate (documentazione ambito valutazione)

Livello 2 (Developing) - Checklist Verifica:

☐ Valutazione completa 100 indicatori completata (tutti domini documentati)

☐ Heat map vulnerabilità mantenuta (rappresentazione visuale, aggiornata regolarmente)

☐ Playbook risposta includono fattori psicologici (rivedere 2+ playbook)

☐ Training psicologia team sicurezza (registri formazione, certificati)

- ☐ CPF Score > 40/100 con indicatori Red < 25%
- ☐ 7+ categorie attivamente monitorate (KPI definiti per ciascuna)
- ☐ Ciclo valutazione trimestrale (4 valutazioni negli ultimi 12 mesi)
- ☐ 75% staff formato (registri presenze formazione)

Livello 3 (Defined) - Checklist Verifica:

- ☐ Dashboard monitoraggio CPF real-time operativo (dimostrazione sistema)
- ☐ Modelli predittivi per stati vulnerabilità (documentazione modello, metriche accuratezza)
- ☐ Integrazione cross-funzionale (verbali riunioni HR/IT/Risk, processi condivisi)
- ☐ Interventi specifici per ruolo (approcci diversi per dipartimento/ruolo)
- ☐ CPF Score > 60/100 senza indicatori Red > 30 giorni
- ☐ Tutte 10 categorie con KPI definiti (revisione dashboard KPI)
- ☐ Valutazione mensile + monitoraggio giornaliero (documentazione frequenza)
- ☐ 90% staff formato + certificazioni specializzate (elenco certificazioni)
- ☐ Reporting CPF a livello board (materiali presentazione board)

Livello 4 (Managed) - Checklist Verifica:

- ☐ Predizione ML-driven > 80% accuratezza (risultati studio validazione)
- ☐ Trigger intervento automatizzato (configurazione sistema, log trigger)
- ☐ Metriche sicurezza psicologica a livello organizzazione (dati survey, tracking)
- ☐ Valutazione rischio terze parti include CPF (template valutazione fornitori)
- ☐ CPF Score > 80/100 con intervento proattivo (prima soglia Yellow)
- ☐ Monitoraggio real-time tutti indicatori (dimostrazione capacità sistema)
- ☐ 100% staff formato + 25% practitioner certificati (verifica certificazioni)
- ☐ ROI 5:1 dimostrabile (documentazione analisi finanziaria)
- ☐ Riduzioni premio assicurativo > 20% (documentazione polizza)

Livello 5 (Optimizing) - Checklist Verifica:

- ☐ Sistemi difesa psicologica autonomi (dimostrazione sistema AI-driven)
- ☐ Contributo ricerca all'evoluzione CPF (paper pubblicati, presentazioni)
- ☐ Condivisione threat intelligence cross-settore (prova membership consorzio)
- ☐ Laboratorio innovazione sicurezza psicologica (facility, staff dedicato)

☐ Chief Psychology Officer certificato board (credenziali CPO)

☐ CPF Score > 90/100 sostenuto (12+ mesi stato green continuo)

☐ 2+ nuovi metodi pubblicati annualmente (lista pubblicazioni)

☐ Accuratezza predizione > 95% inclusi attacchi novel (dati validazione)

☐ 50%+ staff certificato CPF (database certificazioni)

☐ Contributo standard settore (prova partecipazione enti standard)

5.2.2 Dimostrazione Capacità

Oltre alla revisione documentazione, gli auditor verificano capacità pratiche tramite dimostrazione.

Test Pratici Livello 2:

Test 1: Navigazione Heat Map Vulnerabilità

- Richiesta: "Mostratemi le vulnerabilità attuali per dominio"
- Osservare: Lo staff può localizzare e interpretare rapidamente la heat map?
- Verificare: Dati attuali (entro ciclo trimestrale), privacy preservata (n≥10)

Test 2: Integrazione Psicologica Playbook

- Richiesta: "Mostrami il playbook risposta ransomware"
- Osservare: Sono affrontate risposte stress, dinamiche gruppo, pattern authority?
- Verificare: Non solo passi tecnici; include considerazioni psicologiche

Test Pratici Livello 3:

Test 1: Esecuzione Modello Predittivo

- Richiesta: "Prevedete lo stato vulnerabilità per il prossimo fine trimestre"
- Osservare: Modello elabora dati organizzativi, produce forecast rischio
- Verificare: Metodologia predizione documentata, accuratezza storica tracciata

Test 2: Coordinamento Cross-Funzionale

- Richiesta: "Descrivete come HR e IT collaborano sull'onboarding sicurezza"
- Osservare: Evidenza di processi congiunti, metriche condivise, comunicazione regolare
- Verificare: Integrazione genuina, non superficiale

5.2.3 Verifica Prestazioni Sostenute

I livelli di maturità richiedono prestazioni sostenute nel tempo, non raggiungimento puntuale.

Periodi Stabilità Minimi:

- **Livello 2**: 6 mesi al Livello 1 + 3 mesi dimostrando criteri Livello 2
- **Livello 3**: 12 mesi al Livello 2 + 6 mesi dimostrando criteri Livello 3
- **Livello 4**: 18 mesi al Livello 3 + 6 mesi dimostrando criteri Livello 4
- **Livello 5**: 24+ mesi al Livello 4 + innovazione continua

Evidenza Audit di Stabilità:

- Trend storico CPF Score (dati trimestrali per ultimi 12-24 mesi)
- Documentazione progressione livello maturità (date transizioni livello)
- Evidenza miglioramento continuo (azioni correttive, miglioramenti)
- Nessun indicatore regressione (cali temporanei score accettabili se recuperati)

Non Conformità Comune:

Organizzazione rivendica Livello 3 ma ha raggiunto criteri Livello 2 solo 2 mesi fa → **MAJOR**: Periodo stabilità insufficiente, livello maturità sovrastimato.

6 Guida Audit Clausola per Clausola

Questa sezione fornisce procedure di audit specifiche per ogni clausola CPF-27001:2025.

6.1 Clausola 4: Contesto dell'Organizzazione

6.1.1 Obiettivi Audit

Verificare che l'organizzazione abbia:

- Determinato questioni interne ed esterne rilevanti che influenzano il PVMS
- Identificato parti interessate e i loro requisiti
- Definito l'ambito PVMS appropriatamente
- Stabilito processi PVMS allineati con CPF-27001

6.1.2 Procedure di Verifica

4.1 Comprensione dell'Organizzazione e del suo Contesto

Evidenze da Richiedere:

- Documento analisi contesto (questioni interne/esterne)

- Valutazione panorama minacce settore
- Valutazione cultura organizzativa
- Pattern storici incidenti

Domande Audit:

- "Quali fattori psicologici sono specifici della vostra cultura organizzativa?"
- "Come influenzano le minacce specifiche del settore le vostre vulnerabilità psicologiche?"
- "Quali fattori esterni (normativi, competitivi) influenzano il vostro PVMS?"

