CPF Certification Scheme

Version 1.0

CPF Certification Body
Giuseppe Canale, CISSP
Independent Researcher
g.canale@cpf3.org

January 2025

Abstract

This document defines the certification scheme for the Cybersecurity Psychology Framework (CPF), including requirements for individual certifications (CPF Assessor, CPF Practitioner, CPF Auditor) and organizational certifications (CPF Compliance Levels). The scheme is designed in accordance with ISO/IEC 17065:2012 requirements for certification bodies operating product, process, and service certification systems. This certification scheme enables systematic validation of competence in psychological vulnerability assessment and organizational capability in implementing CPF-based security controls. The framework addresses the critical gap between technical security controls and human factors, providing standardized pathways for professionals and organizations to demonstrate mastery of pre-cognitive vulnerability management.

Keywords: certification, competence assessment, ISO/IEC 17065, cybersecurity psychology, professional development, organizational maturity

Contents

1 Introduction

1.1 Purpose and Scope

The CPF Certification Scheme establishes comprehensive requirements for certifying individuals and organizations in the systematic assessment and mitigation of psychological vulnerabilities within cybersecurity contexts. This scheme addresses the fundamental gap in current cybersecurity certification programs, which focus predominantly on technical competencies while neglecting the psychological dimensions that contribute to 82-85% of security incidents.

The scope of this certification scheme includes:

Individual Certifications:

- CPF Assessor Certification: Validates competence in conducting systematic psychological vulnerability assessments using the CPF methodology
- CPF Practitioner Certification: Confirms practical application of CPF principles in organizational settings
- CPF Auditor Certification: Certifies capability to audit CPF implementation and compliance

Organizational Certifications:

- CPF Compliance Level 1-4: Validates organizational maturity in psychological vulnerability management across four progressive levels

This scheme does not replace existing cybersecurity certifications (CISSP, CISM, CEH, etc.) but complements them by addressing the psychological dimensions absent from technical certification programs.

1.2 Certification Benefits

CPF certification provides measurable value to individuals, organizations, and the broader cybersecurity community:

For Individuals:

- Differentiation in competitive cybersecurity job market
- Recognition of interdisciplinary expertise bridging psychology and security
- Career advancement through specialized competence validation
- Professional development pathway in emerging discipline
- Access to CPF professional community and continuing education

For Organizations:

- Reduced human-factor security incidents through systematic psychological vulnerability management
- Enhanced security posture addressing the 82-85% of breaches with human components

- Competitive advantage demonstrating commitment to comprehensive security
- Improved insurance posture through risk reduction validation
- Regulatory compliance support for human-factor security requirements
- Measurable ROI through incident reduction and risk mitigation

For the Community:

- Standardization of psychological vulnerability assessment practices
- Advancement of cybersecurity psychology as recognized discipline
- Knowledge sharing through certified practitioner network
- Research advancement through validated implementation data
- Industry maturation beyond purely technical approaches

1.3 Organizational Structure

The CPF certification ecosystem operates through a structured hierarchy of entities, each with distinct roles and responsibilities.

1.3.1 CPF3 Organization

CPF3 serves dual roles in the certification ecosystem:

Scheme Owner (Permanent Role):

- Owns all intellectual property rights to the CPF framework and methodology
- Defines and maintains certification requirements and standards
- Develops examination content and training curricula
- Authorizes and licenses certification bodies to operate the scheme
- Provides quality oversight of certification activities
- Maintains central certification registry
- Advances research and framework evolution
- Protects CPF brand and trademarks

First Certification Body (Initial Grace Period):

- Operates as primary certification body during market establishment (3-5 year grace period)
- Certifies initial cohorts of professionals and organizations
- Develops operational procedures and quality systems
- Establishes market credibility
- Gradually transitions operations to authorized third-party bodies

1.3.2 Certification Body Ecosystem

As the program matures, multiple certification bodies may be authorized:

Requirements:

- ISO/IEC 17065:2012 accreditation from nationally recognized body
- Authorization from CPF3 through Scheme Licensing Agreement
- Technical competence in cybersecurity and psychology
- Qualified personnel including certified CPF Auditors
- Secure infrastructure for examination and data management

Operations:

- Certify individuals (Assessor, Practitioner, Auditor)
- Certify organizations (Levels 1-4)
- Certify Authorized Service Providers
- Conduct surveillance and recertification
- Report to CPF3 quarterly

1.3.3 Professional Practice Models

Certified professionals may operate through four models:

Independent Practice:

- Freelance consultants providing services directly
- Individual professional liability
- Cannot use "Authorized Service Provider" designation
- Full autonomy over engagements

Employment by Certification Body:

- Typically CPF Auditors
- Conduct organizational audits
- Must maintain independence per ISO 19011
- Cannot consult and audit same organization

Non-Certified Consulting Firm:

- Employs certified professionals
- Can state "We employ CPF certified professionals"

- Cannot use "Authorized Service Provider" mark
- Lower barrier to entry

Authorized Service Provider (Certified Firm):

- Organizational certification for consulting firms
- Minimum certified personnel requirements (varies by size)
- Quality management system required
- Authorization to use "CPF Authorized Service Provider" mark
- Enhanced benefits and referrals
- Higher credibility in market

1.3.4 Authorized Service Provider Overview

Consulting firms may optionally pursue Authorized Service Provider certification:

Requirements Summary:

- Minimum certified personnel (2-20 based on firm size)
- Quality management system
- Privacy protection framework with annual audit
- Professional liability insurance ($1M-$5M based on size)
- Bi-annual surveillance audits

Benefits Summary:

- Use of "CPF Authorized Service Provider" trademark
- Featured directory listing with priority placement
- Referrals from CPF3
- Access to exclusive tools and templates
- Volume discounts on certifications (10-20%)
- Early access to framework updates
- Co-marketing opportunities

See Section 2.3 for complete Authorized Service Provider certification requirements.

1.4 Relationship to ISO/IEC 17065

This certification scheme is designed to be operated by certification bodies conforming to ISO/IEC 17065:2012, which specifies requirements for bodies certifying products, processes, and services. CPF certification constitutes process and service certification under ISO/IEC 17065 definitions.

Key ISO/IEC 17065 principles applied in this scheme:

Impartiality: Certification bodies must maintain independence from training providers, consultancies, and certified entities. Conflicts of interest are systematically identified and managed.

Competence: Certification body personnel must demonstrate competence in both cybersecurity and psychology domains, validated through education, training, and experience requirements.

Consistency: Certification decisions follow standardized evaluation criteria ensuring comparable outcomes across different assessors, organizations, and time periods.

Confidentiality: Assessment data, particularly psychological vulnerability information, receives heightened confidentiality protection beyond standard ISO/IEC 17065 requirements.

Responsiveness to Complaints: Certification bodies implement robust complaint investigation and resolution procedures with appeal mechanisms for certification decisions.

Certification bodies operating this scheme must maintain ISO/IEC 17065 accreditation through nationally recognized accreditation bodies. This ensures international recognition and mutual acceptance of CPF certifications across jurisdictions.

2 Certification Levels

2.1 Individual Certifications

2.1.1 CPF Assessor Certification

The CPF Assessor certification validates competence to conduct systematic psychological vulnerability assessments using the CPF methodology. Assessors must demonstrate both theoretical knowledge and practical capability to identify, score, and document psychological vulnerabilities across all ten CPF domains.

Requirements:

Education:

- Bachelor's degree in Psychology, Behavioral Science, Organizational Psychology, OR
- Bachelor's degree in Cybersecurity, Information Security, Computer Science PLUS 40 hours of documented CPF-specific training in psychological foundations

Experience:

- Minimum 2 years professional experience in cybersecurity OR psychology
- At least 6 months must involve security-relevant work
- Documentation of experience through employer verification or professional portfolio

Training:

- CPF-101: Framework Fundamentals (40 hours)
- CPF-201: Assessment Methodology (40 hours)
- Total: 80 hours of mandatory training
- Training must be completed within 24 months of certification application

Examination:

- Written Examination: 100 questions covering all ten CPF domains, assessment methodology, privacy protection, and ethical considerations
- Duration: 3 hours
- Passing Score: 70% (70 correct responses)
- Question Distribution: 60 multiple-choice, 30 scenario-based, 10 case analysis
- Practical Assessment: Analysis of organizational case study with vulnerability identification, scoring justification, and intervention recommendations
- Duration: 4 hours
- Passing Requirement: Demonstrated competence across all evaluation criteria

Ethical Requirements:

- Agreement to CPF Code of Ethics
- Commitment to privacy-preserving assessment practices
- Understanding of psychological vulnerability sensitivity
- Prohibition on using assessment data for individual performance evaluation

Certification Validity: 3 years from date of issuance

Recertification Requirements:

- 40 Continuing Professional Education (CPE) credits per year (120 total over 3 years)
- Minimum 5 documented assessments using CPF methodology
- Ethics review and updated agreement
- Continuing education in psychological and cybersecurity advances

2.1.2 CPF Practitioner Certification

The CPF Practitioner certification validates practical application of CPF principles within organizational contexts. Practitioners implement CPF-based interventions, translate assessment findings into actionable security improvements, and integrate psychological vulnerability management with existing security programs.

Requirements:

Education:

- Bachelor's degree in relevant field (Psychology, Cybersecurity, Organizational Behavior, Business Administration with security focus)
- Documented understanding of both security and organizational psychology principles

Experience:

- Minimum 1 year using CPF methodology within organizational setting
- Documentation of practical implementation through project portfolio
- Demonstrated integration of CPF with existing security programs
- Evidence of intervention design and implementation

Training:

- CPF-101: Framework Fundamentals (40 hours)
- No additional mandatory training beyond fundamentals
- Recommended: CPF-201 Assessment Methodology for enhanced competence

Examination:

- Written Examination: 75 questions focusing on practical application, intervention design, and organizational integration
- Duration: 2.5 hours
- Passing Score: 70% (53 correct responses)
- Question Distribution: 45 multiple-choice, 20 scenario-based, 10 application problems
- Portfolio Review: Submission of practical work demonstrating CPF implementation
- Evaluation: Evidence of systematic application, intervention effectiveness, organizational integration

Portfolio Requirements:

- Minimum 3 implementation projects with documented outcomes
- Evidence of assessment-to-intervention pipeline
- Integration documentation with existing security controls
- Demonstrated privacy protection in practice
- Stakeholder engagement and communication examples

Certification Validity: 3 years from date of issuance

Recertification Requirements:

- 30 CPE credits per year (90 total over 3 years)
- Updated portfolio demonstrating continued practical application
- Ethics review and agreement renewal
- Participation in CPF practitioner community of practice

2.1.3 CPF Auditor Certification

The CPF Auditor certification validates competence to audit organizational implementation of CPF methodology, assess compliance with CPF-27001:2025 requirements, and evaluate effectiveness of psychological vulnerability management systems.

