CPF Audit Guidelines

Version 1.0

Auditing Psychological Vulnerability Management Systems

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

January 2025

Abstract

This document provides practical guidance for conducting conformity audits against CPF-27001:2025 requirements. Unlike traditional technical security audits, CPF audits require specialized competencies spanning cybersecurity, psychology, privacy law, and audit methodology. The guide establishes privacy-preserving audit techniques that verify organizational psychological vulnerability management without individual profiling. Key differentiators include aggregated evidence collection (minimum n=10), differential privacy verification ($\varepsilon \leq 0.1$), trauma-informed interview protocols, and ethical frameworks that treat psychological vulnerabilities as systemic organizational issues rather than individual failures. The methodology integrates with ISO 19011:2018 while addressing unique challenges of auditing pre-cognitive processes and unconscious group dynamics.

Contents

1 Introduction

1.1 Purpose and Scope

The CPF Audit Guidelines provide systematic methodology for evaluating organizational conformity to CPF-27001:2025 Psychological Vulnerability Management System (PVMS) requirements. This document addresses the unique challenges of auditing human factors in cybersecurity while maintaining rigorous privacy protections and ethical standards.

Intended Audience:

- Third-party certification auditors conducting CPF-27001 audits
- Internal auditors implementing PVMS assurance programs
- Audit program managers designing CPF audit methodologies
- Organizations preparing for CPF-27001 certification

Scope Boundaries:

In Scope:

- Conformity assessment against CPF-27001:2025 requirements
- Privacy-preserving evidence collection techniques
- Psychological vulnerability indicator verification
- PVMS integration with existing ISMS (ISO 27001)
- Organizational maturity level assessment

Out of Scope:

- Individual psychological assessment or clinical evaluation
- Employee performance appraisal or disciplinary processes
- Technical security control effectiveness testing
- Penetration testing or vulnerability scanning
- Social engineering simulation design

1.2 Relationship to Other Standards

ISO 19011:2018 Integration:

CPF audits follow ISO 19011:2018 Guidelines for Auditing Management Systems as foundational methodology, with CPF-specific enhancements for psychological vulnerability auditing.

CPF Document Ecosystem:

- **CPF-27001:2025 Requirements**: Normative standard (Clauses 4-10)
- **CPF Scoring and Maturity Model**: Mathematical verification framework

- **CPF Field Kits**: Operational indicator assessment tools
- **The Cybersecurity Psychology Framework**: Theoretical foundation

Complementary Standards:

- **ISO/IEC 27001:2022**: ISMS integration points
- **ISO/IEC 27006:2015**: Requirements for certification bodies
- **GDPR/Privacy Regulations**: Legal compliance framework

1.3 How to Use This Document

For Lead Auditors:

1. Review Section 1 for CPF audit differentiators
2. Apply Section 2 for risk-based audit planning
3. Use Section 3 for privacy-preserving evidence collection
4. Reference Section 4 for scoring verification
5. Follow Section 6 for compliant reporting

For Organizations:

- Understand auditor expectations and evidence requirements
- Prepare documentation per Section 2 guidance
- Ensure privacy controls meet Section 3 standards
- Self-assess using Section 4 verification methods

Document Navigation:

- **Quick Reference**: Appendix checklists for rapid assessment
- **Detailed Methodology**: Main sections for comprehensive understanding
- **Examples**: Case studies throughout for practical application

2 CPF Audit Differentiators

2.1 Unique Competency Requirements

CPF auditing requires interdisciplinary expertise beyond traditional security auditing. Auditors must integrate knowledge from four distinct domains:

2.1.1 Cybersecurity Fundamentals

Required Knowledge:

- ISO/IEC 27001:2022 ISMS requirements and audit methodology
- Common attack vectors (phishing, social engineering, insider threats)
- Security awareness program evaluation techniques
- Incident response and security operations concepts
- Risk assessment and treatment methodologies

Typical Background: CISSP, CISM, ISO 27001 Lead Auditor certification

2.1.2 Psychological Theory and Practice

Required Knowledge:

- **Psychoanalytic Concepts**: Bion's basic assumptions, Klein's object relations, Jung's shadow/collective unconscious
- **Cognitive Psychology**: Kahneman's dual-process theory, cognitive biases, heuristics
- **Social Psychology**: Cialdini's influence principles, conformity, obedience studies
- **Group Dynamics**: Groupthink, risky shift, diffusion of responsibility
- **Stress Physiology**: Fight/flight/freeze/fawn responses, cortisol effects

Typical Background: Psychology degree, psychoanalytic training, or equivalent structured education (minimum 40 hours CPF-specific training)

2.1.3 Privacy Law and Ethics

Required Knowledge:

- GDPR Articles 5 (data minimization), 9 (special categories), 32 (security)
- Differential privacy mathematical principles (ε-privacy)
- Aggregation and anonymization techniques
- Informed consent requirements for psychological data
- Data protection impact assessment (DPIA) methodology

Typical Background: CIPP/E certification, legal training, or privacy officer experience

2.1.4 Audit Methodology

Required Knowledge:

- ISO 19011:2018 auditing principles and practices
- Sampling theory and statistical validity
- Evidence evaluation and finding classification
- Interview techniques and observation methods
- Report writing and nonconformity documentation

Typical Background: ISO 27001 Lead Auditor or equivalent management system auditor certification

2.2 Ethical Framework for Psychological Auditing

CPF audits operate under a distinct ethical framework that differs fundamentally from technical security audits.

2.2.1 Organizational Focus Principle

Core Tenet: Psychological vulnerabilities are systemic organizational characteristics, NOT individual deficiencies.

Practical Implications:

- Findings describe organizational patterns, never individual behaviors
- Interview data aggregated to minimum n=10 before analysis
- No linkage between assessment results and performance management
- Vulnerable states framed as normal human responses to conditions

Prohibited Practices:

- Identifying specific individuals as "high-risk" or "vulnerable"
- Providing individual feedback or recommendations
- Sharing disaggregated data with management
- Using psychological assessment for hiring/promotion decisions

2.2.2 Non-Maleficence Principle

Core Tenet: Audit process must not harm psychological safety or organizational trust.

Practical Implications:

- Trauma-informed interviewing (see Section 3.3)

- Managing organizational anxiety about psychological assessment
- Transparent communication about audit purpose and data use
- Respecting cultural differences in psychological norms

Pre-Audit Communication:

- Clear explanation that audit assesses organizational systems, not individuals
- Guarantee of anonymity and aggregation
- Right to decline participation without consequence
- Psychological support resources available if audit triggers distress

2.2.3 Justice and Fairness Principle

Core Tenet: Audit methodology must not discriminate or create disparate impact.

Practical Implications:

- Cultural sensitivity in interpreting psychological indicators
- Avoiding pathologization of non-Western psychological patterns
- Recognizing that "vulnerability" may reflect organizational failures, not individual weakness
- Ensuring diverse representation in sampling

2.3 Trauma-Informed Approach

CPF audits adopt trauma-informed principles recognizing that security incidents and organizational stress create trauma responses.

2.3.1 Safety First

Physical and Psychological Safety:

- Private interview spaces without surveillance
- Clear boundaries around confidentiality
- Auditor introduces themselves and explains role
- Interviewee controls pace and depth of discussion

2.3.2 Trustworthiness and Transparency

Building Trust:

- Explain audit process and timeline upfront
- Clarify how data will and will NOT be used
- Share sample questions in advance
- Provide written summary of discussion

2.3.3 Peer Support

Recognizing Shared Experience:

- Frame vulnerabilities as universal human characteristics
- Acknowledge that auditor would respond similarly in same conditions
- Avoid "expert-victim" dynamic
- Validate emotional responses to security stressors

2.3.4 Collaboration and Mutuality

Partnership Approach:

- Invite organizational input on audit plan
- Collaborative problem-solving for identified gaps
- Recognize organization's expertise in their own culture
- Joint development of corrective action plans

2.3.5 Empowerment and Choice

Respecting Autonomy:

- Participants can skip questions or end interview
- Organization chooses timing and sampling approach (within standards)
- Findings presented as opportunities, not judgments
- Organization controls implementation of recommendations

2.4 Integration with ISO 19011:2018

CPF audits extend ISO 19011 principles with psychological-specific guidance:

2.5 Managing Organizational Anxiety

The audit process itself can trigger organizational anxiety and defensive responses. Skilled auditors recognize and address these dynamics.

2.5.1 Common Anxiety Manifestations

Pre-Audit Phase:

- Excessive preparation and "staging" of evidence
- Coaching employees on "correct" responses

Table 1: ISO 19011 Extensions for CPF Audits

ISO 19011 Principle	Standard Application	CPF Extension
Integrity	Honest, truthful reporting	No individual profiling, aggregation enforcement
Fair Presentation	Accurate findings	Trauma-informed language, non-pathologizing
Due Professional Care	Diligence and judgment	Privacy protection, psychological safety
Confidentiality	Secure information	Enhanced anonymization, differential privacy
Independence	Impartiality	No dual role as therapist/counselor
Evidence-Based	Verifiable information	Triangulated data, statistical validity
Risk-Based	Focus on significant risks	Convergence Index, psychological risk scoring

- Attempts to control auditor access or schedule
- Rationalization that "we're different" or "this doesn't apply"

During Audit:

- Defensive reactions to questions
- Minimization of identified vulnerabilities
- Projection of blame onto external factors
- Over-compliance and eagerness to please

2.5.2 Anxiety Management Techniques

Normalization:

- "Every organization has psychological vulnerabilities"
- "We're looking at systems, not judging people"
- "These are normal responses to stressful conditions"

Reframing:

- "Identifying vulnerabilities is the first step to improvement"
- "Your openness enables us to provide valuable insights"
- "This assessment protects your organization and employees"

Containing Anxiety:

- Predictable schedule and clear milestones
- Regular brief-backs to reduce uncertainty
- Calm, professional demeanor modeling
- Acknowledging positive findings alongside gaps

3 Audit Planning

3.1 Pre-Audit Activities

3.1.1 Document Review

Required Documents (Request Minimum 14 Days Before On-Site):

PVMS Documentation:

- CPF Policy (management commitment, scope definition)
- CPF Scope Statement (boundaries, exclusions, organizational units)
- Risk Assessment Methodology (100-indicator assessment approach)
- CPF Score Calculation Worksheets (most recent assessment)
- Privacy Protection Procedures (aggregation, differential privacy, temporal delay)
- Risk Treatment Plans (interventions for Yellow/Red indicators)

Integration Documentation:

- ISMS Policy and Scope (ISO 27001 if applicable)
- Organizational Chart (reporting structures, team sizes)
- Incident Reports (past 12 months, human-factor incidents)
- Security Awareness Program Materials (training content, attendance records)

Evidence of Operation:

- Management Review Minutes (past 2 reviews)
- Internal Audit Reports (if PVMS internal audit conducted)
- Corrective Action Records (nonconformity tracking)
- Monitoring and Measurement Records (KPI tracking)

Document Review Checklist:

☐ CPF Score calculation mathematically correct (verify per Scoring Model)

☐ All 10 domains assessed with documented methodology

☐ Privacy protections documented (n$\geq$10, $\varepsilon \leq 0.1$, 72hr delay)

☐ Integration with ISMS clearly defined

☐ Management commitment evidenced (resources, policy approval)

☐ Competence requirements defined for CPF roles

☐ Risk treatment plans address identified vulnerabilities

3.1.2 Resource Allocation

Audit Team Composition:

Minimum team for comprehensive CPF-27001 audit:

- **Lead Auditor**: CPF Lead Auditor certified, psychology background preferred
- **Technical Auditor**: Cybersecurity expertise (CISSP/CISM level)
- **Privacy Specialist**: GDPR/privacy law expertise (can be Lead if qualified)

Time Allocation (Typical Mid-Size Organization, 250-500 employees):

Table 2: Audit Time Budget

Activity	Days	Auditor-Days
Document Review (off-site)	-	1.5
Opening Meeting	0.5	1.5
Management Interviews	0.5	1.5
Documentation Verification	1.0	3.0
Staff Interviews (aggregated)	1.0	3.0
System/Process Observation	1.0	3.0
Score Recalculation	0.5	1.5
Privacy Controls Testing	0.5	1.5
Team Deliberation	0.5	1.5
Closing Meeting	0.5	1.5
Total On-Site	**5.0**	**19.0**
Report Writing (off-site)	-	2.0
Total Audit	-	**22.5**