Non Conformità Comuni:

- Analisi contesto generica non personalizzata per organizzazione → MINOR
- Nessuna considerazione minacce psicologiche specifiche settore → MAJOR
- Analisi contesto non aggiornata regolarmente → MINOR

4.2 Comprensione Esigenze e Aspettative delle Parti Interessate

Evidenze da Richiedere:

- Registro parti interessate
- Analisi requisiti stakeholder
- Registri comunicazione con parti chiave

Domande Audit:

- "Chi sono gli stakeholder chiave per il vostro PVMS?" (dipendenti, management, clienti, regolatori, assicuratori)
- "Come raccogliete e documentate i loro requisiti?"
- "Come influenzano i requisiti privacy dei dipendenti il design del vostro PVMS?"

4.3 Determinazione dell'Ambito del PVMS

Evidenze da Richiedere:

- Dichiarazione Ambito PVMS
- Giustificazione per esclusioni
- Organigramma che mostra unità coperte

Verifica:

- Ambito definisce chiaramente i confini (località, dipartimenti, funzioni)
- Esclusioni giustificate e documentate
- Ambito coerente con contesto organizzativo

- Integrazione con ambito ISMS (se applicabile)

Non Conformità Comuni:

- Definizione ambito vaga ("intera organizzazione") → MINOR
- Esclusioni ingiustificate (dipartimenti alto rischio esclusi) → MAJOR
- Ambito non approvato dal management → MAJOR

4.4 Sistema di Gestione delle Vulnerabilità Psicologiche

Verifica:

- Processi PVMS documentati e implementati
- Interazioni processi definite
- Ownership processi assegnato
- Monitoraggio e misurazione stabiliti

6.2 Clausola 5: Leadership

6.2.1 Obiettivi Audit

Verificare che il top management dimostri leadership e impegno verso il PVMS.

6.2.2 Procedure di Verifica

5.1 Leadership e Impegno

Evidenze da Richiedere:

- Verbali riunioni board/esecutive che menzionano PVMS
- Approvazioni allocazione risorse
- Comunicazioni esecutive sull'importanza PVMS
- Documentazione budget per attività PVMS

Domande Audit (Intervista Esecutivi):

- "Come supporta la gestione delle vulnerabilità psicologiche gli obiettivi di business?"
- "Quali risorse sono state allocate per l'implementazione PVMS?"
- "Come monitorate l'efficacia del PVMS?"
- "Quale ruolo gioca il board nella supervisione PVMS?"

Segnali di Allarme:

- Delega esecutiva senza coinvolgimento → Mancanza impegno

- Risorse insufficienti allocate → Conformità nominale
- Nessun item PVMS in agende riesame direzione → Mancanza integrazione

5.2 Policy

Evidenze da Richiedere:

- Documento Policy CPF
- Documentazione approvazione policy
- Registri comunicazione policy
- Storico revisione policy

Checklist Verifica:

☐ Policy appropriata allo scopo dell'organizzazione

☐ Impegno a valutazione sistematica vulnerabilità psicologiche

☐ Impegno a protezione privacy (n≥10, $\varepsilon \leq 0.1$, ritardo 72h)

☐ Framework per definire obiettivi CPF

☐ Impegno a miglioramento continuo

☐ Approvata dal top management

☐ Comunicata a tutte le parti rilevanti

☐ Disponibile alle parti interessate (quando appropriato)

Non Conformità Comuni:

- Template policy generico non personalizzato → MINOR
- Impegni privacy mancanti o vaghi → MAJOR
- Policy non approvata da CEO/Board → MAJOR
- Policy non comunicata allo staff → MINOR

5.3 Ruoli, Responsabilità e Autorità Organizzative

Evidenze da Richiedere:

- Struttura organizzativa PVMS
- Descrizioni ruoli (Coordinatore CPF, Privacy Officer, Specialisti Valutazione)
- Documentazione delega autorità
- Requisiti competenza per ruolo

Ruoli Chiave da Verificare:

Domande Audit:

- "Chi è responsabile del PVMS complessivo?" (Intervistare quella persona)
- "Come viene assicurata la protezione privacy?" (Intervistare Privacy Officer)
- "Quale autorità ha il Coordinatore CPF?" (Budget, escalation, richieste risorse)

Tabella 6: Ruoli Chiave PVMS

Ruolo	Responsabilità
Coordinatore CPF	Gestione PVMS complessiva, coordinamento valutazione, reporting management
Privacy Officer	Enforcement protezione privacy, gestione consenso, verifica anonimizzazione
Specialisti Valutazione	Valutazione indicatori, raccolta dati, analisi
Coordinatori Risposta	Implementazione trattamento rischio, design intervento

6.3 Clausola 6: Pianificazione

6.3.1 Obiettivi Audit

Verificare che l'organizzazione abbia pianificato l'implementazione PVMS affrontando rischi e opportunità.

6.3.2 Procedure di Verifica

6.1.1 Generale

Evidenze da Richiedere:

- Registro rischi e opportunità
- Documentazione pianificazione
- Integrazione con pianificazione strategica

6.1.2 Valutazione Vulnerabilità Psicologiche

Focus Audit Critico - Questo è il cuore della conformità CPF-27001.

Evidenze da Richiedere:

- Documento metodologia valutazione
- Procedure protezione privacy
- Procedure raccolta dati (schema OFTLISRV)
- Strumenti e template valutazione
- Materiali formativi per team valutazione

Checklist Verifica:

☐ Tutti i 10 domini CPF valutati

☐ 100 indicatori valutati (o razionale documentato per esclusioni)

☐ Scoring ternario (Green/Yellow/Red) applicato

☐ Minimo 3 fonti dati per indicatore (triangolazione)

☐ Protezioni privacy implementate:

- ☐ Unità aggregazione minima n≥10
- ☐ Privacy differenziale $\varepsilon \leq 0.1$
- ☐ Ritardo temporale $\geq$ 72 ore

☐ Frequenza valutazione definita (minimo annuale)

☐ Valutatori competenti assegnati

Verifica Approfondita (Selezionare 3 Domini):

Per ogni dominio selezionato, audit:

1. **Fonti Dati**: Rivedere evidenze per 2-3 indicatori
2. **Logica Scoring**: Verificare soglie applicate correttamente (Green/Yellow/Red)
3. **Conformità Privacy**: Controllare livello aggregazione (n≥10)
4. **Documentazione**: Valutare completezza e chiarezza

Non Conformità Comuni:

- Meno di 3 fonti dati per indicatore → MAJOR
- Dati livello individuale non aggregati → CRITICAL
- Nessuna privacy differenziale applicata → MAJOR
- Ritardo temporale non imposto → MAJOR
- Metodologia valutazione non documentata → MAJOR
- Domini esclusi senza giustificazione → MAJOR

6.1.3 Trattamento Rischio Psicologico

Evidenze da Richiedere:

- Piano trattamento rischio
- Descrizioni interventi
- Timeline implementazione
- Assegnazioni responsabilità
- Approccio monitoraggio efficacia

Verifica:

- Trattamento rischio affronta indicatori Yellow e Red
- Interventi sono organizzativi (non focalizzati su individui)
- Protocolli risposta definiti (per requisiti Sezione 8.3)
- Risorse allocate per implementazione
- Meccanismi monitoraggio stabiliti

Domande Audit:

- "Come decidete quali vulnerabilità affrontare per prime?"
- "Mostratemi un intervento per un indicatore Red nel dominio Authority"
- "Come misurate l'efficacia degli interventi?"

