

# CPF-401 Piano di Formazione

Progettazione del Corso di Tecniche di Audit  
40 Ore — 60 Slide

Sviluppo Formazione CPF3  
Giuseppe Canale, CISSP  
g.canale@cpf3.org

Gennaio 2025

## Abstract

Questo piano di formazione definisce il design didattico per CPF-401: Tecniche di Audit, il corso specializzato di 40 ore richiesto per la certificazione CPF Auditor. Il documento fornisce outline a livello di modulo che abilitano la generazione sistematica di slide, lo sviluppo di simulazioni di audit e la creazione di valutazioni pratiche. Ogni modulo include obiettivi di apprendimento, struttura dei contenuti, metodi di insegnamento, suddivisione delle slide, strumenti di audit e elementi di valutazione. Questo piano serve come documento di riferimento per creare formazione di audit guidata da istruttore, simulazioni di audit pratiche ed esami di competenza dell'auditor allineati ai requisiti ISO 19011:2018 e CPF-27001:2025.

## Contents

<b>1</b>	<b>Panoramica del Corso</b>	<b>2</b>
1.1	Identificazione del Corso . . . . .	2
1.2	Target Audience . . . . .	2
1.3	Obiettivi di Apprendimento . . . . .	2
1.4	Struttura del Corso . . . . .	2
1.5	Metodo di Valutazione . . . . .	2
1.6	Materiali Forniti . . . . .	2
<b>2</b>	<b>Modulo 1: Fondamenti di Audit</b>	<b>3</b>
2.1	Panoramica . . . . .	3
2.2	Outline dei Contenuti . . . . .	3
2.3	Metodi di Insegnamento . . . . .	3
2.4	Suddivisione Slide . . . . .	3
2.5	Materiali Necessari . . . . .	4
2.6	Elementi di Valutazione . . . . .	4
2.7	Modulo 2: Pianificazione dell'Audit . . . . .	4
2.7.1	Panoramica . . . . .	4
2.7.2	Outline dei Contenuti . . . . .	5

2.7.3	Metodi di Insegnamento . . . . .	7
2.7.4	Suddivisione Slide . . . . .	7
2.7.5	Materiali Necessari . . . . .	8
2.7.6	Elementi di Valutazione . . . . .	8
2.8	Modulo 3: Esecuzione dell'Audit . . . . .	8
2.8.1	Panoramica . . . . .	8
2.8.2	Outline dei Contenuti . . . . .	9
2.8.3	Metodi di Insegnamento . . . . .	17
2.8.4	Suddivisione Slide . . . . .	18
2.8.5	Materiali Necessari . . . . .	19
2.8.6	Elementi di Valutazione . . . . .	19
2.9	Modulo 4: Reporting dell'Audit . . . . .	19
2.9.1	Panoramica . . . . .	19
2.9.2	Outline dei Contenuti . . . . .	20
2.9.3	Metodi di Insegnamento . . . . .	22
2.9.4	Suddivisione Slide . . . . .	22
2.9.5	Materiali Necessari . . . . .	23
2.9.6	Elementi di Valutazione . . . . .	23
2.10	Modulo 5: Follow-Up e Chiusura . . . . .	24
2.10.1	Panoramica . . . . .	24
2.10.2	Outline dei Contenuti . . . . .	24
2.10.3	Metodi di Insegnamento . . . . .	28
2.10.4	Suddivisione Slide . . . . .	28
2.10.5	Materiali Necessari . . . . .	29
2.10.6	Elementi di Valutazione . . . . .	29
<b>3</b>	<b>Appendici</b>	<b>30</b>
<b>A</b>	<b>Inventario Completo Slide</b>	<b>30</b>
<b>B</b>	<b>Sintesi Banca Esercizi</b>	<b>31</b>
B.1	Esercizi Modulo 1 . . . . .	31
B.2	Esercizi Modulo 2 . . . . .	31
B.3	Esercizi Modulo 3 . . . . .	32
B.4	Esercizi Modulo 4 . . . . .	32
B.5	Esercizi Modulo 5 . . . . .	32
<b>C</b>	<b>Blueprint Esame</b>	<b>33</b>

C.1	Struttura Esame Scritto . . . . .	33
C.2	Struttura Esame Pratico . . . . .	34
<b>D</b>	<b>Materiali di Riferimento</b>	<b>35</b>
D.1	Standard e Riferimenti Normativi Richiesti . . . . .	35
D.2	Strumenti e Template Audit . . . . .	35
D.3	Scenari Audit Simulati . . . . .	36
D.4	Risorse Video e Multimediali . . . . .	38
<b>E</b>	<b>Linee Guida Istruttore</b>	<b>39</b>
E.1	Qualifiche Istruttore . . . . .	39
E.2	Approccio Didattico . . . . .	39
E.3	Suggerimenti Facilitazione per Modulo . . . . .	40
E.4	Gestione Situazioni Difficili . . . . .	41
<b>F</b>	<b>Strategie Successo Partecipanti</b>	<b>42</b>
F.1	Preparazione Pre-Corso . . . . .	42
F.2	Suggerimenti Successo Durante Corso . . . . .	42
F.3	Sviluppo Post-Corso . . . . .	43
<b>G</b>	<b>Controllo Documentale</b>	<b>43</b>
G.1	Cronologia Versioni . . . . .	43
G.2	Revisione e Approvazione . . . . .	44
G.3	Programma Revisione . . . . .	44
G.4	Gestione Cambiamenti . . . . .	44
G.5	Distribuzione . . . . .	45
<b>H</b>	<b>Bibliografia</b>	<b>45</b>
H.1	Standard e Riferimenti Normativi . . . . .	45
H.2	Riferimenti Quadro CPF . . . . .	46
H.3	Riferimenti Psicologia Fondazionale . . . . .	46
H.4	Riferimenti Metodologia Audit . . . . .	46
<b>I</b>	<b>Istruzioni Utilizzo</b>	<b>47</b>
I.1	Per Sviluppatori Corso . . . . .	47
I.2	Per Istruttori . . . . .	48
I.3	Per Partecipanti . . . . .	48
<b>J</b>	<b>Informazioni Contatto</b>	<b>49</b>
J.1	Richieste Formazione . . . . .	49

J.2	Domande Certificazione . . . . .	49
J.3	Supporto Tecnico . . . . .	49
J.4	Feedback Corso . . . . .	50

# 1 Panoramica del Corso

## 1.1 Identificazione del Corso

**Codice:** CPF-401 — **Titolo:** Tecniche di Audit — **Durata:** 40 ore (5 giorni intensivi o 10 mezze giornate) — **Slide:** 60 totali — **Formato:** Guidato da istruttore con estesi esercizi pratici

## 1.2 Target Audience

Assessori CPF certificati con minimo 1 anno di esperienza che cercano la certificazione CPF Auditor. Prerequisiti includono certificazione CPF Assessor attuale in regola, completamento di minimo 10 assessment CPF e comprensione di base dei principi di audit ISO 19011:2018.

## 1.3 Obiettivi di Apprendimento

Al completamento, i partecipanti saranno in grado di: (1) Applicare i principi ISO 19011:2018 all'audit delle vulnerabilità psicologiche, (2) Pianificare audit di conformità CPF-27001:2025 completi, (3) Eseguire attività di audit inclusi colloqui mantenendo l'indipendenza, (4) Documentare i findings con appropriata classificazione, (5) Scrivere report di audit chiari, (6) Verificare azioni correttive e chiudere audit, (7) Mantenere l'etica dell'auditor per tutto il ciclo di vita dell'audit.

## 1.4 Struttura del Corso

**Modulo 1 - Fondamenti di Audit (8h):** Principi ISO 19011, panoramica CPF-27001, processo di audit, competenze, indipendenza, etica.

**Modulo 2 - Pianificazione dell'Audit (8h):** Definizione dello scope, pianificazione basata sul rischio, selezione del team, piani di audit, comunicazione, revisione documentale pre-audit.

**Modulo 3 - Esecuzione dell'Audit (12h):** Riunioni di apertura, revisione documentale, colloqui, osservazione, raccolta evidenze, sviluppo dei findings, riunioni di chiusura, audit simulato (4h).

**Modulo 4 - Reporting dell'Audit (6h):** Classificazione NC, struttura del report, scrittura oggettiva, azioni correttive, revisione qualità.

**Modulo 5 - Follow-Up e Chiusura (6h):** Revisione azioni correttive, verifica, valutazione efficacia, criteri di chiusura, esame pratico finale (8h compresso in 6h didattiche).

## 1.5 Metodo di Valutazione

Esame scritto: 80 domande, 3 ore, 75% per passare. Esame pratico: audit simulato di 8 ore con valutazione delle competenze. Entrambi richiesti più 90% di presenza e accordo etico.

## 1.6 Materiali Forniti

Workbook (100 pagine), ISO 19011:2018, CPF-27001:2025, template di audit, scenari simulati (3 organizzazioni), moduli, checklist.

## 2 Modulo 1: Fondamenti di Audit

### 2.1 Panoramica

**Durata:** 8 ore — **Slide:** 12

**Obiettivi di Apprendimento:** Spiegare i principi ISO 19011:2018; descrivere la struttura CPF-27001:2025; articolare il ciclo di vita dell'audit; identificare le competenze dell'auditor; dimostrare comprensione dell'indipendenza; riconoscere sfide etiche.

### 2.2 Outline dei Contenuti

**1. Principi ISO 19011:2018 (90 min):** Sette principi: integrità, presentazione equa, dovuta cura professionale, riservatezza, indipendenza, approccio basato sull'evidenza, approccio basato sul rischio. Privacy potenziata per il contesto CPF. Requisiti di sensibilità psicologica.

**2. Panoramica Requisiti CPF-27001:2025 (120 min):** Struttura standard (Clausole 4-10). Clausola 4 (Contesto), Clausola 5 (Leadership), Clausola 6 (Pianificazione - assessment, trattamento del rischio), Clausola 7 (Supporto - competenza, consapevolezza), Clausola 8 (Operazione - assessment con privacy), Clausola 9 (Valutazione delle Prestazioni), Clausola 10 (Miglioramento). Mappatura su 100 indicatori. Requisiti unici PVMS.

**3. Quadro del Processo di Audit (90 min):** Quattro fasi: Pianificazione (scope, team, programma, revisione documentale), Esecuzione (riunioni, colloqui, evidenze, findings), Reporting (classificazione, scrittura report, emissione), Chiusura (azione correttiva, verifica, chiusura). Tempistiche tipiche per dimensione org.

**4. Competenze dell'Auditor (90 min):** Generiche (ISO 19011): principi di audit, standard MS, contesto organizzativo. Tecniche specifiche CPF: 10 domini/100 indicatori, fondamenti psicoanalitici, psicologia cognitiva, metodologie privacy, integrazione ISMS. Comportamentali: etica, diplomazia, percettività, decisionismo, sensibilità culturale. Percorso di sviluppo.

**5. Indipendenza e Oggettività (60 min):** Quattro tipi di indipendenza: organizzativa, operativa, finanziaria, relazionale. Identificazione e gestione conflitti. Regola speciale CPF: nessun consulting/audit stessa org entro 24 mesi. Minacce e mitigazione.

**6. Condotta Professionale ed Etica (60 min):** Codice etico: integrità, riservatezza, protezione privacy, mai usare findings per profiling, mantenere competenza. Sfide uniche: bilanciare accuratezza con sensibilità, proteggere sicurezza psicologica, evitare stigmatizzazione, differenze culturali, reazioni emotive. Conseguenze violazioni.

### 2.3 Metodi di Insegnamento

**Lezione:** Principi con esempi, walkthrough requisiti, quadri competenze, scenari indipendenza, casi etica.

**Esercizi:** (1) Principi ISO - 5 scenari (30min), (2) Mappatura Clausole - situazioni a clausole (30min), (3) Auto-Valutazione Competenze (20min), (4) Valutazione Indipendenza - 6 scenari (20min), (5) Analisi Etica - 3 dilemmi (30min).

### 2.4 Suddivisione Slide

**Slide 1.1:** "Principi di Audit ISO 19011:2018" - Sette principi con icone, definizioni, enfasi privacy potenziata per CPF.

**Slide 1.2:** "Principi nel Contesto CPF" - Tabella comparativa che mostra applicazioni specifiche CPF con esempi.

**Slide 1.3:** "Struttura CPF-27001:2025" - Organizzazione standard, confronto con ISO 27001, elementi unici PVMS.

**Slide 1.4:** "Clausola 4: Contesto dell'Organizzazione" - Quattro requisiti, considerazioni audit, esempi evidenze, insidie.

**Slide 1.5:** "Clausola 5: Leadership & Clausola 6: Pianificazione" - Requisiti leadership, requisiti pianificazione, aree di focus audit.

**Slide 1.6:** "Clausola 7: Supporto" - Cinque requisiti supporto, importanza competenza/consapevolezza, metodi verifica audit.

**Slide 1.7:** "Clausola 8: Operazione" - Requisiti operativi, approfondimento su 8.2 assessment (100 indicatori, ternario, privacy), tipi di evidenza.

**Slide 1.8:** "Clausole 9 & 10" - Requisiti valutazione prestazioni, requisiti miglioramento, tracce audit.

**Slide 1.9:** "Ciclo di Vita Processo Audit" - Diagramma di flusso a quattro fasi, attività, timeline, deliverable.

**Slide 1.10:** "Competenze dell'Auditor" - Modello a tre livelli (generiche/tecniche CPF/comportamentali), percorso di sviluppo.

**Slide 1.11:** "Indipendenza e Oggettività" - Quattro tipi con esempi, diagramma di flusso conflitti, minacce/mitigazioni, separazione consulting CPF.

**Slide 1.12:** "Condotta Professionale ed Etica" - Codice etico, sfide CPF, conseguenze violazioni, prompt casi.

## 2.5 Materiali Necessari

Workbook Modulo 1 (pp.1-25), ISO 19011:2018 (Sezioni 1-7), CPF-27001:2025 completo, Fogli di lavoro esercizi, template, materiali poster.

## 2.6 Elementi di Valutazione

**Quiz (5):** Q1: Principio ISO che richiede libertà da bias → indipendenza. Q2: Clausola assessment CPF-27001 → 8.2. Q3: CPF auditor non può → consultare/audit stessa org entro 24mesi. Q4: Aggregazione minima → 10 individui. Q5: Classificazione lapse isolato → NC minore.

**Rubrica Esercizio:** Valutazione indipendenza - determinazioni corrette (3pts), razionale (2pts), mitigazioni (1pt). Totale 6pts (4+ pass).

## 2.7 Modulo 2: Pianificazione dell'Audit

### 2.7.1 Panoramica

**Durata:** 8 ore — **Slide:** 10

**Obiettivi di Apprendimento:** Definire scope e obiettivi di audit appropriati allineati al livello di certificazione; applicare il pensiero basato sul rischio per prioritarizzare le attività di audit; selezionare membri del team di audit qualificati; allocare risorse efficacemente; sviluppare

piani di audit completi; comunicare professionalmente con gli auditee; condurre efficace revisione documentale pre-audit.

**Concetti Chiave:** Definizione scope audit, obiettivi livello certificazione, pianificazione basata sul rischio, criteri audit, selezione team, allocazione risorse, struttura piano audit, revisione documentale pre-audit, comunicazione stakeholder.

## 2.7.2 Outline dei Contenuti

**1. Scope e Obiettivi Audit (90 min):** Processo definizione scope: confini organizzativi, funzioni/processi, clausole CPF-27001, esclusioni, numero dipendenti. Obiettivi specifici livello certificazione: Livello 1 (Foundation, 100-149) - implementazione base, 100 indicatori, protezioni privacy, CPF Score, trattamento indicatori Red. Livello 2 (Intermediate, 70-99) - cicli trimestrali, efficacia interventi, integrazione SOC, riduzione incidenti 20

**2. Pianificazione Audit Basata sul Rischio (90 min):** Pensiero basato sul rischio (ISO 19011 Clausola 5.4.3): identificare rischi significativi PVMS, focalizzare su aree alto rischio, risultati audit precedenti, cambiamenti organizzativi, bilanciamento risorse. Valutazione del rischio per CPF-27001: Alto rischio (Clausola 8.2 metodologia assessment con privacy complessa, monitoraggio stato convergente [10.x], integrazione ISMS, competenza assessor, cultura organizzativa che influenza sicurezza psicologica). Rischio medio (adeguatezza risorse, efficacia formazione, qualità revisione management, completezza documentazione). Rischio inferiore (esistenza policy, struttura organizzativa, comunicazione base). Strategia campionamento basata sul rischio. Documentazione valutazione rischio.

**3. Selezione Team Audit (60 min):** Composizione team: responsabilità lead auditor (gestione complessiva, riunioni, approvazione findings, responsabilità report, comunicazione cliente, coordinamento), responsabilità membri team (copertura clausole/domini, colloqui, raccolta evidenze, bozza findings, supporto lead), ruoli esperti tecnici (SME psicologia, specialista privacy, esperto dominio - guida non auditing). Competenze richieste: tutti certificati CPF Auditor, lead minimo 45 giorni audit con 5+ ruoli lead, membri team minimo 20 giorni audit, competenza collettiva attraverso 10 domini, bilanciamento psicologia/cybersecurity, competenza culturale, capacità linguistiche. Linee guida dimensione team: Piccola org (1-50) = 1 auditor, 1 giorno. Media (51-250) = 1-2 auditor, 1-2 giorni. Grande (251-1000) = 2-3 auditor, 2-3 giorni. Molto grande (1000+) = 3-4 auditor, 3-5 giorni. Verifica indipendenza, distribuzione carico lavoro, pianificazione backup.

**4. Allocazione Risorse e Programmazione (60 min):** Fattori stima tempo: dimensione/complessità org, livello certificazione (più alto = più tempo), sedi, risultati audit precedenti, preparazione auditee, tempo viaggio, esperienza team. Creazione programma audit: revisione documentale pre-audit (1-5 giorni prima), Giorno 1 (riunione apertura 1-2h, revisione documentale iniziale, colloqui management, tour facility), Giorno 2+ (osservazione processi, colloqui dipendenti, raccolta evidenze, sviluppo findings, riunioni team giornalieri), Giorno finale (prep riunione chiusura, riunione chiusura 2-3h, logistica follow-up), programma giornaliero con pause, flessibilità per imprevisti. Requisiti risorse: sale riunioni (stanza team privata, spazi colloqui separati), area revisione documentale sicura, accesso sistemi/registri auditee (con protezioni privacy), strumenti comunicazione, storage evidenze (sicuro, confidenziale), viaggio/alloggio.