Scaling Factors:

- Small (¡100 employees): 0.6x multiplier → 13.5 auditor-days
- Large (500-2000 employees): 1.5x multiplier → 33.8 auditor-days
- Very Large (¿2000 employees): 2.0x multiplier → 45 auditor-days
- Multi-site: +0.5 days per additional site
- Crisis audit: +1.0 day for incident analysis

3.1.3 Communication Protocol

Pre-Audit Communication (3-4 Weeks Before):

To Executive Management:

- Audit purpose: Assess PVMS conformity to CPF-27001:2025
- Scope and methodology overview
- Required resources (meeting rooms, staff availability)

- Privacy protections: No individual profiling, aggregated reporting only
- Expected deliverables and timeline

To All Staff (via organization):

- Announcement of upcoming audit
- Emphasis on organizational assessment, NOT individual evaluation
- Voluntary participation in interviews
- Confidentiality and anonymization guarantees
- Contact information for questions/concerns

Sample Staff Communication:

> *"Our organization is undergoing a CPF-27001 audit to assess how well we manage psychological factors in cybersecurity. This is NOT an evaluation of individual employees. Auditors will analyze organizational patterns using aggregated, anonymous data. If selected for an interview, participation is voluntary. All responses are confidential and will be combined with at least 10 others before analysis. This assessment helps us create a safer, less stressful security environment for everyone."*

3.2 Risk-Based Approach

3.2.1 Audit Focus Determination

CPF audits prioritize domains with highest risk based on:

1. **CPF Score Analysis**: Focus on domains with Red indicators (score 14-20/20)
2. **Convergence Index**: Investigate domains contributing to high CI values (>5)
3. **Incident History**: Domains correlated with past security incidents
4. **Organizational Context**: Industry-specific vulnerabilities (e.g., healthcare Authority domain)

Example Risk-Based Planning:

Organization Profile:

- Financial services sector (inherent Authority/Temporal vulnerabilities)
- Recent CEO fraud incident (Authority domain confirmed weakness)
- CPF Score: 58/100 (Fair rating)
- Domains: Authority [1.x] = 16/20 (Red), Temporal [2.x] = 14/20 (Red)

Audit Plan Adjustments:

- Allocate 40% of audit time to Authority and Temporal domains

- Deep-dive on indicators 1.1 (unquestioning compliance) and 2.1 (urgency bypass)
- Interview finance staff specifically (CEO fraud vulnerability)
- Test verification protocols for authority requests
- Verify effectiveness of implemented risk treatments

3.2.2 Sampling Strategy

Privacy-Preserving Sampling Principles:

- **Minimum Sample Size**: n $\geq$ 10 for any analyzed group
- **Representative Sampling**: Proportional to organizational demographics
- **Role-Based Stratification**: Sample across functional areas
- **Random Selection**: Avoid selection bias (organization provides roster, auditor selects)

Sample Size Calculation:

For 95% confidence level, ±10% margin of error:

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

Practical Sampling Guidelines:

Table 3: Sample Sizes by Organization Size

Organization Size	Minimum Sample	Recommended Sample
¡100 employees	20	30
100-500 employees	30	50
500-2000 employees	50	80
¿2000 employees	80	100+

Stratification Example (500-employee organization):

- Executive Management: 3 interviews (5% of sample)
- Middle Management: 8 interviews (15%)
- Technical Staff: 15 interviews (30%)
- Administrative Staff: 12 interviews (24%)
- Operations Staff: 12 interviews (26%)
- **Total: 50 interviews**

3.3 Privacy Impact Assessment for Audit

Before commencing any CPF audit, auditors must conduct a Privacy Impact Assessment (PIA) for the audit process itself.

3.3.1 Data Collection Boundaries

Permitted Data Collection:

- Aggregated behavioral patterns (n≥10)
- System logs showing collective behavior (authentication patterns, alert response times)
- Anonymous survey responses
- Group observation data (team meetings, incident response exercises)
- Role-level analysis (e.g., "finance department" not "Jane Doe")

Prohibited Data Collection:

- Individual psychological profiles or assessments
- Personally identifiable information beyond role/department
- Video/audio recordings of individuals
- Real-time monitoring of specific individuals
- Medical or health information
- Performance evaluation data

3.3.2 Consent Management

Informed Consent Requirements:

- **Written Consent Form** for interview participants covering:
  - Purpose of data collection (PVMS conformity audit)
  - Types of data collected (responses, observations)
  - Anonymization and aggregation methods (n≥10, 72hr delay)
  - Data retention period (destroyed post-audit or 3 years max)
  - Right to withdraw participation
  - Contact for questions/concerns
- **Voluntary Participation**: No penalty for declining
- **Re-consent** if audit scope changes

3.3.3 Anonymization Verification

Auditor Checklist for Privacy Protection:

☐ Interview notes contain no names (use codes: INT-001, INT-002)

☐ Quotes in report sanitized of identifying details

☐ Small group data ($n < 10$) not reported separately

☐ Demographic details generalized ("senior manager" not "VP of Finance")

☐ System logs aggregated with differential privacy noise

☐ Report reviewed for re-identification risks before delivery

3.4 Audit Program Timeline

Typical Initial Certification Audit Schedule:

Table 4: Audit Timeline

Week	Activity	Responsible
-4	Document request sent	Lead Auditor
-3	Documents received	Organization
-2	Document review complete	Audit Team
-1	Pre-audit call, staff communication	Both
1	On-site audit (5 days)	Audit Team
2	Report drafting	Lead Auditor
3	Report delivered to organization	Lead Auditor
4-6	Corrective actions (if needed)	Organization
7	Corrective action verification	Lead Auditor
8	Certificate issuance decision	Certification Body

4 Privacy-Preserving Audit Techniques

4.1 Aggregated Data Analysis

4.1.1 Minimum Aggregation Unit Enforcement

The n≥10 Rule:

No psychological assessment data may be reported or analyzed for groups smaller than 10 individuals. This is the fundamental privacy protection in CPF auditing.

Audit Verification Steps:

1. **Review Assessment Reports**: Check that all reported metrics show n≥10
2. **Test Calculation**: Request organization to demonstrate score calculation with redacted data
3. **Query Database**: If digital system used, verify database constraints prevent n<10 queries
4. **Interview Privacy Officer**: Confirm understanding and enforcement mechanisms

Common Nonconformities:

- Small department (n=7) analyzed separately → **MAJOR**: Privacy violation
- Executive team (n=5) profiled as group → **MAJOR**: Privacy violation
- Dashboard allows filtering to individual level → **CRITICAL**: System design flaw

- "Anonymous" survey results with n=3 respondents → **MAJOR**: Re-identification risk

Example Compliant Approach:

Scenario: Organization has 8-person IT security team (below n=10 threshold)

Prohibited: Report "IT Security Team" indicators separately

Compliant Options:

- Combine with broader "Technical Staff" category (n=45)
- Report at "Organizational Level" only (n=250)
- Exclude IT security team from assessment with documented justification

4.1.2 Statistical Validity Requirements

Confidence Interval Verification:

For reported CPF scores, auditors should verify statistical validity:

$$\text{Margin of Error} = Z \times \sqrt{\frac{p(1-p)}{n}} \tag{2}$$

Where:

- Z = 1.96 (95% confidence level)
- p = observed proportion
- n = sample size

Audit Test:

Select one domain score reported by organization. Verify:

- Sample size documented
- Confidence interval calculated (if claimed)
- Margin of error acceptable for decision-making

Example Verification:

Organization reports: "Authority Domain [1.x] score: 14/20 (Red), n=32"

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

Interpretation: With 95% confidence, true score is 14 ± 3.2 points (10.8-17.2 range). Still firmly in Red zone (14-20), so finding is statistically robust.

4.1.3 Chi-Square Tests for Independence

When organization claims no correlation between domains, auditors may verify using chi-square test.

Null Hypothesis: Domain scores are independent (no correlation)

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

Where O = observed frequency, E = expected frequency

Audit Application:

Test if Red indicators cluster in specific domains vs. random distribution.

4.2 Observation Methods

4.2.1 Non-Invasive Observation Principles

CPF audits rely on observation of organizational patterns, NOT surveillance of individuals.

Permitted Observation:

- Security awareness training sessions (group dynamics)
- Incident response tabletop exercises (stress response patterns)
- Security operations center workflows (cognitive load, alert fatigue)
- All-hands meetings (authority gradient, communication patterns)
- Physical security posture (access control compliance, tailgating)

Prohibited Observation:

- Individual workstation monitoring
- Email content review (metadata analysis only, aggregated)
- Video surveillance of specific individuals
- Real-time tracking of employee movements
- Covert observation without informed consent

Observation Protocol:

1. **Announce Presence**: Auditor introduces self and purpose
2. **Obtain Consent**: Group consent for observation
3. **Record Patterns**: Note organizational behaviors, not individuals
4. **Debrief**: Share general observations with group

4.2.2 System Logs vs. Individual Monitoring

Compliant Log Analysis:

- **Aggregated Authentication Patterns**: "30% of logins occur outside business hours" (n=250)

- **Collective Alert Response**: "Mean response time to high-severity alerts: 47 minutes" (n=12 analysts)
- **Time-of-Day Patterns**: "Phishing click rate: 8% morning, 19% afternoon" (n=500 test recipients)

Non-Compliant Log Analysis:

- "User JDoe clicked phishing link 3 times in 6 months" → Individual profiling
- "Finance department (n=7) has 45% click rate" → Below n=10 threshold
- "Top 5 users by failed login attempts" → Individual ranking

Audit Verification:

Request sample of log analysis reports. Check for:

☐ No individual usernames or identifiers

☐ All reported groups meet n≥10 requirement

☐ Aggregation level appropriate (department, role, time period)

☐ No "league tables" or individual rankings

4.2.3 Behavioral Assessment in Groups

Focus Group Methodology:

CPF audits may use facilitated focus groups to assess psychological vulnerabilities at aggregate level.

Focus Group Protocol:

- **Size**: 8-12 participants (meets n≥10, allows discussion)
- **Composition**: Heterogeneous (cross-functional) or homogeneous (single role)
- **Facilitator**: Trained in group dynamics and trauma-informed techniques
- **Recording**: Notes on themes/patterns, NOT attribution to individuals
- **Consent**: Written consent from all participants

Sample Focus Group Questions (Authority Domain):

- "In general, how comfortable do people feel questioning unusual requests from executives?"
- "What typically happens when someone raises concerns about an authority figure's request?"
- "Can you describe the organizational culture around security exceptions for leadership?"

Analysis Approach:

- Identify recurring themes across multiple participants
- Note group dynamics (consensus, conflict, dominant voices)
- Quote anonymously: "Several participants noted..." or "A common theme was..."
- Never attribute statements to specific individuals in report

4.2.4 Temporal Delay Verification

CPF-27001 requires 72-hour minimum delay between data collection and reporting to prevent real-time surveillance.

Audit Verification:

1. **Review Timestamps**: Check assessment report dates vs. data collection dates
2. **Interview Assessment Team**: "How do you ensure 72-hour delay?"
3. **Test System Controls**: If automated, verify system enforces delay
4. **Review Incident Response**: Check that real-time alerts don't bypass privacy controls

Common Nonconformities:

- Dashboard shows "live" psychological vulnerability metrics → **MAJOR**
- Incident response uses real-time stress indicators → **MAJOR**
- Monthly report generated same day as data collection → **MINOR**

Acceptable Exception:

True emergencies (active security incident, convergent state crisis) may warrant real-time assessment, but requires:

- Executive authorization
- Documented justification
- Immediate post-incident privacy review
- Data destruction after incident resolution

4.3 Interview Techniques

4.3.1 Anonymized Feedback Collection

Interview Setup:

- **Private Space**: No observation by management or colleagues
- **Consent Form**: Signed before interview begins
- **Recording**: Notes only (no audio/video unless specifically consented)

- **Coding System**: Assign code (INT-001) instead of using names
- **Duration**: 30-45 minutes typical

Interview Structure:

1. **Opening (5 min)**: Build rapport, explain purpose, confirm consent
2. **General Questions (15 min)**: Organizational culture, security awareness
3. **Domain-Specific (15 min)**: Targeted questions based on risk assessment
4. **Closing (5 min)**: Any concerns, thank participant, next steps

Sample Interview Guide (Authority Domain Focus):

Opening:

- "Thank you for participating. This is confidential and your responses will be combined with at least 10 others."
- "We're assessing organizational patterns, not evaluating individuals."
- "You can skip any question or stop anytime. Do you have questions before we begin?"