6.2 Obiettivi CPF e Pianificazione

Evidenze da Richiedere:

- Documento obiettivi CPF
- Processo definizione obiettivi
- Meccanismi tracciamento progressi
- Definizioni KPI

Verifica - Obiettivi SMART:

- **Specifici**: Descrizione chiara (es. "Ridurre indicatori Red dominio Authority da 4 a 1")
- **Misurabili**: Metriche quantificabili (conteggi indicatori, target CPF Score)
- **Raggiungibili**: Realistici date le risorse
- **Rilevanti**: Allineati con scopo PVMS
- **Temporizzati**: Date completamento definite

Esempio Obiettivi Conformi:

- "Raggiungere CPF Score >60 entro Q4 2025" (da attuale 58)
- "Ridurre Convergence Index sotto 5 entro 6 mesi" (da attuale 7.2)
- "Eliminare tutti gli indicatori Red nel dominio Authority entro dicembre 2025"
- "Formare 90% dello staff sui concetti CPF entro fine 2025"

6.4 Clausola 7: Supporto

6.4.1 Obiettivi Audit

Verificare che l'organizzazione abbia fornito risorse di supporto necessarie per il PVMS.

6.4.2 Procedure di Verifica

7.1 Risorse

Evidenze da Richiedere:

- Allocazioni budget per PVMS

- Personale per ruoli PVMS
- Investimenti tecnologici (strumenti valutazione, dashboard)
- Budget formazione

Valutazione Adeguatezza:

Confrontare risorse con requisiti livello maturità (riferimento: sezione ROI Maturity Model).

7.2 Competenza

Evidenze da Richiedere:

- Requisiti competenza per ruolo
- CV/curriculum del personale chiave PVMS
- Registri formazione
- Certificazioni (CISSP, CISM, lauree psicologia, certificazioni CPF)
- Analisi gap competenze

Verifica Competenza Coordinatore CPF:

Intervistare Coordinatore CPF e valutare:

- Comprensione fondamenti cybersecurity
- Conoscenza teoria psicologica (Bion, Klein, Kahneman, Cialdini)
- Familiarità con regolamenti privacy (GDPR, privacy differenziale)
- Conoscenza metodologia audit e valutazione

Domande Campione:

- "Spiega gli assunti di base di Bion e la loro rilevanza per la cybersecurity"
- "Come protegge la privacy differenziale la privacy individuale?"
- "Guidami attraverso lo schema OFTLISRV per la valutazione indicatori"

Non Conformità Comuni:

- Coordinatore CPF manca background psicologico → MAJOR
- Nessuna formazione formale in metodologia CPF → MINOR
- Team valutazione manca expertise cybersecurity → MAJOR
- Privacy Officer non familiare con privacy differenziale → MAJOR

7.3 Consapevolezza

Evidenze da Richiedere:

- Materiali campagna awareness

- Registri comunicazione
- Risultati survey staff su awareness CPF
- Registri presenze formazione

Test Awareness (Interviste Staff):

Selezionare 5-10 staff casualmente e chiedere:

- "Siete a conoscenza del programma CPF dell'organizzazione?"
- "Come protegge la valutazione CPF la vostra privacy?"
- "Si tratta di valutare voi personalmente o pattern organizzativi?"

Risultati Accettabili: 70%+ può articolare scopo base CPF e protezioni privacy.

7.4 Comunicazione

Verifica:

- Piano comunicazione interna (cosa, quando, chi, come)
- Protocolli comunicazione esterna (regolatori, assicuratori, enti certificazione)
- Meccanismi feedback
- Procedure comunicazione incidenti

7.5 Informazioni Documentate

Evidenze da Richiedere:

- Procedure controllo documenti
- Registro documenti
- Registri controllo versione
- Controlli accesso per documenti sensibili
- Schedari conservazione

Documenti Richiesti (per CPF-27001):

- Policy CPF
- Ambito PVMS
- Metodologia valutazione
- Procedure privacy
- Piani trattamento rischio
- Requisiti competenza
- Procedure monitoraggio e misurazione
- Programma audit interni
- Registri riesame direzione

6.5 Clausola 8: Operatività

6.5.1 Obiettivi Audit

Verificare che l'organizzazione abbia implementato controlli operativi per il PVMS.

6.5.2 Procedure di Verifica

8.1 Pianificazione e Controllo Operativi

Evidenze da Richiedere:

- Procedure operative per PVMS
- Programmi valutazione
- Protocolli raccolta dati
- Integrazione con operazioni sicurezza
- Procedure gestione cambiamenti

Verifica:

- Cicli valutazione regolari stabiliti (minimo annuale)
- Monitoraggio continuo per indicatori critici
- Raccolta dati che preserva privacy implementata
- Procedure esecuzione trattamento rischio
- Integrazione con controlli operativi ISMS

8.2 Valutazione Vulnerabilità Psicologiche (Operativa)

Verifica Operativa Critica - Focus audit più importante.

Audit Processo Valutazione:

1. **Rivedere Ultimo Report Valutazione**
   - Data valutazione
   - Copertura ambito (tutti i 10 domini?)
   - Score indicatori documentati
   - Protezioni privacy applicate
2. **Verificare Triangolazione Dati**
   - Selezionare 5 indicatori per approfondimento
   - Richiedere evidenze per ciascuno (minimo 3 fonti)
   - Verificare indipendenza fonti
   - Controllare metodologia convergenza (soglia accordo 67%)
3. **Verifica Controlli Privacy**

- Controllare tutte metriche riportate: n≥10?
- Rivedere implementazione privacy differenziale
- Verificare ritardo temporale 72 ore imposto
- Testare controlli accesso database (sistema può fare query n<10?)