**5. Sviluppo Piano Audit (90 min):** Componenti piano audit (ISO 19011 Clausola 6.3): obiettivi e dichiarazione scope, criteri audit (CPF-27001:2025, PVMS auditee), metodi audit (revisione documentale, colloqui, osservazione, campionamento), team audit e ruoli, programma audit con data/ora/durata/attività/partecipanti/luoghi, requisiti risorse e logistica, misure riservatezza e protezione dati, protocolli comunicazione e reporting, firme approvazione. Piano audit basato sul rischio: allocare più tempo a clausole alto rischio (Clausola 8.2 tipicamente



30-40

**6. Comunicazione con Auditee (60 min):** Sequenza comunicazione pre-audit: Contatto iniziale stabilire scopo/scope/programma (2-3 settimane prima), consegna piano audit formale (10-14 giorni prima), lista richiesta documenti (10-14 giorni prima), conferma logistica (5-7 giorni prima), chiamata coordinamento finale (2-3 giorni prima), distribuzione agenda riunione apertura (1-2 giorni prima). Principi comunicazione professionale: scrittura chiara concisa, tono professionale, risposte tempestive (24h), aspettative realistiche, trasparenza sul processo, riservatezza, traccia comunicazione documentata. Gestire preoccupazioni auditee: "Non siamo pronti" - valutare preparazione, riprogrammare se necessario. "È troppo intrusivo" - spiegare protezioni privacy e condotta professionale. "Non capiamo CPF" - breve educazione mantenendo oggettività audit. "Possiamo escludere aree?" - valutare se esclusione appropriata o cambio scope necessario. "Chi vedrà i risultati?" - chiarire riservatezza e distribuzione. Lista richiesta documenti personalizzata per CPF-27001: Clausola 4 (analisi contesto, ID parti interessate, dichiarazione scope PVMS), Clausola 5 (policy CPF, organigramma con ruoli, evidenza impegno management), Clausola 6 (valutazione rischio, report assessment vulnerabilità psicologiche, obiettivi CPF, piani trattamento rischio), Clausola 7 (registri competenza per Coordinatore/Assessor, materiali formazione e registri completamento, piano comunicazione, lista informazioni documentate), Clausola 8 (documentazione metodologia assessment, procedure protezione privacy, programmi e report assessment, evidenza implementazione trattamento rischio), Clausola 9 (KPI e metriche, risultati audit interno, verbali revisione management), Clausola 10 (registri non conformità, azioni correttive, iniziative miglioramento continuo). Richiedere registri mantenendo privacy (solo report aggregati, nessun dato individuale, informazioni time-delayed).

**7. Revisione Documentale Pre-Audit (90 min):** Obiettivi revisione documentale: verificare completezza informazioni documentate per CPF-27001 Clausola 7.5, valutare qualità e chiarezza documentazione, identificare potenziali non conformità prima di on-site, affinare piano audit basato su findings, preparare domande specifiche per colloqui, ottimizzare efficienza tempo on-site. Approccio revisione sistematico: creare checklist allineata a clausole CPF-27001, revisionare ogni documento richiesto contro requisiti, notare conformità/potenziali NCs/aree che necessitano chiarimento, preparare piano raccolta evidenze per verifica on-site, documentare findings revisione in working papers. Documentazione chiave da revisionare: Policy CPF - appropriata all'organizzazione, include impegno assessment sistematico, affronta protezione privacy, fornisce quadro per obiettivi. Dichiarazione scope - confini chiari, esclusioni appropriate giustificate, allineata con scope audit. Valutazione rischio - vulnerabilità psicologiche identificate, domini CPF coperti, priorità trattamento rischio logiche. Report assessment - 100 indicatori affrontati, scoring ternario applicato consistentemente, unità aggregazione mantenute (minimo 10), parametri privacy differenziale documentati, ritardi temporali evidenti, analisi convergenza se applicabile, calcolo CPF Score corretto. Procedure privacy - requisiti aggregazione minima specificati (10+), epsilon privacy differenziale documentato (dovrebbe essere  $\leq 0.1$ ), meccanismi ritardo temporale descritti (minimo 72 ore), divieto profiling individuale esplicito, misure sicurezza gestione dati documentate. Registri competenza - qualifiche Coordinatore CPF verificate, certificazioni Assessor attuali, completamento formazione documentato, registri CPE mantenuti. Evidenza audit interno - programma audit seguito, findings documentati, azioni correttive tracciate, revisione management condotta. Problemi comuni identificati: documenti richiesti mancanti (NCs esistenza documenti), documenti non riflettenti pratica attuale (NCs implementazione durante on-site), parametri privacy non meeting requisiti CPF (epsilon  $\geq 0.1$ , aggregazione  $\geq 10$ , ritardi  $\geq 72$  ore), metodologia assessment incompleta o inconsistente, trattamento rischio non affronta indicatori Red, integrazione con ISMS poco chiara o assente. Preparare domande chiarimento basate su revisione documentale.

**8. Esercizio: Sviluppo Piano Audit Completo (60 min):** Scenario organizzativo: organizzazione sanitaria media, 200 dipendenti, cerca certificazione Livello 2, esistente ISO 27001 cer-

tificata, primo audit CPF. Compito: sviluppare piano audit completo includendo dichiarazione scope con obiettivi livello certificazione, valutazione rischio identificando aree alto/medio/basso rischio, composizione team audit e ruoli, programma audit 2 giorni con allocazioni tempo, lista richiesta documenti, timeline comunicazione pre-audit. Presentazione gruppo piani (10 minuti ciascuno), feedback facilitatore su completezza, allocazione basata sul rischio, appropriatezza, considerazioni pratiche. Discussione approcci diversi e razionale.

### 2.7.3 Metodi di Insegnamento

**Lezione:** Definizione scope con esempi, quadri pianificazione basata sul rischio, matrici composizione team, calcoli allocazione risorse, template piano audit con annotazioni, esempi comunicazione (efficaci e inefficaci), sistematizzazione revisione documentale.

**Esercizi:** (1) Pratica Definizione Scope - 3 scenari organizzativi, scrivere appropriate dichiarazioni scope (20 min), (2) Valutazione Rischio per Audit - dato profilo organizzativo, identificare e prioritarizzare aree alto/medio/basso rischio (30 min), (3) Selezione Team - 5 scenari audit, selezionare appropriata composizione team e dimensione con razionale (20 min), (4) Simulazione Revisione Documentale - revisionare documentazione PVMS campione, identificare problemi e preparare domande (40 min), (5) Sviluppo Piano Audit - completare esercizio come descritto sopra (60 min).

**Discussione:** "Come determinare appropriata profondità audit dato vincoli tempo?", "Bilanciare accuratezza con efficienza?", "Errori pianificazione più comuni?", "Come aggiustare piani quando revisione documentale rivela problemi maggiori?"

**Risorse:** CPF-27001:2025 standard completo, Template Pianificazione Audit, Foglio di Lavoro Valutazione Rischio, Matrice Criteri Selezione Team, Template Lista Richiesta Documenti, Piani Audit Campione (buoni e che necessitano miglioramento), Set Documentazione PVMS Campione, Template Comunicazione Pre-Audit.

### 2.7.4 Suddivisione Slide

**Slide 2.1:** "Definire Scope e Obiettivi Audit" - Elementi scope (confini, funzioni, clausole, esclusioni, dipendenti), tabella obiettivi specifici livello certificazione (Livello 1-4 con requisiti crescenti), considerazioni stakeholder, template dichiarazione scope.

**Slide 2.2:** "Pianificazione Audit Basata sul Rischio" - Definizione pensiero basato sul rischio, aree alto/medio/basso rischio CPF-27001, strategia campionamento basata sul rischio, guida allocazione tempo (30-40)

**Slide 2.3:** "Selezione Team Audit" - Ruoli team (lead auditor, membri team, esperti tecnici), competenze richieste per CPF-27001 (certificazione auditor, conoscenza dominio, bilanciamento psicologia/cybersecurity), linee guida dimensione team per dimensione org, checklist verifica indipendenza.

**Slide 2.4:** "Allocazione Risorse e Programmazione" - Fattori stima tempo, template programma audit con flusso tipico (Giorno 1 apertura/revisione iniziale, Giorno 2+ assessment dettagliato, Giorno finale chiusura), allocazione tempo giornaliera, requisiti risorse oltre personale, pianificazione contingenza.

**Slide 2.5:** "Componenti Piano Audit" - Elementi richiesti ISO 19011 (obiettivi, scope, criteri, metodi, team, programma, risorse, riservatezza, comunicazione, approvazione), aggiunte specifiche CPF-27001 (misure protezione privacy, sensibilità psicologica, integrazione ISMS), struttura template piano.

**Slide 2.6:** "Esempio Piano Audit Basato sul Rischio" - Programma audit 2 giorni campione che mostra allocazione tempo (Clausola 8.2 metodologia assessment 40

**Slide 2.7:** "Comunicazione con Auditee" - Timeline comunicazione pre-audit (2-3 settimane contatto iniziale, 10-14 giorni consegna piano e documenti, 5-7 giorni logistica, 2-3 giorni coordinamento finale), principi comunicazione professionale, gestione preoccupazioni comuni, importanza documentazione.

**Slide 2.8:** "Lista Richiesta Documenti per CPF-27001" - Lista completa organizzata per clausola (4-10), requisiti specifici CPF evidenziati (report assessment, procedure privacy, registri competenza, evidenza integrazione), richiedere in formati privacy-preserving.

**Slide 2.9:** "Processo Revisione Documentale Pre-Audit" - Diagramma di flusso approccio revisione sistematico, creazione checklist, obiettivi revisione (completezza, qualità, potenziali NCs, affinare piano), aree focus documenti chiave, problemi comuni trovati, preparare domande chiarimento.

**Slide 2.10:** "Esercizio Sviluppo Piano Audit" - Scenario organizzazione sanitaria (200 dipendenti, certificazione Livello 2, ISO 27001 certificata, primo audit CPF), istruzioni esercizio (scope, valutazione rischio, team, programma, documenti, comunicazione), formato presentazione e feedback, criteri valutazione.

### 2.7.5 Materiali Necessari

Workbook Modulo 2 (pagine 26-45), standard CPF-27001:2025 con annotazioni checklist, Template Pianificazione Audit (vuoto e campione completato), Foglio di Lavoro Valutazione Rischio, Matrice Criteri Selezione Team, Esercizio 2.1 tre scenari scope, Esercizio 2.2 profilo rischio organizzativo, Esercizio 2.3 cinque casi selezione team, Esercizio 2.4 set documentazione PVMS campione (policy, report assessment, procedure privacy, registri competenza - 15 pagine), Esercizio 2.5 pacchetto scenario organizzazione sanitaria (5 pagine), Template Lista Richiesta Documenti, Template Email Comunicazione Pre-Audit, Piani Audit Campione Buoni e Che-Necessitano-Miglioramento.

### 2.7.6 Elementi di Valutazione

**Quiz (5 domande):** Q1: Percentuale tipica tempo audit per Clausola 8.2 metodologia assessment → 30-40

**Rubrica Esercizio (Sviluppo Piano Audit):** Appropriata dichiarazione scope con obiettivi livello (2 pts), accurata valutazione rischio con giustificazione (2 pts), appropriata composizione team (1 pt), logico programma 2 giorni con allocazione tempo (2 pts), lista richiesta documenti completa (1 pt), timeline comunicazione professionale (1 pt), qualità e completezza piano generale (1 pt). Totale 10 pts (7+ pass).

## 2.8 Modulo 3: Esecuzione dell'Audit

### 2.8.1 Panoramica

**Durata:** 12 ore — **Slide:** 14

**Obiettivi di Apprendimento:** Condurre efficacemente riunioni di apertura; revisionare sistematicamente informazioni documentate contro requisiti CPF-27001; eseguire colloqui usando appropriate tecniche di questioning mantenendo sensibilità psicologica; osservare processi e controlli; raccogliere sufficienti, appropriate evidenze proteggendo privacy; applicare strategie cam-

pionamento; documentare findings chiaramente; classificare findings correttamente; condurre professionali riunioni di chiusura; mantenere coordinamento team audit; adattarsi a situazioni inaspettate; dimostrare competenza audit pratica attraverso audit simulato.

**Concetti Chiave:** Struttura riunione apertura, tecniche revisione documentale, metodologie colloqui, sensibilità psicologica, protocolli osservazione, tipi e qualità evidenze, metodi campionamento, sviluppo findings, criteri classificazione, condotta riunione chiusura, coordinamento team giornaliero, adattabilità.

## 2.8.2 Outline dei Contenuti

**1. Condotta Riunione Apertura (60 min):** Obiettivi riunione apertura: stabilire rapporto professionale e tono collaborativo, confermare scope/obiettivi/criteri/programma audit, spiegare processo e metodi audit, chiarire ruoli e responsabilità, organizzare logistica (spazio lavoro, accesso, programmi), affrontare domande e preoccupazioni, ottenere necessari accessi e permessi, impostare aspettative per comunicazione. Agenda e tempistica tipica (90-120 minuti totali): Presentazioni team audit e personale chiave auditee (10 min), conferma scopo e scope audit (10 min), spiegazione processo audit (20 min), panoramica requisiti CPF-27001 (15 min), walkthrough programma e disponibilità auditee (15 min), assicurazioni riservatezza e protezione privacy (10 min), sessione domande e risposte (20 min), finalizzazione logistica (10 min). Partecipanti: Richiesti (rappresentante top management, Coordinatore CPF, process owner chiave), Opzionali ma raccomandati (coordinatore ISO 27001 se separato, rappresentante HR, consulente legale se preferenza organizzativa, leadership sicurezza). Abilità presentazione professionale: consegna chiara confidente, uso aiuti visivi (agenda, programma, diagramma di flusso processo), ascolto attivo preoccupazioni, affrontare domande approfonditamente, proiettare competenza e equità, stabilire sicurezza psicologica (specialmente importante per audit CPF), gestire partecipanti difficili diplomaticamente. Considerazioni speciali per audit CPF: enfatizzare protezioni privacy (aggregazione, privacy differenziale, ritardi temporali, nessun profiling individuale), assicurare dipendenti che vulnerabilità psicologiche sono normali e focus organizzativo non individuale, spiegare approccio colloqui sarà sensibile e rispettoso, chiarire che findings audit si focalizzano su problemi sistematici non colpa, affrontare proattivamente qualsiasi ansia su assessment psicologico, ribadire riservatezza oltre riservatezza audit standard. Sfide comuni riunione apertura e risposte: ostilità o difensività - riconoscere preoccupazioni, enfatizzare intento miglioramento collaborativo; resistenza ad aspetti psicologici - spiegare approccio evidence-based e benefici organizzativi; confusione su requisiti CPF - fornire breve educazione mantenendo ruolo auditor; conflitti programmazione - negoziare flessibilità dentro piano audit; preparazione inadeguata - valutare preparazione e considerare ritardo se severa. Documentazione: foglio presenza riunione apertura con firme, conferma scope e programma, note su punti discussione significativi, accordo su protocolli comunicazione, foto riunione apertura (opzionale con permesso).

**2. Tecniche Revisione Documentale (90 min):** Approccio revisione documentale sistematico: seguire checklist clausola-per-clausola CPF-27001 preparata durante pianificazione, revisionare ogni documento richiesto contro specifici requisiti, cross-referenziare documenti correlati per consistenza, notare conformità e non conformità con riferimenti evidenze, preparare domande follow-up per chiarimento, verificare implementazione attraverso colloqui e osservazione dopo. Spazio lavoro revisione documentale: area sicura, privata per accesso documenti confidenziali, illuminazione adeguata e comfort per revisione estesa, accesso a documenti elettronici e cartacei come necessario, working papers audit organizzati e protetti, evitare spazi aperti dove informazioni sensibili visibili. Revisionare documenti chiave CPF-27001 in dettaglio: Revisione Policy CPF (appropriata allo scopo per 5.2.a, include impegno assessment sistematico 5.2.b, fornisce quadro per obiettivi 5.2.c, integrazione con policy ISO 27001 se applicabile) - controllare completezza, chiarezza, approvazione management, evidenza comunicazione. Revisione Scope

PVMS (confini organizzativi 4.3, funzioni e processi coperti, esclusioni con giustificazione, integrazione con scope ISMS se applicabile) - verificare scope appropriato e chiaramente definito. Revisione Report Assessment Vulnerabilità Psicologiche (copertura tutti 100 indicatori 8.2.2, applicazione scoring ternario Green/Yellow/Red 8.2.2, unità aggregazione minima mantenute 10+ individui 8.2.3, parametri privacy differenziale documentati  $\epsilon \leq 0.1$  8.2.3, ritardi temporali implementati 72+ ore 8.2.3, analisi role-based non individuale 8.2.3, punteggi categoria e CPF Score calcolati correttamente 8.2.2, analisi convergenza se multipli indicatori Yellow/Red 8.2.2, misure protezione privacy documentate 8.2.3, data e identificazione assessor) - questo è tipicamente revisione documentale più time-consuming, verificare rigore metodologia. Revisione Piani Trattamento Rischio (indicator Red affrontati 8.3, indicatori Yellow monitorati 8.3, opzioni trattamento selezionate modifica/ritieni/evita/condividi 6.2.3, evidenza implementazione attesa 8.3, assegnazioni responsabilità 8.3, timeline realistiche 8.3, approccio misurazione efficacia 9.1) - controllare appropriatezza e completezza trattamento. Revisione Registri Competenza (qualifiche Coordinatore CPF 7.2, 5.3, certificazioni Assessor CPF attuali 7.2, registri completamento formazione 7.2, documentazione CPE 7.2, evidenza valutazione competenza 7.2) - verificare personale qualificato per ruoli. Revisione Procedure Protezione Privacy (unità aggregazione minima specificate 10+ 8.2.3,  $\epsilon$  privacy differenziale documentato  $\leq 0.1$  8.2.3, meccanismi ritardo temporale descritti 72+ ore minimo 8.2.3, divieto profiling individuale esplicito 8.2.3, crittografia dati at rest e in transito 8.2.3, controlli accesso e tracce audit 8.2.3, limiti retention 5 anni massimo 8.2.3, procedure distruzione sicura 8.2.3) - questi sono requisiti conformità critici, qualsiasi deficienza probabile NC maggiore. Revisione Registri Audit Interno (programma audit seguito 9.2, auditor competenti condotti audit 9.2, report audit con findings 9.2, azioni correttive tracciate 9.2, revisione management risultati audit 9.3) - valutare qualità oversight interno. Revisione Verbal Revisione Management (prestazioni PVMS discusse 9.3, raggiungimento obiettivi CPF revisionato 9.3, cambiamenti che influenzano PVMS considerati 9.3, opportunità miglioramento identificate 9.3, decisioni su cambiamenti/risorse documentate 9.3, frequenza regolare mantenuta 9.3) - verificare engagement management. Identificare potenziali non conformità durante revisione documentale: requisiti non affrontati (elementi mancanti), documenti non meeting requisiti dichiarati (problemi qualità), inconsistenze tra documenti correlati, evidenza di pratiche diverse da procedure documentate, parametri privacy non meeting minimi CPF ( $\epsilon$   $\geq 0.1$ , aggregazione  $\geq 10$ , ritardi  $\geq 72$  ore), integrazione con ISMS poco chiara o contraddittoria. Preparare efficaci domande follow-up basate su revisione documentale: domande chiarimento (capire ambiguità prima di concludere NC), domande implementazione (come procedure documentate effettivamente eseguite), richieste evidenze (verificare conformità attraverso registri aggiuntivi), domande razionale (capire pensiero auditee dietro approcci), domande miglioramento (esplorare opportunità oltre conformità).