Requirements:

Prerequisites:

- Current CPF Assessor certification in good standing
- Minimum 1 year experience as certified CPF Assessor
- Documented completion of at least 10 CPF assessments

Education:

- Existing education requirements satisfied through CPF Assessor certification
- Additional training in audit methodology (ISO 19011:2018)
- Understanding of management system auditing principles

Experience:

- Participation in minimum 3 CPF audits under supervision of certified CPF Auditor
- Minimum 20 audit days documented
- Experience across different organizational types and sizes
- Demonstrated competence in audit planning, execution, and reporting

Training:

- CPF-401: Audit Techniques (40 hours)
- ISO 19011:2018 Auditor Training (minimum 24 hours)
- Integration of psychological assessment with management system auditing

Examination:

- Written Examination: 80 questions covering audit methodology, CPF-27001 requirements, auditor competencies, and professional conduct
- Duration: 3 hours
- Passing Score: 75% (60 correct responses)
- Audit Scenario Examination: Conduct mock audit including planning, execution, finding documentation, and report generation
- Duration: 8 hours (full-day practical examination)
- Passing Requirement: Demonstrated audit competence across all evaluation criteria

Professional Conduct Requirements:

- Adherence to ISO 19011 auditor principles (integrity, impartiality, confidentiality)
- Enhanced privacy protection for psychological vulnerability data
- Independence from consulting and implementation services
- Objective evidence-based audit approach

Certification Validity: 3 years from date of issuance

Recertification Requirements:

- 50 CPE credits per year (150 total over 3 years), with minimum 30 credits in audit-specific topics
- Minimum 15 audit days per year as lead or co-auditor (45 total over 3 years)
- Demonstrated continued audit competence through audit report submissions
- Ethics and professional conduct review
- Participation in auditor calibration activities

2.2 Organizational Certifications

2.2.1 CPF Compliance Levels

Organizational certification validates systematic implementation of psychological vulnerability management according to CPF-27001:2025 requirements. Four progressive compliance levels reflect organizational maturity in addressing human-factor security risks.

Scoring Foundation:

Organizational compliance is based on aggregate CPF Scores derived from systematic assessment of all 100 CPF indicators across the organization's scope. The CPF Score ranges from 0-200, with lower scores indicating better security posture (fewer and less severe vulnerabilities).

Scoring methodology:

- Each indicator scored using ternary system: Green (0), Yellow (1), Red (2)
- Category Score = Sum of 10 indicators per category (range 0-20)
- CPF Score = Sum of 10 category scores (range 0-200)
- Assessment conducted by certified CPF Assessor or Auditor
- Minimum assessment scope: Representative sample ensuring privacy-preserving aggregation (minimum 10 individuals per aggregation unit)

Level 1: Foundation (CPF Score 100-149)

Maturity Characteristics:

- Initial CPF implementation with basic psychological vulnerability awareness

- Reactive approach to human-factor incidents
- Limited integration with existing security programs
- Basic privacy-preserving assessment practices

Minimum Requirements:

- CPF Score between 100-149 from certified assessment
- Documented CPF policy approved by senior management
- Designated CPF Coordinator with defined responsibilities
- Completion of CPF-101 training by security leadership
- Basic assessment conducted covering all 10 domains
- Documented risk treatment plan for Red indicators
- Privacy protection procedures implemented
- Integration plan with existing Information Security Management System (ISMS)

Surveillance Requirements:

- Annual assessment by certified CPF Assessor
- Quarterly reporting of Red indicator status
- Annual management review of CPF program

Level 2: Intermediate (CPF Score 70-99)

Maturity Characteristics:

- Systematic psychological vulnerability management processes
- Proactive identification and treatment of vulnerabilities
- Integrated approach combining psychological and technical controls
- Established privacy protection framework
- Demonstrable reduction in human-factor incidents

Minimum Requirements:

- CPF Score between 70-99 from certified assessment
- All Level 1 requirements maintained
- Minimum one certified CPF Assessor on staff or on retainer
- Quarterly assessment cycles covering all domains
- Documented intervention effectiveness tracking
- Integration with Security Operations Center (SOC) for continuous monitoring of critical indicators

- Established Continuing Professional Education (CPE) program for security staff
- Privacy-preserving dashboard for psychological vulnerability monitoring
- Documented reduction in human-factor incidents (minimum 20% year-over-year)

Surveillance Requirements:

- Bi-annual comprehensive assessment by certified CPF Auditor
- Quarterly self-assessment with certified Assessor validation
- Monthly Red indicator reporting
- Semi-annual management review

Level 3: Advanced (CPF Score 40-69)

Maturity Characteristics:

- Mature psychological vulnerability management program
- Predictive identification of convergent states
- Sophisticated integration across all security domains
- Leading privacy protection practices
- Substantial reduction in human-factor breaches
- Organizational culture of psychological security awareness

Minimum Requirements:

- CPF Score between 40-69 from certified assessment
- All Level 1 and Level 2 requirements maintained
- Minimum two certified CPF Assessors on staff
- Continuous monitoring of all 100 indicators integrated with SIEM
- Predictive analytics for convergent state identification
- Automated alerting for critical psychological vulnerability patterns
- Documented 40% reduction in human-factor incidents compared to baseline
- Advanced privacy protection using differential privacy ($\epsilon \leq 0.1$)
- Contribution to CPF research and community knowledge base
- Integration with third-party risk management for supply chain psychological security
- Psychological vulnerability considerations in all change management processes

Surveillance Requirements:

- Annual comprehensive assessment by certified CPF Auditor

- Continuous self-monitoring with quarterly validation
- Real-time Red indicator alerting and response
- Quarterly management review
- Annual external audit of privacy protection practices

Level 4: Exemplary (CPF Score 0-39)

Maturity Characteristics:

- World-class psychological vulnerability management
- Predictive security posture preventing incidents before occurrence
- Complete integration across all organizational functions
- Industry-leading privacy protection and ethical practices
- Near-elimination of preventable human-factor breaches
- Organizational culture of psychological resilience
- Contribution to industry advancement

Minimum Requirements:

- CPF Score between 0-39 from certified assessment
- All Level 1, 2, and 3 requirements maintained
- Dedicated CPF team including multiple certified Assessors and at least one certified Auditor
- Real-time psychological vulnerability monitoring with AI-enhanced predictive analytics
- Zero Red indicators sustained for minimum 6 months
- Maximum 10% Yellow indicators with documented treatment plans
- Documented 60% reduction in human-factor incidents compared to baseline
- Published research or case studies advancing CPF methodology
- Active contribution to CPF community through knowledge sharing, training, or tool development
- Integration of psychological vulnerability management across supply chain
- Psychological security considerations embedded in enterprise risk management
- Advanced privacy protection practices exceeding differential privacy requirements
- Regular third-party validation of privacy and ethical practices

2.3 Authorized Service Provider Certification

The Authorized Service Provider certification validates consulting firms and professional services organizations that provide CPF-related services while meeting specific quality, staffing, and ethical standards.

2.3.1 Purpose and Scope

This optional organizational certification provides market differentiation for firms employing multiple certified CPF professionals and maintaining systematic quality management of CPF services.

Distinction from Other Certifications:

vs. Individual Professional Certification:

- Individual certification validates personal competence
- ASP certification validates organizational capability
- Firms must employ individually certified professionals
- Both are complementary

vs. Organizational Compliance Certification (Levels 1-4):

- Compliance certification validates organization's management of own vulnerabilities
- ASP certification validates capability to provide services to others
- ASP may also pursue Compliance certification (recommended but not required)

2.3.2 Certification Requirements

Staffing Requirements by Firm Size:

Firm Size	Min. Certified	Composition
Micro (1-10)	2	Any combination
Small (11-50)	5	Min. 2 Assessors
Medium (51-250)	10	Min. 5 Assessors + 1 Auditor
Large (250+)	20	Min. 10 Assessors + 2 Auditors

All certified personnel must:

- Hold current, valid CPF certifications in good standing
- Be employed or under exclusive contract (minimum 1-year commitment)
- Be actively engaged in CPF service delivery (minimum 25% time)
- Maintain required CPE credits

Quality Management System:

Firms must establish documented QMS covering:

Standard Operating Procedures:

- Comprehensive assessment methodology documentation
- Ternary scoring application guidelines
- Privacy protection protocols
- Data collection methods and tools

- Report writing standards with templates
- Client communication protocols
- Project management procedures
- Quality control checklists

Quality Review Process:

- Mandatory peer review of all reports by second certified professional
- Quality control checklist for every project
- Client satisfaction survey for every engagement (5-point scale)
- Quarterly quality metrics review
- Root cause analysis for issues
- Corrective and preventive action system
- Lessons learned database

Metrics and Monitoring:

- Client satisfaction scores (target: ¿4.0/5.0)
- Project delivery timeliness
- Assessment accuracy and consistency
- Client retention rates
- Complaint rates (target: ¡5%)
- Staff utilization
- CPE completion rates

Privacy and Ethics Framework:

Privacy Protection Infrastructure:

- Documented privacy protection policy
- Differential privacy implementation ($\epsilon \leq 0.1$)
- Minimum aggregation units enforced (10 individuals)
- Secure data handling:
  - Encryption at rest (AES-256)
  - Encryption in transit (TLS 1.3 minimum)
  - Multi-factor authentication
  - Role-based access controls
  - Audit logging
  - Secure backup

- Data retention policy (maximum 5 years)
- Secure destruction procedures
- Time-delayed reporting (minimum 72 hours)
- Annual privacy impact assessments
- Annual external privacy audit

Ethics Management:

- Adoption of CPF Code of Ethics at organizational level
- Personnel ethics acknowledgment
- Annual ethics training (minimum 2 hours)
- Internal ethics complaint procedures
- Conflict of interest management
- Independence protocols
- Prohibition on unauthorized data use

Insurance Requirements:

Professional Liability (Errors & Omissions):

Firm Size	Per Occurrence	Aggregate
Micro/Small	$1,000,000	$2,000,000
Medium	$2,000,000	$4,000,000
Large	$5,000,000	$10,000,000

Cyber Liability:

- All sizes: Minimum $1,000,000 coverage
- Must cover data breaches, business interruption, cyber extortion

Certification Body and CPF3 must be named as additional insureds.