General Questions:

- "How would you describe the security culture here?"
- "What helps people follow security procedures? What makes it difficult?"
- "Can you think of a time when security and business needs conflicted?"

Authority-Specific Questions:

- "If you received an unusual request from an executive, what would you typically do?"
- "Is there a process for verifying requests that seem urgent or out-of-pattern?"
- "How comfortable do you think people feel questioning authority figures about security?"

Closing:

- "Is there anything important we haven't discussed?"
- "Do you have any concerns about this interview or the audit process?"
- "Your input is valuable for improving organizational security. Thank you."

4.3.2 Psychological Safety in Interviews

Creating Safe Environment:

- **Non-Judgmental Stance**: Validate all responses as legitimate perspectives
- **Normalize Vulnerabilities**: "These are universal human responses"
- **Avoid Leading Questions**: "How do you..." not "Don't you think..."
- **Respect Boundaries**: If participant uncomfortable, move to next topic
- **Manage Power Dynamics**: Acknowledge auditor role, but emphasize partnership

Red Flags for Auditor Self-Monitoring:

- Participant gives only "correct" answers (overly compliant)
- Participant defensive or hostile (perceiving judgment)
- Participant fearful about confidentiality
- Participant blames individuals vs. discussing systems

Recovery Techniques:

- **Reassure Privacy**: "Remember, no names in report, minimum 10 responses combined"
- **Reframe Purpose**: "We're looking at organizational design, not people"
- **Validate Concern**: "I appreciate you raising that; confidentiality is critical"
- **Offer Break**: "Would you like a few minutes before continuing?"

4.3.3 Trauma-Informed Questioning

Organizations that experienced security incidents may have trauma responses. Auditors must recognize and accommodate these.

Trauma Indicators:

- Visible distress when discussing past incidents
- Avoidance of certain topics or time periods
- Hypervigilance or defensive posture
- Blame, shame, or guilt expressed
- Emotional dysregulation (anger, tears, shutdown)

Trauma-Informed Adaptations:

- **Warning**: "I'd like to ask about [incident]. Is this okay to discuss?"

- **Pacing**: Allow extra time, don't rush through emotional content
- **Control**: "We can skip this or come back to it later"
- **Grounding**: If participant dissociates, redirect to present ("You're safe here now")
- **Support**: Have employee assistance resources available

Example Trauma-Informed Question Progression:

Instead of: "Tell me about the ransomware incident last year."

Trauma-Informed:

1. "I understand your organization experienced a significant security event. Is it okay to discuss this?"
2. (If yes) "We don't need details about what happened. I'm interested in how the organization responded and what's changed since then."
3. (If distress evident) "I can see this is difficult. Would you prefer to focus on current procedures instead?"

5 Scoring and Maturity Verification

5.1 CPF Score Recalculation

Auditors must independently verify the organization's CPF Score calculation to ensure mathematical accuracy and methodological compliance.

5.1.1 Sampling Methodology for Verification

Audit Sampling Approach:

Rather than re-assessing all 100 indicators (time-prohibitive), auditors sample strategically:

Minimum Sample: 20 indicators (20% coverage)

Recommended Sample: 30 indicators (30% coverage)

Sampling Strategy:

- **Risk-Based Selection**: All Red indicators (score 2) must be verified
- **Proportional by Domain**: Sample proportionally from each domain
- **Random Component**: 50% of sample selected randomly
- **Critical Indicators**: Include indicators with highest weights

Example Sampling Plan (30 indicators):

Table 5: Indicator Sampling Distribution

Domain	Total Indicators	Red Count	Sample Size
Authority [1.x]	10	4	5 (all 4 Red + 1 random)
Temporal [2.x]	10	3	4 (all 3 Red + 1 random)
Social Influence [3.x]	10	1	3 (1 Red + 2 random)
Affective [4.x]	10	2	3 (2 Red + 1 random)
Cognitive Overload [5.x]	10	3	4 (all 3 Red + 1 random)
Group Dynamics [6.x]	10	1	3 (1 Red + 2 random)
Stress Response [7.x]	10	2	3 (2 Red + 1 random)
Unconscious [8.x]	10	0	2 (2 random)
AI-Specific [9.x]	10	1	2 (1 Red + 1 random)
Convergent [10.x]	10	1	1 (1 Red)
Total	**100**	**18**	**30**

5.1.2 Indicator Verification Process

For each sampled indicator, auditor performs independent assessment:

Step 1: Evidence Collection

Request organization's evidence for indicator. Per Field Kit methodology, minimum 3 independent data sources required.

Example - Indicator 1.1 (Unquestioning Compliance):

- Data Source 1: Email gateway logs (unusual request patterns)
- Data Source 2: Security audit observations (verification compliance)
- Data Source 3: Anonymous survey results (authority questioning comfort)

Step 2: Triangulation Verification

Assess if organization achieved minimum 67% source agreement (2 of 3 sources converge).

Step 3: Independent Scoring

Apply ternary scoring logic (Green/Yellow/Red) based on evidence thresholds:

- **Green (0)**: Exception rate $< 5\%$, controls effective
- **Yellow (1)**: Exception rate 5-15%, monitoring needed
- **Red (2)**: Exception rate $> 15\%$, immediate intervention required

Step 4: Compare with Organization Score

- **Agreement**: Move to next indicator
- **One-Level Difference**: Document rationale, accept with note
- **Two-Level Difference**: Flag as potential nonconformity, investigate further

Acceptable Variance:

- $\leq$ **20% disagreement rate**: Assessment methodology conformant
- **20-30% disagreement**: Minor nonconformity (methodology refinement needed)
- $>$ **30% disagreement**: Major nonconformity (systematic assessment failure)

5.1.3 Calculation Accuracy Check

Domain Score Verification:

Select 2-3 domains for full calculation verification:

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

Audit Test:

Organization Reports: Authority Domain [1.x] = 16/20

Auditor Verifies:

- Sum individual indicator scores: 1.1(2) + 1.2(1) + 1.3(2) + 1.4(2) + 1.5(1) + 1.6(2) + 1.7(2) + 1.8(1) + 1.9(2) + 1.10(1) = 16 ✓
- Check: Range 0-20? Yes ✓
- Classification: 14-20 = Red? Yes ✓

Overall CPF Score Verification:

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

Audit Procedure:

1. Obtain domain scores from organization
2. Verify domain weights used (reference: CPF Scoring Model, Section 4.2)
3. Recalculate weighted sum
4. Apply 2.5 multiplier
5. Verify final score matches organization's reported score

Example Calculation Verification:

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

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

Common Calculation Errors:

- Wrong domain weights applied → **MAJOR** nonconformity
- Arithmetic errors in summation → **MINOR** nonconformity
- Incorrect multiplier (not 2.5) → **MAJOR** nonconformity
- Rounding errors > 2 points → **MINOR** nonconformity

5.1.4 Convergence Index Validation

CI Formula Verification:

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

where v_i = normalized vulnerability score (Red=1.0, Yellow=0.5), n = Yellow/Red indicator count

Audit Steps:

1. **Identify Vulnerable Indicators**: Count all Yellow (1) and Red (2) indicators
2. **Normalize Scores**: Yellow → 0.5, Red → 1.0
3. **Calculate Product**: $(1 + v_1) \times (1 + v_2) \times ... \times (1 + v_n)$
4. **Verify Threshold Classification**:
   - CI < 2: Low risk
   - $2 \leq$ CI < 5: Moderate risk
   - $5 \leq$ CI < 10: High risk
   - CI $\geq$ 10: Critical risk

Example CI Verification:

Organization Data:

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

Auditor Calculation:

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

Finding: CI $\gg$ 10, indicating catastrophic convergence state requiring emergency response.

5.2 Maturity Level Assessment

5.2.1 Evidence Requirements by Level

Auditors verify maturity level claims against CPF Maturity Model criteria.

Level 1 (Initial) - Verification Checklist:

- ☐ Executive awareness briefing documented (meeting minutes, presentation)
- ☐ Initial assessment conducted (minimum 20 indicators, not full 100)
- ☐ Psychological factors in incident reports (review 3+ recent incidents)
- ☐ Basic psychology in awareness program (training materials reference CPF concepts)
- ☐ CPF Score > 20/100 (verify calculation)
- ☐ Minimum 3 of 10 categories assessed (documentation of assessment scope)

Level 2 (Developing) - Verification Checklist:

- ☐ Full 100-indicator assessment completed (all domains documented)
- ☐ Vulnerability heat map maintained (visual representation, regularly updated)
- ☐ Response playbooks include psychological factors (review 2+ playbooks)
- ☐ Security team psychology training (training records, certificates)
- ☐ CPF Score > 40/100 with Red indicators < 25%
- ☐ 7+ categories actively monitored (KPIs defined for each)
- ☐ Quarterly assessment cycle (4 assessments in past 12 months)
- ☐ 75% staff trained (training attendance records)

Level 3 (Defined) - Verification Checklist:

- ☐ Real-time CPF monitoring dashboard operational (system demonstration)
- ☐ Predictive models for vulnerability states (model documentation, accuracy metrics)
- ☐ Cross-functional integration (HR/IT/Risk meeting minutes, shared processes)
- ☐ Role-specific interventions (different approaches by department/role)
- ☐ CPF Score > 60/100 with no Red indicators > 30 days
- ☐ All 10 categories with defined KPIs (KPI dashboard review)
- ☐ Monthly assessment + daily monitoring (frequency documentation)
- ☐ 90% staff trained + specialized certifications (certification roster)
- ☐ Board-level CPF reporting (board presentation materials)

Level 4 (Managed) - Verification Checklist:

- ☐ ML-driven prediction > 80% accuracy (validation study results)
- ☐ Automated intervention triggers (system configuration, trigger logs)
- ☐ Organization-wide psychological safety metrics (survey data, tracking)
- ☐ Third-party risk assessment includes CPF (vendor assessment templates)
- ☐ CPF Score > 80/100 with proactive intervention (before Yellow threshold)
- ☐ Real-time monitoring all indicators (system capability demonstration)
- ☐ 100% staff trained + 25% certified practitioners (certification verification)
- ☐ Demonstrable 5:1 ROI (financial analysis documentation)
- ☐ Insurance premium reductions > 20% (policy documentation)

Level 5 (Optimizing) - Verification Checklist:

- ☐ Autonomous psychological defense systems (AI-driven system demonstration)
- ☐ Research contribution to CPF evolution (published papers, presentations)
- ☐ Cross-industry threat intelligence sharing (consortium membership proof)
- ☐ Psychological security innovation lab (facility, dedicated staff)
- ☐ Board-certified Chief Psychology Officer (CPO credentials)
- ☐ CPF Score > 90/100 sustained (12+ months continuous green state)
- ☐ 2+ new methods published annually (publication list)
- ☐ Prediction accuracy > 95% including novel attacks (validation data)
- ☐ 50%+ staff CPF certified (certification database)
- ☐ Industry standards contribution (standards body participation proof)

5.2.2 Capability Demonstration

Beyond documentation review, auditors verify practical capabilities through demonstration.

Level 2 Practical Tests:

Test 1: Vulnerability Heat Map Navigation

- Request: "Show me current vulnerabilities by domain"
- Observe: Can staff quickly locate and interpret heat map?
- Verify: Data current (within quarterly cycle), privacy-preserved (n≥10)

Test 2: Playbook Psychological Integration

- Request: "Walk through ransomware response playbook"
- Observe: Are stress responses, group dynamics, authority patterns addressed?
- Verify: Not just technical steps; includes psychological considerations

Level 3 Practical Tests:

Test 1: Predictive Model Execution

- Request: "Predict vulnerability state for next quarter-end"
- Observe: Model inputs organizational data, outputs risk forecast
- Verify: Prediction methodology documented, historical accuracy tracked

Test 2: Cross-Functional Coordination

- Request: "Describe how HR and IT collaborate on onboarding security"
- Observe: Evidence of joint processes, shared metrics, regular communication
- Verify: Integration genuine, not superficial

5.2.3 Sustained Performance Verification

Maturity levels require sustained performance over time, not point-in-time achievement.