4. **Revisione Analisi Basata su Ruoli**
   - Verificare analisi per ruolo/dipartimento, non individui
   - Controllare reporting piccoli gruppi (violazioni n<10)
   - Rivedere tecniche anonimizzazione

Verifica Uso Field Kit:

Se organizzazione usa CPF Field Kit:

- Rivedere Field Kit completati per 2-3 indicatori
- Verificare tutte sezioni completate (Quick Assessment, Evidence Collection, Scoring, Solutions)
- Controllare note campo per conformità privacy
- Confermare razionale scoring documentato

Non Conformità Comuni:

- Valutazione non eseguita negli ultimi 12 mesi → MAJOR
- Copertura domini incompleta (meno di 10 domini) → MAJOR
- Violazioni privacy (n<10, nessun ritardo temporale) → CRITICAL
- Singola fonte dati per indicatore (no triangolazione) → MAJOR
- Nessun razionale scoring documentato → MINOR

8.3 Trattamento Rischio Psicologico (Operativo)

Evidenze da Richiedere:

- Registri implementazione trattamento rischio
- Descrizioni e timeline interventi
- Documentazione protocollo risposta
- Dati monitoraggio efficacia
- Allocazione risorse per interventi

Verifica Protocollo Risposta Graduata:

Test Audit:

Selezionare 2 indicatori Red dall'ultima valutazione:

- La risposta è stata iniziata entro 7-14 giorni? (Verifica timeline)

Tabella 7: Conformità Protocollo Risposta

Stato	Risposta Richiesta
Green (0)	Monitoraggio standard, nessuna azione immediata
Yellow (1)	Monitoraggio potenziato, interventi preventivi entro 30-60 giorni
Red (2)	Escalation immediata, trattamento emergenza entro 7-14 giorni
CI Critico (>10)	Procedure risposta emergenza attivate

- Quale intervento è stato implementato? (Rivedere piano intervento)
- Chi era responsabile? (Verificare assegnazione ed esecuzione)
- L'efficacia è stata misurata? (Valutazione post-intervento)

Esempio Risposta Conforme:

Indicatore Red: Dominio Authority 1.1 (Conformità Acritica) = Red (2)

Implementazione Risposta:

- **Data Rilevamento:** 15 marzo 2025
- **Escalation:** 16 marzo 2025 (Coordinatore CPF notificato)
- **Piano Intervento:** 22 marzo 2025 (entro 7 giorni)
  - Protocollo verifica dual-channel implementato
  - Autenticazione email aggiornata (DMARC/SPF/DKIM)
  - Formazione challenge authority distribuita
- **Rivalutazione:** 15 giugno 2025 (3 mesi post-intervento)
- **Risultato:** Indicatore migliorato a Yellow (1)

Non Conformità Comuni:

- Indicatori Red senza risposta documentata → MAJOR
- Risposta ritardata oltre requisito 14 giorni → MINOR
- Interventi mirano individui vs. sistemi organizzativi → MAJOR
- Nessun monitoraggio efficacia → MINOR
- Stato convergente (CI>10) senza risposta emergenza → CRITICAL

8.4 Monitoraggio Continuo

Evidenze da Richiedere:

- Dashboard o report monitoraggio
- Configurazione alerting real-time (se applicabile)
- Documentazione integrazione SIEM

- Definizioni KPI monitoraggio
- Log risposta alert

Verifica:

- Indicatori critici monitorati continuamente (non solo valutazione annuale)
- Integrazione con security operations center (SOC)
- Alerting automatizzato per superamento soglie
- Protezioni privacy mantenute nel monitoraggio (n≥10, ritardo temporale)

Domande Audit:

- "Quali indicatori sono monitorati in real-time vs. valutati periodicamente?"
- "Come bilanciate monitoraggio continuo con ritardo temporale 72 ore?"
- "Mostratemi esempio di alert automatizzato innescato da soglia vulnerabilità psicologica"

6.6 Clausola 9: Valutazione Prestazioni

6.6.1 Obiettivi Audit

Verificare che l'organizzazione monitori, misuri, analizzi e valuti l'efficacia PVMS.

6.6.2 Procedure di Verifica

9.1 Monitoraggio, Misurazione, Analisi e Valutazione

Evidenze da Richiedere:

- Definizioni e target KPI
- Procedure monitoraggio e misurazione
- Report prestazioni (ultimi 12 mesi)
- Analisi trend
- Registri valutazione efficacia

Indicatori Prestazioni Chiave da Verificare:

Verifica Analisi Trend:

Richiedere CPF Score trimestrali per ultimi 12 mesi. Verificare:

- Score documentati coerentemente
- Direzione trend analizzata (miglioramento/stabile/declino)
- Cause radice trend investigate
- Azioni intraprese basate su trend

Tabella 8: Indicatori Prestazione CPF

KPI	**Target**	**Misurazione**
CPF Score	Trend crescente	Valutazione trimestrale
Conteggio Indicatori Red	Trend decrescente	Per valutazione
Conteggio Indicatori Yellow	Stabile o decrescente	Per valutazione
Convergence Index	CI < 5	Per valutazione
Incidenti Fattore Umano	Trend decrescente	Report incidenti mensili
Tempo Risposta (Red)	< 14 giorni	Log interventi
Completamento Formazione	$> 75\%$	Sistema formazione
Copertura Valutazione	100% (tutti domini)	Report valutazione

Valutazione Efficacia:

Per 2-3 interventi implementati:

- L'efficacia è stata misurata post-implementazione?
- Quali metriche sono state usate? (Cambiamento score indicatore, riduzione incidenti)
- I risultati sono stati documentati e comunicati?
- Sono stati fatti aggiustamenti basati su dati efficacia?

Non Conformità Comuni:

- KPI definiti ma non tracciati → MAJOR
- Nessuna analisi trend eseguita → MINOR
- Efficacia non valutata post-intervento → MINOR
- Dati monitoraggio non usati per decision-making → MAJOR

9.2 Audit Interno

Evidenze da Richiedere:

- Programma/calendario audit interni
- Report audit interni (ultimi 12 mesi)
- Registri competenza auditor
- Documentazione follow-up audit
- Tracciamento azioni correttive

Verifica Programma Audit Interno:

☐ Programma audit copre tutti processi PVMS

☐ Frequenza audit appropriata (minimo annuale)

☐ Pianificazione audit basata su rischio (focus domini alto rischio)

☐ Indipendenza auditor (non audita proprio lavoro)

☐ Competenza auditor appropriata (conoscenza CPF richiesta)

Valutazione Competenza Auditor:

Intervistare auditor interno/i:

- "Quale formazione avete ricevuto in metodologia CPF?"
- "Come verificate le protezioni privacy durante l'audit?"
- "Spiegate la differenza tra valutazione organizzativa e individuale"

Accettabile: Auditor interno ha formazione specifica CPF (minimo 8 ore) o esperienza equivalente.

Non Accettabile: Auditor ISO 27001 generico senza formazione CPF → Non conformità MAJOR

Revisione Report Audit:

Rivedere ultimo report audit interno:

- Copre l'ambito PVMS in modo completo?
- I finding sono documentati chiaramente?
- Le protezioni privacy sono verificate?
- Le azioni correttive sono tracciate?