2.3.3 Certification Process

Phase 1: Application (Weeks 1-4)

Firm submits comprehensive application including:

- Organizational information
- List of certified personnel with certificate numbers
- Quality management documentation
- Privacy framework and audit report
- Ethics policies and training records

- Insurance certificates
- Sample deliverables (minimum 3 redacted reports)
- Client references (minimum 5)
- Organizational chart
- Application fee

Certification Body conducts:

- Desktop review of application
- Verification of certified personnel status
- Reference checks (minimum 3 contacted)
- Preliminary assessment of QMS adequacy

Phase 2: Certification Audit (Weeks 6-8)

Audit duration: 2-4 days based on firm size

Audit Activities:

- Opening meeting
- QMS review and walkthrough
- Personnel interviews (certified staff, management, quality manager)
- Project file review (3-5 completed projects)
- Infrastructure assessment (data security, tools, systems)
- Privacy framework evaluation
- Ethics program assessment
- Insurance verification
- Client satisfaction analysis
- Closing meeting with findings

Findings classified as:

- Conformity: Requirements met
- Minor Nonconformity: Isolated lapse, correctable within 90 days
- Major Nonconformity: Systemic failure, must correct before certification
- Observation: Improvement opportunity

Audit report delivered within 15 business days.

Phase 3: Corrective Actions (If Needed)

If nonconformities identified:

- Firm submits corrective action plan within 30 days
- Major NCs must be corrected before certification granted
- Minor NCs may be corrected within 90 days after certification
- Certification Body verifies effectiveness

Phase 4: Certification Decision

Within 15 business days of audit completion or corrective action verification:

If Granted:

- Certificate issued (electronic within 3 days, physical within 10 days)
- Digital badge provided
- Added to Authorized Service Provider directory with featured profile
- Welcome package with marketing toolkit
- Access to exclusive resources
- Surveillance schedule established

If Denied:

- Written explanation of deficiencies
- Guidance on remediation
- Right to appeal (30 days)
- Option to reapply after addressing issues

2.3.4 Benefits and Privileges

Marketing and Branding:

- Use of "CPF Authorized Service Provider" trademark
- Official ASP logo in multiple formats
- Digital badge for website and email
- Authorization to display mark on marketing materials, website, proposals
- Approved messaging templates

Featured Directory Listing:

- Priority placement in search results
- Enhanced profile with logo, description (500 words), services, coverage
- Team size and certified personnel indicators
- Contact information and CTAs

- Analytics on profile views and inquiries

Business Development:

- Referrals from CPF3 for organizations seeking services
- Preferred provider status for large engagements
- Access to RFPs requiring ASP status
- Reduced client due diligence burden
- Higher win rates and premium pricing justification

Resources and Support:

- Exclusive assessment tools and templates
- Professional report templates
- Early access to framework updates (90 days advance)
- Dedicated CPF3 account manager
- Technical support priority queue
- Volume discounts on certifications:
  - 10% for 1-5 certifications/year
  - 15% for 6-10 certifications/year
  - 20% for 11+ certifications/year
- Free CPF webinars and e-learning access
- Complimentary conference passes (limited)

Community and Networking:

- Annual CPF Provider Summit
- Quarterly virtual roundtables
- Private online provider forum
- Regional chapter participation
- Collaboration opportunities

2.3.5 Ongoing Obligations

Annual Certification Update:

Due 30 days before anniversary, includes:

- Current certified personnel roster
- Quality metrics summary

- Number of projects completed
- Client satisfaction data
- Updated insurance certificates
- Privacy audit results
- Ethics training records
- Material changes notification

Bi-annual Surveillance Audits:

Every 18 months (1-3 days):

- Focused review (not as comprehensive as initial)
- Sample-based approach (2-3 projects, subset of personnel)
- Verification of continued conformity
- Review of corrective actions
- Assessment of changes since last audit

Performance Monitoring:

Certification Body monitors:

- Maintenance of minimum certified personnel
- Client satisfaction trends (must maintain ¿4.0/5.0)
- Complaint rates (must stay ¡5%)
- Insurance coverage status
- Privacy audit results

Change Notifications:

Immediate (5 business days):

- Fall below minimum personnel
- Insurance lapse
- Privacy/data breach
- Ethics complaints
- Legal actions
- Major personnel loss

30-day notification:

- Ownership changes
- Reorganizations
- Name changes
- Office openings/closures

2.3.6 Suspension and Revocation

Grounds for Suspension (max 180 days):

- Fall below minimum certified personnel
- Insurance lapse
- Failure to complete surveillance
- Failure to pay fees
- Client complaints under investigation
- Privacy breach requiring investigation
- Major NC not corrected within 90 days
- Client satisfaction ¡3.5/5.0 for two quarters

During suspension:

- Restriction on new ASP Mark use
- Directory status: "Suspended - Under Review"
- Referrals suspended
- Must add "Status Under Review" to existing materials
- 180-day remediation period or revocation

Grounds for Revocation:

- Failure to remediate suspension
- Severe privacy violations (profiling, data selling, major breach)
- Fraud or misrepresentation
- Systematic quality failures
- Material ethics violations
- Persistent Mark misuse
- Loss of insurance ¿60 days
- Firm dissolution/bankruptcy

Revocation process:

- Written notice with grounds
- 30 days to respond
- Independent review by ethics committee
- Final decision within 45 days

- Right to appeal

Effect of revocation:

- Immediate cessation of ALL ASP Mark use
- Removal from directory
- Public notice (visible 12 months)
- No refunds
- Reapplication prohibition: 2-5 years or permanent
- Must notify clients

Voluntary Withdrawal:

- 60 days advance notice
- No negative record
- May reapply after 12 months
- Simplified process if within 24 months

2.3.7 Fees

Application Fee:

Firm Size	Fee
Micro	$1,000
Small	$2,000
Medium	$3,500
Large	$5,000

Certification Audit Fee:

Firm Size	Fee
Micro	$3,000
Small	$6,000
Medium	$10,000
Large	$15,000

Additional days: $1,500/day

Certification Fee:

Firm Size	Fee
Micro	$1,500
Small	$2,500
Medium	$4,000
Large	$6,000

Annual Surveillance: Same as certification fee

Recertification (every 3 years):

- Audit: 75% of initial

- Certification: Same as initial

All fees non-refundable. Payment terms: 30 days. Late payment: 1.5% monthly interest.

Surveillance Requirements:

- Annual comprehensive assessment by external certified CPF Auditor
- Continuous self-monitoring with monthly validation
- Real-time convergent state monitoring with automated response
- Monthly management review
- Quarterly external audit of privacy and ethical practices
- Bi-annual peer review by other Level 4 organizations

3 Certification Requirements

3.1 Education Requirements

Education requirements validate foundational knowledge necessary for CPF competence. The interdisciplinary nature of CPF requires understanding of both psychological and cybersecurity principles.

Acceptable Degrees (Bachelor's or Higher):

For Assessor Certification:

- Psychology
- Behavioral Science
- Organizational Psychology
- Industrial/Organizational Psychology
- Cognitive Science
- Cybersecurity (with required supplemental psychology training)
- Information Security (with required supplemental psychology training)
- Computer Science (with required supplemental psychology training)

For Practitioner Certification:

- All degrees acceptable for Assessor certification
- Business Administration with security focus
- Human Resources with security or organizational psychology focus
- Risk Management

Degree Equivalency:

Candidates without formal degrees may qualify through combination of:

- Relevant professional certifications (CISSP, CISM, CEH for security; Licensed Psychologist, SHRM-SCP for psychology)
- Documented professional experience (5 years minimum)
- Completion of all required CPF training
- Passage of enhanced examination demonstrating knowledge equivalent to degree requirements

International Degree Recognition:

Degrees from non-US institutions evaluated using:

- National recognition in degree-granting country
- Equivalency evaluation by credential evaluation service
- Demonstration of English language proficiency for examinations

3.2 Experience Requirements

Experience requirements validate practical capability beyond theoretical knowledge. Experience must demonstrate security-relevant work and exposure to organizational human factors.

Verification Methods:

- Employer verification letters on official letterhead
- Detailed professional portfolio documenting projects and responsibilities
- Professional references from supervisors or clients
- Documented project deliverables (with confidential information redacted)

Qualifying Experience Categories:

Security Experience:

- Security operations and monitoring
- Incident response and investigation
- Security assessment and testing
- Security program management
- Risk assessment and management
- Security awareness program development
- Security policy development and implementation

Psychology Experience:

- Organizational psychology consulting
- Behavioral assessment and intervention

- Human factors analysis
- Organizational development
- Change management
- Training and development program design

Integrated Experience (Counts Double):

- Security awareness program psychology
- Human factors in security design
- Social engineering testing and analysis
- Insider threat program psychology
- Security culture development

3.3 Training Requirements

Mandatory training ensures standardized understanding of CPF methodology, assessment techniques, and ethical practices. Training must be completed through CPF-approved training providers meeting quality and curriculum standards.