Minimum Stability Periods:

- **Level 2**: 6 months at Level 1 + 3 months demonstrating Level 2 criteria
- **Level 3**: 12 months at Level 2 + 6 months demonstrating Level 3 criteria
- **Level 4**: 18 months at Level 3 + 6 months demonstrating Level 4 criteria
- **Level 5**: 24+ months at Level 4 + continuous innovation

Audit Evidence of Stability:

- Historical CPF Score trend (quarterly data for past 12-24 months)
- Maturity level progression documentation (dates of level transitions)
- Continuous improvement evidence (corrective actions, enhancements)
- No regression indicators (temporary score drops acceptable if recovered)

Common Nonconformity:

Organization claims Level 3 but only achieved Level 2 criteria 2 months ago → **MAJOR**: Insufficient stability period, maturity level overclaimed.

6 Clause-by-Clause Audit Guidance

This section provides specific audit procedures for each CPF-27001:2025 clause.

6.1 Clause 4: Context of the Organization

6.1.1 Audit Objectives

Verify that the organization has:

- Determined relevant internal and external issues affecting PVMS
- Identified interested parties and their requirements
- Defined PVMS scope appropriately
- Established PVMS processes aligned with CPF-27001

6.1.2 Verification Procedures

4.1 Understanding the Organization and Its Context

Evidence to Request:

- Context analysis document (internal/external issues)
- Industry threat landscape assessment
- Organizational culture assessment
- Historical incident patterns

Audit Questions:

- "What psychological factors are specific to your organizational culture?"
- "How do industry-specific threats influence your psychological vulnerabilities?"
- "What external factors (regulatory, competitive) affect your PVMS?"

Common Nonconformities:

- Generic context analysis not tailored to organization → MINOR
- No consideration of industry-specific psychological threats → MAJOR
- Context analysis not updated regularly → MINOR

4.2 Understanding Needs and Expectations of Interested Parties

Evidence to Request:

- Interested party register
- Stakeholder requirement analysis
- Communication records with key parties

Audit Questions:

- "Who are the key stakeholders for your PVMS?" (employees, management, customers, regulators, insurers)
- "How do you gather and document their requirements?"
- "How do privacy requirements from employees influence your PVMS design?"

4.3 Determining the Scope of the PVMS

Evidence to Request:

- PVMS Scope Statement
- Justification for exclusions
- Organizational chart showing covered units

Verification:

- Scope clearly defines boundaries (locations, departments, functions)
- Exclusions justified and documented
- Scope consistent with organizational context
- Integration with ISMS scope (if applicable)

Common Nonconformities:

- Vague scope definition ("entire organization") → MINOR
- Unjustified exclusions (high-risk departments excluded) → MAJOR
- Scope not approved by management → MAJOR

4.4 Psychological Vulnerability Management System

Verification:

- PVMS processes documented and implemented
- Process interactions defined
- Process ownership assigned
- Monitoring and measurement established

6.2 Clause 5: Leadership

6.2.1 Audit Objectives

Verify that top management demonstrates leadership and commitment to PVMS.

6.2.2 Verification Procedures

5.1 Leadership and Commitment

Evidence to Request:

- Board/executive meeting minutes mentioning PVMS
- Resource allocation approvals
- Executive communications on PVMS importance
- Budget documentation for PVMS activities

Audit Questions (Executive Interview):

- "How does psychological vulnerability management support business objectives?"
- "What resources have been allocated to PVMS implementation?"
- "How do you monitor PVMS effectiveness?"
- "What role does the board play in PVMS oversight?"

Red Flags:

- Executive delegation without engagement → Lack of commitment
- Insufficient resources allocated → Nominal compliance
- No PVMS items in management review agendas → Lack of integration

5.2 Policy

Evidence to Request:

- CPF Policy document
- Policy approval documentation
- Policy communication records
- Policy review history

Verification Checklist:

☐ Policy appropriate to organization's purpose

☐ Commitment to systematic psychological vulnerability assessment

☐ Commitment to privacy protection (n≥10, $\varepsilon \leq 0.1$, 72hr delay)

☐ Framework for setting CPF objectives

☐ Commitment to continual improvement

☐ Approved by top management

☐ Communicated to all relevant parties

☐ Available to interested parties (as appropriate)

Common Nonconformities:

- Generic policy template not customized → MINOR
- Privacy commitments missing or vague → MAJOR
- Policy not approved by CEO/Board → MAJOR
- Policy not communicated to staff → MINOR

5.3 Organizational Roles, Responsibilities and Authorities

Evidence to Request:

- PVMS organizational structure
- Role descriptions (CPF Coordinator, Privacy Officer, Assessment Specialists)
- Delegation of authority documentation
- Competence requirements by role

Key Roles to Verify:

Table 6: PVMS Key Roles

Role	**Responsibilities**
CPF Coordinator	Overall PVMS management, assessment coordination, management reporting
Privacy Officer	Privacy protection enforcement, consent management, anonymization verification
Assessment Specialists	Indicator evaluation, data collection, analysis
Response Coordinators	Risk treatment implementation, intervention design

Audit Questions:

- "Who is responsible for overall PVMS?" (Interview that person)
- "How is privacy protection ensured?" (Interview Privacy Officer)
- "What authority does CPF Coordinator have?" (Budget, escalation, resource requests)

6.3 Clause 6: Planning

6.3.1 Audit Objectives

Verify that organization has planned PVMS implementation addressing risks and opportunities.

6.3.2 Verification Procedures

6.1.1 General

Evidence to Request:

- Risk and opportunity register
- Planning documentation
- Integration with strategic planning

6.1.2 Psychological Vulnerability Assessment

Critical Audit Focus - This is the heart of CPF-27001 compliance.

Evidence to Request:

- Assessment methodology document
- Privacy protection procedures
- Data collection procedures (OFTLISRV schema)
- Assessment tools and templates
- Training materials for assessment team

Verification Checklist:

- ☐ All 10 CPF domains assessed
- ☐ 100 indicators evaluated (or documented rationale for exclusions)
- ☐ Ternary scoring (Green/Yellow/Red) applied
- ☐ Minimum 3 data sources per indicator (triangulation)
- ☐ Privacy protections implemented:
  - ☐ Minimum aggregation unit n≥10
  - ☐ Differential privacy $\varepsilon \leq 0.1$
  - ☐ Temporal delay $\geq$ 72 hours
- ☐ Assessment frequency defined (minimum annually)
- ☐ Competent assessors assigned

Deep-Dive Verification (Select 3 Domains):

For each selected domain, audit:

1. **Data Sources**: Review evidence for 2-3 indicators
2. **Scoring Logic**: Verify thresholds applied correctly (Green/Yellow/Red)
3. **Privacy Compliance**: Check aggregation level (n≥10)
4. **Documentation**: Assess completeness and clarity

Common Nonconformities:

- Fewer than 3 data sources per indicator → MAJOR
- Individual-level data not aggregated → CRITICAL
- No differential privacy applied → MAJOR
- Temporal delay not enforced → MAJOR
- Assessment methodology not documented → MAJOR
- Domains excluded without justification → MAJOR

6.1.3 Psychological Risk Treatment

Evidence to Request:

- Risk treatment plan
- Intervention descriptions
- Implementation timelines
- Responsibility assignments
- Effectiveness monitoring approach

Verification:

- Risk treatment addresses Yellow and Red indicators
- Interventions are organizational (not individual-focused)
- Response protocols defined (per Section 8.3 requirements)
- Resources allocated for implementation
- Monitoring mechanisms established

Audit Questions:

- "How do you decide which vulnerabilities to address first?"
- "Show me an intervention for a Red indicator in Authority domain"
- "How do you measure intervention effectiveness?"

6.2 CPF Objectives and Planning

Evidence to Request:

- CPF objectives document
- Objective-setting process
- Progress tracking mechanisms
- KPI definitions

Verification - SMART Objectives:

- **Specific**: Clear description (e.g., "Reduce Authority domain Red indicators from 4 to 1")
- **Measurable**: Quantifiable metrics (indicator counts, CPF Score targets)
- **Achievable**: Realistic given resources
- **Relevant**: Aligned with PVMS purpose
- **Time-bound**: Defined completion dates

Example Compliant Objectives:

- "Achieve CPF Score >60 by Q4 2025" (from current 58)
- "Reduce Convergence Index below 5 within 6 months" (from current 7.2)
- "Eliminate all Red indicators in Authority domain by December 2025"
- "Train 90% of staff in CPF concepts by end of 2025"

6.4 Clause 7: Support

6.4.1 Audit Objectives

Verify that organization has provided necessary support resources for PVMS.

6.4.2 Verification Procedures

7.1 Resources

Evidence to Request:

- Budget allocations for PVMS
- Staffing for PVMS roles
- Technology investments (assessment tools, dashboards)
- Training budget

Adequacy Assessment:

Compare resources to maturity level requirements (reference: Maturity Model ROI section).

7.2 Competence

Evidence to Request:

- Competence requirements by role
- CV/resumes of key PVMS personnel
- Training records
- Certifications (CISSP, CISM, psychology degrees, CPF certifications)

- Competence gap analysis

CPF Coordinator Competence Verification:
Interview CPF Coordinator and assess:

- Understanding of cybersecurity fundamentals
- Knowledge of psychological theory (Bion, Klein, Kahneman, Cialdini)
- Familiarity with privacy regulations (GDPR, differential privacy)
- Audit and assessment methodology knowledge

Sample Questions:

- "Explain Bion's basic assumptions and their relevance to cybersecurity"
- "How does differential privacy protect individual privacy?"
- "Walk me through the OFTLISRV schema for indicator assessment"

Common Nonconformities:

- CPF Coordinator lacks psychology background → MAJOR
- No formal training in CPF methodology → MINOR
- Assessment team lacks cybersecurity expertise → MAJOR
- Privacy Officer unfamiliar with differential privacy → MAJOR

7.3 Awareness

Evidence to Request:

- Awareness campaign materials
- Communication records
- Staff survey results on CPF awareness
- Training attendance records

Awareness Testing (Staff Interviews):
Select 5-10 staff randomly and ask:

- "Are you aware of the organization's CPF program?"
- "How does CPF assessment protect your privacy?"
- "Is this about evaluating you personally or organizational patterns?"

Acceptable Results: 70%+ can articulate basic CPF purpose and privacy protections.

7.4 Communication

Verification:

- Internal communication plan (what, when, who, how)
- External communication protocols (regulators, insurers, certification bodies)
- Feedback mechanisms
- Incident communication procedures

7.5 Documented Information

Evidence to Request:

- Document control procedures
- Document register
- Version control records
- Access controls for sensitive documents
- Retention schedules

Required Documents (per CPF-27001):

- CPF Policy
- PVMS Scope
- Assessment methodology
- Privacy procedures
- Risk treatment plans
- Competence requirements
- Monitoring and measurement procedures
- Internal audit program
- Management review records

6.5 Clause 8: Operation

6.5.1 Audit Objectives

Verify that organization has implemented operational controls for PVMS.

6.5.2 Verification Procedures

8.1 Operational Planning and Control

Evidence to Request:

- Operational procedures for PVMS
- Assessment schedules

- Data collection protocols
- Integration with security operations
- Change management procedures

Verification:

- Regular assessment cycles established (minimum annually)
- Continuous monitoring for critical indicators
- Privacy-preserving data collection implemented
- Risk treatment execution procedures
- Integration with ISMS operational controls

8.2 Psychological Vulnerability Assessment (Operational)

Critical Operational Verification - Most important audit focus.