**3. Metodologie di Colloquio (120 min):** Obiettivi del colloquio negli audit CPF-27001: verificare che le procedure documentate siano comprese e implementate, valutare l'efficacia dell'implementazione del PVMS, raccogliere evidenze di conformità o non conformità, comprendere la cultura organizzativa che influisce sulla sicurezza psicologica, identificare opportunità di miglioramento, convalidare i risultati della revisione documentale attraverso molteplici prospettive, valutare la competenza del personale chiave. Tipi di colloquio e scopi: colloqui con il management (comprensione dei requisiti CPF, impegno per il PVMS, fornitura di risorse, comunicazione della policy, attività di supervisione), colloqui con i responsabili di processo (Coordinatore CPF, responsabili della sicurezza - comprensione delle responsabilità, implementazione della metodologia di assessment, pratiche di protezione della privacy, decisioni sul trattamento del rischio, integrazione con le operazioni di sicurezza), colloqui con il personale operativo (consapevolezza della policy CPF, partecipazione agli assessment, comprensione delle protezioni della privacy, esperienza con gli interventi, percezione della sicurezza psicologica), colloqui interfunzionali (IT, HR, conformità - punti di integrazione, supporto al PVMS, consapevolezza dei requisiti). Preparazione del colloquio: rivedere i documenti pertinenti in anticipo, preparare

domande aperte allineate ai requisiti, identificare le prove chiave da ottenere, considerare il ruolo e la prospettiva dell'intervistato, pianificare la sequenza dei colloqui per l'efficienza, preparare una guida al colloquio con domande principali e di approfondimento. Tecniche di questioning efficaci: domande aperte (Come fai..., Qual è il tuo processo per..., Raccontami di..., Descrivimi..., Guidami attraverso...), domande di approfondimento (Puoi farmi un esempio?, Cosa è successo poi?, Come verifichi...?, Quali prove hai...?), evitare domande leading (Non chiedere: "Fai X, vero?" Chiedi: "Come gestisci X?"), usare il silenzio in modo efficace (pausa dopo le risposte per l'approfondimento), ascolto attivo con conferma verbale e non verbale. Sensibilità psicologica nei colloqui per gli audit CPF: approccio informato sul trauma se si discutono incidenti di sicurezza (evitare la re-traumatizzazione, consentire pause emotive, rispettare i confini), linguaggio rispettoso riguardo alle vulnerabilità (enfaticizzare caratteristiche umane normali non fallimenti, focus organizzativo non colpa individuale, evitare termini stigmatizzanti), sensibilità culturale (adattare lo stile di comunicazione, rispettare le gerarchie nelle culture ad alta distanza di potere, considerare le barriere linguistiche, essere consapevoli delle diverse espressioni di vulnerabilità), creare sicurezza psicologica (spazio colloquio privato, rassicurazioni sulla riservatezza, contegno non giudicante, permesso di declinare domande, enfaticizzare lo scopo di miglioramento non punitivo), gestire le reazioni emotive (angoscia dell'intervistato - convalidare le emozioni, offrire una pausa, assicurare la disponibilità di supporto; disagio dell'auditor con argomenti psicologici - compostezza professionale, deferire all'esperto tecnico se necessario). Aree di colloquio specifiche per CPF-27001: Comprensione della policy e degli obiettivi CPF (chiedere: "Qual è la policy CPF dell'organizzazione?", "Quali sono i tuoi obiettivi CPF?", "Come si integra il CPF con la strategia di sicurezza?"), Implementazione della metodologia di assessment (chiedere: "Guidami attraverso il tuo ultimo assessment CPF", "Come garantisci le unità di aggregazione minime?", "Come viene applicata la privacy differenziale?", "Qual è il tuo processo per lo scoring ternario?", "Come identifichi gli stati convergenti?"), Pratiche di protezione della privacy (chiedere: "Come previeni il profiling individuale?", "Mostrami come vengono implementati i ritardi temporali", "Chi ha accesso ai dati di assessment?", "Come vengono crittati i dati?", "Cosa succede dopo il limite di retention di 5 anni?"), Competenza e formazione (chiedere: "Quale formazione CPF hai completato?", "Come mantieni la competenza?", "Qual è la tua comprensione di [dominio specifico]?"), Efficacia del trattamento del rischio (chiedere: "Fammi un esempio di trattamento del rischio per un indicatore Red", "Come misuri l'efficacia dell'intervento?", "Quali miglioramenti hai visto?"), Integrazione con ISMS (chiedere: "Come informa il CPF la tua valutazione del rischio ISO 27001?", "Come sono coordinati CPF e ISMS?", "Dove confluiscono i risultati nelle operazioni di sicurezza?"). Condurre il colloquio: stabilire un rapporto e spiegare lo scopo (2-3 minuti), porre le domande preparate in modo sistematico (15-30 minuti a seconda del ruolo), prendere appunti dettagliati delle risposte (citazioni dirette per potenziali findings), richiedere prove o dimostrazioni quando appropriato, sondare incongruenze o lacune diplomaticamente, confermare la comprensione attraverso la sintesi, ringraziare l'intervistato e spiegare i prossimi passi. Sfide comuni nei colloqui: l'intervistato non conosce le risposte - valutare se è un problema di competenza (potenziale NC) o un intervistato sbagliato, sondare delicatamente senza imbarazzo; risposte preparate o scriptate - approfondire con follow-up, chiedere esempi, osservare il linguaggio del corpo; contraddizioni con i documenti - esplorare con tatto, cercare di capire prima di concludere un NC, può indicare un gap di implementazione; intervistato difensivo o ostile - rimanere professionale e calmo, riconoscere le preoccupazioni, ricollegarsi alle prove, escalare al lead auditor se necessario; barriere linguistiche o di comunicazione - usare un linguaggio semplice, confermare la comprensione, considerare un interprete se necessario; reazioni emotive ad argomenti psicologici - convalidare i sentimenti, offrire una pausa, assicurare la disponibilità di supporto, continuare con sensibilità o rinviare. Documentazione: appunti del colloquio con data, ora, nome/ruolo dell'intervistato, punti chiave, prove ottenute, potenziali findings; firme dell'intervistato opzionali (possono creare difensività); foto delle prove con il permesso; elementi di follow-up identificati.

**4. Tecniche di Osservazione (60 min):** Obiettivi dell'osservazione: verificare che i processi avvengano come documentato, valutare l'efficacia dei controlli nella pratica, osservare comportamenti e cultura organizzativa, identificare opportunità di miglioramento, convalidare le risposte dei colloqui attraverso l'osservazione diretta, raccogliere prove che non possono essere ottenute attraverso documenti o colloqui. Cosa osservare negli audit CPF-27001: processo di assessment in azione (se i tempi lo consentono - assessor che conduce l'assessment, applicazione dello scoring ternario, metodi di raccolta delle prove, protezioni della privacy nella pratica, collaborazione con i responsabili di processo), integrazione delle operazioni di sicurezza (dashboard di monitoraggio che mostrano indicatori di vulnerabilità psicologica, risposta agli alert per anomalie comportamentali, procedure di risposta agli incidenti che considerano fattori psicologici, dinamiche di team nel centro operativo di sicurezza), erogazione della formazione (sessioni di formazione sulla consapevolezza CPF, attività di sviluppo delle competenze, creazione di sicurezza psicologica), implementazione del trattamento del rischio (attività di intervento, coinvolgimento dei dipendenti con i controlli di sicurezza, cambiamenti comportamentali dai trattamenti, misurazione dell'efficacia), indicatori di cultura organizzativa (modelli di comunicazione, dinamiche di autorità, evidenza di sicurezza psicologica, presenza/assenza di stigmatizzazione o biasimo, integrazione del CPF nelle operazioni normali), pratiche di protezione della privacy (controlli di accesso per i dati di assessment, sicurezza fisica dei documenti sensibili, discussioni che mantengono l'aggregazione e la riservatezza, pratiche di reporting con ritardo temporale). Protocollo di osservazione: minimizzare l'interruzione alle attività osservate, rimanere discreto mantenendo la visibilità, prendere appunti dettagliati oggettivamente (cosa osservato non opinioni), richiedere chiarimenti al personale osservato se appropriato, rispettare i confini se l'osservazione viene rifiutata, mantenere la riservatezza delle informazioni osservate, verificare le osservazioni con altre fonti di prova. Sfide di osservazione nel contesto della vulnerabilità psicologica: effetto dell'osservatore (le persone si comportano in modo diverso quando sono osservate - osservare per periodi prolungati se possibile, confrontare con altre prove, tenerne conto nelle conclusioni), finestre di osservazione limitate (i processi non avvengono sempre durante l'audit - fare affidamento su registri e colloqui, richiedere dimostrazioni se critici), vincoli di privacy (non è possibile osservare l'assessment individuale per proteggere la privacy - osservare invece l'analisi aggregata e la reportistica, verificare la privacy nella metodologia non nel contenuto), interpretare la cultura organizzativa (osservazioni soggettive richiedono più punti dati, triangolare con colloqui e risultati), valutazione della sicurezza psicologica (difficile da osservare direttamente - cercare indicatori come il mettere in discussione l'autorità apertamente, la segnalazione di errori, l'espressione di prospettive diverse, l'assenza di linguaggio di biasimo). Documentazione: appunti di osservazione con data, ora, luogo, attività osservata, partecipanti, descrizione oggettiva dettagliata, prove ottenute, potenziali findings; foto con permesso; conferma del flusso del processo.

**5. Raccolta delle Prove e Campionamento (90 min):** Tipi di prove e caratteristiche: Documenti (politiche, procedure, report, registri, email, verbali di riunione) - prontamente disponibili, possono verificare esistenza e contenuto, potrebbero non riflettere la pratica effettiva; Registri (report di assessment, report di incidenti, registri di formazione, documentazione delle competenze, log di audit) - dimostrano l'implementazione, con timestamp, stabiliscono modelli nel tempo; Risposte ai colloqui (dichiarazioni del personale) - forniscono contesto e comprensione, soggettivi, richiedono corroborazione; Osservazioni (processi e comportamenti testimoniati) - dimostrano la pratica effettiva, soggetti all'effetto dell'osservatore, finestre di tempo limitate; Prove elettroniche (configurazioni di sistema, query di database per la verifica dell'aggregazione, log, dashboard) - oggettive se autentiche, richiedono competenza tecnica, considerazioni sulla privacy. Caratteristiche di qualità delle prove di audit (ISO 19011 Clausola 6.5): Sufficienti - prove sufficienti per supportare le conclusioni, tiene conto della variabilità e della validità statistica; Rilevanti - relazione logica con i requisiti e gli obiettivi di audit, focalizzati sui criteri di audit; Affidabili - prove da fonti indipendenti, coerenti tra più fonti, processo di generazione

delle prove affidabile. Approcci di campionamento per gli audit CPF-27001: Censimento (esaminare tutti gli elementi) - per popolazioni piccole, requisiti critici, aree ad alto rischio, controlli critici per la privacy; Campionamento per giudizio (l'auditor seleziona gli elementi in base al rischio/conoscenza) - per focus di audit basato sul rischio, circostanze insolite, aree problematiche note; Campionamento casuale (selezione statistica) - per grandi popolazioni, valutazione rappresentativa, intervalli di confidenza; Campionamento stratificato (dividere la popolazione in sottogruppi poi campionare ciascuno) - per organizzazioni multi-sede, diversi dipartimenti, vari domini di indicatori. Strategie di campionamento per i requisiti CPF: Campionamento dei report di assessment (se assessment trimestrali, campionare 2-3 trimestri, verificare che tutti i 100 indicatori siano coperti tra i campioni, controllare i parametri di privacy in ogni report, convalidare i calcoli del CPF Score, rivedere le analisi di convergenza), Verifica delle unità di aggregazione dei dipendenti (esaminare la metodologia per più unità, confermare che nessuna unità >10 individui, verificare che la reportistica cross-unità non consenta il profiling, controllare che l'analisi per ruolo mantenga la privacy), Campionamento del trattamento del rischio (campionare i trattamenti per gli indicatori Red tutti o alta percentuale, campionare i trattamenti per gli indicatori Yellow campione rappresentativo, verificare l'implementazione attraverso più tipi di prove, valutare la misurazione dell'efficacia), Campionamento dei registri di formazione (campionare tra diversi ruoli e periodi di tempo, verificare il completamento e la comprensione, controllare i CPE per gli Assessor CPF, confermare che l'onboarding dei nuovi dipendenti includa il CPF), Campionamento dell'audit interno (rivedere l'audit più recente più un campione di audit precedenti, verificare la copertura dello scope, controllare la competenza dell'auditor, rivedere la qualità dei findings e il tracciamento delle azioni correttive). Determinazione della dimensione del campione: considerare la dimensione della popolazione, il livello di confidenza desiderato, il livello di rischio del requisito, i risultati di audit precedenti (puliti = campione più piccolo, problemi = campione più grande), vincoli di tempo e risorse, vincoli di privacy per il CPF (deve mantenere l'aggregazione nei campioni). Documentazione dell'approccio di campionamento: piano di campionamento con la ratio, caratteristiche della popolazione, calcolo della dimensione del campione, metodo di selezione, campioni selezionati, prove ottenute da ciascun campione, conclusioni tratte. Sfide comuni nella raccolta delle prove: prove non disponibili (può indicare NC, requisito di esistenza del documento, o programmazione per dopo), prove contrastanti (triangolare con fonti aggiuntive, investigare l'inconsistenza, può indicare un gap di implementazione), prove insufficienti (raccolgere più prove, espandere il campione, documentare la limitazione se il tempo è vincolato), accesso a prove protette dalla privacy (verificare che i controlli sulla privacy funzionino ma non è possibile accedere ai dati dettagliati, utilizzare dimostrazioni aggregate), prove elettroniche che richiedono accesso tecnico (coordinarsi con IT, garantire la competenza dell'auditor, mantenere l'integrità dei dati). Documentazione: registro delle prove con descrizione, fonte, ubicazione, data di ottenimento, rilevanza per i requisiti, contributo ai findings; archiviazione delle prove sicura e organizzata; riferimenti incrociati ai working papers e ai findings.

**6. Sviluppo e Classificazione dei Findings (120 min):** Processo di sviluppo del finding: identificare una potenziale non conformità durante la raccolta delle prove, raccogliere prove sufficienti per supportare il finding (regola del tre - tre elementi di prova minimo), confrontare le prove con uno specifico requisito CPF-27001, discutere il finding preliminare con il team di audit per la convalida, discutere con l'auditee per confermare i fatti e ottenere una risposta, classificare il finding appropriatamente (conformità, NC minore, NC maggiore, osservazione), documentare il finding chiaramente con tutti gli elementi richiesti, ottenere il riconoscimento dell'auditee. Elementi del finding (ISO 19011 Clausola 6.5.5): Requisito (specifica clausola CPF-27001 e dichiarazione del requisito), Condizione (cosa è stato trovato nella realtà, descrizione oggettiva), Prove (documentazione di supporto, appunti del colloquio, osservazioni), Effetto o potenziale effetto (impatto sull'efficacia del PVMS), Analisi della causa principale (motivo sottostante della non conformità se determinabile). Criteri di classificazione: Conformità - le prove dimostrano



la piena conformità al requisito, l'implementazione è efficace, nessuna azione richiesta, può essere notata come area di forza; Osservazione (opportunità di miglioramento) - non è una non conformità ma è stata identificata un'opportunità di miglioramento, non influisce sullo stato di conformità, può diventare NC se non affrontata, documentata per il miglioramento continuo; Non Conformità Minore - fallimento o lapse isolato, scope o effetto limitato, occorrenza una tantum o che interessa un singolo elemento, documentazione incompleta ma la pratica esiste, non conformità recente in fase di correzione, implementazione sistematica altrimenti efficace, correzione entro 90 giorni prevista; Non Conformità Maggiore - fallimento sistematico che interessa più aree o processi, completa assenza di un elemento richiesto (esempio: nessuna procedura di protezione della privacy documentata, nessun Coordinatore CPF assegnato, nessun assessment condotto), non conformità minori ripetute che indicano un problema sistemico, effetto significativo sull'efficacia del PVMS o sugli obiettivi, requisito fondamentale non implementato (esempio: assessment non utilizzano 100 indicatori, unità di aggregazione >10 in tutto, privacy differenziale non implementata, divieto di profiling non applicato), correzione immediata richiesta prima della certificazione. Considerazioni di classificazione specifiche per CPF-27001: Non conformità dei requisiti di privacy (qualsiasi violazione dell'aggregazione minima, privacy differenziale, ritardi temporali o divieto di profiling è probabile NC MAGGIORE a causa dell'importanza fondamentale e del rischio legale), Lacune nella metodologia di assessment (domini o indicatori mancanti = maggiore, documentazione incompleta di un assessment = minore, scoring ternario applicato in modo inconsistente su alcuni indicatori = minore, nessun sistema di scoring documentato = maggiore), Problemi di competenza (Coordinatore CPF privo di qualifiche di base = maggiore, CPE carente di un assessor = minore, nessun requisito di competenza definito = maggiore), Carenze di integrazione (i findings del CPF non informano ISO 27001 come documentato = maggiore se disconnessione completa / minore se lacune occasionali, processo di integrazione documentato non seguito = maggiore, integrazione non documentata ma in atto = osservazione minore). Scenari comuni di finding ed esempi di classificazione: Scenario 1: Il report di assessment del Q2 2024 mostra un'unità di aggregazione di 8 individui per il dipartimento Finanza. Classificazione: NC Maggiore. Requisito: 8.2.3 aggregazione minima 10 individui. Violazione della privacy requisito fondamentale. Scenario 2: Il Coordinatore CPF ha completato la formazione CPF-101 ma il certificato di formazione CPF-201 non è nel file, sebbene il Coordinatore dimostri competenza nei colloqui e la qualità dell'assessment sia buona. Classificazione: NC Minore. Requisito: 7.2 competenza documentata. Lacuna documentale ma competenza evidente. Scenario 3: Il piano di trattamento del rischio per l'indicatore Red 5.1 (affaticamento da alert) mostra il trattamento selezionato e approvato ma l'evidenza di implementazione non è disponibile e i colloqui indicano che il trattamento non è ancora iniziato dopo 120 giorni. Classificazione: NC Maggiore. Requisito: 8.3 implementazione del trattamento del rischio. Fallimento sistematico nell'implementazione, durata prolungata. Scenario 4: Audit interno condotto 14 mesi fa invece che annualmente come da procedura. Classificazione: NC Minore. Requisito: 9.2 frequenza audit interno. Ritardo una tantum, correggibile. Scenario 5: I report di assessment non includono l'analisi di convergenza quando sono presenti multiple indicatori Red. Classificazione: NC Maggiore se l'analisi di convergenza è documentata come requisito per 8.2.2 (omissione sistematica di elemento richiesto); NC Minore se la pratica di analisi di convergenza esiste ma è documentata in modo inconsistente. Scenario 6: L'organizzazione ha implementato tutti i requisiti CPF ma è stata notata una certa inconsistenza nello scoring ternario tra diversi assessor sull'interpretazione dell'indicatore 3.4. Esiste un buon processo di calibrazione e sta essere migliorato. Classificazione: Osservazione (opportunità di miglioramento). Non è un NC, elemento di miglioramento continuo. Sviluppo collaborativo del finding: discutere i findings con l'auditee man mano che si sviluppano, non come sorpresa alla chiusura, confermare che i fatti siano accurati e che le prove siano comprese, ascoltare le spiegazioni dell'auditee o le azioni correttive già in corso, adeguare il finding se le prove contraddicono la conclusione preliminare, mantenere l'oggettività pur essendo equi e aperti, documentare la risposta dell'auditee ai find-

ings, i disaccordi vengono escalati al lead auditor. Documentazione: moduli dei findings con tutti gli elementi richiesti, prove di supporto allegate o referenziate, risposta dell'auditee annotata, classificazione con ratio, azione correttiva preliminare se discussa (non richiesta ma utile), firma dell'auditee (opzionale, raccomandata per NC maggiori).