CPF-101: Framework Fundamentals (40 hours)

Course Objectives:

- Understand theoretical foundations: psychoanalytic theory, cognitive psychology, group dynamics
- Master CPF architecture: 10 domains, 100 indicators, ternary scoring
- Apply privacy-preserving assessment principles
- Integrate CPF with existing security frameworks (ISO 27001, NIST CSF)

Course Outline:

1. Introduction to Cybersecurity Psychology (4 hours)
    - Failure of conscious-level security interventions
    - Pre-cognitive processing and security decisions
    - Overview of CPF framework
2. Theoretical Foundations (8 hours)
    - Psychoanalytic contributions: Bion, Klein, Jung, Winnicott
    - Cognitive psychology: Kahneman, Cialdini, Miller
    - Group dynamics and organizational unconscious
    - AI psychology and human-AI interaction
3. CPF Domain Deep-Dive (20 hours - 2 hours per domain)

- Authority-Based Vulnerabilities [1.x]
- Temporal Vulnerabilities [2.x]
- Social Influence Vulnerabilities [3.x]
- Affective Vulnerabilities [4.x]
- Cognitive Overload Vulnerabilities [5.x]
- Group Dynamic Vulnerabilities [6.x]
- Stress Response Vulnerabilities [7.x]
- Unconscious Process Vulnerabilities [8.x]
- AI-Specific Bias Vulnerabilities [9.x]
- Critical Convergent States [10.x]

4. Privacy and Ethics (4 hours)
    - Privacy-preserving assessment methodology
    - Differential privacy and aggregation requirements
    - Ethical considerations in psychological assessment
    - Prohibition on individual profiling
5. Integration and Application (4 hours)
    - Integration with ISO 27001 and NIST CSF
    - Organizational implementation strategies
    - Case studies and practical applications

CPF-201: Assessment Methodology (40 hours)

Course Objectives:

- Master systematic assessment process for all 100 indicators
- Develop data collection and analysis skills
- Apply ternary scoring methodology consistently
- Create actionable assessment reports

Course Outline:

1. Assessment Planning (6 hours)
2. Data Collection Methods (8 hours)
3. Scoring and Analysis (12 hours)
4. Privacy-Preserving Techniques (6 hours)
5. Report Writing and Communication (8 hours)

CPF-301: Advanced Implementation (40 hours)

Optional Advanced Training for Practitioners

Course Objectives:

- Design effective interventions for identified vulnerabilities
- Implement continuous monitoring systems
- Integrate psychological and technical controls
- Measure intervention effectiveness

CPF-401: Audit Techniques (40 hours)

Required for Auditor Certification

Course Objectives:

- Apply ISO 19011 auditing principles to CPF context
- Conduct CPF-27001 compliance audits
- Evaluate psychological vulnerability management systems
- Document audit findings and recommendations

3.4 Examination Requirements

Examinations validate knowledge acquisition and practical capability. All examinations are developed using psychometric principles ensuring validity, reliability, and fairness.

Written Examination Structure:

Question Development:

- Item difficulty distribution: 30% easy, 50% moderate, 20% difficult
- Bloom's taxonomy coverage: 20% knowledge, 40% comprehension/application, 40% analysis/synthesis
- Pilot testing and validation before operational use
- Regular statistical analysis and item improvement

Domain Coverage (All Certifications):

- Authority-Based Vulnerabilities: 10%
- Temporal Vulnerabilities: 10%
- Social Influence Vulnerabilities: 10%
- Affective Vulnerabilities: 10%
- Cognitive Overload Vulnerabilities: 10%
- Group Dynamic Vulnerabilities: 10%
- Stress Response Vulnerabilities: 10%
- Unconscious Process Vulnerabilities: 10%
- AI-Specific Bias Vulnerabilities: 10%

- Critical Convergent States: 10%

Exam Administration:

- Computer-based testing at authorized test centers
- Remote proctoring available with enhanced security
- Closed-book examination with no reference materials
- Immediate preliminary results (pending quality review)
- Official results within 5 business days

Passing Standards:

- Assessor/Practitioner Written: 70% minimum
- Auditor Written: 75% minimum (higher standard reflecting advanced role)
- No minimum score per domain, but comprehensive coverage required
- Candidates failing may retake after 30-day waiting period
- Maximum 3 attempts within 12-month period

Practical Examination Structure:

Assessor Practical:

- Case study: Realistic organizational scenario with psychological vulnerability indicators
- Task: Conduct assessment, apply ternary scoring, justify ratings, recommend interventions
- Duration: 4 hours
- Evaluation criteria: Accuracy, justification quality, privacy protection, communication clarity

Auditor Practical:

- Mock audit: Full-day audit simulation including planning, interviews, document review, finding documentation, report generation
- Duration: 8 hours (full business day)
- Evaluation criteria: Audit methodology, evidence collection, finding quality, professional conduct, report clarity

4 Certification Process

4.1 Application

The application process ensures candidates meet eligibility requirements before examination registration.

Application Steps:

1. **Eligibility Self-Assessment**
   - Review certification requirements
   - Verify education qualifications
   - Confirm experience requirements
   - Ensure training completion
2. **Documentation Preparation**
   - Official transcripts or degree certificates
   - Experience verification letters or portfolio
   - Training completion certificates
   - Professional references (minimum 2)
   - Current resume/CV
3. **Application Submission**
   - Complete online application form
   - Upload required documentation
   - Pay application review fee (non-refundable)
   - Electronic signature on Code of Ethics
4. **Application Review**
   - Eligibility verification by certification body
   - Documentation completeness check
   - Reference contact (if needed)
   - Approval or request for additional information
   - Timeline: 10 business days from complete application

Application Fees:

- CPF Assessor: $300 (application review)
- CPF Practitioner: $200 (application review)
- CPF Auditor: $400 (application review)
- Organizational Certification: $500-$2000 based on organization size and scope

4.2 Verification

Verification ensures authenticity and accuracy of submitted documentation.

Education Verification:

- Direct contact with degree-granting institution
- Verification of degree type, major, and conferral date
- International degree equivalency evaluation

- Timeline: 5-10 business days

Experience Verification:

- Contact with listed employers or clients
- Confirmation of employment dates and responsibilities
- Portfolio review for self-employed candidates
- Timeline: 10-15 business days

Reference Checks:

- Contact minimum 2 professional references
- Verification of candidate's competence and professional conduct
- Assessment of suitability for certification
- Confidential feedback to certification body

Training Verification:

- Direct verification with approved training providers
- Confirmation of course completion and dates
- Verification of attendance and assessment results
- Timeline: 3-5 business days

4.3 Examination

Examination validates knowledge and competence through standardized assessment.

Scheduling:

- Exam eligibility notification within 3 business days of verification completion
- Candidate selects exam date and location from available options
- Minimum 14 days advance scheduling required
- Rescheduling permitted up to 48 hours before exam (fee may apply)

Exam Delivery Options:

In-Person Testing:

- Authorized Pearson VUE or Prometric test centers
- Secure testing environment with proctoring
- Identity verification required
- No personal items permitted in testing room

Online Proctored Testing:

- Remote examination via secure platform
- Live proctor monitoring via webcam
- Environmental scan required
- System requirements: Computer, webcam, microphone, stable internet
- Identity verification via government-issued photo ID

Examination Fees:

- CPF Assessor Written: $400
- CPF Assessor Practical: $600
- CPF Practitioner Written: $300
- CPF Practitioner Portfolio Review: $400
- CPF Auditor Written: $450
- CPF Auditor Practical: $800
- Retake Fee: 50% of original exam fee

Retake Policy:

- Failed candidates may retake after 30-day waiting period
- Maximum 3 attempts within 12 months
- After 3 failures, candidate must complete additional training and wait 6 months
- Each retake requires new examination fee
- Practical examination may be retaken independently of written examination

Accommodations:

- Reasonable accommodations provided for documented disabilities
- Request must be submitted with application
- Documentation from qualified professional required
- Examples: Extended time, separate room, screen reader, breaks

4.4 Certification Decision

Certification decisions are made by qualified certification body personnel based on standardized criteria.

Decision Criteria:

Individual Certification:

- Verification of all eligibility requirements
- Passing score on written examination
- Passing evaluation on practical examination/portfolio
- Satisfactory reference checks
- Agreement to Code of Ethics
- Payment of all applicable fees

Organizational Certification:

- Valid CPF assessment by certified Assessor/Auditor
- CPF Score within targeted compliance level range
- Documentation of required policies and procedures
- Evidence of systematic implementation
- Management commitment demonstrated
- Surveillance requirements agreed

Decision Timeline:

- Individual Certification: 10 business days from examination completion
- Organizational Certification: 15 business days from audit completion
- Expedited review available for additional fee

Decision Outcomes:

Certification Granted:

- Certificate issued electronically and in hardcopy
- Entry in public certification registry
- Access to certification holder benefits
- Authorization to use certification marks

Certification Denied:

- Written explanation of deficiencies

- Guidance on remediation steps
- Right to appeal decision
- Option to reapply after addressing deficiencies

Appeal Process:

- Appeals must be submitted in writing within 30 days
- Independent review by appeals panel (not involved in original decision)
- Review of all evidence and decision rationale
- Decision within 30 days of appeal submission
- Appeal fee: $200 (refunded if appeal successful)
- Final decision binding, but candidate may reapply after addressing issues

Certificate Issuance:

- Electronic certificate (PDF) issued within 3 business days
- Physical certificate mailed within 10 business days
- Digital badge for online professional profiles
- Entry in public certification registry within 5 business days
- Certification wallet card for physical identification

5 Maintaining Certification

5.1 Continuing Education

Continuing Professional Education (CPE) ensures certified individuals maintain current knowledge as CPF methodology and cybersecurity landscape evolve.

CPE Requirements:

CPF Assessor:

- 40 CPE credits per year (120 over 3-year cycle)
- Minimum 20 credits in CPF-specific topics
- Maximum 10 credits from single activity/source per year
- Minimum 5 credits in ethics and privacy annually

CPF Practitioner:

- 30 CPE credits per year (90 over 3-year cycle)
- Minimum 15 credits in CPF-specific topics

- Maximum 10 credits from single activity/source per year
- Minimum 3 credits in ethics annually

CPF Auditor:

- 50 CPE credits per year (150 over 3-year cycle)
- Minimum 30 credits in audit-specific topics
- Minimum 10 credits in CPF methodology updates
- Maximum 10 credits from single activity/source per year
- Minimum 5 credits in ethics and professional conduct annually

Accepted CPE Activities:

Category A: Formal Education (1 hour = 1 credit)

- Approved CPF training courses
- Academic courses in psychology or cybersecurity
- Professional certification training (CISSP, CISM, etc.)
- Webinars and virtual training

Category B: Professional Development (1 hour = 1 credit)

- Conference attendance (cybersecurity or psychology)
- Professional association meetings
- CPF community of practice participation
- Mentoring certified candidates (maximum 5 credits/year)

Category C: Self-Study (2 hours = 1 credit)

- Reading professional journals and publications
- Review of CPF methodology updates
- Independent research in relevant topics
- Online courses without assessment

Category D: Contributions (Special Credit)

- Publishing CPF research or case studies: 10 credits
- Developing CPF training materials: 15 credits
- Speaking at conferences on CPF topics: 5 credits per presentation
- Serving on CPF advisory committees: 10 credits/year

- Contributing to CPF methodology development: 20 credits

Documentation Requirements:

- Certificate of completion for formal training
- Attendance records for conferences
- Reading logs with summaries for self-study
- Publication citations for authored works
- Verification from benefiting organizations for volunteer work
- All documentation maintained for 5 years

CPE Tracking:

- Online CPE portal for activity logging
- Automatic credit for approved activities
- Upload capability for supporting documentation
- Progress dashboard showing credit accumulation
- Automated reminders for approaching deadlines

CPE Audit:

- Random audit of 10% of certification holders annually
- Request for documentation of claimed CPE activities
- Verification of activity completion and credit calculation
- 30-day response period for documentation submission
- Non-compliance may result in certification suspension

5.2 Recertification

Recertification occurs every 3 years and validates continued competence and ethical practice.