Assessment Process Audit:

1. **Review Latest Assessment Report**
   - Date of assessment
   - Scope coverage (all 10 domains?)
   - Indicator scores documented
   - Privacy protections applied
2. **Verify Data Triangulation**
   - Select 5 indicators for deep-dive
   - Request evidence for each (minimum 3 sources)
   - Verify source independence
   - Check convergence methodology (67% agreement threshold)
3. **Privacy Controls Verification**
   - Check all reported metrics: $n \geq 10$?
   - Review differential privacy implementation
   - Verify 72-hour temporal delay enforced
   - Test database access controls (can system query $n < 10$?)
4. **Role-Based Analysis Review**
   - Verify analysis by role/department, not individuals
   - Check for small group reporting ($n < 10$ violations)
   - Review anonymization techniques

Field Kit Usage Verification:

If organization uses CPF Field Kits:

- Review completed Field Kits for 2-3 indicators
- Verify all sections completed (Quick Assessment, Evidence Collection, Scoring, Solutions)
- Check field notes for privacy compliance
- Confirm scoring rationale documented

Common Nonconformities:

- Assessment not performed in past 12 months → MAJOR
- Incomplete domain coverage (less than 10 domains) → MAJOR
- Privacy violations (n<10, no temporal delay) → CRITICAL
- Single data source per indicator (no triangulation) → MAJOR
- No documented scoring rationale → MINOR

8.3 Psychological Risk Treatment (Operational)

Evidence to Request:

- Risk treatment implementation records
- Intervention descriptions and timelines
- Response protocol documentation
- Effectiveness monitoring data
- Resource allocation for interventions

Graduated Response Protocol Verification:

Table 7: Response Protocol Compliance

Status	**Required Response**
Green (0)	Standard monitoring, no immediate action
Yellow (1)	Enhanced monitoring, preventive interventions within 30-60 days
Red (2)	Immediate escalation, emergency treatment within 7-14 days
Critical CI (>10)	Emergency response procedures activated

Audit Test:

Select 2 Red indicators from latest assessment:

- Was response initiated within 7-14 days? (Timeline verification)
- What intervention was implemented? (Review intervention plan)
- Who was responsible? (Verify assignment and execution)
- Has effectiveness been measured? (Post-intervention assessment)

Example Compliant Response:

Red Indicator: Authority Domain 1.1 (Unquestioning Compliance) = Red (2)

Response Implementation:

- **Detection Date:** March 15, 2025
- **Escalation:** March 16, 2025 (CPF Coordinator notified)
- **Intervention Plan:** March 22, 2025 (within 7 days)
  - Dual-channel verification protocol implemented
  - Email authentication upgraded (DMARC/SPF/DKIM)
  - Authority challenge training deployed
- **Re-assessment:** June 15, 2025 (3 months post-intervention)
- **Result:** Indicator improved to Yellow (1)

Common Nonconformities:

- Red indicators with no documented response → MAJOR
- Response delayed beyond 14-day requirement → MINOR
- Interventions target individuals vs. organizational systems → MAJOR
- No effectiveness monitoring → MINOR
- Convergent state (CI>10) without emergency response → CRITICAL

8.4 Continuous Monitoring

Evidence to Request:

- Monitoring dashboard or reports
- Real-time alerting configuration (if applicable)
- SIEM integration documentation
- Monitoring KPI definitions
- Alert response logs

Verification:

- Critical indicators monitored continuously (not just annual assessment)
- Integration with security operations center (SOC)
- Automated alerting for threshold breaches
- Privacy protections maintained in monitoring ($n \geq 10$, temporal delay)

Audit Questions:

- "Which indicators are monitored in real-time vs. assessed periodically?"
- "How do you balance continuous monitoring with 72-hour temporal delay?"
- "Show me an example of an automated alert triggered by psychological vulnerability threshold"

6.6 Clause 9: Performance Evaluation

6.6.1 Audit Objectives

Verify that organization monitors, measures, analyzes and evaluates PVMS effectiveness.

6.6.2 Verification Procedures

9.1 Monitoring, Measurement, Analysis and Evaluation

Evidence to Request:

- KPI definitions and targets
- Monitoring and measurement procedures
- Performance reports (past 12 months)
- Trend analysis
- Effectiveness evaluation records

Key Performance Indicators to Verify:

Table 8: CPF Performance Indicators

KPI	**Target**	**Measurement**
CPF Score	Increasing trend	Quarterly assessment
Red Indicator Count	Decreasing trend	Per assessment
Yellow Indicator Count	Stable or decreasing	Per assessment
Convergence Index	CI < 5	Per assessment
Human-Factor Incidents	Decreasing trend	Monthly incident reports
Response Time (Red)	< 14 days	Intervention logs
Training Completion	$> 75\%$	Training system
Assessment Coverage	100% (all domains)	Assessment reports

Trend Analysis Verification:

Request quarterly CPF Scores for past 12 months. Verify:

- Scores documented consistently
- Trend direction analyzed (improving/stable/declining)
- Root causes of trends investigated
- Actions taken based on trends

Effectiveness Evaluation:

For 2-3 implemented interventions:

- Was effectiveness measured post-implementation?
- What metrics were used? (Indicator score change, incident reduction)
- Were results documented and communicated?

- Were adjustments made based on effectiveness data?

Common Nonconformities:

- KPIs defined but not tracked → MAJOR
- No trend analysis performed → MINOR
- Effectiveness not evaluated post-intervention → MINOR
- Monitoring data not used for decision-making → MAJOR

9.2 Internal Audit

Evidence to Request:

- Internal audit program/schedule
- Internal audit reports (past 12 months)
- Auditor competence records
- Audit follow-up documentation
- Corrective action tracking

Internal Audit Program Verification:

☐ Audit program covers all PVMS processes

☐ Audit frequency appropriate (minimum annually)

☐ Risk-based audit planning (focus on high-risk domains)

☐ Auditor independence (not auditing own work)

☐ Auditor competence appropriate (CPF knowledge required)

Auditor Competence Assessment:

Interview internal auditor(s):

- "What training have you received in CPF methodology?"
- "How do you verify privacy protections during audit?"
- "Explain the difference between organizational and individual assessment"

Acceptable: Internal auditor has CPF-specific training (minimum 8 hours) or equivalent experience.

Not Acceptable: General ISO 27001 auditor with no CPF training → MAJOR nonconformity

Audit Report Review:

Review latest internal audit report:

- Does it cover PVMS scope comprehensively?

- Are findings clearly documented?
- Are privacy protections verified?
- Is corrective action tracked?

9.3 Management Review

Evidence to Request:

- Management review schedule
- Management review meeting minutes (past 2 reviews minimum)
- Management review input documentation
- Management review output decisions
- Action item tracking

Required Inputs (per CPF-27001 Clause 9.3):

☐ Status of actions from previous management reviews

☐ Changes in external and internal issues

☐ Performance information including trends

☐ Feedback from interested parties

☐ Results of psychological vulnerability assessments

☐ Audit results (internal and external)

☐ Effectiveness of risk treatment

☐ Opportunities for continual improvement

Required Outputs:

☐ Decisions related to continual improvement opportunities

☐ Decisions related to changes needed to PVMS

☐ Resource needs

Audit Questions (Executive Interview):

- "How frequently does management review PVMS performance?"
- "What CPF metrics are reported to senior management?"
- "Can you give an example of a management review decision that led to PVMS improvement?"
- "How does the board receive information about psychological vulnerability status?"

Common Nonconformities:

- Management review not conducted annually → MAJOR
- Required inputs missing from review → MINOR per missing input
- No documented outputs/decisions → MAJOR
- Actions from previous review not tracked → MINOR
- Management review perfunctory (no substantive discussion) → MAJOR

6.7 Clause 10: Improvement

6.7.1 Audit Objectives

Verify that organization continually improves PVMS suitability, adequacy, and effectiveness.

6.7.2 Verification Procedures

10.1 Nonconformity and Corrective Action

Evidence to Request:

- Nonconformity register
- Corrective action procedures
- Root cause analysis records
- Corrective action effectiveness verification
- Closure documentation

Corrective Action Process Verification:

Select 2-3 closed nonconformities and trace through process:

1. **Reaction**: Was nonconformity controlled/corrected immediately?
2. **Root Cause**: Was cause analyzed (5-Why, Fishbone, etc.)?
3. **Action**: Was corrective action appropriate to eliminate root cause?
4. **Implementation**: Was action implemented as planned?
5. **Review**: Was effectiveness verified before closure?
6. **Update**: Were PVMS documents updated if needed?

Common PVMS Nonconformities (from previous audits):

- Privacy violations (n<10, no temporal delay)
- Inadequate data triangulation
- Missing domain coverage
- Insufficient competence

- No risk treatment for Red indicators
- Assessment not performed timely

Example Compliant Corrective Action:

Nonconformity: "Finance department (n=7) analyzed separately, violating n≥10 requirement"

Root Cause Analysis: Assessment team misunderstood aggregation requirement, no validation check in process

Corrective Action:

- Retrain assessment team on privacy requirements
- Implement automated check in assessment tool (prevents n<10 reports)
- Reprocess finance data combined with broader "administrative staff" category (n=45)
- Update assessment procedure to include privacy validation step

Effectiveness Verification: Next assessment properly aggregates all groups to n≥10 ✓

10.2 Continual Improvement

Evidence to Request:

- Continual improvement plan
- Improvement initiatives documentation
- CPF Score trend (12-24 months)
- Process improvement records
- Innovation efforts

Continual Improvement Evidence:

- CPF Score improving over time (quarterly trend upward)
- Indicator status improving (Red → Yellow → Green)
- Assessment methodology refinements
- Privacy protection enhancements
- Integration improvements with technical security
- Intervention effectiveness increasing
- Maturity level progression

Audit Questions:

- "How has your PVMS improved in the past year?"
- "What specific enhancements have you made to assessment methodology?"
- "How do you identify opportunities for improvement?"

- "What innovations are you considering for future PVMS development?"

Red Flag: Organization at same maturity level with static CPF Score for 12+ months with no documented improvement initiatives → Lack of continual improvement (MAJOR)

10.3 Framework Updates

Evidence to Request:

- Framework update procedure
- Review cycle documentation
- Change management records
- Communication of updates
- Backward compatibility considerations

Verification:

- Process exists for updating CPF indicators/methodology
- Updates reviewed through change management
- Changes validated before implementation
- Updates documented with rationale
- Stakeholders informed of framework changes

Audit Question:

"How do you handle updates to the CPF framework when new vulnerabilities are identified or attack techniques evolve?"

7 Audit Reporting

7.1 Report Structure

7.1.1 Executive Summary

The executive summary provides high-level overview for senior management and board.

Required Elements:

- **Overall Conformity Decision**: Conformant / Conformant with Minor Nonconformities / Major Nonconformity / Critical Nonconformity
- **CPF Score**: Current score and rating (Excellent/Good/Fair/Poor/Critical)
- **Maturity Level**: Current level and progression status
- **Critical Findings**: Summary of CRITICAL and MAJOR nonconformities (maximum 5 bullet points)

- **Strengths**: Positive observations (2-3 items)
- **Recommendations**: Top 3 priority actions

Length: Maximum 2 pages

Example Executive Summary Opening:

> *"This report presents findings from the CPF-27001:2025 certification audit of [Organization Name] conducted [dates]. The organization demonstrates CONFORMANCE WITH MINOR NONCONFORMITIES to CPF-27001 requirements. The current CPF Score is 73/100 (Good rating, Low-Moderate risk level), representing Maturity Level 2 (Developing). Three minor nonconformities were identified related to documentation completeness, assessment frequency, and training coverage. No major or critical nonconformities were found. The organization has established a solid foundation for psychological vulnerability management with particular strengths in executive commitment and privacy protection implementation."*

7.1.2 Detailed Findings

Organization by Clause:

For each CPF-27001 clause (4-10):

- **Conformity Statement**: Conformant / Nonconformant
- **Evidence Reviewed**: Summary of documents, interviews, observations
- **Positive Observations**: Strengths and good practices
- **Nonconformities**: Detailed description if any
- **Opportunities for Improvement**: Suggestions (not required for conformity)

Alternative Organization by Domain:

For domain-focused reports:

- Summary by CPF domain [1.x] through [10.x]
- Domain scores and status (Green/Yellow/Red)
- Specific indicator findings
- Risk treatment effectiveness

7.1.3 Nonconformity Classification

CRITICAL Nonconformity:

Definition: Privacy violation or systematic failure that creates immediate harm risk.

Examples:

- Individual-level psychological data reported without aggregation
- Assessment data used for employee performance evaluation

- No differential privacy protections implemented
- Systematic profiling of individuals

Impact: Immediate suspension of certification process. Must be corrected before certificate can be issued.

MAJOR Nonconformity:

Definition: Absence or total failure of a CPF-27001 requirement.

Examples:

- No psychological vulnerability assessment conducted in past 12 months
- Fewer than 7 of 10 domains assessed
- No privacy protection procedures documented or implemented
- CPF Coordinator lacks required competencies
- Red indicators with no documented response
- No management review conducted

Impact: Certificate cannot be issued until corrected. Recertification may require follow-up audit.

MINOR Nonconformity:

Definition: Isolated lapse or deficiency that does not constitute total failure.

Examples:

- Assessment delayed 2 weeks beyond annual deadline
- One domain incompletely assessed (partial indicator coverage)
- Training completion at 68% (target 75%)
- Documentation incomplete for 2 of 10 domains
- Management review input missing one required element

Impact: Certificate can be issued with corrective action plan. Must be corrected before next surveillance audit.