**7. Condotta della Riunione di Chiusura (60 min):** Obiettivi della riunione di chiusura: presentare le conclusioni dell'audit al management, rivedere i findings (conformità, osservazioni, non conformità) con le prove di supporto, chiarire eventuali incomprensioni sui findings, spiegare il processo di azione correttiva e follow-up, fornire una valutazione complessiva dell'efficacia del PVMS, raccomandare la decisione di certificazione (per audit di certificazione), ringraziare l'auditee per la cooperazione, discutere i tempi del report e i prossimi passi. Agenda e tempistica tipica (2-3 ore): Presentazioni e scopo della riunione (5 min), ripasso scope e processo di audit (5 min), osservazioni generali e findings positivi (15 min), osservazioni (opportunità di miglioramento) con prove (15 min per osservazione, varia per numero), non conformità minori con prove (15 min per finding), non conformità maggiori con prove (20 min per finding), sintesi dei findings e raccomandazione di certificazione (10 min), spiegazione del processo di azione correttiva e verifica (15 min), domande e preoccupazioni dell'auditee (30 min), prossimi passi e timeline (10 min), osservazioni finali e ringraziamenti (5 min). Partecipanti: Richiesti (top management, Coordinatore CPF, personale chiave coinvolto nelle NC), Opzionali (team di management più ampio, personale che vuole sentire i risultati, rappresentante dell'organismo di certificazione se presente). Presentare efficacemente i findings: iniziare con aspetti positivi e punti di forza osservati, presentare i findings oggettivamente senza emozioni, utilizzare le prove per supportare ogni finding, mostrare il riferimento al requisito specifico per ogni NC, presentare una descrizione chiara della condizione, spiegare l'effetto o potenziale effetto sul PVMS, consentire la risposta e la discussione dell'auditee dopo ogni finding, rimanere aperti a prove che potrebbero cambiare le conclusioni, separare i findings dalle opinioni o raccomandazioni, utilizzare aiuti visivi (tabella di sintesi dei findings, riferimenti ai requisiti). Gestire la riunione di chiusura: iniziare in orario e controllare i tempi, bilanciare accuratezza con efficienza, facilitare una discussione produttiva, affrontare la difensività professionalmente, chiarire le incomprensioni con pazienza, mantenere il focus sui findings non sulle personalità, documentare i punti chiave della discussione, gestire le aspettative degli stakeholder, rimanere fermi sui findings con prove sufficienti, essere flessibili se le prove contraddicono il finding, concludere in modo professionale e costruttivo. Considerazioni speciali per le riunioni di chiusura CPF: enfatizzare il focus organizzativo non la colpa individuale, riconoscere che implementare il PVMS è complesso e in evoluzione, riconoscere la natura sensibile della discussione sulla vulnerabilità psicologica, evidenziare i progressi positivi e le implementazioni efficaci, posizionare le NC come opportunità di miglioramento, assicurare la continuità della riservatezza post-audit, incoraggiare domande sugli aspetti psicologici. Raccomandazione di certificazione (per audit di certificazione): Livello di conformità raggiunto (1-4) se nessuna NC maggiore in sospeso, le NC maggiori impediscono la certificazione fino a correzione e verifica, le NC minori possono essere corrette entro 90 giorni senza impedire la certificazione, dichiarare chiaramente la raccomandazione con condizioni se applicabile, spiegare i prossimi passi (report, azione correttiva, verifica, decisione). Situazioni difficili nella riunione di chiusura: auditee in disaccordo con i findings - ascoltare la ratio, rivedere insieme le prove, essere aperti a revisioni se giustificato, mantenere l'oggettività se le prove sono chiare, spiegare il processo di appello; reazioni emotive - convalidare i sentimenti, rimanere professionali e calmi, focalizzarsi sulle prove, enfatizzare l'intento di miglioramento, offrire una pausa se necessario; ostilità o accuse - non impegnarsi in litigi, affermare i fatti con calma, coinvolgere il senior management, documentare comportamenti preoccupanti; management non presente - riprogrammare se possibile, documentare l'assenza, presentare al personale disponibile, follow-up con comunicazione scritta; pressione temporale per concludere rapidamente - bilanciare il rispetto del tempo con l'accuratezza, prioritarizzare i findings critici, offrire una riunione aggiuntiva se necessario. Documentazione: presenza alla riunione di chiusura con firme, materiali di presentazione (sintesi

dei findings, evidenziazione delle prove), note sulle discussioni e risposte dell'auditee, conferma della comprensione, foto della riunione di chiusura (opzionale con permesso).

**8. Coordinamento Giornaliero del Team (30 min):** Obiettivi della riunione giornaliera del team: condividere findings e osservazioni, garantire coerenza nella valutazione delle prove e nella classificazione dei findings, coordinare le attività del giorno successivo, identificare problemi o sfide, adeguare il piano di audit se necessario, mantenere il morale e l'efficacia del team. Tempistica e struttura della riunione giornaliera: fine di ogni giorno di audit (30-60 minuti), luogo privato lontano dall'auditee, guidata dal lead auditor, tutti i membri del team partecipano. Punti dell'agenda: ogni membro del team riferisce su attività, prove raccolte, potenziali findings; discutere i potenziali findings come team - prove sufficienti, classificazione appropriata, coerenza con gli standard del team; identificare elementi aperti che richiedono follow-up il giorno successivo; rivedere il programma per il giorno successivo e adeguare se necessario; discutere eventuali sfide o problemi; pianificare attività collaborative se necessario; confermare che il team sia allineato sull'approccio. Best practice per il coordinamento del team: comunicazione regolare durante il giorno non solo alla riunione, escalare i problemi al lead auditor tempestivamente, supportarsi a vicenda e condividere competenze, mantenere standard di prova coerenti, verificare incrociata dei findings per coerenza, documentare le decisioni prese, costruire coesione del team. Responsabilità del lead auditor: facilitare riunioni di team efficaci, garantire una valutazione delle prove coerente, prendere decisioni finali sui findings, coordinarsi con l'auditee per adeguamenti del programma, mantenere il morale del team, affrontare problemi interpersonali, monitorare i progressi dell'audit rispetto al piano, autorizzare cambiamenti di scope o programma se necessario.

**9. Adattabilità durante l'Esecuzione (30 min):** Situazioni inaspettate comuni: espansione dello scope scoperta (aree incluse non pianificate - valutare la criticità, discutere con l'auditee, determinare se il programma di audit consente la copertura, documentare la chiarificazione dello scope, potrebbe richiedere audit di follow-up), non conformità inaspettate (NC maggiori trovate non anticipate - allocare tempo per raccogliere prove sufficienti, potrebbe influenzare il programma per altre aree, comunicare l'impatto all'auditee, adeguare il piano di conseguenza), personale chiave non disponibile (malattia, emergenza, viaggio - identificare intervistati alternativi, riprogrammare se persona critica, adeguare il programma per accomodare, documentare deviazione dal piano), documenti non disponibili (persi, ritardati, riservatezza - valutare se le prove sono ottenibili altrove, determinare se NC per documenti mancanti, programmare follow-up se critico, documentare limitazione), auditee non cooperativo (resistente, ostacolante - escalare al top management, documentare problemi di cooperazione, valutare se l'audit può continuare efficacemente, potrebbe richiedere sospensione), sforamenti di tempo (findings complessi, prove estese - prioritarizzare le attività rimanenti, focalizzarsi su aree ad alto rischio, estendere l'audit se fattibile e necessario, documentare limitazioni se il tempo viene ridotto). Principi per adattarsi durante l'esecuzione: mantenere il focus sugli obiettivi dell'audit, applicare il pensiero basato sul rischio per prioritarizzare le attività, comunicare i cambiamenti con l'auditee e il team, documentare le ragioni degli adattamenti, garantire prove sufficienti per le conclusioni, bilanciare accuratezza con vincoli pratici, escalare problemi significativi al lead auditor e all'organismo di certificazione se necessario. Autorità decisionale: Livello membro del team (adeguamenti minori del programma, domande aggiuntive, richieste di prove), Livello lead auditor (chiarificazioni dello scope, estensioni del programma, classificazioni dei findings, modifiche al piano), Livello organismo di certificazione (cambiamenti maggiori dello scope, sospensione o terminazione dell'audit, impatto sulla decisione di certificazione).

**10. Simulazione di Audit Simulato (240 minuti = 4 ore):** Panoramica della simulazione: i partecipanti conducono un audit completo di un'organizzazione simulata (Midwest Regional Bank, 150 dipendenti, cerca certificazione Livello 2, ha ISO 27001 esistente, alcuni elementi PVMS implementati). Materiali forniti (pacchetto scenario di audit realistico): background

dell'organizzazione, settore, dimensione, sedi, storia implementazione CPF; informazioni documentate PVMS (politica, scope, report di assessment, procedure privacy, piani trattamento rischio, registri competenza, audit interno, revisione management - alcuni con non conformità intenzionali); profili del personale chiave; layout della facility; programma di audit per 1,5 giorni. Attività di simulazione: Assegnazione del team (3-4 partecipanti per team, ruoli assegnati - lead auditor, membri del team), Pianificazione dell'audit (30 min) - rivedere i documenti forniti, identificare problemi potenziali, preparare domande per i colloqui, assegnare responsabilità del team; Simulazione riunione di apertura (20 min) - simulata con l'istruttore che interpreta il management, il team conduce la riunione di apertura; Attività di esecuzione dell'audit parallele (90 min) - postazioni allestite per diverse attività (postazione revisione documentale, simulazioni di colloqui con role-player, scenario di osservazione, valutazione delle prove), i team ruotano attraverso le postazioni; Riunione giornaliera del team (15 min) - i team si riuniscono per coordinare i findings; Sviluppo dei findings (45 min) - i team documentano i findings utilizzando moduli di finding, classificano appropriatamente, si preparano per la riunione di chiusura; Simulazione riunione di chiusura (40 min) - i team presentano i findings al management simulato, gestiscono domande e risposte. Criteri di valutazione: efficacia della riunione di apertura (condotta professionale, spiegazione chiara, sicurezza psicologica creata), accuratezza della revisione documentale (problemi identificati, prove documentate), abilità di colloquio (domande appropriate, sensibilità psicologica, prove ottenute), qualità dei findings (chiaro riferimento al requisito, accurata descrizione della condizione, prove sufficienti, classificazione appropriata), presentazione della riunione di chiusura (consegna professionale, basata sulle prove, gestisce le risposte dell'auditee), coordinamento del team (collaborazione, coerenza, supporto), competenza complessiva dell'audit (approccio sistematico, focus basato sul rischio, mantiene l'indipendenza, condotta etica). Ruolo dell'istruttore: interpreta il personale auditee chiave con script, fornisce prove quando richiesto appropriatamente, sfida i team con situazioni difficili (difensività, disaccordo, pressione temporale), osserva e valuta utilizzando rubriche, fornisce feedback durante e dopo la simulazione. Debriefing (30 min): i team presentano i loro findings e raccomandazioni, confronto di diversi approcci di team, feedback del facilitatore su punti di forza e aree di miglioramento, discussione delle lezioni apprese, connessione a situazioni di audit reali. Obiettivi di apprendimento raggiunti: applicare il processo di audit completo dalla pianificazione alla chiusura, dimostrare una condotta di audit professionale, esercitare abilità di audit specifiche CPF-27001, praticare lo sviluppo e la classificazione dei findings, sperimentare il coordinamento del team, costruire fiducia per audit reali.

### 2.8.3 Metodi di Insegnamento

**Lezione:** Struttura riunione apertura con esempio video, dimostrazioni revisione documentale con documenti campione, tecniche colloquio con esempi buoni e poveri, protocolli osservazione con scenari, valutazione qualità prove, metodi campionamento con calcoli, albero decisionale classificazione findings, struttura riunione chiusura con video.

**Esercizi:** (1) Role-Play Riunione Apertura - coppie conducono riunioni apertura con feedback (30 min), (2) Pratica Revisione Documentale - revisionare report assessment campione, identificare problemi (40 min), (3) Simulazione Colloquio - role-play colloqui con sensibilità psicologica (45 min), (4) Valutazione Prove - dati set di prove, valutare sufficienza e affidabilità (30 min), (5) Sviluppo Piano Campionamento - calcolare campioni per varie popolazioni (30 min), (6) Classificazione Findings - 10 scenari, classificare e giustificare (40 min), (7) Documentazione Findings - scrivere finding completo con tutti gli elementi (30 min), (8) Prova Riunione Chiusura - presentare findings a management simulato (30 min), (9) Simulazione Audit Simulato - completare esercizio audit 4 ore (240 min).

**Discussione:** "Aspetto più impegnativo delle riunioni di apertura?", "Come mantenere sensi-

bilità psicologica mentre si raccolgono prove?", "Quando le prove sono sufficienti?", "NC maggiore vs minore - aree grigie?", "Gestire disaccordo auditee con findings?", "Cosa ti ha sorpreso nell'audit simulato?"

**Role-Plays:** Multiple simulazioni di colloqui e riunioni con istruttore e colleghi che interpretano ruoli auditee, script forniti con risposte attese, feedback su tecnica e professionalità.

**Audit Simulato:** Simulazione completa di 4 ore con materiali realistici, role-player, rubriche di valutazione, feedback dettagliato, debriefing di team.

## 2.8.4 Suddivisione Slide

**Slide 3.1:** "Struttura Riunione Apertura" - Obiettivi riunione, agenda tipica con tempistica (90-120 min), partecipanti richiesti, abilità presentazione professionale, considerazioni specifiche CPF (rassicurazioni privacy, enfasi sicurezza psicologica), sfide comuni e risposte.

**Slide 3.2:** "Tecniche Revisione Documentale" - Approccio sistematico (checklist clausola-per-clausola, confronto requisiti, cross-check coerenza), focus documenti chiave CPF-27001, identificare potenziali NCs, preparazione efficaci domande follow-up.

**Slide 3.3:** "Revisione Documentale Report Assessment" - Checklist dettagliata per revisionare report assessment vulnerabilità psicologiche (copertura 100 indicatori, scoring ternario, aggregazione minima 10+, privacy differenziale epsilon  $\leq 0.1$ , ritardi temporali 72+ ore, analisi role-based, calcolo CPF Score, analisi convergenza, misure privacy, ID assessor), problemi comuni.

**Slide 3.4:** "Metodologie di Colloquio" - Obiettivi colloquio, tipi di colloquio (management, process owner, operativo, interfunzionale), passi preparazione, tecniche questioning efficaci (aperte, di approfondimento, evitare leading, usare silenzio, ascolto attivo), sensibilità psicologica per CPF (informato sul trauma, linguaggio rispettoso, sensibilità culturale, sicurezza psicologica, gestione emotiva).

**Slide 3.5:** "Domande di Colloquio per CPF-27001" - Esempi di domande specifiche per area requisito (comprensione policy CPF, implementazione metodologia assessment, pratiche protezione privacy, competenza/formazione, efficacia trattamento rischio, integrazione ISMS), follow-up di approfondimento, richieste prove durante colloqui.

**Slide 3.6:** "Tecniche di Osservazione" - Obiettivi osservazione, cosa osservare in audit CPF (processo assessment in azione, integrazione operazioni sicurezza, erogazione formazione, implementazione trattamento rischio, indicatori cultura organizzativa, pratiche protezione privacy), protocollo osservazione, sfide (effetto osservatore, finestre limitate, vincoli privacy, interpretazione cultura).

**Slide 3.7:** "Raccolta Prove e Qualità" - Tipi di prove (documenti, registri, colloqui, osservazioni, elettroniche), caratteristiche qualità (sufficienti, rilevanti, affidabili per ISO 19011), approcci campionamento (censimento, giudizio, casuale, stratificato), strategie campionamento per requisiti CPF, determinazione dimensione campione, requisiti documentazione.

**Slide 3.8:** "Processo Sviluppo Findings" - Processo passo-passo (identificare potenziale NC, raccogliere prove sufficienti, confrontare con requisito, convalidare con team, discutere con auditee, classificare, documentare, ottenere riconoscimento), elementi finding (requisito, condizione, prove, effetto, causa principale), approccio sviluppo collaborativo, standard documentazione.

**Slide 3.9:** "Criteri Classificazione Findings" - Quattro tipi di classificazione con definizioni ed esempi: Conformità, Osservazione, NC Minore, NC Maggiore con criteri specifici per ciascuno.

**Slide 3.10:** "Esempi Classificazione CPF-27001" - Sei scenari di finding comuni con riferimenti requisito, descrizioni prove, e giustificazioni classificazione.

**Slide 3.11:** "Condotta Riunione Chiusura" - Obiettivi riunione, agenda tipica con tempistica (2-3 ore), partecipanti richiesti, tecniche presentazione efficaci, gestione situazioni difficili.

**Slide 3.12:** "Coordinamento Giornaliero Team" - Obiettivi riunione giornaliera, tempistica e struttura, punti agenda, best practice coordinamento team, responsabilità lead auditor.

**Slide 3.13:** "Adattabilità durante Esecuzione" - Situazioni inaspettate comuni, principi per adattarsi, livelli autorità decisionale.

**Slide 3.14:** "Panoramica Simulazione Audit Simulato" - Struttura simulazione, sequenza attività, criteri valutazione, obiettivi apprendimento raggiunti.

### 2.8.5 Materiali Necessari

Workbook Modulo 3 (pagine 46-75), ISO 19011:2018 Sezioni 6-7, CPF-27001:2025 completo con checklist clausole, tutti i materiali degli esercizi, Pacchetto Scenario Audit Simulato per Midwest Regional Bank (30 pagine), Moduli Findings, guide, template, script role-player, rubriche di valutazione, esempi video (20 min totale).

### 2.8.6 Elementi di Valutazione

**Quiz (5 domande):** Q1: Elemento finding che descrive cosa è stato trovato → condizione corretto. Q2: Classificazione per lacuna documentale isolata con competenza dimostrata → NC minore corretto. Q3: Qualità prove ISO 19011 che significa prove sufficienti → sufficienti corretto. Q4: Unità aggregazione minima CPF-27001 → 10 individui corretto. Q5: Finding che richiede correzione immediata → NC maggiore corretto.

**Rubrica Esercizio (Documentazione Finding):** Finding completo con tutti gli elementi (2 pts), accurato riferimento requisito con clausola (1 pt), chiara descrizione condizione oggettiva (2 pts), sufficienti prove di supporto elencate (2 pts), appropriata classificazione con giustificazione (2 pts), qualità scrittura professionale (1 pt). Totale 10 pts (7+ pass).

**Rubrica Audit Simulato:** Efficacia riunione apertura (3 pts), accuratezza revisione documentale (3 pts), abilità colloquio (4 pts), qualità findings (5 pts), presentazione riunione chiusura (3 pts), coordinamento team (2 pts), competenza audit complessiva (5 pts). Totale 25 pts (18+ pass = competente).

## 2.9 Modulo 4: Reporting dell'Audit

### 2.9.1 Panoramica

**Durata:** 6 ore — **Slide:** 12

**Obiettivi di Apprendimento:** Applicare quadro coerente classificazione non conformità; documentare efficacemente osservazioni e opportunità; strutturare report di audit completi; scrivere findings chiari e oggettivi; sviluppare raccomandazioni azioni correttive azionabili; condurre accurata revisione qualità report; gestire approvazione e distribuzione report; gestire professionalmente domande auditee; mantenere riservatezza; consegnare report entro tempistiche; dimostrare competenza scrittura report.

**Concetti Chiave:** Coerenza classificazione NC, documentazione osservazioni, struttura report audit, scrittura oggettiva, raccomandazioni azioni correttive, revisione qualità, approvazione report, riservatezza, tempestività, comunicazione professionale.