Recertification Requirements:

All Individual Certifications:

- Completion of all CPE requirements for 3-year cycle
- Continued professional experience in relevant role
- No substantiated ethics violations
- Payment of recertification fee
- Updated agreement to Code of Ethics
- Demonstration of current competence

Additional Assessor Requirements:

- Minimum 5 documented CPF assessments over 3-year period
- Peer review of at least one assessment report
- Participation in assessor calibration activities

Additional Auditor Requirements:

- Minimum 45 audit days over 3-year period (15/year average)
- Lead auditor role in minimum 5 audits
- Audit report quality review
- Participation in auditor competence evaluation

Recertification Process:

1. **Notification** (180 days before expiration)
   - Certification body sends recertification notice
   - Candidate reviews requirements and current status
   - CPE deficit identification and remediation plan if needed
2. **Documentation Submission** (90 days before expiration)
   - CPE records submitted via online portal
   - Experience documentation uploaded
   - Professional references provided (if required)
   - Ethics attestation completed
3. **Review and Verification** (60 days before expiration)
   - Certification body reviews submission
   - CPE audit (if selected)
   - Experience verification
   - Ethics record check
4. **Recertification Decision** (30 days before expiration)
   - Approval or request for additional information
   - New certificate issued upon approval
   - Updated certification period in registry

Recertification Fees:

- CPF Assessor: $400
- CPF Practitioner: $300
- CPF Auditor: $500

- Late recertification (within 90 days after expiration): Additional $100
- Reinstatement (beyond 90 days after expiration): Full certification process required

Grace Period:

- 90-day grace period after expiration
- Certification status changes to "Pending Recertification"
- Use of certification marks restricted during grace period
- Late fee applies for recertification during grace period
- After grace period, full recertification process required

Organizational Recertification:

- Annual surveillance audits required
- Full reassessment every 3 years
- Continuous monitoring of CPF Score
- Compliance level may be upgraded or downgraded based on performance
- Significant organizational changes trigger reassessment

5.3 Ethics and Professional Conduct

Ethics requirements ensure certification holders maintain professional standards and protect stakeholder interests.

Code of Ethics - Core Principles:

1. **Integrity**
   - Honest representation of qualifications and capabilities
   - Accurate reporting of assessment findings
   - Transparent communication with stakeholders
   - No falsification of documentation or data
2. **Objectivity**
   - Unbiased assessment and evaluation
   - No conflicts of interest
   - Independence from commercial pressures
   - Evidence-based decision making
3. **Confidentiality**
   - Protection of assessment data
   - Secure handling of psychological vulnerability information
   - No unauthorized disclosure

- Enhanced privacy protection for sensitive data

4. **Competence**
   - Practice within areas of demonstrated competence
   - Continuous professional development
   - Recognition of competence limitations
   - Referral when expertise insufficient
5. **Professional Responsibility**
   - Adherence to CPF methodology standards
   - Compliance with applicable laws and regulations
   - Reporting of unethical behavior
   - Contribution to professional community

Specific Ethical Requirements:

Privacy Protection:

- Never use assessment data for individual profiling
- Maintain minimum aggregation units (10 individuals)
- Implement differential privacy protections
- Secure storage and transmission of all data
- Prohibition on secondary use without explicit consent
- Time-delayed reporting (minimum 72 hours)
- Role-based rather than individual analysis

Conflict of Interest:

- Disclosure of all potential conflicts before engagement
- No financial interest in assessment outcomes
- Independence from training providers when assessing
- No consulting and auditing for same organization simultaneously
- Prohibition on accepting gifts or incentives

Scope of Practice:

- CPF assessment is organizational, not clinical psychological assessment
- No individual diagnosis or therapeutic interventions
- Recognition that psychological vulnerabilities are normal human characteristics
- No stigmatization or blame of individuals for vulnerabilities
- Clear boundaries between CPF and clinical psychology

Data Handling:

- Encryption of all assessment data at rest and in transit
- Access controls limiting data to authorized personnel
- Audit trails for all data access
- Retention limits (maximum 5 years unless legally required)
- Secure destruction of data after retention period
- No cross-border data transfer without appropriate safeguards

Disciplinary Process:

Complaint Submission:

- Anyone may file complaint against certified individual or organization
- Complaint submitted in writing with specific allegations
- Supporting evidence provided
- Complainant identity protected (option for anonymous complaints)

Investigation:

- Initial review within 10 business days
- Investigation by ethics committee (independent from certification decisions)
- Opportunity for accused party to respond
- Evidence gathering and witness interviews
- Investigation completed within 60 days (extendable if complex)

Findings and Sanctions:

Finding: No Violation

- Complaint dismissed
- No record on certification file
- Parties notified of outcome

Finding: Minor Violation

- Written warning issued
- Corrective action plan required
- Enhanced CPE requirements
- Progress monitoring

Finding: Significant Violation

- Certification suspension (6-12 months)
- Remediation requirements before reinstatement
- Probationary period after reinstatement
- Public disclosure in certification registry

Finding: Severe Violation

- Certification revocation
- Prohibition on reapplication (2-5 years or permanent)
- Public disclosure
- Notification to relevant authorities if legal violations involved

Appeal of Disciplinary Action:

- Appeal must be filed within 30 days of decision
- Independent appeals panel reviews case
- No new evidence permitted (review of process and proportionality)
- Decision within 45 days
- Appeal fee: $500 (refunded if appeal successful)

6 Certification Bodies

6.1 Accreditation Requirements

Certification bodies operating this scheme must maintain appropriate accreditation and demonstrate specific competencies.

ISO/IEC 17065 Accreditation:

- Accreditation from nationally recognized accreditation body
- Accreditation scope includes process and service certification
- Annual surveillance audits by accreditation body
- Full reassessment every 4 years
- Compliance with all ISO/IEC 17065 requirements

CPF-Specific Competencies:

Personnel Requirements:

- Certification scheme manager with expertise in both cybersecurity and psychology
- Minimum 2 technical experts with CPF Auditor certification

- Access to subject matter experts in psychoanalytic theory and cognitive psychology
- Examination development personnel with psychometric expertise
- Privacy and ethics specialists

Technical Competence:

- Understanding of all ten CPF domains and 100 indicators
- Knowledge of privacy-preserving assessment methodologies
- Familiarity with differential privacy and aggregation requirements
- Integration knowledge for ISO 27001 and NIST CSF
- Competence in psychological ethics and professional conduct

Infrastructure Requirements:

- Secure examination development and storage systems
- Encrypted candidate database with access controls
- Online application and CPE tracking platforms
- Secure communication channels for sensitive information
- Backup and disaster recovery capabilities

Quality Management System:

Documentation:

- Certification scheme procedures fully documented
- Decision-making criteria clearly defined
- Appeals and complaints procedures established
- Records retention and management procedures
- Confidentiality and impartiality procedures

Process Controls:

- Standardized application review process
- Consistent examination administration
- Calibrated decision-making across personnel
- Regular competence evaluation of staff
- Internal audits of certification processes

Continuous Improvement:

- Regular review of examination statistics
- Analysis of appeals and complaints for systemic issues
- Stakeholder feedback mechanisms
- Benchmarking against other certification bodies
- Implementation of corrective and preventive actions

6.2 Quality Assurance

Quality assurance ensures consistency, reliability, and credibility of certification decisions.

Audits of Certification Bodies:

Accreditation Body Audits:

- Annual surveillance by ISO/IEC 17065 accreditation body
- Review of certification files and decisions
- Witness assessments and examinations
- Evaluation of competence management
- Full reassessment every 4 years

CPF Scheme Owner Audits:

- Annual audit of CPF-specific requirements compliance
- Review of examination quality and validity
- Assessment of technical competence in CPF domains
- Evaluation of privacy protection practices
- Verification of ethics and disciplinary procedures

Peer Review:

- Cross-audits between certification bodies
- Sharing of best practices
- Calibration of decision-making
- Identification of improvement opportunities

Complaint Handling:

Types of Complaints:

- Certification process complaints (delays, communication, fairness)
- Examination complaints (quality, administration, fairness)
- Certified personnel complaints (ethics, competence, conduct)

- Organizational certification complaints (audit quality, decisions)

Complaint Process:

1. Complaint submission (written, with details)
2. Acknowledgment within 3 business days
3. Investigation within 30 days
4. Resolution and response to complainant
5. Corrective action if warranted
6. Trend analysis for systemic issues

Complaint Records:

- All complaints logged in complaint register
- Investigation documentation maintained
- Resolution and corrective actions recorded
- Regular review by management
- Annual summary reporting to accreditation body

Continuous Improvement:

Performance Metrics:

- Application processing time
- Examination pass rates and statistics
- Appeals and complaints rates
- Certification holder retention rates
- Stakeholder satisfaction scores

Improvement Mechanisms:

- Regular management review of quality metrics
- Analysis of examination statistics for validity
- Review of appeals for decision consistency
- Stakeholder surveys and feedback
- Implementation of identified improvements
- Sharing of lessons learned across certification bodies

6.3 Appeals and Complaints

Robust appeals and complaints procedures ensure fairness and provide recourse for stakeholders.