9.3 Riesame Direzione

Evidenze da Richiedere:

- Calendario riesame direzione
- Verbali riunioni riesame direzione (minimo ultimi 2 riesami)
- Documentazione input riesame direzione
- Decisioni output riesame direzione
- Tracciamento action item

Input Richiesti (per CPF-27001 Clausola 9.3):

☐ Stato azioni da precedenti riesami direzione

☐ Cambiamenti in questioni esterne e interne

☐ Informazioni prestazioni inclusi trend

☐ Feedback da parti interessate

☐ Risultati valutazioni vulnerabilità psicologiche

☐ Risultati audit (interni ed esterni)

☐ Efficacia trattamento rischio

☐ Opportunità per miglioramento continuo

Output Richiesti:

- ☐ Decisioni relative a opportunità miglioramento continuo
- ☐ Decisioni relative a cambiamenti necessari al PVMS
- ☐ Necessità risorse

Domande Audit (Intervista Esecutivi):

- "Con quale frequenza il management rivede le prestazioni PVMS?"
- "Quali metriche CPF sono riportate al senior management?"
- "Può darmi esempio di decisione riesame direzione che ha portato a miglioramento PVMS?"
- "Come riceve il board informazioni sullo stato vulnerabilità psicologiche?"

Non Conformità Comuni:

- Riesame direzione non condotto annualmente → MAJOR
- Input richiesti mancanti dal riesame → MINOR per input mancante
- Nessun output/decisione documentati → MAJOR
- Azioni da riesame precedente non tracciate → MINOR
- Riesame direzione superficiale (nessuna discussione sostanziale) → MAJOR

6.7 Clausola 10: Miglioramento

6.7.1 Obiettivi Audit

Verificare che l'organizzazione migliori continuamente l'idoneità, adeguatezza ed efficacia del PVMS.

6.7.2 Procedure di Verifica

10.1 Non Conformità e Azioni Correttive

Evidenze da Richiedere:

- Registro non conformità
- Procedure azioni correttive
- Registri analisi causa radice
- Verifica efficacia azioni correttive
- Documentazione chiusura

Verifica Processo Azioni Correttive:

Selezionare 2-3 non conformità chiuse e tracciare attraverso processo:

1. **Reazione**: La non conformità è stata controllata/corretta immediatamente?
2. **Causa Radice**: La causa è stata analizzata (5-Perché, Fishbone, ecc.)?
3. **Azione**: L'azione correttiva era appropriata per eliminare causa radice?
4. **Implementazione**: L'azione è stata implementata come pianificato?
5. **Revisione**: L'efficacia è stata verificata prima della chiusura?
6. **Aggiornamento**: I documenti PVMS sono stati aggiornati se necessario?

Non Conformità PVMS Comuni (da audit precedenti):

- Violazioni privacy (n<10, nessun ritardo temporale)
- Triangolazione dati inadeguata
- Copertura domini mancante
- Competenza insufficiente
- Nessun trattamento rischio per indicatori Red
- Valutazione non eseguita tempestivamente

Esempio Azione Correttiva Conforme:

Non Conformità: "Dipartimento finance (n=7) analizzato separatamente, violando requisito n≥10"

Analisi Causa Radice: Team valutazione ha frainteso requisito aggregazione, nessun controllo validazione nel processo

Azione Correttiva:

- Riqualificare team valutazione su requisiti privacy
- Implementare controllo automatizzato in strumento valutazione (previene report n<10)
- Rielaborare dati finance combinati con categoria più ampia "staff amministrativo" (n=45)
- Aggiornare procedura valutazione per includere passo validazione privacy

Verifica Efficacia: Prossima valutazione aggrega correttamente tutti gruppi a n≥10 ✓

10.2 Miglioramento Continuo

Evidenze da Richiedere:

- Piano miglioramento continuo
- Documentazione iniziative miglioramento
- Trend CPF Score (12-24 mesi)
- Registri miglioramento processi
- Sforzi innovazione

Evidenza Miglioramento Continuo:

- CPF Score migliora nel tempo (trend trimestrale crescente)
- Stato indicatori migliora (Red → Yellow → Green)
- Raffinamenti metodologia valutazione
- Miglioramenti protezione privacy
- Miglioramenti integrazione con sicurezza tecnica
- Efficacia interventi crescente
- Progressione livello maturità

Domande Audit:

- "Come è migliorato il vostro PVMS nell'ultimo anno?"
- "Quali miglioramenti specifici avete fatto alla metodologia valutazione?"
- "Come identificate opportunità di miglioramento?"
- "Quali innovazioni state considerando per lo sviluppo futuro PVMS?"

Segnale Allarme: Organizzazione allo stesso livello maturità con CPF Score statico per 12+ mesi senza iniziative miglioramento documentate → Mancanza miglioramento continuo (MAJOR)

10.3 Aggiornamenti Framework

Evidenze da Richiedere:

- Procedura aggiornamento framework
- Documentazione ciclo revisione
- Registri gestione cambiamenti
- Comunicazione aggiornamenti
- Considerazioni compatibilità retroattiva

Verifica:

- Esiste processo per aggiornare indicatori/metodologia CPF
- Aggiornamenti rivisti attraverso gestione cambiamenti
- Cambiamenti validati prima implementazione
- Aggiornamenti documentati con razionale
- Stakeholder informati di cambiamenti framework

Domanda Audit:

"Come gestite aggiornamenti al framework CPF quando vengono identificate nuove vulnerabilità o evolvono tecniche di attacco?"

7 Audit Reporting

7.1 Struttura Report

7.1.1 Sommario Esecutivo

Il sommario esecutivo fornisce panoramica alto livello per senior management e board.

Elementi Richiesti:

- **Decisione Conformità Complessiva**: Conforme / Conforme con Non Conformità Minori / Non Conformità Maggiore / Non Conformità Critica
- **CPF Score**: Score attuale e rating (Excellent/Good/Fair/Poor/Critical)
- **Livello Maturità**: Livello attuale e stato progressione
- **Finding Critici**: Riepilogo non conformità CRITICAL e MAJOR (massimo 5 bullet point)
- **Punti Forza**: Osservazioni positive (2-3 item)
- **Raccomandazioni**: Top 3 azioni prioritarie

Lunghezza: Massimo 2 pagine

Esempio Apertura Sommario Esecutivo:

> *"Questo report presenta i finding dall'audit certificazione CPF-27001:2025 di [Nome Organizzazione] condotto [date]. L'organizzazione dimostra CONFORMITÀ CON NON CONFORMITÀ MINORI ai requisiti CPF-27001. L'attuale CPF Score è 73/100 (rating Good, livello rischio Low-Moderate), rappresentando Livello Maturità 2 (Developing). Tre non conformità minori sono state identificate relative a completezza documentazione, frequenza valutazione e copertura formazione. Nessuna non conformità maggiore o critica è stata trovata. L'organizzazione ha stabilito una solida base per la gestione vulnerabilità psicologiche con punti di forza particolari nell'impegno esecutivo e implementazione protezione privacy."*

7.1.2 Finding Dettagliati

Organizzazione per Clausola:

Per ogni clausola CPF-27001 (4-10):

- **Dichiarazione Conformità**: Conforme / Non Conforme
- **Evidenze Riviste**: Riepilogo documenti, interviste, osservazioni
- **Osservazioni Positive**: Punti di forza e buone pratiche
- **Non Conformità**: Descrizione dettagliata se presenti
- **Opportunità di Miglioramento**: Suggerimenti (non richiesti per conformità)

Organizzazione Alternativa per Dominio:

Per report focalizzati su domini:

- Riepilogo per dominio CPF [1.x] fino a [10.x]
- Score domini e stato (Green/Yellow/Red)
- Finding indicatori specifici
- Efficacia trattamento rischio

7.1.3 Classificazione Non Conformità

Non Conformità CRITICAL:

Definizione: Violazione privacy o fallimento sistemico che crea rischio danno immediato.