## 2.9.2 Outline dei Contenuti

**1. Quadro Classificazione Non Conformità (90 min):** Revisione criteri classificazione: Conformità, Osservazione, NC Minore, NC Maggiore. Approfondimento processo decisionale: applicazione albero decisionale (fallimento sistematico? assenza completa? effetto significativo? fallimento isolato?), valutare "sistematico" vs "isolato", valutare significatività effetto, aggregare findings correlati. Linee guida specifiche CPF-27001: violazioni requisiti privacy (qualsiasi fallimento in aggregazione/privacy differenziale/ritardi temporali/divieto profiling = NC MAGGIORE presuntivo), completezza metodologia assessment (domini mancanti = maggiore, indicatori mancanti = maggiore se sistematico), requisiti competenza (Coordinatore non qualificato = maggiore, carenza CPE assessor individuale = minore), integrazione con ISMS (processo assente = maggiore, non seguito = maggiore, lacune occasionali = minore), implementazione trattamento rischio (indicator Red non affrontati = maggiore, ritardi prolungati = maggiore). Sfide classificazione comuni e risoluzioni. Coerenza attraverso team audit. Impatto classificazione su certificazione. Documentazione classificazione con ratio.

**2. Documentazione Osservazioni e Opportunità (45 min):** Scopo osservazioni: supportare miglioramento continuo (CPF-27001 Clausola 10.2), identificare buone pratiche, notare rischi emergenti, fornire approfondimenti a valore aggiunto, riconoscere punti di forza. Quando documentare osservazioni: opportunità miglioramento che non sono NCs, pratiche che eccedono requisiti (positive), trend emergenti, aree per azione proattiva, approcci innovativi, guadagni efficienza/efficacia. Struttura documentazione osservazioni: titolo/sintesi, contesto, descrizione, raccomandazione, priorità, prove di supporto. Esempi osservazioni CPF-27001: positive (ML avanzato per predizione convergenza), opportunità miglioramento (aggiungere grafici analisi trend), rischio emergente (crescita rapida che sfida unità aggregazione), opportunità efficienza (automatizzare calcoli privacy differenziale), pratica positiva (cultura sicurezza psicologica). Differenziare osservazioni da NCs. Comunicare efficacemente osservazioni.

**3. Struttura e Contenuto Report Audit (90 min):** Requisiti report audit ISO 19011 (Clausola 6.6): obiettivi/scope, ID cliente audit/auditee, membri team audit, date/luoghi, criteri audit, findings/conclusioni, dichiarazione conformità, opportunità miglioramento, azioni follow-up, dichiarazione distribuzione, dichiarazione riservatezza. Sezioni specifiche report CPF-27001: Sintesi esecutiva (maturità PVMS, livello certificazione raggiunto/raccomandato con CPF Score, conteggio findings sintesi, punti di forza complessivi, aree miglioramento prioritarie, max 1-2 pagine), Dettagli audit (scope/confini, livello cercato, date/programma, composizione team, personale intervistato, documenti revisionati, aree osservate), Valutazione efficacia PVMS (raggiungimento obiettivi CPF, valutazione integrazione ISMS, implementazione protezione privacy, cultura organizzativa che supporta sicurezza psicologica, qualità metodologia assessment, efficacia trattamento rischio, maturità PVMS complessiva), Findings dettagliati (conformità/punti di forza per clausola, osservazioni con dettagli completi, NCs minori con requisito/condizione/prove/effetto/causa principale/raccomandazione, NCs maggiori con documentazione completa), Raccomandazione certificazione (raccomanda livello se nessuna NC maggiore in sospeso, condizionale con requisiti azione correttiva se NCs minori, non certificare se NCs maggiori in sospeso, condizioni/timeline per verifica), Opportunità per miglioramento continuo (sintesi osservazioni, suggerimenti oltre conformità, best practice identificate), Appendici (piano audit, fogli presenza, tabella sintesi findings, template tracciamento azioni correttive, lista documentazione revisionata). Formato e presentazione report: documento business professionale, chiare intestazioni sezioni/numerazione, sintesi esecutiva all'inizio, flusso logico, findings organizzati per clausola o tema, tabelle/grafici per chiarezza, numerazione pagine/controllo versione, dichiarazione distribuzione/riservatezza, formattazione formale organismo certificazione. Considerazioni lunghezza report: tipico 15-25 pagine escluse appendici, piccola org/audit pulito = più corto (10-15), grande org/multiple NCs = più lungo (25-40), sintesi esecutiva sempre breve (1-2 pagine), bilanciare completezza con leggibilità.

**4. Tecniche Scrittura Chiara e Oggettiva (90 min):** Principi scrittura efficace report audit: Oggettività (affermare fatti senza opinioni, evitare aggettivi di giudizio, linguaggio neutrale, distinguere osservazioni da interpretazioni), Chiarezza (linguaggio semplice diretto, evitare gergo a meno che definito, un concetto per frase, paragrafi brevi), Accuratezza (verificare affermazioni contro prove, controllare nomi/titoli/date/numeri, citare requisiti correttamente, proofread accuratamente), Completezza (includere tutti gli elementi finding richiesti, fornire sufficiente contesto, affrontare tutte le aree scope, documentare punti di forza e debolezze), Conciseness (eliminare ridondanza, focalizzare sugli essenziali, usare voce attiva, rispettare tempo lettore). Scrivere efficaci dichiarazioni finding: Sezione Requisito (citare specifica clausola CPF-27001, citare o parafrasare requisito accuratamente, fornire contesto se complesso), Sezione Condizione (descrivere cosa effettivamente trovato, usare dettagli specifici, includere quantificazione, fornire contesto, evitare linguaggio conclusorio), Sezione Prove (elencare prove specifiche con nomi/date, descrivere prove chiaramente, garantire verificabile, multiple fonti rafforzano), Sezione Effetto (spiegare impatto efficacia PVMS, descrivere potenziali conseguenze, connettere a obiettivi CPF, valutare significatività proporzionata all'impatto), Sezione Causa Principale opzionale ma preziosa (identificare motivo sottostante, distinguere sintomi da cause, suggerire miglioramenti sistemici). Debolezze scrittura comuni e correzioni con esempi. Considerazioni tono: professionale throughout, approccio costruttivo, linguaggio senza colpa, professionalità empatica. Proofreading e controllo qualità.

**5. Raccomandazioni Azioni Correttive (45 min):** Scopo raccomandazioni azioni correttive: guidare efficace correzione NC, supportare miglioramento sistemico non fixing sintomo, prevenire ricorrenza, dimostrare valore aggiunto auditor, facilitare efficiente verifica. Caratteristiche raccomandazioni efficaci: affronta causa principale non sintomo, specifica e azionabile, appropriata a severità NC, considera contesto organizzativo, suggerisce approccio non prescrive soluzione, multiple opzioni quando possibile, timeline realistica, misurabile per verifica. Esempi raccomandazioni per findings CPF-27001 con confronti deboli vs migliori. Componenti raccomandazione: correzione immediata, revisione sistematica, miglioramento processo, formazione/competenza, aggiornamento documentazione, approccio verifica, timeline. Evitare raccomandazioni prescrittive: non dettare tools/vendors, non imporre strutture org, non richiedere formati documentazione, permettere flessibilità implementazione, mantenere indipendenza auditor. Documentare raccomandazioni: includere in ogni finding, distinguere requisiti da raccomandazioni, notare se multiple approcci possibili, allineare con requisiti CPF-27001 e buone pratiche.

**6. Revisione Qualità e Approvazione Report (90 min):** Processo revisione qualità interna: auto-revisione lead auditor (completezza, documentazione findings, classificazione coerente, proofread, prove supportano conclusioni, tono appropriato), revisione peer da altro auditor qualificato (secondo auditor revisiona report completo, controlla qualità findings/coerenza classificazione, verifica sufficienza/rilevanza prove, valuta chiarezza/oggettività scrittura, fornisce feedback, firma), revisione tecnica se necessaria (esperto psicologia/privacy revisiona aspetti tecnici, esperto CPF-27001 revisiona interpretazioni requisiti, revisore tecnico organismo certificazione controlla implicazioni certificazione), revisione organismo certificazione (revisione management conclusioni audit, verifica competenza/indipendenza auditor, valutazione appropriatezza raccomandazione certificazione, autorità approvazione per emissione report finale, controllo qualità per integrità programma certificazione). Checklist revisione qualità: Completezza (tutti elementi ISO 19011, tutte aree scope affrontate, tutti findings da riunione chiusura, sintesi esecutiva adeguata, appendici complete), Accuratezza (tutti nomi/titoli/date/numeri corretti, riferimenti requisiti accurati, descrizioni prove verificabili, calcoli CPF Score controllati, nessun errore fattuale), Coerenza (terminologia coerente, classificazione uniforme, formato segue template, tono coerente, stile raccomandazione uniforme), Chiarezza (findings comprensibili, sintesi esecutiva accessibile, linguaggio requisiti chiaro, descrizioni prove specifiche, raccomandazioni azionabili), Prove di supporto (ogni finding ha prove sufficienti, qualità prove meeting standard ISO 19011, traccia prove verificabile, nessun finding senza supporto, osservazione e conclusione



distinte), Qualità professionale (aspetto professionale, grammatica/ortografia/punteggiatura corretti, tono appropriato, rispettoso di auditee, libero da bias, mantiene riservatezza). Problemi qualità comuni e correzioni. Tempistica revisione e workflow approvazione: completamento bozza da lead auditor (5-7 giorni lavorativi dopo chiusura), revisione peer (2-3 giorni lavorativi), revisioni basate su feedback peer (1-2 giorni lavorativi), revisione tecnica se necessaria (2-3 giorni lavorativi), revisioni basate su feedback tecnico (1-2 giorni lavorativi), revisione management organismo certificazione (2-3 giorni lavorativi), approvazione finale ed emissione (1 giorno lavorativo), timeline totale tipicamente 10-15 giorni lavorativi da chiusura a emissione report. Gestire commenti revisione e revisioni: mantenere controllo versione bozza, documentare commenti revisione e risoluzioni, prioritarizzare commenti (obbligatori/importanti/opzionali), consultare revisori su feedback poco chiaro, mantenere prove audit, autorità finale con lead auditor soggetto a organismo certificazione. Gestire disaccordi in revisione. Approvazione e sign-off report: firma lead auditor (attesta accuratezza/completeness, accetta responsabilità, conferma indipendenza mantenuta), firma approvazione organismo certificazione (autorizza emissione report, conferma standard qualità meeting, abilita decisione certificazione), mantenimento lista distribuzione (protezione riservatezza).

### 2.9.3 Metodi di Insegnamento

**Lezione:** Albero decisionale classificazione con esempi, documentazione osservazioni con campioni, struttura report con esempi annotati, tecniche scrittura con confronti prima/dopo, esempi azioni correttive, diagramma di flusso processo revisione qualità.

**Esercizi:** (1) Pratica Classificazione - 10 scenari classificare con giustificazione (40 min), (2) Scrittura Osservazioni - 3 situazioni documentare come osservazioni (30 min), (3) Scrittura Dichiarazione Finding - riscrivere findings deboli per meeting standard (45 min), (4) Bozza Sezione Report - scrivere sintesi esecutiva per scenario (30 min), (5) Revisione Qualità - revisionare report campione identificare problemi (45 min), (6) Scrittura Report Completo - esercizio completo (90 min).

**Discussione:** "Decisioni classificazione più difficili?", "Bilanciare brevità con completezza in report?", "Debolezze scrittura più comuni?", "Valore revisione qualità vs investimento tempo?", "Gestire dispute auditee su contenuto report?"

### 2.9.4 Suddivisione Slide

**Slide 4.1:** "Albero Decisionale Classificazione NC" - Diagramma di flusso con punti decisione (sistematico? assenza? effetto significativo? isolato?), criteri per ogni classificazione, considerazioni specifiche CPF-27001 evidenziate.

**Slide 4.2:** "Classificazione NC Privacy CPF-27001" - Guida speciale per violazioni privacy (aggregazione/privacy differenziale/ritardi temporali/divieto profiling), status NC maggiore preventivo, eccezioni solo per errori isolati involontari.

**Slide 4.3:** "Struttura Documentazione Osservazioni" - Template con titolo/contesto/descrizione/raccomandazioni esempi (osservazione positiva, opportunità miglioramento, rischio emergente, opportunità efficienza), differenziare da NCs.

**Slide 4.4:** "Struttura Report Audit" - Outline report completo con requisiti ISO 19011 e sezioni specifiche CPF-27001, conteggi pagine tipici, diagramma flusso.

**Slide 4.5:** "Best Practice Sintesi Esecutiva" - Elementi da includere (maturità PVMS, livello certificazione/CPF Score, conteggio findings, punti di forza, priorità), limite 1-2 pagine, linguaggio accessibile, esempio sintesi.

**Slide 4.6:** "Scrivere Efficaci Dichiarazioni Finding" - Cinque elementi (requisito, condizione, prove, effetto, causa principale) con guida dettagliata per ciascuno, esempi deboli vs migliori.

**Slide 4.7:** "Tecniche Scrittura Oggettiva" - Cinque principi (oggettività, chiarezza, accuratezza, completezza, conciseness) con tecniche specifiche per ciascuno, debolezze comuni con correzioni.

**Slide 4.8:** "Raccomandazioni Azioni Correttive" - Caratteristiche raccomandazioni efficaci, esempi per findings CPF-27001 comuni (deboli vs migliori), checklist componenti raccomandazione.

**Slide 4.9:** "Evitare Raccomandazioni Prescrittive" - Cosa non fare (dettare tools/vendors, imporre strutture org, richiedere formati doc), mantenere indipendenza auditor, permettere flessibilità.

**Slide 4.10:** "Processo Revisione Qualità" - Revisione a quattro livelli (auto-revisione lead auditor, revisione peer, revisione tecnica se necessaria, revisione organismo certificazione), tempistica/workflow, checklist revisione.

**Slide 4.11:** "Checklist Revisione Qualità" - Sei categorie (completezza, accuratezza, coerenza, chiarezza, prove di supporto, qualità professionale) con voci specifiche per ciascuna.

**Slide 4.12:** "Approvazione e Distribuzione Report" - Workflow approvazione con firme, mantenimento lista distribuzione, protezione riservatezza, obiettivi tempistiche (10-15 giorni lavorativi chiusura a emissione).

### 2.9.5 Materiali Necessari

Workbook Modulo 4 (pagine 76-90), CPF-27001:2025 con guida classificazione findings, Esercizio 4.1 dieci scenari classificazione, Esercizio 4.2 tre situazioni osservazione, Esercizio 4.3 dichiarazioni finding deboli per riscrittura, Esercizio 4.4 scenario per sintesi esecutiva, Esercizio 4.5 report campione con problemi intenzionali (20 pagine), Esercizio 4.6 scenario completo per report completo (pacchetto scenario 8 pagine), Template Report Audit, Template Modulo Finding, Checklist Revisione Qualità, Report audit campione eccellenti (2 esempi), guida stile scrittura.

### 2.9.6 Elementi di Valutazione

**Quiz (5 domande):** Q1: Classificazione per fallimento sistematico che interessa multiple aree → NC maggiore corretto. Q2: Classificazione violazione privacy (aggregazione j10) → NC maggiore corretto. Q3: Distinzione osservazione vs NC → osservazione è opportunità miglioramento non influente conformità corretto. Q4: Elemento finding che descrive situazione attuale → condizione corretto. Q5: Tempistica tipica emissione report dopo riunione chiusura → 10-15 giorni lavorativi corretto.

**Rubrica Esercizio (Scrittura Report Completo):** Qualità sintesi esecutiva - concisa, completa, accessibile (2 pts), Struttura report - segue template, flusso logico, sezioni complete (2 pts), Documentazione findings - tutti elementi presenti, chiari, oggettivi (3 pts), Accuratezza classificazione - appropriata con giustificazione (1 pt), Qualità scrittura - oggettiva, chiara, professionale (1 pt), Auto-controllo revisione qualità - evidenza proofreading, correzioni (1 pt). Totale 10 pts (7+ pass).

## 2.10 Modulo 5: Follow-Up e Chiusura

### 2.10.1 Panoramica

**Durata:** 6 ore — **Slide:** 10

**Obiettivi di Apprendimento:** Revisionare e valutare piani azioni correttive; verificare efficacemente implementazione azioni correttive; valutare efficacia correzioni; applicare appropriati criteri chiusura; supportare miglioramento continuo da findings audit; gestire processo decisione certificazione; condurre esame pratico finale dimostrando competenza auditor completa.

**Concetti Chiave:** Revisione piano azione correttiva, metodi verifica, valutazione efficacia, criteri chiusura, miglioramento continuo, decisione certificazione, esame pratico finale.

### 2.10.2 Outline dei Contenuti

**1. Revisione Piano Azione Correttiva (60 min):** Requisiti piano azione correttiva (PAC): affronta non conformità identificata (causa principale non solo sintomo), azioni specifiche con timeline, responsabilità assegnate con accountability, approccio verifica proposto, criteri misurazione efficacia. Revisionare submission PAC auditee: verificare PAC affronta causa principale identificata in finding, valutare se azioni proposte sufficienti a correggere NC e prevenire ricorrenza, valutare appropriatezza timeline (NC minore = 90 giorni tipico, NC maggiore = azione immediata richiesta con verifica prima certificazione), confermare assegnazioni responsabilità chiare e appropriate, revisionare approccio verifica per fattibilità, controllare criteri misurazione efficacia adatti. Fornire feedback su PACs: approvazione se PAC adeguato ad affrontare finding, approvazione condizionale con specifiche modifiche necessarie, rifiuto se PAC fundamentalmente inadeguato con ratio dettagliata, guida per miglioramento senza prescrivere soluzioni (mantenere indipendenza audit), comunicazione professionale e costruttiva, documentazione revisione e decisione. Carenze PAC comuni: affronta sintomi non cause principali (esempio: "correggi questo assessment" vs "implementa formazione calcolo unità aggregazione e miglioramento procedura"), azioni vaghe ("migliora documentazione" senza specifiche), timeline irrealistiche (troppo corte per complessità o inutilmente estese), responsabilità poco chiare (nessuna persona specifica accountable), nessun approccio verifica proposto, misurazione efficacia mancante. Esempi PAC buoni vs inadeguati per findings CPF-27001 comuni. Tempistiche submission e revisione PAC: auditee sottomette PAC entro 30 giorni emissione report (NCs minori), entro 14 giorni per NCs maggiori (urgenza per certificazione), auditor revisiona e fornisce feedback entro 10 giorni lavorativi ricezione PAC, raffinamento iterativo se necessario fino PAC accettabile approvato, documentazione intero processo revisione PAC.