Appeal Process:

Appealable Decisions:

- Certification denial
- Examination failure (procedural issues only, not score)
- Disciplinary actions
- Recertification denial
- Certification suspension or revocation

Appeal Procedure:

1. Appeal submitted in writing within 30 days of decision
2. Appeal fee payment ($200-$500 based on decision type)
3. Specification of grounds for appeal
4. Supporting documentation provided
5. Independent appeals panel assigned (no involvement in original decision)
6. Review of all evidence and decision rationale
7. Opportunity for appellant to provide additional information
8. Panel deliberation and decision
9. Decision communicated within 30 days of appeal submission
10. Options: Uphold original decision, Modify decision, Reverse decision, Remand for reconsideration
11. Fee refunded if appeal successful
12. Decision is final (no further appeals)

Complaint Investigation:

Investigation Process:

1. Complaint submission with specific allegations
2. Initial review for completeness and jurisdiction
3. Assignment to investigator (independent from subject)
4. Notice to subject of complaint with opportunity to respond
5. Evidence gathering and witness interviews
6. Investigation report with findings

7. Decision on complaint validity and corrective actions
8. Communication to complainant and subject
9. Implementation of corrective actions
10. Follow-up to verify effectiveness

Resolution Procedures:

Informal Resolution:

- Mediation between parties
- Clarification of misunderstandings
- Corrective action by certification body
- Withdrawal of complaint if resolved

Formal Resolution:

- Official investigation findings
- Corrective or disciplinary actions
- Changes to certification body procedures
- Compensation or remediation if warranted
- Prevention measures to avoid recurrence

6.4 Scheme Licensing

CPF3, as Scheme Owner, authorizes qualified certification bodies to operate the CPF Certification Scheme through a formal licensing process. This ensures consistency, quality, and integrity of certifications across multiple certification bodies globally.

6.4.1 Licensing Objectives

The licensing model serves multiple strategic objectives:

- *Scalability:* Enable geographic and market expansion beyond CPF3's direct capacity
- *Accessibility:* Increase access to certification services globally
- *Localization:* Allow regional adaptation within consistent framework
- *Competition:* Foster healthy competition improving service quality
- *Risk Distribution:* Diversify operational risk across independent entities
- *Revenue Generation:* Create sustainable revenue for scheme development
- *Quality Control:* Maintain centralized oversight with distributed operations
- *Brand Protection:* Ensure consistent standards protecting CPF reputation

Licensing Philosophy:

- *Selective Authorization:* Rigorous standards ensure only capable bodies authorized
- *Active Oversight:* CPF3 maintains continuous monitoring and intervention rights
- *Collaborative Relationship:* Licensed bodies are partners in shared success
- *Continuous Improvement:* Feedback informs scheme evolution
- *Consistency First:* Adaptation acceptable only where consistency maintained
- *Long-term Partnerships:* Structured for sustained relationships

6.4.2 Licensing Requirements

Foundational Accreditation Prerequisites:

ISO/IEC 17065:2012 Accreditation:

- Current, valid accreditation from IAF MLA signatory accreditation body
- Examples: ANAB (USA), UKAS (UK), DAkkS (Germany), JAS-ANZ (Australia/NZ)
- Scope must include:
  - Product, process, and service certification
  - Management system certification
  - Personnel certification
- Good standing: No major nonconformities in recent audit
- Minimum 2 years operational history under current accreditation

Technical Competence:

Personnel Requirements:

- *Scheme Manager:*
  - Master's degree in Psychology, Cybersecurity, or related (or equivalent)
  - 5+ years certification operations OR psychology/cybersecurity consulting
  - Understanding of both psychological and security contexts
  - Minimum 0.5 FTE dedicated to CPF
- *Technical Expert - Psychology:*
  - Master's/PhD in Psychology (I/O Psychology preferred)
  - 3+ years organizational psychology experience
  - Role: Technical review, examination development, training
  - Minimum 1 FTE total
- *Technical Expert - Cybersecurity:*
  - Professional certifications (CISSP, CISM, or equivalent)

  - 5+ years cybersecurity/risk management experience
  - Role: Security context review, integration guidance
  - Minimum 1 FTE total
- *Certified CPF Auditors:*
  - Minimum 2 certified CPF Auditors on staff or exclusive contract
  - Current, valid CPF Auditor certification
  - Available for organizational certification audits
- *Examination Development Specialist:*
  - Competency in psychometrics and test development
  - Degree in psychometrics, educational measurement, or equivalent
  - 2+ years examination development experience
  - May be contracted specialist
- *Privacy and Data Protection Specialist:*
  - Expertise in GDPR, CCPA, and data protection laws
  - CIPP (Certified Information Privacy Professional) or equivalent
  - Understanding of differential privacy techniques
  - May be contracted specialist

Collective Competence:

Beyond individual roles, must demonstrate:

- Coverage of all 10 CPF domains
- Understanding of psychoanalytic foundations (Bion, Klein, Jung, Winnicott)
- Understanding of cognitive psychology (Kahneman, Cialdini, Miller)
- Knowledge of ISO 27001, NIST CSF
- Cultural and language capabilities for service territories

Infrastructure Requirements:

Examination Security:

- Secure development environment (isolated network, AES-256 encryption)
- Multi-factor authentication and audit logging
- Physical security for printed materials (locked safe, restricted access)
- Secure test delivery platform (Pearson VUE, Prometric, or equivalent)
- Remote proctoring capability
- Identity verification procedures
- Incident reporting protocols

Candidate Management:

- Encrypted candidate database (GDPR/CCPA compliant)
- Role-based access controls with audit trails
- Online application portal
- CPE tracking platform
- Integration with CPF3 central registry
- Certificate generation with anti-counterfeiting features
- Digital badge distribution

Communication Infrastructure:

- Encrypted email (S/MIME or PGP)
- Secure file sharing (SFTP or secure portal)
- Secure video conferencing
- API or data exchange with CPF3 registry

Business Continuity:

- Daily encrypted backups with offsite storage
- Disaster recovery plan (RTO: 48 hours, RPO: 24 hours)
- Quarterly tested recovery procedures
- Alternative operations site identified
- ISO 22301 compliance recommended

Financial Requirements:

Demonstrated Stability:

- Minimum 3 years audited financial statements
- Positive equity position
- Adequate cash reserves (6 months operating expenses)
- No bankruptcy or insolvency proceedings

Licensing Fees:

- Application fee: $10,000 (non-refundable)
- Initial licensing fee: $25,000 - $100,000 (based on territory)
- Annual licensing fee: $15,000 - $50,000
- Royalty fees: 10-15% of certification revenues

- Minimum annual royalty: $10,000
- Examination licensing: $5,000 annually
- Estimated setup costs: $50,000 - $150,000

Insurance Requirements:

- Professional liability: $5M per occurrence, $10M aggregate
- Cyber liability: $2M coverage
- CPF3 named as additional insured
- Certificates provided annually

6.4.3 Licensing Process

Timeline: 6-12 months from application to operational status

Phase 1: Application (Month 1-2)

Prospective body submits comprehensive package:

- Executive summary and motivation
- Organizational information and legal documentation
- ISO/IEC 17065 accreditation certificate and recent audit report
- Personnel competency documentation (resumes, certifications)
- Infrastructure documentation (IT systems, security measures)
- Quality management system manual and procedures
- Financial statements (3 years) and business plan
- Proposed territory and market analysis
- Insurance certificates
- References (accreditation body, scheme owners, clients)
- Application fee payment ($10,000)

CPF3 Initial Review (30 days):

- Completeness check
- Eligibility assessment
- Accreditation verification
- Financial stability review
- Personnel competency evaluation
- Infrastructure adequacy assessment

- Territory availability confirmation
- Outcome: Approved for assessment / Conditional / Denied

Phase 2: Assessment Audit (Month 3-5)

On-Site Assessment (3-5 days):

CPF3 assessment team conducts comprehensive audit:

- Day 1: Opening meeting, QMS review, procedures walkthrough
- Day 2: Personnel interviews and competency assessment
- Day 3: Infrastructure and security testing, systems demonstration
- Day 4: Business operations, facilities, records management
- Day 5: Findings development, closing meeting

Assessment covers:

- Quality management system effectiveness
- Certification procedures and decision-making
- Personnel competence and availability
- Infrastructure security and capabilities
- Examination security measures
- Financial systems and business planning
- Compliance with all licensing requirements

Assessment Report (2 weeks):

- Executive summary and readiness determination
- Detailed findings with evidence
- Classification: Conformity / Gaps / Concerns
- Strengths and capabilities
- Required corrective actions (if any)
- Recommendations for improvement

Gap Remediation (If Needed):

- Certification body submits remediation plan (30 days)
- Implements corrections
- CPF3 verifies remediation (desktop or follow-up visit)

- Must complete before proceeding to licensing

Phase 3: Licensing Agreement (Month 6-7)

Commercial Negotiation:

Parties negotiate terms:

- Territory definition (exclusive or non-exclusive)
- Initial and annual licensing fees
- Royalty rates and minimum guarantees
- Performance metrics and targets
- Support services from CPF3
- Marketing and co-branding terms
- Term length (typically 5 years) and renewal

Legal Execution:

- Draft Scheme Licensing Agreement prepared
- Legal review by both parties
- Negotiation of specific terms
- Execution by authorized signatories
- Payment of initial licensing fee
- Effective date established

Phase 4: Implementation (Month 8-12)

Personnel Training (Month 8-9):

- Scheme Manager: 5-day comprehensive training
- Technical experts: CPF-101 and CPF-201 (80 hours)
- Auditors: CPF-401 plus CB-specific procedures
- Support staff: Systems, procedures, customer service
- Fast-track certification for key personnel
- Competency validation through practical exercises

Systems Integration (Month 9-10):

- API setup with CPF3 central registry
- Test data exchange and synchronization

- Examination platform configuration
- Remote proctoring setup
- Marketing materials development
- Website integration
- All systems tested end-to-end

Shadow Operations (Month 11):
Pilot phase with CPF3 oversight:

- Shadow audits: CB auditors accompany CPF3 on 3 audits
- Pilot certifications: Process 5-10 under supervision
- Mock examinations to test procedures
- Quality review of all pilot outputs
- Issue identification and resolution
- Final procedure adjustments

Launch Approval (Month 12):

- Final readiness assessment
- Approval to commence independent operations
- Public announcement of new licensed CB
- Addition to CPF3 website directory
- Coordinated marketing launch
- Transition to standard ongoing support

6.4.4 Ongoing Oversight

Annual Audits by CPF3:
Comprehensive annual audit (2-4 days):
Scope:

- Certification process compliance (sample 10-15 decisions)
- Examination administration and security
- Personnel competency maintenance
- QMS effectiveness
- Privacy and confidentiality controls
- Complaint and appeals handling

- Registry accuracy
- Financial reporting and royalty calculations
- Marketing and trademark usage
- Client satisfaction

Process:

- 30 days advance notice
- Findings documented and classified
- Report within 15 business days
- Corrective action for nonconformities (30 days)
- Verification of actions
- CPF3 bears routine costs; CB pays for follow-up if major NCs

Quarterly Reporting:

Certification bodies submit detailed reports including:

- Certification statistics by type
- Applications, approvals, denials
- Examination pass/fail rates
- Appeals and complaints summary
- Financial data and royalty calculation
- Quality metrics
- Significant incidents or changes

Due: Within 30 days of quarter end

Inter-CB Calibration:

Bi-annual workshops (mandatory attendance):

- Scoring consistency exercises
- Discussion of challenging cases
- Best practice sharing
- Scheme updates and training
- Performance benchmarking
- Peer learning

Costs shared between CPF3 and participating CBs.