Esempi:

- Dati psicologici livello individuale riportati senza aggregazione
- Dati valutazione usati per valutazione prestazioni dipendenti
- Nessuna protezione privacy differenziale implementata
- Profilazione sistematica di individui

Impatto: Sospensione immediata processo certificazione. Deve essere corretto prima che certificato possa essere emesso.

Non Conformità MAJOR:

Definizione: Assenza o fallimento totale di requisito CPF-27001.

Esempi:

- Nessuna valutazione vulnerabilità psicologiche condotta negli ultimi 12 mesi
- Meno di 7 su 10 domini valutati
- Nessuna procedura protezione privacy documentata o implementata
- Coordinatore CPF manca competenze richieste
- Indicatori Red senza risposta documentata
- Nessun riesame direzione condotto

Impatto: Certificato non può essere emesso fino a correzione. Ricertificazione può richiedere audit follow-up.

Non Conformità MINOR:

Definizione: Lasso isolato o deficienza che non costituisce fallimento totale.

Esempi:

- Valutazione ritardata 2 settimane oltre scadenza annuale
- Un dominio incompletamente valutato (copertura parziale indicatori)
- Completamento formazione al 68% (target 75%)
- Documentazione incompleta per 2 su 10 domini

- Input riesame direzione manca un elemento richiesto

Impatto: Certificato può essere emesso con piano azione correttiva. Deve essere corretto prima del prossimo audit sorveglianza.

OBSERVATION (Non una Non Conformità):

Definizione: Opportunità miglioramento o suggerimento best practice.

Esempi:

- "Considerare implementazione dashboard automatizzata per monitoraggio real-time"
- "Uso Field Kit potrebbe migliorare consistenza valutazione"
- "Integrazione con onboarding HR potrebbe migliorare awareness"

Impatto: Nessuna azione correttiva richiesta. Organizzazione può scegliere di implementare o no.

7.1.4 Raccomandazioni

Framework Prioritizzazione:

1. **Alta Priorità**: Affronta non conformità MAJOR o vulnerabilità alto rischio
2. **Media Priorità**: Affronta non conformità MINOR o gap rischio moderato
3. **Bassa Priorità**: Opportunità miglioramento per avanzamento maturità

Formato Raccomandazione:

Per ogni raccomandazione:

- **Riferimento Finding**: Link a non conformità o osservazione specifica
- **Azione Raccomandata**: Descrizione chiara, azionabile
- **Razionale**: Perché questo miglioramento è importante
- **Beneficio Atteso**: Impatto anticipato su CPF Score o riduzione rischio
- **Timeline Suggerita**: Timeframe implementazione realistico
- **Sforzo Stimato**: Requisiti risorse (Basso/Medio/Alto)

7.2 Reporting Conforme Privacy

7.2.1 Requisiti Anonimizzazione

Divieti Rigorosi nei Report Audit:

- **NESSUN Nome Individuale**: Usare solo ruoli ("Finance Manager" non "John Smith")
- **NESSUN Dato Piccoli Gruppi**: Se n<10, non riportare separatamente

- **NESSUN Dettaglio Identificativo**: Rimuovere informazioni biografiche che consentono re-identificazione
- **NESSUNA Citazione con Attribuzione**: Anonimizzare tutte citazioni interviste

Esempi Reporting Conformi:

Finding: "Dati interviste da 15 membri staff finance indicano che 73% riporta disagio nel questionare richieste esecutive."

Citazione: "Più partecipanti hanno notato che 'questionare l'autorità è scoraggiato in pratica nonostante la policy ufficiale.'"

Osservazione: "Il team IT security (n=8) è stato combinato con staff tecnico più ampio (n=45) per analisi per mantenere protezioni privacy."

Esempi Non Conformi (NON USARE):

- × "Jane Doe in Finance ha cliccato 3 simulazioni phishing"
- × "L'assistente del CFO bypassa frequentemente la sicurezza"
- × "Dipartimento marketing (n=6) ha score vulnerabilità più alto"
- × "Come John ha menzionato nella nostra intervista, 'Non mi fido del team sicurezza'"

7.2.2 Standard Aggregazione

Unità Minime Reporting:

Tabella 9: Livelli Aggregazione che Preservano Privacy

Livello Aggregazione	n Minimo	Esempio
Organizzativo	Dipendenti totali	"CPF Score a livello organizzazione: 73"
Dipartimentale	≥10 per dept	"Funzioni amministrative (n=45): ..."
Basato su Ruolo	≥10 per ruolo	"Manager (n=32): ..."
Per Località	≥10 per sito	"Sede centrale (n=250): ..."

Gestione Piccoli Gruppi:

Scenario: Organizzazione ha team esecutivo 8 persone e team security 6 persone.

Vietato: Riportare score team esecutivo o security separatamente

Opzioni Conformi:

1. Combinare con categoria più grande: "Staff leadership e tecnico (n=65)"
2. Riportare solo livello organizzazione: "CPF Score Organizzativo"
3. Escludere con giustificazione documentata: "Team esecutivo e security esclusi da valutazione per vincoli dimensionali"

7.2.3 Distribuzione Sicura Report

Controlli Accesso:

- Report classificati come CONFIDENTIAL
- Distribuzione limitata a destinatari autorizzati:
  - Management esecutivo organizzazione
  - Coordinatore CPF
  - Privacy Officer
  - Ente certificazione (se applicabile)
- Trasmissione cifrata (TLS 1.3+ per email, trasferimento file cifrato)
- Watermarking o numerazione copie controllata

Conservazione e Distruzione:

- Carte lavoro audit: 3 anni conservazione, poi distruzione sicura
- Report finali: 7 anni conservazione per requisiti ISO 27006
- Dati valutazione grezzi: Distruzione entro 90 giorni post-audit (salvo requisito normativo)
- Registrazioni interviste (se presenti): Distruzione immediata post-emissione report