OBSERVATION (Not a Nonconformity):

Definition: Opportunity for improvement or best practice suggestion.

Examples:

- "Consider implementing automated dashboard for real-time monitoring"
- "Field Kit usage could enhance assessment consistency"
- "Integration with HR onboarding could improve awareness"

Impact: No corrective action required. Organization may choose to implement or not.

7.1.4 Recommendations

Prioritization Framework:

1. **High Priority**: Addresses MAJOR nonconformities or high-risk vulnerabilities
2. **Medium Priority**: Addresses MINOR nonconformities or moderate-risk gaps
3. **Low Priority**: Improvement opportunities for maturity advancement

Recommendation Format:

For each recommendation:

- **Finding Reference**: Link to specific nonconformity or observation
- **Recommended Action**: Clear, actionable description
- **Rationale**: Why this improvement is important
- **Expected Benefit**: Anticipated impact on CPF Score or risk reduction
- **Suggested Timeline**: Realistic implementation timeframe
- **Estimated Effort**: Resource requirements (Low/Medium/High)

7.2 Privacy-Compliant Reporting

7.2.1 Anonymization Requirements

Strict Prohibitions in Audit Reports:

- **NO Individual Names**: Use roles only ("Finance Manager" not "John Smith")
- **NO Small Group Data**: If n<10, do not report separately
- **NO Identifying Details**: Remove biographical information that enables re-identification
- **NO Quotes with Attribution**: Anonymize all interview quotes

Compliant Reporting Examples:

Finding: "Interview data from 15 finance staff members indicates 73% report discomfort questioning executive requests."

Quote: "Multiple participants noted that 'questioning authority is discouraged in practice despite official policy.'"

Observation: "The IT security team (n=8) was combined with broader technical staff (n=45) for analysis to maintain privacy protections."

Non-Compliant Examples (DO NOT USE):

- × "Jane Doe in Finance clicked 3 phishing simulations"
- × "The CFO's assistant frequently bypasses security"
- × "Marketing department (n=6) has highest vulnerability score"
- × "As John mentioned in our interview, 'I don't trust the security team'"

7.2.2 Aggregation Standards

Minimum Reporting Units:

Table 9: Privacy-Preserving Aggregation Levels

Aggregation Level	Minimum n	Example
Organizational	Total employees	"Organization-wide CPF Score: 73"
Departmental	≥10 per dept	"Administrative functions (n=45): ..."
Role-Based	≥10 per role	"Managers (n=32): ..."
Locational	≥10 per site	"Headquarters (n=250): ..."

Handling Small Groups:

Scenario: Organization has 8-person executive team and 6-person security team.

Prohibited: Report executive team or security team scores separately

Compliant Options:

1. Combine with larger category: "Leadership and technical staff (n=65)"
2. Report organization-level only: "Organizational CPF Score"
3. Exclude with documented justification: "Executive and security teams excluded from assessment due to size constraints"

7.2.3 Secure Report Distribution

Access Controls:

- Reports classified as CONFIDENTIAL
- Distribution limited to authorized recipients:
  - Organization's executive management
  - CPF Coordinator
  - Privacy Officer
  - Certification body (if applicable)
- Encrypted transmission (TLS 1.3+ for email, encrypted file transfer)
- Watermarking or controlled copy numbering

Retention and Destruction:

- Audit working papers: 3 years retention, then secure destruction
- Final reports: 7 years retention per ISO 27006 requirements
- Raw assessment data: Destruction within 90 days post-audit (unless regulatory requirement)
- Interview recordings (if any): Destruction immediately post-report issuance

7.3 Corrective Action Planning

7.3.1 Timeframe Assignment

Table 10: Corrective Action Timeframes

Nonconformity Type	Required Timeframe	Verification
CRITICAL	Immediate (0-7 days)	On-site re-audit
MAJOR	30-90 days	Document review or re-audit
MINOR	90-180 days	Document review

7.3.2 Root Cause Analysis

Auditors should guide organizations toward root cause identification:

Common Root Causes in CPF Audits:

- **Competence Gap**: Insufficient training in CPF methodology or privacy requirements
- **Resource Constraint**: Inadequate time/budget allocated for PVMS
- **Process Deficiency**: Assessment procedures incomplete or poorly documented
- **Cultural Resistance**: Organizational skepticism about psychology in security
- **Integration Failure**: PVMS not properly connected with ISMS
- **Management Disengagement**: Lack of executive commitment

5-Why Example:

Nonconformity: Assessment data not aggregated to n≥10

1. *Why?* Assessment team reported small department separately
2. *Why?* Team didn't understand aggregation requirement
3. *Why?* Training didn't adequately cover privacy protections
4. *Why?* Training materials focused on scoring, not privacy
5. *Why?* Training developed by security team without privacy expertise
6. **Root Cause:** Lack of privacy subject matter expert in training development

7.3.3 Follow-up Procedures

Corrective Action Verification Process:

1. **Organization Submits**:
   - Root cause analysis
   - Corrective action plan with timeline

- Evidence of implementation

2. **Auditor Reviews**:
   - Is root cause plausible and adequately analyzed?
   - Is corrective action appropriate to address root cause?
   - Is evidence sufficient to demonstrate implementation?
3. **Verification Method**:
   - CRITICAL: On-site re-audit required
   - MAJOR: Document review or on-site (auditor discretion)
   - MINOR: Document review acceptable
4. **Effectiveness Check**:
   - Has nonconformity recurred?
   - Is process now functioning as intended?
   - Have related risks been addressed?
5. **Closure Decision**:
   - ACCEPT: Corrective action effective, close nonconformity
   - REJECT: Insufficient evidence or ineffective action, remain open

8 Special Audit Scenarios

8.1 Initial Certification Audit

8.1.1 Stage 1: Readiness Review (Off-Site)

Objectives:

- Confirm PVMS documentation complete
- Verify audit readiness
- Identify critical gaps before Stage 2

Activities:

- Document review (all required CPF-27001 documents)
- Preliminary assessment methodology evaluation
- Privacy protection procedure review
- Competence verification (key personnel CVs)
- Scope confirmation

Duration: 1-2 days (off-site)

Output: Stage 1 report identifying any gaps that must be addressed before Stage 2

8.1.2 Stage 2: Implementation Verification (On-Site)

Objectives:

- Verify PVMS implementation per CPF-27001 requirements
- Assess effectiveness of controls
- Determine conformity

Activities:

- Full clause-by-clause audit (Clauses 4-10)
- CPF Score recalculation and verification
- Privacy controls testing
- Staff interviews and observations
- Management interviews
- Evidence examination

Duration: 3-5 days on-site (depending on organization size)
Output: Certification audit report with conformity decision

8.1.3 Decision Criteria

Certificate Issuance:

- NO CRITICAL nonconformities
- NO MAJOR nonconformities OR all MAJOR closed before decision
- MINOR nonconformities acceptable (with corrective action plan)

Certificate Deferral:

- CRITICAL nonconformity present
- Multiple MAJOR nonconformities (typically ≥ 3)
- Systematic failure of PVMS implementation

8.2 Surveillance Audit

8.2.1 Purpose and Scope

Annual surveillance audits verify continued conformity and PVMS maintenance.
Reduced Scope:

- Focus on changes since last audit

- Sample of PVMS processes (not all clauses in depth)
- Verification of corrective actions from previous audit
- Review of management review and internal audit

Typical Coverage:

- 30-50% of full audit scope
- Mandatory: Clauses 9 (Performance Evaluation) and 10 (Improvement)
- Risk-based selection of operational clauses
- Focus on domains with deteriorating scores

8.2.2 Sampling Approach

Annual Surveillance Sample:

- 10-15 indicators (vs. 20-30 for full audit)
- Prioritize Red and Yellow indicators
- Verify improvements from previous findings
- Random sample of Green indicators for stability check

8.2.3 Frequency

Standard: Annual surveillance (12 months ± 2 months from last audit)
Increased Frequency: May be required if:

- Significant PVMS changes
- Major organizational changes (M&A, restructuring)
- Performance deterioration
- Stakeholder complaints

8.3 Recertification Audit

8.3.1 Three-Year Cycle Review

Recertification audits occur every 3 years and are more comprehensive than surveillance.
Scope:

- Full system audit (similar to initial certification)
- All CPF-27001 clauses covered
- Three-year performance trend analysis

- PVMS evolution and improvement verification
- Framework adaptation assessment

Additional Focus Areas:

- Maturity level progression over 3 years
- Sustained performance (not just current state)
- Integration enhancements since initial certification
- Innovation and continuous improvement evidence

8.3.2 Continuous Improvement Evidence

Three-Year Expectations:

- CPF Score improvement (minimum +10 points over 3 years)
- Maturity level progression (at least one level advancement)
- Red indicator count reduction
- Incident rate reduction (human-factor breaches)
- Process refinements and enhancements
- Technology improvements (tools, automation)

Stagnation Indicators (Concern):

- Static CPF Score for 3 years
- No maturity level progression
- Same vulnerabilities persisting
- No innovation or methodology improvements
- Mechanical compliance without learning

8.3.3 Framework Evolution Adaptation

Auditor Verification:

- How has organization adapted to CPF framework updates?
- Are new indicators incorporated into assessments?
- Has methodology evolved with emerging threats?
- Is organization contributing to framework evolution?

8.4 Crisis Audit

8.4.1 Post-Incident Trigger

Crisis audits may be required after:

- Major security breach with human-factor root cause
- Convergent state materialization (CI>10 realized)
- Significant PVMS failure
- Regulatory investigation

8.4.2 Convergence State Analysis

Special Focus:

- Reconstruct psychological state at time of incident
- Analyze indicator convergence that enabled breach
- Identify "perfect storm" conditions
- Assess why PVMS failed to predict/prevent
- Evaluate emergency response effectiveness

Trauma-Informed Approach Critical:
Organization likely experiencing collective trauma post-incident. Auditor must:

- Approach with empathy and support
- Avoid blame-focused questioning
- Focus on system failures, not individual failures
- Provide psychological safety in interviews
- Recognize emotional responses as normal

8.4.3 Emergency Response Effectiveness

Evaluation Criteria:

- Was convergent state detected before materialization?
- Were emergency protocols activated appropriately?
- How quickly did organization respond?
- Were psychological factors addressed in response?
- What prevented PVMS from preventing incident?

Output:

Crisis audit report with:

- Incident psychological root cause analysis
- PVMS gap analysis
- Emergency corrective actions (immediate)
- Strategic corrective actions (long-term)
- Maturity level reassessment (may result in downgrade)

9 Auditor Competence and Training

9.1 Required Knowledge Areas

CPF Lead Auditors must demonstrate competence across four distinct knowledge domains.