Performance Monitoring:

CPF3 monitors key indicators:

- Examination pass rates (within 15% of scheme average)
- Appeal rates (¡5% of decisions)
- Complaint substantiation (¡10%)
- Certification cycle time (¡90 days average)
- Client satisfaction (¿4.0/5.0)

Intervention triggered if standards not met for two consecutive quarters.

6.4.5 License Suspension and Termination

Grounds for Suspension (max 180 days):

- Major NC in annual audit not corrected within timeframe
- Loss of ISO/IEC 17065 accreditation or major finding
- Significant increase in appeals/complaints
- Pass/fail rates outside acceptable range
- Financial instability or fee non-payment (60+ days)
- Privacy or confidentiality breach
- Personnel competence deficiencies
- Insurance lapse

During suspension:

- No new applications accepted
- Existing certifications remain valid
- Must correct within 180 days or face termination

Grounds for Immediate Termination:

- Failure to remediate suspension (180 days)
- Loss of ISO/IEC 17065 accreditation
- Fraud, misrepresentation, or severe ethics violations
- Material breach of licensing agreement
- Bankruptcy or insolvency

- Unauthorized use of CPF IP
- Systematic quality failures damaging scheme reputation

Post-Termination Succession:

Critical provisions ensure continuity:

- All certifications issued remain valid until normal expiration
- Certified parties may transfer to another licensed CB
- Terminated CB transfers all records to CPF3 (30 days)
- CPF3 or designated successor provides ongoing support
- Terminated CB ceases all CPF mark use immediately
- No refund of licensing fees
- Financial obligations settled (90 days)

6.4.6 Financial Terms Summary

Fees Paid to CPF3:

Fee Type	Amount	When Due
Application	$10,000	With application
Initial License	$25K-$100K	Upon agreement execution
Annual License	$15K-$50K	Annually on anniversary
Exam Materials	$5,000/year	Annually
Royalties	10-15%	Quarterly
Min. Annual Royalty	$10,000	If actual ¡minimum

Royalty Structure:

- Individual certifications (Assessor, Practitioner, Auditor): 15%
- Organizational certifications (Levels 1-4): 10%
- Authorized Service Provider certifications: 12%
- Recertification fees: Same percentage
- Examination retakes: 15%

Payment terms: Quarterly reporting and remittance within 30 days of quarter end.

6.4.7 Benefits of Licensed Status

For Certification Bodies:

- Authorization to operate recognized certification scheme
- Access to established brand and methodology

- Marketing support and co-branding opportunities
- Technical support from CPF3
- Examination materials and item banks
- Training resources and materials
- Central registry integration
- Participation in global certification community
- Revenue generation from growing market

For the Ecosystem:

- Geographic expansion and accessibility
- Local market presence and cultural adaptation
- Competition driving service quality improvements
- Diverse perspectives enhancing scheme evolution
- Risk distribution across multiple entities
- Scalability enabling market growth
- Mutual recognition across territories

This comprehensive licensing framework enables controlled expansion of the CPF certification ecosystem while maintaining quality, consistency, and integrity essential for long-term credibility and market acceptance.

Appendices

A Sample Exam Questions

A.1 CPF Assessor Sample Questions

Multiple Choice Questions:

Question 1: Which of the following best describes the primary purpose of CPF assessment?

a) To identify employees who pose security risks
b) To measure conscious security awareness levels
c) To identify organizational-level pre-cognitive psychological vulnerabilities
d) To evaluate individual psychological fitness for security roles

Correct Answer: c

Question 2: According to CPF methodology, what is the minimum aggregation unit for reporting assessment data?

a) 5 individuals
b) 10 individuals

c) 25 individuals
d) 50 individuals

Correct Answer: b

Question 3: In the ternary scoring system, a Yellow (1) indicator represents:

a) Minimal vulnerability with no action required
b) Moderate vulnerability requiring monitoring
c) Critical vulnerability requiring immediate intervention
d) Eliminated vulnerability

Correct Answer: b

Scenario-Based Questions:

Question 4: An organization's finance department consistently processes urgent wire transfer requests from anyone with "CEO" in their email signature without additional verification. This behavior primarily indicates vulnerability in which CPF domain?

a) [2.x] Temporal Vulnerabilities
b) [1.x] Authority-Based Vulnerabilities
c) [3.x] Social Influence Vulnerabilities
d) [5.x] Cognitive Overload Vulnerabilities

Correct Answer: b - Authority-Based Vulnerabilities, specifically indicator 1.1 (Unquestioning compliance with apparent authority)

Question 5: During end-of-quarter periods, security incident rates increase by 35%, primarily involving employees bypassing approval processes to meet deadlines. Which convergent vulnerability state does this represent?

a) Pure [2.x] Temporal Vulnerability
b) [10.4] Swiss cheese alignment of temporal and authority vulnerabilities
c) [6.1] Groupthink security blind spots
d) [5.2] Decision fatigue errors

Correct Answer: b - This represents convergence of temporal pressure ([2.3] Deadline-driven risk acceptance) with organizational patterns creating perfect storm conditions

A.2 CPF Practitioner Sample Questions

Application Questions:

Question 6: An assessment reveals high Red scores in Domain 5 (Cognitive Overload) with alert fatigue affecting 70% of security team. Which intervention would be MOST effective according to CPF principles?

a) Additional security awareness training
b) Disciplinary action for ignored alerts
c) Reduction of false positive alerts and alert consolidation
d) Hiring additional security personnel

Correct Answer: c - Addresses root cause of cognitive overload rather than symptoms

Question 7: When integrating CPF with an existing ISO 27001 ISMS, psychological vulnerability assessment results should be primarily incorporated into which ISMS component?

a) Asset inventory
b) Risk assessment process
c) Access control procedures

d) Incident response plan

Correct Answer: b - Psychological vulnerabilities are risk factors requiring systematic risk assessment and treatment

A.3 CPF Auditor Sample Questions

Audit Methodology Questions:

Question 8: During a CPF-27001 compliance audit, you discover that assessment data includes individual identifiers that could enable profiling. This represents a nonconformity with which CPF-27001 requirement?

a) Section 7.3 (Awareness)
b) Section 8.2.3 (Privacy-Preserving Measures)
c) Section 9.1 (Monitoring, Measurement, Analysis and Evaluation)
d) Section 10.1 (Nonconformity and Corrective Action)

Correct Answer: b - Privacy-Preserving Measures explicitly prohibit individual profiling

Question 9: An organization claims CPF Level 3 certification but CPF Score is 75. What is the appropriate audit conclusion?

a) Certification should be downgraded to Level 2 (70-99 range)
b) Certification should be maintained with surveillance
c) Certification should be suspended pending corrective action
d) Certification is appropriate as score is within Level 3 range

Correct Answer: a - CPF Score of 75 falls in Level 2 range (70-99), not Level 3 (40-69)

Professional Conduct Questions:

Question 10: You are offered a consulting engagement to help an organization improve their CPF Score before your scheduled audit. What is the appropriate response?

a) Accept if consulting occurs 6+ months before audit
b) Accept but recuse yourself from audit
c) Decline due to conflict of interest
d) Accept but disclose to certification body

Correct Answer: c - Auditors must maintain independence and cannot provide consulting to organizations they audit

B CPF Training Curriculum

B.1 CPF-101: Framework Fundamentals (40 hours)

Module 1: Introduction to Cybersecurity Psychology (4 hours)

- 1.1 The Human Factor Gap in Cybersecurity
- 1.2 Failure of Conscious-Level Interventions
- 1.3 Pre-Cognitive Processing and Security Decisions
- 1.4 Overview of CPF Framework
- 1.5 CPF Integration with Security Frameworks

Module 2: Psychoanalytic Foundations (4 hours)

- 2.1 Bion's Basic Assumptions Theory
- 2.2 Klein's Object Relations Theory
- 2.3 Jung's Analytical Psychology
- 2.4 Winnicott's Transitional Space
- 2.5 Application to Organizational Security

Module 3: Cognitive Psychology Foundations (4 hours)

- 3.1 Kahneman's Dual-Process Theory
- 3.2 Cialdini's Influence Principles
- 3.3 Miller's Cognitive Load Theory
- 3.4 Heuristics and Biases in Security
- 3.5 Decision-Making Under Uncertainty

Modules 4-13: CPF Domain Deep-Dives (20 hours, 2 hours each)

- Module 4: Authority-Based Vulnerabilities [1.x]
- Module 5: Temporal Vulnerabilities [2.x]
- Module 6: Social Influence Vulnerabilities [3.x]
- Module 7: Affective Vulnerabilities [4.x]
- Module 8: Cognitive Overload Vulnerabilities [5.x]
- Module 9: Group Dynamic Vulnerabilities [6.x]
- Module 10: Stress Response Vulnerabilities [7.x]
- Module 11: Unconscious Process Vulnerabilities [8.x]
- Module 12: AI-Specific Bias Vulnerabilities [9.x]
- Module 13: Critical Convergent States [10.x]

Module 14: Privacy and Ethics (4 hours)

- 14.1 Privacy-Preserving Assessment Principles
- 14.2 Differential Privacy and Aggregation Requirements
- 14.3 Ethical Considerations in Psychological Assessment
- 14.4 Prohibition on Individual Profiling
- 14.5 Professional Conduct and Boundaries
- 14.6 Data Handling and Confidentiality

Module 15: Integration and Application (4 hours)

- 15.1 CPF and ISO/IEC 27001:2022 Integration
- 15.2 CPF and NIST CSF 2.0 Integration
- 15.3 Organizational Implementation Strategies
- 15.4 Case Studies and Practical Applications
- 15.5 Common Implementation Challenges
- 15.6 Course Review and Assessment

B.2 CPF-201: Assessment Methodology (40 hours)

Module 1: Assessment Planning (6 hours)

- 1.1 Scope Definition and Boundaries
- 1.2 Stakeholder Engagement
- 1.3 Resource Planning
- 1.4 Privacy Impact Assessment
- 1.5 Assessment Schedule and Timeline
- 1.6 Risk Assessment for Assessment Process