**2. Verifica Azioni Correttive (90 min):** Obiettivi verifica: confermare azioni correttive implementate come pianificato, raccogliere evidenza implementazione, valutare integrazione sistemica, preparare per valutazione efficacia, abilitare decisione chiusura. Metodi verifica: revisione documentale (procedure revisionate, materiali formazione, report assessment, configurazioni sistema, verbali riunioni, evidenza implementazione), colloqui remoti (personale chiave descrive implementazione, dimostra comprensione cambiamenti, conferma implementazione sostenuta), visite verifica on-site (osservare processi corretti in azione, intervistare personale interessato, revisionare evidenza fisica, valutare integrazione culturale - tipicamente per NCs maggiori o multiple NCs minori), campionamento registri (verificare correzione applicata sistematicamente non solo istanza isolata, controllare pattern nel tempo, assicurare requisiti aggregazione/privacy meeting nella pratica). Approcci verifica specifici CPF-27001: Correzioni violazioni privacy (unità aggregazione >10 corretta) - revisionare tutti report assessment da correzione, verificare metodologia aggregazione documentata e compresa, intervistare assessor su calcolo aggregazione, controllare procedure privacy aggiornate, campionare multiple assessment

confermare conformità. Lacune metodologia assessment corrette (domini/indicatori mancanti) - revisionare report assessment confermare copertura completa, verificare formazione assessor su elementi mancanti, intervistare assessor dimostrare competenza, controllare template assessment aggiornati. Carenze competenza corrette (formazione/CPE mancanti) - verificare certificati ottenuti, revisionare file competenza completi, intervistare personale dimostrare conoscenza, controllare procedura gestione competenza stabilita. Trattamento rischio non implementato corretto - verificare trattamento effettivamente operativo, osservare trattamento in pratica se possibile, intervistare personale interessato esperienza cambiamenti, revisionare metriche efficacia, controllare oversight management implementazione. Lacune integrazione corrette (CPF non informa ISMS) - revisionare procedure integrazione aggiornate, verificare esempi recenti flusso informazioni CPF-ISMS, intervistare coordinatori descrivere integrazione, osservare integrazione in riunioni/decisioni. Tempistica verifica: NCs minori verificate entro 90 giorni approvazione PAC, NCs maggiori verificate immediatamente dopo implementazione dichiarata (prima certificazione concessa), verifica follow-up 6-12 mesi post-certificazione (sorveglianza) conferma implementazione sostenuta, programma verifica comunicato chiaramente auditee. Evidenza richiesta per verifica: evidenza oggettiva implementazione (documenti, registri, foto, screenshot sistema), multiple tipi evidenza rafforzano verifica (documenti + colloqui + osservazione), evidenza proporzionata a severità NC (NC maggiore = evidenza più estesa), evidenza dimostra cambiamento sistematico non fix isolato, evidenza temporale mostra implementazione sostenuta nel tempo. Sfide verifica: auditee dichiara implementazione senza evidenza - richiedere evidenza aggiuntiva, ritardare verifica fino evidenza fornita; evidenza mostra implementazione parziale - identificare lacune, richiedere completamento prima chiusura; evidenza contraddice dichiarazioni auditee - investigare discrepanza, documentare accuratamente; verifica non possibile dentro timeframe - estendere scadenza con giustificazione o raccomandare non certificare; nuove NCs correlate scoperte durante verifica - documentare come nuovi findings, potrebbe richiedere PAC aggiuntivo. Documentazione: piano verifica con metodi/programma, evidenza raccolta durante verifica con fonti/date, report verifica con findings (implementato / parzialmente implementato / non implementato / non efficace), raccomandazione chiusura con ratio, comunicazione auditee risultati verifica.

**3. Valutazione Efficacia (60 min):** Efficacia vs implementazione: implementazione conferma azioni intraprese, efficacia conferma NC risolto e ricorrenza prevenuta. Criteri valutazione efficacia: non conformità non esiste più (obiettivo immediato raggiunto), causa principale affrontata (problema sottostante risolto), miglioramento sistemico evidente (oltre fix isolato), misure preventive in posto (ricorrenza improbabile), metriche mostrano miglioramento (evidenza quantitativa), sostenuto nel tempo (non conformità temporanea). Quando valutare efficacia: non immediatamente dopo implementazione (necessario tempo per efficacia manifestarsi), tipicamente 3-6 mesi post-implementazione per valutazione significativa, durante audit sorveglianza (6-12 mesi post-certificazione), periodo valutazione più lungo per cambiamenti culturali/comportamentali (CPF-specifico, cambi cultura psicologica richiedono tempo). Indicatori efficacia per correzioni CPF-27001: Violazioni privacy - nessuna nuova violazione privacy in assessment successivi (zero unità aggregazione  $\geq 10$ , privacy differenziale mantenuta, ritardi temporali consistenti, nessun incidente profiling), auditee dimostra comprensione requisiti privacy, procedure privacy seguite consistentemente, cultura privacy incorporata. Metodologia assessment - copertura indicatori completa in tutti assessment da correzione, scoring ternario applicato consistentemente, competenza assessor evidente in qualità report, procedura metodologia assessment seguita sistematicamente. Miglioramenti competenza - personale mantiene certificazioni/CPE richieste, lacune competenza non ricorrono, procedura gestione competenza previene future lacune, efficacia formazione dimostrata. Implementazione trattamento rischio - trattamenti operativi e producono risultati intesi, metriche efficacia mostrano miglioramento (se trattamento per affaticamento alert, risposta alert migliorata), trattamenti sostenuti senza degradazione, miglioramento continuo trattamenti evidente. Miglioramenti integrazione - findings CPF consistentemente infor-

mano valutazione rischio ISO 27001, procedure integrazione seguite nella pratica, coordinatori collaborano efficacemente, integrazione visibile in decisioni management. Metodi valutazione efficacia: revisione registri su periodo tempo (analisi pattern), colloqui follow-up valutando cambiamento sostenuto e comprensione, osservazione durante audit sorveglianza, analisi metriche mostrando trend miglioramento, auto-valutazione auditee efficacia (con validazione auditor). Correzioni inefficaci: se valutazione efficacia mostra NC non veramente risolto o ricorrenza occorsa, riaprire NC richiedendo azione correttiva aggiuntiva, investigare perché correzione iniziale insufficiente, potrebbe indicare necessità approccio diverso o analisi causa principale più profonda, preoccupazione maggiore per mantenimento certificazione se persistente. Documentazione: piano valutazione efficacia con criteri e metodi, evidenza raccolta su periodo valutazione, analisi indicatori efficacia, determinazione efficacia (efficace / parzialmente efficace / inefficace), raccomandazioni per miglioramento continuo anche se efficace, se inefficace - requisito per azione correttiva aggiuntiva.

**4. Criteri Chiusura Audit (45 min):** Criteri chiusura per findings: NCs minori - implementazione verificata entro 90 giorni e indicatori efficacia iniziali positivi (efficacia completa valutata durante sorveglianza), NCs maggiori - implementazione verificata E efficacia dimostrata prima certificazione iniziale concessa (più stringente), osservazioni - nessuna chiusura richiesta ma progresso notato in audit sorveglianza, conformità - documentate come punti di forza, nessuna ulteriore azione. Processo decisionale chiusura: lead auditor fa raccomandazione chiusura basata su evidenza verifica e valutazione efficacia, organismo certificazione revisiona e approva raccomandazione chiusura, traccia documentazione supporta decisione chiusura, auditee notificato decisioni chiusura, file audit chiuso quando tutti findings affrontati. Chiusura file audit: tutti findings classificati correttamente, tutte azioni correttive verificate, efficacia valutata appropriatamente, documentazione completa e organizzata, sintesi audit finale preparata, lessons learned catturate, file audit archiviato per politica retention (tipicamente 5 anni minimo), decisione certificazione presa e comunicata. Scenari chiusura parziale: alcuni NCs chiusi mentre altri rimangono aperti (progresso misto), certificazione può essere condizionale su chiusura NCs outstanding, certificazione prevenuta se NCs maggiori non chiusi, comunicazione chiara auditee su status, audit follow-up programmato se necessario per elementi outstanding. Riapertura findings chiusi: se audit sorveglianza rivela ricorrenza o correzione inefficace, finding riaperto con documentazione ricorrenza, processo azione correttiva riavviato, potrebbe impattare status certificazione (rischio sospensione), investigazione perché chiusura iniziale prematura. Aspettative timeline chiusura: NCs minori chiusi tipicamente entro 90-120 giorni emissione report (30 giorni PAC + 90 giorni implementazione + verifica), NCs maggiori chiusi prima certificazione iniziale concessa (timeline urgente), audit sorveglianza confermano chiusura sostenuta, comunicazione aspettative timeline auditee. Documentazione: raccomandazione chiusura con ratio, evidenza supportante decisione chiusura, approvazione organismo certificazione chiusura, comunicazione auditee chiusura, sintesi audit finale con tutte disposizioni findings, lessons learned catturate, checklist chiusura file audit completata.

**5. Miglioramento Continuo da Findings (30 min):** Apprendere da findings audit: identificare pattern attraverso findings (cause principali comuni, problemi sistemici, best practice), condividere lessons learned dentro organismo certificazione (calibrare auditor, migliorare approcci audit, aggiornare formazione), contribuire a miglioramento quadro CPF (identificare indicatori che necessitano chiarimento, suggerire indicatori aggiuntivi, proporre miglioramenti metodologia), comunicare trend industria a comunità CPF (pattern findings anonimizzati, vulnerabilità emergenti, interventi efficaci). Miglioramento continuo auditee: osservazioni forniscono roadmap miglioramento oltre conformità, analisi trend findings su multiple audit mostra progressione maturità, best practice identificate in un audit condivise con altri auditee (anonimizzate), livelli certificazione motivano avanzamento continuo (Livello 1 → 2 → 3 → 4), engagement con comunità CPF supporta apprendimento. Miglioramento continuo auditor: riflessione su ogni audit (cosa andata bene, cosa potrebbe migliorare), incorporazione feedback peer, sviluppo abilità

tecniche basate su lacune identificate, miglioramenti efficienza audit, perfezionamento abilità comunicazione, rimanere aggiornati con aggiornamenti metodologia CPF e ricerca. Miglioramento continuo organismo certificazione: analisi metriche programma audit (tassi pass/fail, NCs comuni, tempi ciclo audit, soddisfazione auditee), valutazione performance e sviluppo auditor, aggiornamenti schema certificazione basato su esperienza, collaborazione con CPF3 su evoluzione quadro, miglioramento sistema gestione qualità. Feedback loops: feedback auditee su qualità processo audit, feedback auditor su sfide audit e preparazione auditee, feedback organismo certificazione a CPF3 su chiarezza standard e applicabilità, feedback comunità ricerca su efficacia quadro, ciclo miglioramento continuo mantenuto attraverso tutti stakeholder.

**6. Esame Pratico Finale (180 min = 3 ore didattiche, 8 ore totale con tempo lavoro candidato):** Panoramica esame finale: dimostrazione competenza audit completa, scenario organizzazione realistica (TechCorp Inc, 300 dipendenti, cerca certificazione Livello 3, esistente Livello 2 con storia 18 mesi, PVMS complesso con alcuni problemi), candidati performano come lead auditor, valutati contro tutte competenze CPF Auditor. Materiali forniti (pacchetto realistico esteso): background organizzazione e contesto industria, documentazione PVMS completa con conformità e non conformità intenzionali attraverso tutte clausole (politica, scope, assessment, procedure privacy, trattamenti rischio, registri competenza, audit interni, revisioni management, metriche efficacia - 40+ pagine), report audit precedente da certificazione Livello 2 (per contesto), profili personale chiave e organigramma, dettagli facility e operativi. Componenti esame (8 ore totale tempo candidato, 3 ore facilitazione didattica): Pianificazione Audit (90 min) - sviluppare piano audit basato rischio, identificare aree alto rischio da revisione documentale, preparare domande colloquio, creare piano campionamento verifica, documentare ratio pianificazione. Revisione Documentale e Sviluppo Findings (180 min) - revisione sistematica documentazione PVMS fornita contro requisiti CPF-27001, identificare conformità e non conformità, sviluppare findings completi con tutti elementi richiesti (requisito/condizione/prove/effetto/causa principale), classificare findings appropriatamente (conformità/osservazione/NC minore/NC maggiore), documentare traccia prove. Simulazione Colloquio (60 min) - condurre colloqui simulati con istruttore che interpreta Coordinatore CPF e altro personale chiave (scripted con risposte realistiche e rivelazioni intenzionali), raccogliere evidenza aggiuntiva attraverso questioning, dimostrare sensibilità psicologica e condotta professionale, integrare findings colloquio con revisione documentale. Scrittura Report (180 min) - scrivere sintesi esecutiva per management, documentare findings dettagliati seguendo struttura report, scrivere findings chiari oggettivi evitando debolezze comuni, sviluppare appropriate raccomandazioni azioni correttive, preparare raccomandazione certificazione con ratio. Presentazione (30 min) - presentare conclusioni audit a panel management simulato (panel istruttore), sintetizzare findings chiave e raccomandazione certificazione, gestire domande e obiezioni professionalmente, dimostrare competenza comunicazione. Criteri valutazione (rubrica completa): Pianificazione audit - approccio basato rischio, copertura completa, campionamento appropriato, ratio documentata (10 pts). Revisione documentale - revisione sistematica accurata, problemi identificati, evidenza documentata, mappatura requisiti corretta (15 pts). Sviluppo findings - findings completi con tutti elementi, chiaro requisito/condizione/prove/effetto/causa principale, sufficiente evidenza per ogni finding, appropriata analisi causa principale (20 pts). Classificazione findings - classificazione accurata con giustificazione, applicazione consistente criteri, considerazioni specifiche CPF-27001 applicate correttamente (15 pts). Scrittura report - scrittura chiara oggettiva, qualità professionale, sintesi esecutiva efficace, struttura appropriata, raccomandazioni azionabili (15 pts). Abilità colloquio - questioning efficace, sensibilità psicologica, raccolta evidenze, condotta professionale (10 pts). Presentazione - consegna professionale, comunicazione chiara, gestisce domande efficacemente, fiducia e competenza proiettate (10 pts). Competenza auditor complessiva - approccio sistematico, condotta etica, indipendenza mantenuta, focus basato rischio, integra ISO 19011 e CPF-27001 (5 pts). Totale 100 punti (70+ richiesto per passare = auditor competente). Feedback e debriefing (30 min): feedback individuale su punti di forza

e aree sviluppo, debriefing gruppo discutendo sfide comuni e best practice, discussione come scenari esame relazionano ad audit reali, chiarificazione eventuali incomprensioni su requisiti o metodologia, celebrazione raggiungimento competenza e percorso forward come CPF Auditor. Determinazione Pass/Fail: candidati che segnano 70+ punti attraverso tutti criteri passano e dimostrano competenza auditor completa, candidati che segnano <70 punti richiedono sviluppo aggiuntivo - lacune specifiche identificate con piano rimedio (formazione aggiuntiva, audit supervisionati, riesame dopo periodo sviluppo), competenza parziale riconosciuta (forte in alcune aree, sviluppo necessario in altre) con rimedio mirato, candidati che passano esame pratico finale eleggibili per certificazione CPF Auditor al completamento tutti altri requisiti (passaggio esame scritto, accordo etica firmato, requisiti presenza meeting).

### 2.10.3 Metodi di Insegnamento

**Lezione:** Criteri revisione PAC con esempi, dimostrazione metodi verifica, quadri valutazione efficacia, diagrammi di flusso decisione chiusura, cicli miglioramento continuo, istruzioni esame finale e spiegazione rubrica.

**Esercizi:** (1) Revisione PAC - valutare 3 PACs submitted, fornire feedback (40 min), (2) Pianificazione Verifica - sviluppare piano verifica per scenari (30 min), (3) Valutazione Efficacia - valutare efficacia per 3 NCs corretti (30 min), (4) Decisione Chiusura - determinare chiusura per findings misti (20 min), (5) Esame Pratico Finale - dimostrazione competenza audit completa 8 ore (480 min totale con 180 min didattiche).

**Discussione:** "Aspetto più difficile revisione PAC?", "Come determinare se correzione veramente efficace?", "Quando riaprire findings chiusi?", "Bilanciare accuratezza con efficienza audit?", "Lessons learned da audit pratici?", "Livello confidenza per audit reali post-formazione?"

**Esame Finale:** Esame pratico completo con materiali realistici, interazioni simulate, rubrica valutazione estesa, feedback individuale, certificazione competenza al passaggio.

### 2.10.4 Suddivisione Slide

**Slide 5.1:** "Requisiti Piano Azione Correttiva" - Elementi PAC (affronta causa principale, azioni specifiche, timeline, responsabilità, approccio verifica, misurazione efficacia), criteri revisione, decisioni approvazione/condizionale/rifiuto.

**Slide 5.2:** "Esempi PAC Buoni vs Inadeguati" - Confronto side-by-side per findings CPF-27001 comuni (violazione privacy, lacuna assessment, carenza competenza, ritardo trattamento rischio) che mostra PAC inadeguato e versione migliorata.

**Slide 5.3:** "Metodi Verifica" - Quattro metodi (revisione documentale, colloqui remoti, visite on-site, campionamento registri) con quando usare ciascuno, requisiti evidenza, approcci verifica specifici CPF-27001.

**Slide 5.4:** "Requisiti Evidenza Verifica" - Tipi di evidenza (evidenza oggettiva implementazione, multiple tipi evidenza, proporzionata a severità NC, dimostra cambiamento sistematico, evidenza temporale), tempistica verifica, esempi evidenza.

**Slide 5.5:** "Valutazione Efficacia" - Distinzione implementazione vs efficacia, criteri efficacia (NC risolto, causa principale affrontata, miglioramento sistematico, misure preventive, metriche migliorano, sostenute nel tempo), quando valutare (3-6 mesi tipico, audit sorveglianza).

**Slide 5.6:** "Indicatori Efficacia per CPF-27001" - Indicatori specifici per tipo NC (violazioni privacy, metodologia assessment, competenza, trattamento rischio, integrazione) con cosa cercare, metriche da tracciare.

**Slide 5.7:** "Criteri Chiusura Audit" - Criteri chiusura per tipo finding (NCs minori, NCs maggiori, osservazioni, conformità), processo decisionale chiusura, requisiti documentazione, scenari chiusura parziale.

**Slide 5.8:** "Aspettative Timeline Chiusura" - Diagramma di flusso timeline da emissione report attraverso chiusura (submission PAC, periodo implementazione, verifica, valutazione efficacia, decisione chiusura), durate tipiche, punti comunicazione.

**Slide 5.9:** "Ciclo Miglioramento Continuo" - Apprendere da findings (pattern, lessons learned, miglioramento quadro, trend industria), miglioramento per auditees/auditors/organismo certificazione, diagramma feedback loops.

**Slide 5.10:** "Esame Pratico Finale" - Struttura esame (pianificazione, revisione documentale, colloqui, scrittura report, presentazione), panoramica scenario TechCorp, sintesi rubrica valutazione (100 punti, 70+ pass), tempistica componenti esame, aspettative dimostrazione competenza.

### 2.10.5 Materiali Necessari

Workbook Modulo 5 (pagine 91-100), ISO 19011:2018 guida verifica, CPF-27001:2025 requisiti chiusura, Esercizio 5.1 tre submission PAC per revisione, Esercizio 5.2 scenari pianificazione verifica, Esercizio 5.3 tre casi valutazione efficacia, Esercizio 5.4 scenario decisione chiusura findings misti, Pacchetto Esame Pratico Finale TechCorp (documentazione PVMS completa 40+ pagine, profili personale, report audit precedente, contesto organizzativo, istruzioni esame), Rubrica Valutazione Esame Finale (scoring dettagliato 100 punti), script colloqui simulati per istruttore, criteri valutazione presentazione, moduli feedback.

### 2.10.6 Elementi di Valutazione

**Quiz (5 domande):** Q1: PAC deve affrontare → causa principale non solo sintomo corretto. Q2: Tempistica verifica NC minore → entro 90 giorni approvazione PAC corretto. Q3: Chiusura NC maggiore prima → certificazione iniziale concessa corretto. Q4: Tempistica tipica valutazione efficacia → 3-6 mesi post-implementazione corretto. Q5: Punteggio passaggio esame finale → 70+ punti corretto.

**Rubrica Esercizio (Revisione PAC):** Appropriata valutazione tutti 3 PACs (3 pts), chiaro feedback con specifiche aree miglioramento (3 pts), accurate decisioni approvazione/condizionale/rifiuto (2 pts), mantiene indipendenza auditor in feedback (1 pt), tono comunicazione professionale (1 pt). Totale 10 pts (7+ pass).