9.1.1 Cybersecurity Fundamentals

Core Knowledge Requirements:

- **Information Security Management Systems**: ISO/IEC 27001:2022 requirements and controls
- **Threat Landscape**: Current attack vectors, social engineering tactics, insider threats
- **Security Operations**: SOC functions, incident response, security monitoring
- **Risk Management**: Risk assessment methodologies, treatment options, residual risk
- **Security Awareness**: Traditional awareness programs, limitations, effectiveness measures
- **Compliance Frameworks**: GDPR, NIS2, DORA, sector-specific regulations

Recommended Certifications:

- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- ISO/IEC 27001 Lead Auditor
- CISA (Certified Information Systems Auditor)

Minimum Requirement: 3+ years cybersecurity experience OR recognized certification

9.1.2 Psychological Theory

Core Knowledge Requirements:

Psychoanalytic Theory:

- **Bion's Basic Assumptions**: Dependency (baD), Fight-Flight (baF), Pairing (baP)
- **Klein's Object Relations**: Splitting, projection, paranoid-schizoid vs. depressive positions
- **Jung's Analytical Psychology**: Shadow, collective unconscious, archetypes
- **Winnicott's Concepts**: Transitional space, holding environment, good-enough mother
- **Defense Mechanisms**: Denial, rationalization, displacement, sublimation

Cognitive Psychology:

- **Kahneman's Dual-Process Theory**: System 1 (fast) vs. System 2 (slow) thinking
- **Cognitive Biases**: Anchoring, availability, confirmation, hindsight
- **Heuristics**: Recognition, affect, availability, representativeness
- **Cognitive Load Theory**: Working memory limitations, attention, multitasking effects

Social Psychology:

- **Cialdini's Influence Principles**: Reciprocity, commitment, social proof, authority, liking, scarcity, unity
- **Conformity Studies**: Asch, Milgram, Stanford Prison Experiment
- **Group Dynamics**: Groupthink, risky shift, diffusion of responsibility
- **Authority and Obedience**: Milgram's findings, organizational hierarchies

Neuroscience Basics:

- **Brain Structure**: Amygdala, prefrontal cortex, limbic system
- **Stress Response**: HPA axis, cortisol, fight/flight/freeze/fawn
- **Decision Timing**: Pre-cognitive processing (300-500ms before awareness)

Recommended Education:

- Psychology degree (Bachelor's or higher) OR
- Psychoanalytic training (minimum 100 hours) OR
- CPF-specific training (minimum 40 hours covering all required theory)

Minimum Requirement: CPF Foundation certification (40-hour course) covering all theoretical foundations

9.1.3 Privacy Regulations

Core Knowledge Requirements:

GDPR Provisions:

- **Article 5**: Data minimization, purpose limitation, storage limitation
- **Article 6**: Lawful basis for processing (legitimate interest for PVMS)
- **Article 9**: Special categories of data (psychological data as sensitive)
- **Article 25**: Privacy by design and by default
- **Article 32**: Security of processing (PVMS as security measure)
- **Article 35**: Data Protection Impact Assessment (DPIA for PVMS)

Differential Privacy:

- **Mathematical Foundation**: ε-privacy definition
- **Privacy Budget**: ε value selection and management
- **Noise Injection**: Laplace mechanism, Gaussian mechanism
- **Composition Theorems**: Sequential and parallel composition

Anonymization Techniques:

- **Aggregation**: Minimum group size ($n \geq 10$)
- **Generalization**: Reducing data precision
- **Suppression**: Removing identifying attributes
- **Temporal Delay**: Time-shifted reporting
- **K-Anonymity**: Set-based anonymization

Recommended Certifications:

- CIPP/E (Certified Information Privacy Professional/Europe)
- CIPM (Certified Information Privacy Manager)
- FIP (Fellow of Information Privacy)

Minimum Requirement: Privacy training covering GDPR and differential privacy fundamentals (minimum 16 hours)

9.1.4 Audit Standards

Core Knowledge Requirements:

ISO 19011:2018:

- **Audit Principles**: Integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach
- **Audit Program Management**: Planning, risk-based scheduling, resource allocation
- **Audit Activities**: Opening meeting, document review, interviews, observations, closing meeting
- **Audit Evidence**: Evaluation, sufficiency, reliability
- **Audit Findings**: Classification, documentation, reporting

ISO/IEC 27006:2015:

- **Certification Body Requirements**: Impartiality, competence, resources
- **Stage 1 and Stage 2 Audits**: Scope, activities, decision criteria
- **Surveillance**: Frequency, scope, focus areas
- **Recertification**: Three-year cycle, comprehensive review

Audit Skills:

- **Interview Techniques**: Open questions, active listening, probing
- **Sampling**: Statistical sampling, risk-based selection
- **Observation**: Behavioral observation, process assessment
- **Evidence Evaluation**: Triangulation, sufficiency, validity
- **Report Writing**: Clear, concise, objective documentation

Required Certification:

- ISO/IEC 27001 Lead Auditor (minimum) OR
- ISO 9001/14001/45001 Lead Auditor + cybersecurity experience

9.2 Practical Skills

9.2.1 Behavioral Observation

Observable Patterns in CPF Audits:

Authority Domain Observation:

- How staff respond to executive requests in meetings
- Verification behavior when unusual requests occur

- Comfort level challenging authority figures
- Hierarchical communication patterns

Group Dynamics Observation:

- Groupthink indicators in security meetings
- Dominant/submissive roles in discussions
- Conflict avoidance behaviors
- Scapegoating or blame patterns

Stress Response Observation:

- Visible stress indicators (body language, tone)
- Cognitive overload signs (confusion, errors)
- Defensive reactions to questions
- Burnout symptoms (disengagement, cynicism)

Skill Development:

- Shadow experienced CPF auditors during observations
- Practice behavioral coding exercises
- Study group dynamics in video scenarios
- Receive feedback on observation accuracy

9.2.2 Interview Techniques

CPF-Specific Interview Skills:

Building Psychological Safety:

- Warm opening, clear explanation of purpose
- Emphasis on organizational vs. individual focus
- Privacy guarantee reinforcement
- Non-judgmental stance throughout

Questioning Techniques:

- **Open Questions**: "Tell me about..." "How do you..." "Describe a time when..."
- **Probing**: "Can you give me an example?" "What happened next?"
- **Clarifying**: "When you say X, do you mean Y?" "Help me understand..."
- **Hypothetical**: "What would happen if..." "How would you respond to..."

Trauma-Informed Adaptation:

- Warning before sensitive topics
- Pacing adjustment for emotional content
- Grounding techniques if dissociation observed
- Immediate support resources available

Skill Development:

- Role-play interview scenarios with feedback
- Review recorded interviews (with consent) for technique analysis
- Practice trauma-informed questioning
- Develop repertoire of follow-up questions

9.2.3 Statistical Analysis

Required Statistical Competencies:

Descriptive Statistics:

- Mean, median, mode calculation
- Standard deviation and variance
- Frequency distributions
- Percentiles and quartiles

Inferential Statistics:

- Confidence intervals
- Hypothesis testing basics
- Chi-square test for independence
- Correlation vs. causation

Sampling Theory:

- Sample size determination
- Sampling error calculation
- Stratified sampling design
- Random selection methods

Differential Privacy Calculations:

- ε-privacy verification

- Privacy budget tracking
- Noise addition validation
- Composition calculation

Practical Application:
Auditors must be able to:

- Recalculate CPF Scores and verify accuracy
- Assess sample size adequacy for reported findings
- Evaluate statistical validity of organization's claims
- Identify when data analysis violates privacy requirements

Skill Development:

- Statistical software training (R, Python, Excel)
- Work through CPF Score calculation examples
- Practice differential privacy implementations
- Complete statistical reasoning exercises

9.2.4 Report Writing

CPF Audit Report Requirements:
Clarity and Precision:

- Clear finding descriptions (what, where, evidence)
- Unambiguous nonconformity classification
- Specific clause references
- Objective language (avoid judgmental terms)

Privacy Compliance:

- No individual identification
- Aggregated data only
- Anonymized quotes
- Small group protection ($n \geq 10$)

Actionability:

- Findings lead to clear corrective actions
- Recommendations are specific and practical

- Timelines are realistic
- Resource requirements estimated

Common Report Writing Errors:

- Vague findings: "Assessment not adequate" (too general)
- Individual identification: Using names or unique identifiers
- Judgmental language: "Poor understanding" vs. "Gap in knowledge"
- Missing evidence: Claims without supporting documentation
- Inconsistent classification: Similar findings with different severity

Skill Development:

- Review sample CPF audit reports
- Practice writing findings from case scenarios
- Peer review of draft reports with feedback
- Learn from experienced auditor report examples

9.3 Certification Path

9.3.1 CPF Foundation (CPF-F)

Target Audience:

- Security practitioners learning CPF concepts
- Internal auditors preparing for PVMS audits
- Privacy officers working with PVMS
- Management overseeing CPF implementation

Course Content (40 hours):

- CPF theoretical foundations (8 hours)
- 10 vulnerability domains overview (8 hours)
- Privacy-preserving assessment (6 hours)
- CPF-27001 requirements overview (6 hours)
- Scoring and maturity model (4 hours)
- Implementation basics (4 hours)
- Case studies and exercises (4 hours)

Assessment:

- 60-question multiple choice exam
- 70% passing score
- 90-minute time limit
- Open book (CPF reference materials allowed)

Certification Validity: 3 years
Recertification: 20 CPE hours in CPF-related topics OR retake exam
Cost: Approximately €500-750

9.3.2 CPF Practitioner (CPF-P)

Prerequisites:

- CPF-F certification OR equivalent knowledge
- 2+ years cybersecurity experience
- Involvement in PVMS implementation or audit

Course Content (5 days / 40 hours):

- Advanced psychological theory (8 hours)
- Indicator assessment methodology deep-dive (8 hours)
- Privacy controls implementation (6 hours)
- Risk treatment design (6 hours)
- Audit techniques (6 hours)
- Practical exercises and simulations (6 hours)

Assessment:

- 100-question exam (multiple choice + scenario-based)
- Case study analysis (written submission)
- Practical assessment exercise
- 75% overall passing score

Certification Validity: 3 years
Recertification: 40 CPE hours including 20 hours CPF-specific OR retake exam
Cost: Approximately €1,500-2,000

9.3.3 CPF Lead Auditor (CPF-LA)

Prerequisites:

- CPF-P certification
- ISO/IEC 27001 Lead Auditor certification (or equivalent)
- Privacy training (GDPR, differential privacy)
- 3+ witnessed CPF audits as observer

Course Content (5 days / 40 hours):

- CPF-27001 clause-by-clause audit methodology (12 hours)
- Privacy-preserving audit techniques (8 hours)
- Trauma-informed interviewing (6 hours)
- Report writing and finding classification (4 hours)
- Auditor competence and ethics (2 hours)
- Mock audit exercises (8 hours)

Assessment:

- Written exam (100 questions)
- Mock audit performance (observed and evaluated)
- Audit report writing exercise
- Oral examination (audit scenario discussion)
- 80% overall passing score

Witnessed Audits:
Before independent auditing, candidates must:

- Participate in 3 CPF-27001 audits as trainee
- Minimum 15 audit days total
- At least 1 initial certification and 1 surveillance audit
- Documented competence assessment by supervising Lead Auditor

Certification Validity: 3 years
Recertification:

- 40 CPE hours (30 hours CPF-specific)
- Minimum 5 CPF audits conducted in 3-year period
- Peer review of 1 audit report
- OR retake course and exam

Cost: Approximately €2,500-3,500

9.3.4 Continuing Professional Development

CPE Requirements by Certification:

Table 11: CPE Requirements

Certification	Total CPE	CPF-Specific	Period
CPF-F	20 hours	10 hours	3 years
CPF-P	40 hours	20 hours	3 years
CPF-LA	40 hours	30 hours	3 years

Acceptable CPE Activities:

- CPF training courses and workshops
- Conference attendance (psychology, cybersecurity, privacy)
- Webinar participation
- Academic coursework in relevant fields
- Publishing articles or research
- Teaching CPF-related content
- Participation in CPF framework development
- Professional reading (with documentation)

CPE Documentation:

Maintain records of:

- Activity description and date
- Duration (hours)
- Learning objectives and outcomes
- Provider/organizer
- Certificate or proof of completion

A Audit Planning Checklist

A.1 Pre-Audit Preparation

4 Weeks Before Audit:

☐ Audit team assigned (Lead Auditor, Technical Auditor, Privacy Specialist)

☐ Audit dates confirmed with organization

☐ Document request sent to organization (14-day advance notice)

☐ Pre-audit communication to executive management

☐ Staff notification communication prepared (organization to distribute)

☐ Logistics arranged (meeting rooms, accommodation, access)

2 Weeks Before Audit:

☐ Documents received and reviewed

☐ Document review findings documented

☐ Stage 1 gaps identified (if initial certification)

☐ Audit plan finalized (risk-based focus areas)

☐ Sampling strategy determined

☐ Interview schedule drafted

☐ Audit checklist customized for organization

1 Week Before Audit:

☐ Pre-audit call conducted with CPF Coordinator

☐ Interview schedule finalized and shared

☐ Special requirements communicated (systems access, data requests)

☐ Consent forms prepared for participant interviews

☐ Privacy Impact Assessment for audit process completed

☐ Team briefing conducted (audit approach, roles, focus areas)

A.2 On-Site Audit Checklist

Day 1 - Opening and Context:

☐ Opening meeting conducted (scope, methodology, logistics confirmed)

☐ Management interviews (executive commitment, policy, resources)

☐ CPF Coordinator interview (PVMS overview, competence assessment)

☐ Privacy Officer interview (privacy controls, compliance)

☐ Document verification (policy, scope, procedures)

☐ Clause 4 (Context) and Clause 5 (Leadership) audit

Day 2 - Planning and Support:

☐ Assessment methodology review (all 10 domains)