7.3 Pianificazione Azioni Correttive

7.3.1 Assegnazione Timeframe

Tabella 10: Timeframe Azioni Correttive

Tipo Non Conformità	Timeframe Richiesto	Verifica
CRITICAL	Immediato (0-7 giorni)	Ri-audit in loco
MAJOR	30-90 giorni	Revisione documenti o ri-audit
MINOR	90-180 giorni	Revisione documenti

7.3.2 Analisi Causa Radice

Gli auditor dovrebbero guidare le organizzazioni verso identificazione causa radice:

Cause Radice Comuni in Audit CPF:

- **Gap Competenza**: Formazione insufficiente in metodologia CPF o requisiti privacy
- **Vincolo Risorse**: Tempo/budget inadeguato allocato per PVMS
- **Deficienza Processo**: Procedure valutazione incomplete o mal documentate
- **Resistenza Culturale**: Scetticismo organizzativo sulla psicologia nella sicurezza
- **Fallimento Integrazione**: PVMS non propriamente connesso con ISMS
- **Disimpegno Management**: Mancanza impegno esecutivo

Esempio 5-Perché:

Non Conformità: Dati valutazione non aggregati a n≥10

1. *Perché?* Team valutazione ha riportato piccolo dipartimento separatamente
2. *Perché?* Team non ha capito requisito aggregazione
3. *Perché?* Formazione non ha coperto adeguatamente protezioni privacy
4. *Perché?* Materiali formativi focalizzati su scoring, non privacy
5. *Perché?* Formazione sviluppata da team sicurezza senza expertise privacy
6. **Causa Radice:** Mancanza subject matter expert privacy nello sviluppo formazione

7.3.3 Procedure Follow-up

Processo Verifica Azione Correttiva:

1. **Organizzazione Sottopone**:
   - Analisi causa radice
   - Piano azione correttiva con timeline
   - Evidenza implementazione
2. **Auditor Rivede**:
   - La causa radice è plausibile e adeguatamente analizzata?
   - L'azione correttiva è appropriata per affrontare causa radice?
   - L'evidenza è sufficiente a dimostrare implementazione?
3. **Metodo Verifica**:
   - CRITICAL: Ri-audit in loco richiesto
   - MAJOR: Revisione documenti o in loco (discrezione auditor)
   - MINOR: Revisione documenti accettabile
4. **Controllo Efficacia**:
   - La non conformità si è ripresentata?
   - Il processo funziona ora come previsto?
   - I rischi correlati sono stati affrontati?
5. **Decisione Chiusura**:
   - ACCETTARE: Azione correttiva efficace, chiudere non conformità
   - RIFIUTARE: Evidenza insufficiente o azione inefficace, rimane aperta

8 Scenari Audit Speciali

8.1 Audit Certificazione Iniziale

8.1.1 Stage 1: Revisione Preparazione (Fuori Sede)

Obiettivi:

- Confermare documentazione PVMS completa
- Verificare preparazione audit
- Identificare gap critici prima Stage 2

Attività:

- Revisione documenti (tutti documenti CPF-27001 richiesti)
- Valutazione preliminare metodologia valutazione
- Revisione procedura protezione privacy
- Verifica competenza (CV personale chiave)
- Conferma ambito

Durata: 1-2 giorni (fuori sede)
Output: Report Stage 1 che identifica gap da affrontare prima Stage 2

8.1.2 Stage 2: Verifica Implementazione (In Loco)

Obiettivi:

- Verificare implementazione PVMS per requisiti CPF-27001
- Valutare efficacia controlli
- Determinare conformità

Attività:

- Audit completo clausola per clausola (Clausole 4-10)
- Ricalcolo e verifica CPF Score
- Test controlli privacy
- Interviste staff e osservazioni
- Interviste management
- Esame evidenze

Durata: 3-5 giorni in loco (dipende da dimensione organizzazione)
Output: Report audit certificazione con decisione conformità

8.1.3 Criteri Decisione

Emissione Certificato:

- NESSUNA non conformità CRITICAL
- NESSUNA non conformità MAJOR O tutte MAJOR chiuse prima decisione
- Non conformità MINOR accettabili (con piano azione correttiva)

Differimento Certificato:

- Non conformità CRITICAL presente
- Multiple non conformità MAJOR (tipicamente $\geq$3)
- Fallimento sistemico implementazione PVMS

8.2 Audit Sorveglianza

8.2.1 Scopo e Ambito

Audit sorveglianza annuali verificano conformità continuata e manutenzione PVMS.

Ambito Ridotto:

- Focus su cambiamenti dall'ultimo audit
- Campione processi PVMS (non tutte clausole in profondità)
- Verifica azioni correttive da audit precedente
- Revisione riesame direzione e audit interno

Copertura Tipica:

- 30-50% dell'ambito audit completo
- Obbligatorio: Clausole 9 (Valutazione Prestazioni) e 10 (Miglioramento)
- Selezione basata su rischio di clausole operative
- Focus su domini con score deteriorati

8.2.2 Approccio Campionamento

Campione Sorveglianza Annuale:

- 10-15 indicatori (vs. 20-30 per audit completo)
- Prioritizzare indicatori Red e Yellow
- Verificare miglioramenti da finding precedenti
- Campione casuale indicatori Green per controllo stabilità

8.2.3 Frequenza

Standard: Sorveglianza annuale (12 mesi ± 2 mesi dall'ultimo audit)

Frequenza Aumentata: Può essere richiesta se:

- Cambiamenti significativi PVMS
- Cambiamenti organizzativi maggiori (M&A, ristrutturazione)
- Deterioramento prestazioni
- Reclami stakeholder

8.3 Audit Ricertificazione

8.3.1 Revisione Ciclo Triennale

Audit ricertificazione avvengono ogni 3 anni e sono più completi della sorveglianza.

Ambito:

- Audit sistema completo (simile a certificazione iniziale)
- Tutte clausole CPF-27001 coperte
- Analisi trend prestazioni triennale
- Verifica evoluzione e miglioramento PVMS
- Valutazione adattamento framework

Aree Focus Aggiuntive:

- Progressione livello maturità in 3 anni
- Prestazioni sostenute (non solo stato attuale)
- Miglioramenti integrazione da certificazione iniziale
- Evidenza innovazione e miglioramento continuo

8.3.2 Evidenza Miglioramento Continuo

Aspettative Triennali:

- Miglioramento CPF Score (minimo +10 punti in 3 anni)
- Progressione livello maturità (almeno un avanzamento livello)
- Riduzione conteggio indicatori Red
- Riduzione tasso incidenti (breach fattore umano)
- Raffinamenti e miglioramenti processi
- Miglioramenti tecnologici (strumenti, automazione)

Indicatori Stagnazione (Preoccupazione):

- CPF Score statico per 3 anni
- Nessuna progressione livello maturità
- Stesse vulnerabilità persistenti
- Nessuna innovazione o miglioramento metodologia
- Conformità meccanica senza apprendimento

8.3.3 Adattamento Evoluzione Framework

Verifica Auditor:

- Come si è adattata l'organizzazione agli aggiornamenti framework CPF?
- Nuovi indicatori incorporati nelle valutazioni?
- La metodologia è evoluta con minacce emergenti?
- L'organizzazione contribuisce all'evoluzione framework?