**Rubrica Esame Pratico Finale:** Vedere rubrica dettagliata 100 punti in slide 5.10 e materiali esame. Pass = 70+ punti dimostrando competenza CPF Auditor completa attraverso tutti criteri valutazione (pianificazione, revisione documentale, sviluppo findings, classificazione, scrittura report, abilità colloquio, presentazione, competenza auditor complessiva).



### 3 Appendici

#### A Inventario Completo Slide

Modulo	Slide	Titolo	Tipo	Durata
Modulo 1	1.1	Principi di Audit ISO 19011:2018	Lezione	15 min
Modulo 1	1.2	Principi nel Contesto CPF	Lezione	10 min
Modulo 1	1.3	Struttura CPF-27001:2025	Lezione	15 min
Modulo 1	1.4	Clausola 4: Contesto dell'Organizzazione	Lezione	15 min
Modulo 1	1.5	Clausola 5: Leadership & Clausola 6: Pianificazione	Lezione	20 min
Modulo 1	1.6	Clausola 7: Supporto	Lezione	15 min
Modulo 1	1.7	Clausola 8: Operazione	Lezione	20 min
Modulo 1	1.8	Clausole 9 & 10	Lezione	15 min
Modulo 1	1.9	Ciclo di Vita Processo Audit	Lezione	20 min
Modulo 1	1.10	Competenze dell'Auditor	Lezione	20 min
Modulo 1	1.11	Indipendenza e Oggettività	Lezione	15 min
Modulo 1	1.12	Condotta Professionale ed Etica	Lezione	20 min
Modulo 2	2.1	Definire Scope e Obiettivi Audit	Lezione	20 min
Modulo 2	2.2	Pianificazione Audit Basata sul Rischio	Lezione	20 min
Modulo 2	2.3	Selezione Team Audit	Lezione	15 min
Modulo 2	2.4	Allocazione Risorse e Programmazione	Lezione	15 min
Modulo 2	2.5	Componenti Piano Audit	Lezione	20 min
Modulo 2	2.6	Esempio Piano Audit Basato sul Rischio	Lezione	15 min
Modulo 2	2.7	Comunicazione con Auditee	Lezione	15 min
Modulo 2	2.8	Lista Richiesta Documenti per CPF-27001	Lezione	15 min
Modulo 2	2.9	Processo Revisione Documentale Pre-Audit	Lezione	20 min
Modulo 2	2.10	Esercizio Sviluppo Piano Audit	Esercizio	60 min
Modulo 3	3.1	Struttura Riunione Apertura	Lezione	15 min
Modulo 3	3.2	Tecniche Revisione Documentale	Lezione	20 min
Modulo 3	3.3	Revisione Documentale Report Assessment	Lezione	20 min
Modulo 3	3.4	Metodologie di Colloquio	Lezione	25 min
Modulo 3	3.5	Domande di Colloquio per CPF-27001	Lezione	20 min
Modulo 3	3.6	Tecniche di Osservazione	Lezione	15 min
Modulo 3	3.7	Raccolta Prove e Qualità	Lezione	20 min
Modulo 3	3.8	Processo Sviluppo Findings	Lezione	25 min
Modulo 3	3.9	Criteri Classificazione Findings	Lezione	20 min
Modulo 3	3.10	Esempi Classificazione CPF-27001	Lezione	20 min
Modulo 3	3.11	Condotta Riunione Chiusura	Lezione	15 min
Modulo 3	3.12	Coordinamento Giornaliero Team	Lezione	10 min
Modulo 3	3.13	Adattabilità durante Esecuzione	Lezione	10 min
Modulo 3	3.14	Panoramica Simulazione Audit Simulato	Esercizio	240 min
Modulo 4	4.1	Albero Decisionale Classificazione NC	Lezione	20 min
Modulo 4	4.2	Classificazione NC Privacy CPF-27001	Lezione	15 min
Modulo 4	4.3	Struttura Documentazione Osservazioni	Lezione	10 min
Modulo 4	4.4	Struttura Report Audit	Lezione	20 min
Modulo 4	4.5	Best Practice Sintesi Esecutiva	Lezione	15 min
Modulo 4	4.6	Scrivere Efficaci Dichiarazioni Finding	Lezione	20 min

Modulo	Slide	Titolo	Tipo	Durata
Modulo 4	4.7	Tecniche Scrittura Oggettiva	Lezione	20 min
Modulo 4	4.8	Raccomandazioni Azioni Correttive	Lezione	15 min
Modulo 4	4.9	Evitare Raccomandazioni Prescrittive	Lezione	10 min
Modulo 4	4.10	Processo Revisione Qualità	Lezione	20 min
Modulo 4	4.11	Checklist Revisione Qualità	Lezione	15 min
Modulo 4	4.12	Approvazione e Distribuzione Report	Lezione	10 min
Modulo 5	5.1	Requisiti Piano Azione Correttiva	Lezione	15 min
Modulo 5	5.2	Esempi PAC Buoni vs Inadeguati	Lezione	15 min
Modulo 5	5.3	Metodi Verifica	Lezione	20 min
Modulo 5	5.4	Requisiti Evidenza Verifica	Lezione	15 min
Modulo 5	5.5	Valutazione Efficacia	Lezione	15 min
Modulo 5	5.6	Indicatori Efficacia per CPF-27001	Lezione	15 min
Modulo 5	5.7	Criteri Chiusura Audit	Lezione	15 min
Modulo 5	5.8	Aspettative Timeline Chiusura	Lezione	10 min
Modulo 5	5.9	Ciclo Miglioramento Continuo	Lezione	10 min
Modulo 5	5.10	Esame Pratico Finale	Esercizio	480 min
<b>Totale: 60 slide, 40 ore (2400 minuti)</b>				

## B Sintesi Banca Esercizi

### B.1 Esercizi Modulo 1

- 1.1 Applicazione Principi ISO (30 min): 5 scenari audit, identificare quali principi applicano e come
- 1.2 Mappatura Clausole CPF-27001 (30 min): Date situazioni organizzative, identificare clausole e requisiti rilevanti
- 1.3 Auto-Valutazione Competenze (20 min): Partecipanti si valutano contro criteri competenza auditor, identificano bisogni sviluppo
- 1.4 Valutazione Indipendenza (20 min): 6 scenari conflitto, determinare se indipendenza compromessa
- 1.5 Analisi Casi Etica (30 min): 3 dilemmi etici, discussione gruppo risposte appropriate

### B.2 Esercizi Modulo 2

- 2.1 Pratica Definizione Scope (20 min): 3 scenari organizzativi, scrivere appropriate dichiarazioni scope
- 2.2 Valutazione Rischio per Audit (30 min): Dato profilo organizzativo, identificare e prioritarizzare aree alto/medio/basso rischio
- 2.3 Selezione Team (20 min): 5 scenari audit, selezionare appropriata composizione team e dimensione con ratio
- 2.4 Simulazione Revisione Documentale (40 min): Revisionare documentazione PVMS campione, identificare problemi e preparare domande
- 2.5 Sviluppo Piano Audit (60 min): Completare esercizio - scenario organizzazione sanitaria, sviluppare piano audit completo

### B.3 Esercizi Modulo 3

- 3.1 Role-Play Riunione Apertura (30 min): Coppie conducono riunioni apertura con feedback
- 3.2 Pratica Revisione Documentale (40 min): Revisionare report assessment campione, identificare problemi
- 3.3 Simulazione Colloquio (45 min): Role-play colloqui con sensibilità psicologica
- 3.4 Valutazione Prove (30 min): Dati set di prove, valutare sufficienza e affidabilità
- 3.5 Sviluppo Piano Campionamento (30 min): Calcolare campioni per varie popolazioni
- 3.6 Classificazione Findings (40 min): 10 scenari, classificare e giustificare
- 3.7 Documentazione Findings (30 min): Scrivere finding completo con tutti elementi
- 3.8 Prova Riunione Chiusura (30 min): Presentare findings a management simulato
- 3.9 Simulazione Audit Simulato (240 min): Completare esercizio audit 4 ore - scenario Midwest Regional Bank

### B.4 Esercizi Modulo 4

- 4.1 Pratica Classificazione (40 min): 10 scenari classificare con giustificazione
- 4.2 Scrittura Osservazioni (30 min): 3 situazioni documentare come osservazioni
- 4.3 Scrittura Dichiarazione Finding (45 min): Riscrivere findings deboli per meeting standard
- 4.4 Bozza Sezione Report (30 min): Scrivere sintesi esecutiva per scenario
- 4.5 Revisione Qualità (45 min): Revisionare report campione identificare problemi
- 4.6 Scrittura Report Completo (90 min): Esercizio completo con scenario completo

### B.5 Esercizi Modulo 5

- 5.1 Revisione PAC (40 min): Valutare 3 PACs submitted, fornire feedback
- 5.2 Pianificazione Verifica (30 min): Sviluppare piano verifica per scenari
- 5.3 Valutazione Efficacia (30 min): Valutare efficacia per 3 NCs corretti
- 5.4 Decisione Chiusura (20 min): Determinare chiusura per findings misti
- 5.5 Esame Pratico Finale (480 min totale, 180 min didattiche): Dimostrazione competenza audit completa 8 ore - scenario TechCorp

**Totale: 30+ esercizi attraverso 40 ore**

## C Blueprint Esame

### C.1 Struttura Esame Scritto

**Formato:** 80 domande, 3 ore, closed-book, computer-based

**Tipi Domanda:**

- 50 Scelta Multipla: Singola risposta corretta da 4 opzioni
- 20 Basate su Scenario: Breve scenario con domanda che richiede analisi
- 10 Giudizio Audit: Situazioni audit complesse che richiedono giudizio professionale

**Distribuzione Contenuto per Modulo:**

Modulo	Domande	Aree Focus
Modulo 1	16	Principi ISO 19011, clausole CPF-27001, competenze, indipendenza, etica
Modulo 2	12	Definizione scope, pianificazione basata rischio, selezione team, piani audit, revisione documentale
Modulo 3	24	Riunioni apertura/chiusura, colloqui, osservazione, prove, campionamento, sviluppo/classificazione findings
Modulo 4	16	Classificazione NC, osservazioni, struttura report, scrittura oggettiva, revisione qualità
Modulo 5	12	Revisione PAC, verifica, efficacia, criteri chiusura, miglioramento continuo
<b>Totale</b>	<b>80</b>	

**Distribuzione Livello Cognitivo:**

- Conoscenza/Recall: 20% (16 domande) - Fatti, definizioni, requisiti
- Applicazione/Analisi: 50% (40 domande) - Applicare concetti, analizzare situazioni
- Valutazione/Sintesi: 30% (24 domande) - Giudizio professionale, integrazione complessa

**Standard Passaggio:** 75% (60 risposte corrette) - più alto di CPF-101 per criticità ruolo auditor

**Processo Sviluppo Domanda:**

- Validazione psicometrica con gruppi pilota
- Distribuzione difficoltà item: 25% facile, 50% moderato, 25% difficile
- Analisi statistica regolare (indice discriminazione, indice difficoltà)
- Miglioramento continuo basato su dati performance
- Ciclo revisione e aggiornamento annuale

**Politica Ripristino:**

- Primo ripristino: periodo attesa 30 giorni, 50% fee
- Secondo ripristino: periodo attesa 30 giorni, 50% fee
- Dopo tre fallimenti: Esperienza audit supervisionata aggiuntiva richiesta (minimo 3 audit), periodo attesa 6 mesi, formazione rimediale raccomandata

**C.2 Struttura Esame Pratico**

**Formato:** Audit simulato full-day (8 ore tempo lavoro candidato, 3 ore facilitazione didattica)

**Componenti:**

1. Pianificazione Audit (90 min) - Sviluppo piano basato rischio
2. Revisione Documentale e Sviluppo Findings (180 min) - Revisione sistematica, documentazione findings
3. Simulazione Colloquio (60 min) - Colloqui simulati con role-player scripted
4. Scrittura Report (180 min) - Sintesi esecutiva, findings dettagliati, raccomandazioni
5. Presentazione (30 min) - Presentare conclusioni a panel management simulato

**Criteri Valutazione (100 punti totali):**

- Pianificazione Audit: 10 punti
- Revisione Documentale: 15 punti
- Sviluppo Findings: 20 punti
- Classificazione Findings: 15 punti
- Scrittura Report: 15 punti
- Abilità Colloquio: 10 punti
- Presentazione: 10 punti
- Competenza Auditor Complessiva: 5 punti

**Standard Passaggio:** 70+ punti = Competente attraverso tutti criteri

**Caratteristiche Scenario:**

- Organizzazione realistica (TechCorp Inc, 300 dipendenti, certificazione Livello 3 cercata)
- Documentazione PVMS completa (40+ pagine con problemi intenzionali)
- Cronologia audit precedente fornita per contesto
- Conformità e non conformità miste attraverso tutte clausole
- Sfide privacy e sensibilità psicologica incorporate
- Complessità culturale e organizzativa rappresentativa di audit reali

**Politica Ripristino per Esame Pratico:**

- Primo ripristino: periodo attesa 60 giorni (permette sviluppo abilità), scenario diverso, 50% fee
- Secondo ripristino: periodo attesa 90 giorni, partecipazione audit supervisionato obbligatoria (minimo 2 audit), scenario diverso, 50% fee
- Dopo tre fallimenti: Piano rimedio completo richiesto includendo formazione aggiuntiva, esperienza audit supervisionata (minimo 5 audit), rivalutazione competenza prima riesame permesso

**D Materiali di Riferimento****D.1 Standard e Riferimenti Normativi Richiesti****Standard Primari:**

- ISO 19011:2018 - Linee guida per l'audit di sistemi di gestione (documento completo)
- CPF-27001:2025 - Sistema di Gestione della Vulnerabilità Psicologica - Requisiti (standard completo)
- ISO/IEC 27001:2022 - Sistemi di gestione per la sicurezza delle informazioni (per comprensione integrazione)
- ISO/IEC 17065:2012 - Requisiti per organismi di certificazione di prodotti, processi e servizi (per contesto certificazione)

**Documenti CPF di Supporto:**

- The Cybersecurity Psychology Framework - Tassonomia completa con tutti 100 indicatori
- CPF-27002:2025 - Codice di Pratica (quando disponibile)
- Schema Certificazione CPF - Requisiti certificazione professionale e percorsi
- Field Kit Library - Tutti 100 field kit indicatori (fondamentale, operativo, field kit per ciascuno)

**D.2 Strumenti e Template Audit****Strumenti Pianificazione:**

- Template Pianificazione Audit (formato completo con tutti requisiti ISO 19011)
- Foglio di Lavoro Valutazione Rischio (specifico CPF-27001 con livelli rischio dominio)
- Matrice Criteri Selezione Team (strumento matching competenze)
- Template Lista Richiesta Documenti (clausola-per-clausola per CPF-27001)
- Template Email Comunicazione Pre-Audit (formati standard professionali)

**Strumenti Esecuzione:**

- Template Agenda Riunione Apertura
- Checklist Audit CPF-27001 (clausola-per-clausola con requisiti specifici)
- Banca Domande Colloquio (organizzata per clausola e ruolo)
- Guida Osservazione (cosa osservare per CPF-27001)
- Template Registro Prove (con caratteristiche qualità tracking)
- Foglio di Lavoro Piano Campionamento (con calcoli dimensione campione)
- Template Modulo Finding (tutti elementi richiesti con guida)
- Template Agenda Riunione Team Giornaliera
- Template Presentazione Riunione Chiusura

**Strumenti Reporting:**

- Template Report Audit (struttura completa con sezioni)
- Template Tabella Sintesi Findings
- Albero Decisionale Classificazione NC (aiuto visivo)
- Template Documentazione Osservazioni
- Template Sintesi Esecutiva (formato 1-2 pagine)
- Checklist Revisione Qualità (criteri revisione completi)

**Strumenti Chiusura:**

- Template Revisione Piano Azione Correttiva
- Template Piano Verifica (metodi, programma, requisiti evidenza)
- Template Valutazione Efficacia (criteri, indicatori, valutazione)
- Checklist Decisione Chiusura
- Checklist Chiusura File Audit

**D.3 Scenari Audit Simulati**

Tre scenari audit realistici completi forniti per formazione:

**Scenario 1: Midwest Regional Bank**

- Organizzazione: Banca regionale, 150 dipendenti, cerca certificazione Livello 2
- Contesto: ISO 27001 esistente, primo audit CPF, industria servizi finanziari
- Complessità: Media - alcuni elementi PVMS implementati, preparazione mista

- Problemi: Lacune parametri privacy, documentazione competenza incompleta, ritardi trattamento rischio
- Uso: Simulazione audit simulato Modulo 3 (4 ore)

### **Scenario 2: HealthTech Solutions**

- Organizzazione: Azienda tecnologia sanitaria, 80 dipendenti, cerca certificazione Livello 1
- Contesto: Nessun ISMS esistente, nuovo a CPF, industria sanitaria con considerazioni HIPAA
- Complessità: Inferiore - implementazione base, fase apprendimento
- Problemi: Lacune metodologia assessment, integrazione poco chiara, procedure privacy base
- Uso: Esercizi pratica, formazione team, calibrazione auditor

### **Scenario 3: TechCorp Inc**

- Organizzazione: Azienda servizi tecnologia, 300 dipendenti, cerca certificazione Livello 3
- Contesto: Livello 2 certificato esistente (18 mesi), ISMS maturo, PVMS sofisticato
- Complessità: Alta - implementazione avanzata, alcuni problemi complessi, cambiamento organizzativo
- Problemi: Lacune monitoraggio stato convergente, domande implementazione privacy avanzata, sfide cultura
- Uso: Esame pratico finale (8 ore)

### **Componenti Scenario (ciascuno):**

- Background organizzazione e contesto industria (3-5 pagine)
- Documentazione PVMS completa (20-40 pagine dipendente maturità)
- Profili personale chiave e organigrammi
- Report audit precedenti se applicabile
- Dettagli facility e operativi
- Conformità e non conformità intenzionali attraverso clausole
- Risposte colloqui scripted per role-player
- Rubriche valutazione per valutazione istruttore



## **D.4 Risorse Video e Multimediali**

### **Modulo 1 - Fondamenti Audit:**

- Panoramica Principi ISO 19011 (8 min)
- Walkthrough Clausole CPF-27001 (15 min)
- Discussione Competenze Auditor (6 min)
- Etica in Audit Vulnerabilità Psicologica (10 min)

### **Modulo 2 - Pianificazione Audit:**

- Dimostrazione Pianificazione Basata Rischio (7 min)
- Comunicazione Efficace Auditee (5 min)
- Best Practice Revisione Documentale (8 min)

### **Modulo 3 - Esecuzione Audit:**

- Riunione Apertura - Esempio Efficace (12 min)
- Riunione Apertura - Esempio Inefficace per Discussione (8 min)
- Tecniche Colloquio - Esempi Buoni e Poveri (15 min)
- Sensibilità Psicologica in Audit (10 min)
- Riunione Chiusura - Esempio Efficace (15 min)
- Gestione Situazioni Audit Difficili (12 min)

### **Modulo 4 - Reporting Audit:**

- Tecniche Scrittura Oggettiva (8 min)
- Errori Comuni Scrittura Report (6 min)
- Walkthrough Processo Revisione Qualità (10 min)