- ☐ Privacy protection verification (n≥10, $\varepsilon \leq 0.1$, 72hr delay)
- ☐ Risk treatment plan review
- ☐ Competence records verification
- ☐ Training and awareness assessment
- ☐ Clause 6 (Planning) and Clause 7 (Support) audit

Day 3 - Operations and Evidence:

- ☐ Assessment process deep-dive (indicator sampling and verification)
- ☐ Data triangulation verification (minimum 3 sources per indicator)
- ☐ Privacy controls testing (database queries, access controls)
- ☐ Risk treatment implementation review
- ☐ Staff interviews (aggregated sampling, n≥10)
- ☐ Behavioral observations (meetings, training, SOC operations)
- ☐ Clause 8 (Operation) audit

Day 4 - Performance and Verification:

- ☐ CPF Score recalculation (20-30 indicator sample)
- ☐ Maturity level assessment
- ☐ KPI and monitoring review
- ☐ Internal audit program evaluation
- ☐ Management review minutes analysis
- ☐ Corrective action tracking review
- ☐ Clause 9 (Performance Evaluation) and Clause 10 (Improvement) audit

Day 5 - Closure:

- ☐ Team deliberation (findings discussion, classification)
- ☐ Draft report preparation
- ☐ Closing meeting (findings presentation, Q&A)
- ☐ Conformity decision communicated (preliminary)
- ☐ Next steps explained (corrective actions, report delivery)
- ☐ Appreciation expressed to organization

B Privacy Compliance Verification Checklist

B.1 Aggregation Requirements

☐ All reported metrics meet n≥10 minimum

☐ No small groups (n<10) analyzed separately

☐ Dashboard/tools cannot query below n=10 threshold

☐ Executive team/small departments properly aggregated or excluded

☐ Role-based analysis used (not individual-level)

B.2 Differential Privacy

☐ ε value documented and justified ($\varepsilon \leq 0.1$ required)

☐ Noise injection mechanism documented (Laplace, Gaussian)

☐ Privacy budget tracking implemented

☐ Composition calculations performed for multiple queries

☐ Privacy-utility tradeoff analysis documented

B.3 Temporal Delay

☐ Minimum 72-hour delay between collection and reporting

☐ Real-time dashboards do not display individual psychological data

☐ Incident response does not violate temporal delay without justification

☐ System enforces delay (not just policy)

☐ Emergency exceptions documented with executive approval

B.4 Consent and Transparency

☐ Informed consent obtained for interview participants

☐ Consent forms explain data use, anonymization, aggregation

☐ Voluntary participation clearly communicated

☐ Right to withdraw explained

☐ Privacy notice accessible to all staff

☐ DPIA conducted for PVMS assessment activities

B.5 Data Protection

- ☐ Access controls on assessment data (role-based access)
- ☐ Encryption for data at rest and in transit
- ☐ Data retention policy defined and implemented
- ☐ Secure destruction procedures for expired data
- ☐ Audit trail for all data access
- ☐ No secondary use for performance evaluation

B.6 Report Privacy

- ☐ No individual names in audit report
- ☐ All quotes anonymized
- ☐ Small groups not reported separately
- ☐ Identifying details removed from case examples
- ☐ Report reviewed for re-identification risks before delivery

C Sample Audit Questions by Clause

C.1 Clause 4: Context

- "What psychological factors are unique to your organizational culture?"
- "How do industry-specific threats influence your psychological vulnerabilities?"
- "Who are the key stakeholders for your PVMS and what are their requirements?"
- "How is your PVMS scope defined? Are there any exclusions?"
- "How does PVMS integrate with your existing ISMS?"

C.2 Clause 5: Leadership

- "How does executive management demonstrate commitment to PVMS?"
- "What resources have been allocated for CPF implementation?"
- "Can you show me the CPF Policy and explain how it was developed?"
- "How is CPF performance reported to the board?"
- "Who has overall responsibility for PVMS and what authority do they have?"

C.3 Clause 6: Planning

- "Walk me through your psychological vulnerability assessment methodology."
- "How do you ensure privacy protection during assessments? (n≥10, ε, 72hr)"
- "Show me how you score indicators using the ternary system (Green/Yellow/Red)."
- "What data sources do you use for indicator assessment? (minimum 3)"
- "How do you prioritize risk treatment for identified vulnerabilities?"
- "What are your CPF objectives for this year? How do you measure progress?"

C.4 Clause 7: Support

- "What training has the assessment team received in CPF methodology?"
- "Explain Bion's basic assumptions and their relevance to cybersecurity." (Competence test)
- "How does differential privacy protect individual privacy?" (Privacy Officer)
- "What awareness activities ensure staff understand CPF and privacy protections?"
- "How is PVMS documentation controlled and maintained?"

C.5 Clause 8: Operation

- "Show me your most recent assessment report. How was it conducted?"
- "For indicator [X.Y], what evidence did you collect? From which sources?"
- "How do you ensure n≥10 aggregation in practice?"
- "Walk through the response process for a Red indicator."
- "Which indicators do you monitor continuously vs. assess periodically?"
- "How has risk treatment been implemented for Yellow/Red indicators?"

C.6 Clause 9: Performance Evaluation

- "What KPIs do you track for PVMS effectiveness?"
- "Show me CPF Score trends over the past 12 months. What do they indicate?"
- "How do you verify effectiveness of interventions post-implementation?"
- "Walk me through your internal audit program for PVMS."
- "What CPF topics were discussed in the last management review?"
- "Show me corrective action tracking from the last internal audit."

C.7 Clause 10: Improvement

- "How has your PVMS improved in the past year?"
- "Show me a closed nonconformity. How was root cause determined?"
- "What enhancements have you made to assessment methodology?"
- "How do you identify opportunities for PVMS improvement?"
- "How do you handle updates to the CPF framework when new vulnerabilities emerge?"

D Sample Finding Formats

D.1 CRITICAL Nonconformity Example

Finding NC-001 (CRITICAL): Privacy Violation - Individual Profiling

Clause: 6.1.2 Psychological Vulnerability Assessment (Privacy Requirements)

Evidence:

- Assessment dashboard allows filtering to individual employee level
- Interview with Privacy Officer confirms n<10 queries are possible
- Sample report dated 2025-01-15 shows "IT Security Team (n=8)" analyzed separately
- Database access controls do not prevent individual-level queries

Nonconformity Description:

CPF-27001 Clause 6.1.2 requires minimum aggregation unit of n≥10 to prevent individual profiling. The organization's assessment system allows queries below this threshold. During audit, evidence was found of:

1. Dashboard capability to filter to individual level
2. Recent report analyzing 8-person team separately
3. No technical controls preventing n<10 queries

This constitutes a CRITICAL privacy violation as it enables individual psychological profiling contrary to fundamental CPF privacy protections.

Required Action:

1. Immediate: Disable dashboard queries below n=10 threshold
2. Immediate: Recall and destroy reports violating aggregation requirement
3. Within 7 days: Implement database-level constraint preventing n<10 queries
4. Within 7 days: Retrain assessment team on privacy requirements
5. Within 7 days: Conduct privacy audit of all historical reports

Verification: On-site re-audit required within 30 days.

D.2 MAJOR Nonconformity Example

Finding NC-002 (MAJOR): Assessment Methodology - Insufficient Data Triangulation

Clause: 6.1.2 Psychological Vulnerability Assessment

Evidence:

- Assessment methodology document reviewed (dated 2024-06-10)
- Indicator assessment worksheets for domains [4.x] and [7.x] examined
- Interview with Assessment Specialist confirms single-source scoring in some cases
- Field Kit for indicator 4.3 shows only one data source documented

Nonconformity Description:

CPF-27001 Clause 6.1.2 requires minimum three independent data sources per indicator to enable triangulation. Audit found that indicators in Affective [4.x] and Stress Response [7.x] domains were scored using single data sources (survey data only, without system logs or behavioral observations). This fails to meet triangulation requirements and reduces score validity.

Specifically:

- Indicator 4.3 (Trust Transference): Survey only, no supporting evidence
- Indicator 7.5 (Freeze Response Paralysis): Incident reports only, no triangulation
- Assessment methodology does not mandate minimum 3 sources

Required Action:

1. Within 30 days: Update assessment methodology to mandate 3+ data sources
2. Within 60 days: Re-assess indicators 4.3 and 7.5 with proper triangulation
3. Within 60 days: Train assessment team on triangulation requirements
4. Within 90 days: Implement checklist to verify 3+ sources before indicator scoring

Verification: Document review of updated methodology and re-assessment evidence.

D.3 MINOR Nonconformity Example

Finding NC-003 (MINOR): Training Coverage Below Target

Clause: 7.3 Awareness

Evidence:

- Training completion report dated 2025-01-20
- HR records show 342 of 500 employees completed CPF awareness (68.4%)
- Organization's target: 75% completion per CPF-27001 Level 2 requirements
- Interview with Training Manager confirms tracking and follow-up processes exist

Nonconformity Description:

Organization established 75% training completion target for CPF awareness (aligned with Maturity Level 2 requirements). Current completion rate is 68.4%, falling 6.6 percentage points short of target. While training program is implemented and tracked, completion rate has not yet reached established objective.

Required Action:

1. Within 90 days: Implement targeted outreach to 158 untrained staff
2. Within 120 days: Achieve 75% completion target (375 of 500 staff)
3. Within 180 days: Implement automated reminders for training completion

Verification: Document review of updated training completion report.

D.4 Observation (Not a Nonconformity) Example

Observation OBS-001: Opportunity for Enhanced Monitoring

Context: During review of Clause 8 (Operation), continuous monitoring capabilities were assessed.

Observation:

The organization currently performs quarterly assessments of all 100 indicators, meeting CPF-27001 minimum requirements (annual assessment). However, no continuous monitoring is implemented for critical high-risk indicators.

Opportunity for Improvement:

Consider implementing continuous monitoring for critical indicators such as:

- Authority domain [1.x] indicators (organization's highest risk area, score 16/20)
- Temporal domain [2.x] indicators (seasonal vulnerability patterns observed)
- Convergence Index calculation (monthly vs. quarterly for earlier warning)

Potential Benefits:

- Earlier detection of deteriorating conditions
- More timely intervention for emerging vulnerabilities
- Reduced time to identify convergent states
- Alignment with Maturity Level 3 capabilities

Suggested Implementation:

- Phase 1 (3 months): Identify 10-15 critical indicators for continuous monitoring
- Phase 2 (6 months): Implement automated data collection with privacy protections
- Phase 3 (9 months): Deploy dashboard with monthly/weekly updates
- Budget estimate: €15,000-25,000 for tooling and integration

Note: This is not a nonconformity. Implementation is optional at organization's discretion.

E Glossary of Audit Terms

Aggregation: Combining individual data points into group-level metrics to protect privacy (minimum n=10 in CPF audits).

Conformity: Fulfillment of specified CPF-27001 requirements.

Convergence Index (CI): Multiplicative risk metric measuring alignment of multiple vulnerabilities.

Corrective Action: Action to eliminate the cause of a detected nonconformity.

CPF Score: Overall organizational psychological vulnerability score (0-100 scale, higher = better resilience).

Differential Privacy: Mathematical framework ensuring individual privacy through controlled noise injection (ε-privacy).

Major Nonconformity: Absence or total failure of a CPF-27001 requirement.

Minor Nonconformity: Isolated lapse or deficiency not constituting total failure.

Nonconformity: Non-fulfillment of a CPF-27001 requirement.

Observation: Statement of fact made during audit that does not constitute nonconformity.

Privacy Budget: Maximum allowable privacy loss (ε) across all queries.

PVMS (Psychological Vulnerability Management System): Management system for identifying and mitigating psychological vulnerabilities per CPF-27001.

Surveillance Audit: Periodic audit verifying continued conformity (typically annual).

Temporal Delay: Minimum 72-hour delay between data collection and reporting to prevent real-time surveillance.

Ternary Scoring: Three-level vulnerability assessment (Green=0, Yellow=1, Red=2).

Triangulation: Verification through multiple independent data sources (minimum 3 for CPF indicators).

F References and Bibliography

F.1 CPF Framework Documents

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

F.2 Audit Standards

- ISO 19011:2018. *Guidelines for auditing management systems*. International Organization for Standardization.

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

F.3 Psychological Theory

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

F.4 Privacy and Data Protection

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

F.5 Cybersecurity Research

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

CPF Audit Guidelines v1.0

January 2025

For updates, training, and certification information:
https://cpf3.org