8.4 Audit Crisi

8.4.1 Trigger Post-Incidente

Audit crisi possono essere richiesti dopo:

- Grave breach sicurezza con causa radice fattore umano
- Materializzazione stato convergente (CI>10 realizzato)
- Fallimento significativo PVMS
- Indagine normativa

8.4.2 Analisi Stato Convergenza

Focus Speciale:

- Ricostruire stato psicologico al momento incidente
- Analizzare convergenza indicatori che ha abilitato breach
- Identificare condizioni "tempesta perfetta"
- Valutare perché PVMS ha fallito nel predire/prevenire
- Valutare efficacia risposta emergenza

Approccio Trauma-Informed Critico:
Organizzazione probabilmente sta vivendo trauma collettivo post-incidente. Auditor deve:

- Avvicinarsi con empatia e supporto
- Evitare domande focalizzate su colpa
- Focalizzarsi su fallimenti sistema, non fallimenti individui
- Fornire sicurezza psicologica nelle interviste
- Riconoscere risposte emotive come normali

8.4.3 Efficacia Risposta Emergenza

Criteri Valutazione:

- Lo stato convergente è stato rilevato prima materializzazione?
- I protocolli emergenza sono stati attivati appropriatamente?
- Quanto velocemente ha risposto l'organizzazione?
- I fattori psicologici sono stati affrontati nella risposta?
- Cosa ha impedito al PVMS di prevenire l'incidente?

Output:
Report audit crisi con:

- Analisi causa radice psicologica incidente
- Analisi gap PVMS
- Azioni correttive emergenza (immediate)
- Azioni correttive strategiche (lungo termine)
- Rivalutazione livello maturità (può risultare in downgrade)

A Checklist Pianificazione Audit

A.1 Preparazione Pre-Audit

4 Settimane Prima Audit:

- ☐ Team audit assegnato (Lead Auditor, Auditor Tecnico, Specialista Privacy)
- ☐ Date audit confermate con organizzazione
- ☐ Richiesta documenti inviata a organizzazione (preavviso 14 giorni)
- ☐ Comunicazione pre-audit a management esecutivo
- ☐ Comunicazione notifica staff preparata (organizzazione da distribuire)
- ☐ Logistica organizzata (sale riunioni, alloggio, accesso)

2 Settimane Prima Audit:

- ☐ Documenti ricevuti e rivisti
- ☐ Finding revisione documenti documentati
- ☐ Gap Stage 1 identificati (se certificazione iniziale)
- ☐ Piano audit finalizzato (aree focus basate su rischio)
- ☐ Strategia campionamento determinata
- ☐ Programma interviste abbozzato
- ☐ Checklist audit personalizzata per organizzazione

1 Settimana Prima Audit:

- ☐ Chiamata pre-audit condotta con Coordinatore CPF
- ☐ Programma interviste finalizzato e condiviso
- ☐ Requisiti speciali comunicati (accesso sistemi, richieste dati)
- ☐ Moduli consenso preparati per interviste partecipanti
- ☐ Privacy Impact Assessment per processo audit completato
- ☐ Briefing team condotto (approccio audit, ruoli, aree focus)

B Glossario Termini Audit

Aggregazione: Combinazione punti dati individuali in metriche livello gruppo per proteggere privacy (minimo n=10 in audit CPF).

Conformità: Soddisfacimento requisiti CPF-27001 specificati.

Convergence Index (CI): Metrica rischio moltiplicativa che misura allineamento multiple vulnerabilità.

Azione Correttiva: Azione per eliminare causa di non conformità rilevata.

CPF Score: Score vulnerabilità psicologica organizzativa complessivo (scala 0-100, più alto = migliore resilienza).

Privacy Differenziale: Framework matematico che assicura privacy individuale attraverso iniezione rumore controllato (ε-privacy).

Non Conformità Maggiore: Assenza o fallimento totale requisito CPF-27001.

Non Conformità Minore: Lasso isolato o deficienza che non costituisce fallimento totale.

Non Conformità: Non soddisfacimento requisito CPF-27001.

Osservazione: Dichiarazione di fatto fatta durante audit che non costituisce non conformità.

Privacy Budget: Massima perdita privacy consentita (ε) attraverso tutte le query.

PVMS (Psychological Vulnerability Management System): Sistema gestione per identificare e mitigare vulnerabilità psicologiche per CPF-27001.

Audit Sorveglianza: Audit periodico che verifica conformità continuata (tipicamente annuale).

Ritardo Temporale: Ritardo minimo 72 ore tra raccolta dati e reporting per prevenire sorveglianza real-time.

Scoring Ternario: Valutazione vulnerabilità a tre livelli (Green=0, Yellow=1, Red=2).

Triangolazione: Verifica attraverso fonti dati indipendenti multiple (minimo 3 per indicatori CPF).

C Riferimenti e Bibliografia

C.1 Documenti Framework CPF

- Canale, G. (2025). *CPF-27001:2025 Psychological Vulnerability Management System – Requirements*. CPF Foundation.
- Canale, G. (2025). *CPF Scoring and Maturity Model v1.0*. CPF Foundation.
- Canale, G. (2025). *CPF Field Kits: Indicator Assessment Tools*. CPF Foundation.
- Canale, G. (2025). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model. *Preprint*.

C.2 Standard Audit

- ISO 19011:2018. *Guidelines for auditing management systems*. International Organization for Standardization.
- ISO/IEC 27006:2015. *Requirements for bodies providing audit and certification of information security management systems*. International Organization for Standardization.
- ISO/IEC 27001:2022. *Information security management systems – Requirements*. International Organization for Standardization.

C.3 Teoria Psicologica

- Bion, W. R. (1961). *Experiences in groups*. London: Tavistock Publications.
- Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.
- Jung, C. G. (1969). *The Archetypes and the Collective Unconscious*. Princeton: Princeton University Press.
- Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.
- Klein, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psychoanalysis*, 27, 99-110.
- Milgram, S. (1974). *Obedience to authority*. New York: Harper & Row.

C.4 Privacy e Protezione Dati

- Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4), 211-407.
- European Parliament. (2016). *General Data Protection Regulation (GDPR)*. Regulation (EU) 2016/679.
- Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57, 1701-1777.

C.5 Ricerca Cybersecurity

- Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Enterprise Solutions.
- IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.
- SANS Institute. (2024). *Security Awareness Report 2024*. SANS Security Awareness.

Linee Guida per l'Audit CPF v1.0

Gennaio 2025

Per aggiornamenti, formazione e informazioni certificazione:
https://cpf3.org