### **Modulo 5 - Follow-Up e Chiusura:**

- Metodi Verifica Efficaci (8 min)
- Approcci Valutazione Efficacia (7 min)
- Miglioramento Continuo da Audit (6 min)

**Totale multimediali: 3 ore integrate attraverso corso**

## **E Linee Guida Istruttore**

### **E.1 Qualifiche Istruttore**

#### **Requisiti Minimi:**

- Certificazione CPF Auditor attuale in regola
- Minimo 5 anni esperienza audit (almeno 2 anni come CPF Auditor o equivalente)
- Minimo 100 giorni audit esperienza documentata
- Esperienza lead auditor su minimo 20 audit
- Esperienza erogazione formazione (minimo 40 ore tempo didattico)
- Certificazione istruttore CPF-101 e CPF-201 (o concorrente con CPF-401)

#### **Qualifiche Preferite:**

- Laurea Magistrale in Psicologia, Comportamento Organizzativo, o campo correlato
- Formazione ed esperienza Lead Auditor ISO 19011 oltre CPF
- Esperienza audit multi-industria (dimostra ampiezza)
- Esperienza sviluppo formazione
- Lavori pubblicati o presentazioni su audit o CPF

### **E.2 Approccio Didattico**

#### **Principi Apprendimento Adulti:**

- Rispettare esperienza professionale partecipanti (molti hanno background audit)
- Collegare contenuti a situazioni audit mondo reale
- Bilanciare lezione con esercizi interattivi (40% lezione, 60% interattivo)
- Fornire immediate opportunità applicazione pratica
- Facilitare apprendimento peer e discussione
- Adattare ritmo a bisogni partecipanti mantenendo programma

#### **Strategie Coinvolgimento:**

- Usare scenari realistici throughout (non esempi accademici artificiosi)
- Incorporare esperienze audit reali (anonimizzate) per discussione
- Incoraggiare domande e dibattito professionale
- Creare ambiente psicologicamente sicuro per pratica abilità
- Fornire feedback costruttivo su esercizi

- Riconoscere complessità e ambiguità in situazioni audit
- Modellare comportamenti auditor professionali in tutte interazioni

### **Gestione Tempo:**

- Rispetto stretto tempistica modulo (40 ore è intensivo)
- Costruire 10% buffer in ogni modulo per overflow (incluso in tempi)
- Usare "parcheggio" per discussioni tangenziali ma rilevanti (affrontare durante pause o fine giornata)
- Monitorare tempi completamento esercizi e aggiustare se necessario
- Prioritarizzare esercizi pratici su lezioni estese se tempo pressato
- Assicurare audit simulato e esame finale ricevano pieno tempo allocato (non negoziabile)

## **E.3 Suggerimenti Facilitazione per Modulo**

### **Modulo 1 - Fondamenti Audit:**

- Enfatizzare CPF-27001 differisce da audit ISO 27001 (sensibilità psicologica)
- Usare casi etica per generare discussione e auto-riflessione
- Riconoscere disagio alcuni possono sentire con aspetti psicologici
- Stabilire indipendenza come principio non negoziabile da inizio

### **Modulo 2 - Pianificazione Audit:**

- Enfatizzare qualità pianificazione determina qualità audit
- Usare pensiero basato rischio throughout (non solo audit check-the-box)
- Esercizio scenario sanitario richiede tempo significativo - non fretta
- Dimostrare multiple approcci pianificazione accettabili (nessun singolo modo "giusto")

### **Modulo 3 - Esecuzione Audit:**

- Questo è modulo più lungo (12 ore) - dosare attentamente
- Simulazioni colloquio critiche - assicurare tutti partecipanti praticano
- Audit simulato è pezzo centrale - allocare piene 4 ore senza interruzione
- Debriefing audit simulato approfonditamente - ricca opportunità apprendimento
- Enfatizzare sensibilità psicologica throughout senza compromettere rigore audit

### **Modulo 4 - Reporting Audit:**

- Qualità scrittura varia tra partecipanti - fornire feedback individuale

- Decisioni classificazione generano dibattito - facilitare professionalmente
- Usare esempi report reali (buoni e che necessitano miglioramento) estesamente
- Revisione qualità può sembrare noiosa ma enfatizzare importanza

### **Modulo 5 - Follow-Up e Chiusura:**

- Esercizi revisione PAC emergono comuni incomprensioni - affrontare approfonditamente
- Esame pratico finale è completo - istruzioni chiare critiche
- Fornire ambiente supportivo per esame finale mantenendo rigore valutazione
- Feedback dopo esame finale dovrebbe essere di sviluppo e incoraggiante

## **E.4 Gestione Situazioni Difficili**

### **Sfide Partecipanti:**

- Partecipante eccessivamente confidente che domina discussioni - riconoscere esperienza, invitare altri, reindirizzare privatamente se necessario
- Partecipante che lotta con concetti psicologici - fornire risorse aggiuntive, accoppiare con peer più forte per esercizi, offrire supporto post-classe
- Disaccordo su classificazione o approccio audit - facilitare dibattito professionale, riconoscere differenze legittime, chiarire quando standard richiede approccio specifico vs giudizio professionale
- Ansia partecipante su esame finale - normalizzare ansia, rivedere strategie preparazione, enfatizzare scopo di sviluppo non punitivo
- Partecipante che fallisce esercizi o esami - fornire feedback specifico, sviluppare piano rimedio, mantenere empatia professionale

### **Sfide Logistiche:**

- Fallimenti tecnologia - avere materiali backup (slide stampate, video offline), mantenere flessibilità
- Partecipanti assenti - fornire materiali per self-study, richiedere dimostrazione make-up competenza
- Sforamenti tempo - prioritarizzare esercizi pratici, comprimere lezione se necessario, estendere giornata se fattibile e partecipanti d'accordo
- Facility inadeguate - adattare esercizi a vincoli, comunicare impatti a coordinatore formazione

## F Strategie Successo Partecipanti

### F.1 Preparazione Pre-Corso

#### **Preparazione Raccomandata (2-3 settimane prima corso):**

- Rivedere ISO 19011:2018 (al minimo leggere Clausole 1-7)
- Rileggere CPF-27001:2025 approfonditamente (dovrebbe essere familiare da lavoro CPF Assessor)
- Rivedere materiali CPF-101 (rinfrescare conoscenza fondazionale)
- Rivedere propri report assessment CPF (riflettere su metodologia e qualità)
- Preparare domande su sfide audit incontrate in pratica
- Assicurare prerequisiti meeting (certificazione CPF Assessor attuale, 10+ assessment completati)

#### **Materiali da Portare:**

- Laptop con capacità word processing (per esercizi e esame finale)
- Copie ISO 19011:2018 e CPF-27001:2025 (stampate o elettroniche)
- Esempi propri assessment CPF (anonimizzati) per riferimento
- Taccuino per note aggiuntive oltre workbook
- Abbigliamento business professionale per presentazione esame finale

### F.2 Suggerimenti Successo Durante Corso

#### **Coinvolgimento:**

- Partecipare attivamente tutti esercizi (apprendere facendo è critico per abilità audit)
- Chiedere domande quando concetti poco chiari (meglio in classe che durante audit reale)
- Condividere esperienze professionali per arricchire discussioni (anonimizzate)
- Praticare sensibilità psicologica in tutti role-plays (costruisce memoria muscolare)
- Collaborare con colleghi (audit è attività team, costruire relazioni)
- Prendere seriamente audit simulato e esame finale (miglior predittore performance audit reale)

#### **Gestione Tempo:**

- Arrivare in orario ogni giorno (presenza tracciata per certificazione)
- Usare pause produttivamente (rivedere note, preparare per sezione successiva, network con colleghi)
- Gestire energia (40 ore intensive, mantenere focus e stamina)

- Completare esercizi dentro tempo allocato (costruisce abilità efficienza audit)
- Non procrastinare preparazione esame finale (inizia da Modulo 1)

#### **Strategie Apprendimento:**

- Collegare nuovi concetti a precedente esperienza audit o assessment
- Usare template e strumenti forniti (non reinventare, adattare approcci provati)
- Praticare scrittura findings giornalmente (abilità costruisce con ripetizione)
- Rivedere contenuto giornata stessa sera (rinforza apprendimento)
- Identificare aree sviluppo personali presto e focalizzare su miglioramento
- Cercare feedback istruttore su esercizi (valutazione formativa supporta apprendimento)

### **F.3 Sviluppo Post-Corso**

#### **Azioni Immediate (entro 1 settimana):**

- Rivedere materiali corso e note personali
- Organizzare strumenti e template audit per uso futuro
- Riflettere su punti di forza e aree sviluppo identificate
- Pianificare primo audit reale o partecipazione audit supervisionato
- Rivedere risultati esame scritto e affrontare lacune conoscenza
- Rivedere feedback esame pratico finale e sviluppare piano miglioramento

#### **Sviluppo Continuo (ongoing):**

- Partecipare ad audit regolarmente (minimo 15 giorni audit/anno per recertificazione)
- Cercare opportunità lead auditor quando pronti
- Richiedere feedback da clienti audit e membri team
- Rimanere aggiornati con aggiornamenti metodologia CPF
- Guadagnare crediti CPE richiesti (50/anno per auditor)
- Impegnarsi con comunità auditor CPF per apprendimento peer
- Considerare contribuire a sviluppo CPF (ricerca, case study, formazione)

## **G Controllo Documentale**

### **G.1 Cronologia Versioni**

Versione	Data	Cambiamenti
0.1	Dicembre 2024	Bozza iniziale outline
0.5	Gennaio 2025	Sviluppo contenuto completo
1.0	Gennaio 2025	Revisione finale e approvazione per release

## G.2 Revisione e Approvazione

**Proprietario Documento:** Sviluppo Formazione CPF3

**Revisione Tecnica:**

- Giuseppe Canale, CISSP - Autore Quadro CPF
- Panel CPF Auditor - Tre CPF Auditors certificati (programma pilota)
- Revisore Esperto ISO 19011
- Quality Manager Organismo Certificazione

**Autorità Approvazione:** Giuseppe Canale, CISSP (Direttore CPF3)

**Data Approvazione:** Gennaio 2025

## G.3 Programma Revisione

**Revisione Regolare:**

- Revisione annuale seguendo cicli erogazione corso
- Revisione maggiore ogni 3 anni o quando CPF-27001 aggiornato
- Miglioramento continuo basato su feedback partecipanti e performance esame
- Prossima revisione programmata: Gennaio 2026

**Trigger per Revisione Non Programmata:**

- Revisione o emendamento standard CPF-27001
- Aggiornamento standard ISO 19011
- Cambiamenti significativi requisiti organismo certificazione
- Pattern difficoltà partecipanti che indicano problemi contenuto
- Nuova ricerca o best practices in metodologia audit
- Cambiamenti regolatori o legali che influenzano requisiti auditor

## G.4 Gestione Cambiamenti

**Cambiamenti Minori (nessun incremento versione):**

- Correzioni tipografiche
- Chiarificazione contenuto esistente senza cambiamento sostanziale
- Esempi aggiornati mantenendo stessi principi
- Miglioramenti formattazione
- Registrato in log cambiamenti, nessuna redistribuzione richiesta

**Cambiamenti Maggiori (incremento versione):**

- Aggiunta o rimozione moduli contenuto
- Cambiamenti significativi obiettivi apprendimento o valutazione
- Aggiornamenti per allineare con revisioni standard
- Ristrutturazione flusso corso o tempistica
- Cambiamenti a requisiti esame
- Richiede revisione tecnica, approvazione, redistribuzione

**G.5 Distribuzione****Destinatari Autorizzati:**

- Tutti istruttori CPF-401 approvati (attuali e in-training)
- Team sviluppo formazione CPF3
- Organismi certificazione autorizzati erogare CPF-401
- Personale assurance qualità e revisione tecnica CPF3

**Riservatezza:**

- Questo blueprint è proprietario di CPF3
- Distribuzione ristretta a personale autorizzato solo
- Non per release pubblica (materiali corso derivati da blueprint possono essere pubblici)
- Contiene informazioni sviluppo esame che richiedono protezione
- Destinatari devono mantenere riservatezza per accordo

**Accesso:**

- Versione elettronica: Portale formazione sicuro CPF3
- Controllo versione: Aggiornamenti automatici a utenti autorizzati
- Archivio: Versioni precedenti mantenute per 5 anni
- Copie stampate: Distribuzione controllata con tracking

**H Bibliografia****H.1 Standard e Riferimenti Normativi****References**

- [1] ISO 19011:2018, *Linee guida per l'audit di sistemi di gestione*. International Organization for Standardization.



- [2] CPF-27001:2025, *Sistema di Gestione della Vulnerabilità Psicologica - Requisiti*. Organizzazione CPF3.
- [3] ISO/IEC 27001:2022, *Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti*. International Organization for Standardization.
- [4] ISO/IEC 17065:2012, *Valutazione della conformità - Requisiti per organismi che certificano prodotti, processi e servizi*. International Organization for Standardization.
- [5] NIST (2024). *Cybersecurity Framework 2.0*. National Institute of Standards and Technology.

## H.2 Riferimenti Quadro CPF

### References

- [1] Canale, G. (2025). *The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences*. Preprint.
- [2] CPF3 (2025). *Schema Certificazione CPF Versione 1.0*. Organizzazione CPF3.
- [3] CPF-27002:2025, *Gestione Vulnerabilità Psicologica - Codice di Pratica*. Organizzazione CPF3. (In sviluppo)
- [4] CPF3 (2025). *CPF Field Kit Library - Collezione Completa di 100 Kit Indicatori*. Organizzazione CPF3.

## H.3 Riferimenti Psicologia Fondazionale

### References

- [1] Bion, W. R. (1961). *Esperienze nei Gruppi*. Londra: Tavistock Publications.
- [2] Klein, M. (1946). Note su alcuni meccanismi schizoidi. *International Journal of Psychoanalysis*, 27, 99-110.
- [3] Jung, C. G. (1969). *Gli Archetipi e l'Inconscio Collettivo*. Princeton: Princeton University Press.
- [4] Kahneman, D. (2011). *Pensieri lenti e veloci*. New York: Farrar, Straus and Giroux.
- [5] Cialdini, R. B. (2007). *Influenza: La Psicologia della Persuasione*. New York: Collins.
- [6] Milgram, S. (1974). *Obbedienza all'Autorità*. New York: Harper & Row.

## H.4 Riferimenti Metodologia Audit

### References

- [1] Russell, J. P. (Ed.). (2013). *The ASQ Auditing Handbook* (4th ed.). Milwaukee: ASQ Quality Press.

- [2] Arter, D. R. (2003). *Quality Audits for Improved Performance* (3rd ed.). Milwaukee: ASQ Quality Press.
- [3] Mills, D. (2016). *Quality Auditing: An Introduction*. London: Routledge.
- [4] Karapetrovic, S., & Willborn, W. (2010). Audit system: Concepts and practices. *Total Quality Management*, 12(1), 13-28.

## I Istruzioni Utilizzo

### I.1 Per Sviluppatori Corso

Questo blueprint abilita sviluppo sistematico materiali corso:

#### **Workflow Generazione Slide:**

1. Selezionare modulo da Sezione 2 (Strutture Moduli)
2. Revisionare panoramica modulo, obiettivi apprendimento, outline contenuti
3. Riferirsi a suddivisione slide per slide specifica (Sezione 2.X Suddivisione Slide)
4. Usare outline contenuti per sviluppare contenuto slide
5. Includere note insegnamento da sezione "Metodi Insegnamento"
6. Riferirsi a materiali necessari per contenuto supporto
7. Incorporare esercizi a punti specificati
8. Generare elementi valutazione usando guida sezione valutazione

#### **Workflow Sviluppo Esercizi:**

1. Identificare esercizio da Appendice B (Sintesi Banca Esercizi)
2. Revisionare descrizione esercizio e allocazione tempistica
3. Sviluppare scenario realistico o materiali
4. Creare istruzioni partecipante chiaramente
5. Sviluppare rubrica valutazione da sezione elementi valutazione
6. Testare esercizio con gruppo pilota
7. Affinare basato su tempistica e efficacia apprendimento
8. Documentare note facilitatore per istruttori

#### **Workflow Sviluppo Valutazione:**

1. Revisionare Appendice C (Blueprint Esame) per requisiti
2. Sviluppare domande allineate a distribuzione contenuto
3. Assicurare distribuzione livello cognitivo appropriata

4. Test pilota domande con piccolo gruppo
5. Condurre analisi item per difficoltà e discriminazione
6. Affinare domande basate su analisi statistica
7. Mantenere banca domande con metadata
8. Ciclo revisione e aggiornamento regolare

## **I.2 Per Istruttori**

Questo blueprint supporta efficace erogazione corso:

### **Preparazione:**

1. Revisionare blueprint completo prima prima erogazione
2. Studiare tutti cinque moduli in profondità
3. Familiarizzare con tutti esercizi e scenari
4. Praticare facilitazione audit simulato
5. Revisionare tutte rubriche valutazione
6. Preparare esempi personali per discussione
7. Allestire ambiente apprendimento per requisiti

### **Erogazione:**

1. Seguire struttura modulo e linee guida tempistica
2. Usare sezione "Metodi Insegnamento" per ogni modulo
3. Incorporare "Linee Guida Istruttore" (Appendice D) throughout
4. Facilitare esercizi per descrizioni Banca Esercizi
5. Applicare raccomandazioni "Suggerimenti Facilitazione per Modulo"
6. Gestire tempo strettamente (40 ore è intensivo)
7. Fornire feedback usando rubriche valutazione
8. Documentare lessons learned per miglioramento continuo

## **I.3 Per Partecipanti**

Questo blueprint informa preparazione partecipante:

### **Prima Corso:**

- Revisionare "Strategie Successo Partecipanti" (Appendice E)
- Completare raccomandazioni preparazione pre-corso
- Assicurare prerequisiti meeting e documentati

- Raccogliere materiali richiesti
- Preparare domande da esperienza audit pratica

**Durante Corso:**

- Seguire strategie coinvolgimento
- Partecipare pienamente tutti esercizi
- Prendere seriamente audit simulato e esame finale
- Cercare feedback su aree sviluppo
- Costruire rete peer per futura collaborazione

**Dopo Corso:**

- Rivedere raccomandazioni sviluppo post-corso
- Applicare apprendimento in audit supervisionati
- Mantenere requisiti CPE
- Impegnarsi con comunità auditor
- Contribuire a sviluppo CPF

## **J Informazioni Contatto**

### **J.1 Richieste Formazione**

#### **Sviluppo Formazione CPF3**

Sito web: <https://cpf3.org/training>

Email: [training@cpf3.org](mailto:training@cpf3.org)

Telefono: +39 [da determinare]

### **J.2 Domande Certificazione**

#### **Organismo Certificazione CPF**

Sito web: <https://cpf3.org/certification>

Email: [certification@cpf3.org](mailto:certification@cpf3.org)

### **J.3 Supporto Tecnico**

#### **Domande Tecniche Quadro CPF**

Email: [technical@cpf3.org](mailto:technical@cpf3.org)

## J.4 Feedback Corso

### Feedback e Suggerimenti Partecipanti

Email: [feedback@cpf3.org](mailto:feedback@cpf3.org)

Sondaggio: Disponibile fine corso e via portale formazione

---

## CPF-401: Piano di Formazione Tecniche di Audit

*Versione 1.0 - Gennaio 2025*

*Preparando CPF Auditors Competenti per Eccellenza Professionale*

© 2025 Organizzazione CPF3. Tutti i diritti riservati.

Questo documento è proprietario e confidenziale.

Distribuzione non autorizzata è vietata.

---