Module 2: Data Collection Methods (8 hours)

- 2.1 Behavioral Observation Techniques
- 2.2 Interview Methodologies
- 2.3 Document Review and Analysis
- 2.4 Survey Design and Administration
- 2.5 Technical Log Analysis
- 2.6 Combining Multiple Data Sources
- 2.7 Avoiding Hawthorne Effect
- 2.8 Practical Exercise: Data Collection Planning

Module 3: Scoring and Analysis (12 hours)

- 3.1 Ternary Scoring Methodology
- 3.2 Evidence-Based Rating Decisions
- 3.3 Indicator-by-Indicator Assessment
- 3.4 Category Score Calculation
- 3.5 CPF Score Computation

- 3.6 Convergence Index Analysis
- 3.7 Statistical Analysis Techniques
- 3.8 Trend Analysis and Historical Comparison
- 3.9 Inter-Rater Reliability
- 3.10 Practical Exercise: Scoring Case Studies

Module 4: Privacy-Preserving Techniques (6 hours)

- 4.1 Minimum Aggregation Units Implementation
- 4.2 Differential Privacy Mathematics
- 4.3 Temporal Delay Mechanisms
- 4.4 Role-Based Analysis
- 4.5 Data Anonymization Techniques
- 4.6 Secure Data Storage and Transmission
- 4.7 Practical Exercise: Privacy Implementation

Module 5: Report Writing and Communication (8 hours)

- 5.1 Executive Summary Development
- 5.2 Technical Findings Documentation
- 5.3 Visualization of Assessment Results
- 5.4 Risk Treatment Recommendations
- 5.5 Stakeholder-Specific Communication
- 5.6 Presentation Skills
- 5.7 Handling Sensitive Findings
- 5.8 Final Assessment: Complete Report Development

B.3 CPF-301: Advanced Implementation (40 hours)

Module 1: Intervention Design (10 hours)

- 1.1 From Assessment to Action
- 1.2 Evidence-Based Intervention Selection
- 1.3 Psychological Intervention Principles
- 1.4 Technical Control Integration
- 1.5 Organizational Change Management
- 1.6 Intervention Pilot Testing

Module 2: Continuous Monitoring (10 hours)

- 2.1 Real-Time Indicator Monitoring
- 2.2 SIEM Integration Strategies
- 2.3 Automated Alerting Systems
- 2.4 Dashboard Design and Implementation
- 2.5 Convergent State Detection
- 2.6 Continuous Monitoring Privacy Protections

Module 3: Integration Strategies (10 hours)

- 3.1 Security Operations Integration
- 3.2 Incident Response Enhancement
- 3.3 Threat Intelligence Augmentation
- 3.4 Security Architecture Considerations
- 3.5 Governance and Compliance Integration
- 3.6 Enterprise Risk Management Alignment

Module 4: Effectiveness Measurement (10 hours)

- 4.1 Metrics and KPIs
- 4.2 ROI Calculation Methodologies
- 4.3 Incident Reduction Analysis
- 4.4 Before-After Comparison Studies
- 4.5 Continuous Improvement Processes
- 4.6 Capstone Project: Implementation Plan

B.4 CPF-401: Audit Techniques (40 hours)

Module 1: Audit Fundamentals (8 hours)

- 1.1 ISO 19011:2018 Principles
- 1.2 CPF-27001:2025 Requirements Overview
- 1.3 Audit Process Overview
- 1.4 Auditor Competencies and Ethics
- 1.5 Independence and Objectivity
- 1.6 Professional Conduct Standards

Module 2: Audit Planning (8 hours)

- 2.1 Audit Scope and Objectives
- 2.2 Risk-Based Audit Planning
- 2.3 Audit Team Selection
- 2.4 Resource Allocation
- 2.5 Audit Plan Development
- 2.6 Communication with Auditee

Module 3: Audit Execution (12 hours)

- 3.1 Opening Meeting Conduct
- 3.2 Document Review Techniques
- 3.3 Interview Methodologies
- 3.4 Sampling Strategies
- 3.5 Evidence Collection and Documentation
- 3.6 Observation Techniques
- 3.7 Finding Development
- 3.8 Closing Meeting Conduct
- 3.9 Practical Exercise: Mock Audit

Module 4: Audit Reporting (6 hours)

- 4.1 Nonconformity Classification
- 4.2 Observation and Opportunity Documentation
- 4.3 Audit Report Structure
- 4.4 Clear and Objective Writing
- 4.5 Corrective Action Recommendations
- 4.6 Report Review and Quality Assurance

Module 5: Follow-Up and Closure (6 hours)

- 5.1 Corrective Action Plan Review
- 5.2 Verification of Corrections
- 5.3 Effectiveness Evaluation
- 5.4 Audit Closure Criteria
- 5.5 Continuous Improvement from Audit Findings
- 5.6 Final Practical Examination Preparation

C Application Forms

C.1 Individual Certification Application Template

CPF Certification Application

Certification Type (Select One):

☐ CPF Assessor

☐ CPF Practitioner

☐ CPF Auditor

Personal Information:

- Full Legal Name: _____
- Preferred Name: _____
- Date of Birth: _____
- Email Address: _____
- Phone Number: _____
- Mailing Address: _____
- _____

Education (Bachelor's or Higher):

- Institution: _____
- Degree Type: _____ Major: _____
- Date Conferred: _____
- Official Transcript Attached: ☐ Yes ☐ No

Professional Experience:

Current/Most Recent Position:

- Employer: _____
- Position Title: _____
- Dates: _____ to _____
- Relevant Responsibilities: _____
- _____
- _____

Additional Relevant Experience (attach additional pages if needed):

Training Completion:

☐ CPF-101: Framework Fundamentals

- Date Completed: _____
- Training Provider: _____
- Certificate Number: _____

☐ CPF-201: Assessment Methodology (Assessor/Auditor only)

- Date Completed: _____
- Training Provider: _____
- Certificate Number: _____

☐ CPF-401: Audit Techniques (Auditor only)

- Date Completed: _____
- Training Provider: _____
- Certificate Number: _____

☐ ISO 19011 Auditor Training (Auditor only)

- Date Completed: _____
- Training Provider: _____

Professional References (Minimum 2):

Reference 1:

- Name: _____ Title: _____
- Organization: _____
- Email: _____ Phone: _____
- Relationship: _____

Reference 2:

- Name: _____ Title: _____
- Organization: _____
- Email: _____ Phone: _____
- Relationship: _____

Code of Ethics Acknowledgment:

I have read and agree to abide by the CPF Code of Ethics, including:

☐ Maintaining integrity and objectivity

☐ Protecting confidentiality of assessment data

☐ Practicing within competence boundaries

☐ Implementing privacy-preserving methodologies

☐ Never using assessment data for individual profiling

☐ Adhering to all professional conduct requirements

Declaration:

I declare that the information provided in this application is true, complete, and accurate to the best of my knowledge. I understand that false or misleading information may result in denial of certification or revocation of certification if already granted.

Signature: _____ Date: _____

Required Attachments:

☐ Official transcript(s) or degree certificate(s)

☐ Experience verification letters or professional portfolio

☐ Training completion certificates

☐ Current resume/CV

☐ Application fee payment confirmation

☐ Government-issued photo ID (copy)

Application Fee:

- CPF Assessor: $300
- CPF Practitioner: $200
- CPF Auditor: $400

Payment Method: ☐ Credit Card ☐ Bank Transfer ☐ Check

Submit completed application with all required attachments to:

CPF Certification Body
Certification Applications Department
Email: certification@cpf-cert.org
Web Portal: https://apply.cpf-cert.org

C.2 Organizational Certification Application Template

CPF Organizational Certification Application

Target Certification Level (Select One):

☐ Level 1: Foundation (CPF Score 100-149)

☐ Level 2: Intermediate (CPF Score 70-99)

☐ Level 3: Advanced (CPF Score 40-69)

☐ Level 4: Exemplary (CPF Score 0-39)

Organization Information:

- Legal Organization Name: _____
- Operating Name (if different): _____
- Industry Sector: _____
- Organization Size: ☐ 1-50 ☐ 51-250 ☐ 251-1000 ☐ 1000+
- Headquarters Location: _____
- Website: _____

Primary Contact:

- Name: _____ Title: _____
- Email: _____ Phone: _____

CPF Coordinator:

- Name: _____ Title: _____
- Email: _____ Phone: _____
- CPF Certification (if applicable): _____

Certification Scope:

- Locations Covered: _____
- _____
- Business Units Covered: _____
- _____
- Total Personnel in Scope: _____
- Exclusions (if any): _____
- _____

CPF Assessment Information:

- Assessment Date: _____
- Certified Assessor/Auditor Name: _____
- Certification Number: _____
- CPF Score: _____ (Range: 0-200)
- Assessment Report Attached: ☐ Yes ☐ No

Existing Certifications:

☐ ISO/IEC 27001 - Certificate Number: _____

☐ ISO 9001 - Certificate Number: _____

☐ SOC 2 - Report Date: _____

☐ Other: _____

Implementation Status:

CPF Program Elements (Check all implemented):

☐ Documented CPF Policy

☐ Designated CPF Coordinator

☐ Privacy Protection Procedures

☐ Risk Treatment Plans

☐ Continuous Monitoring (if applicable)

☐ Integration with ISMS

☐ Management Review Process

☐ CPE Program for Staff

Management Commitment:

I, as authorized representative of the organization, commit to:

☐ Maintaining systematic psychological vulnerability management

☐ Providing necessary resources for CPF implementation

☐ Complying with surveillance requirements

☐ Implementing corrective actions as needed

☐ Protecting privacy in all CPF activities

☐ Participating in required management reviews

Authorization:

Name: _____ Title: _____

Signature: _____ Date: _____

Required Attachments:

☐ CPF Assessment Report (complete)

☐ CPF Policy Document

☐ Organizational Chart showing CPF roles

☐ Privacy Protection Procedures

☐ Risk Treatment Plans for Red Indicators

☐ Evidence of ISMS integration (if applicable)

☐ Application fee payment confirmation

Application Fee (Based on Organization Size):

- 1-50 employees: $500
- 51-250 employees: $1,000
- 251-1000 employees: $1,500
- 1000+ employees: $2,000

Payment Method: ☐ Credit Card ☐ Bank Transfer ☐ Check

Submit completed application with all required attachments to:

CPF Certification Body
Organizational Certification Department
Email: org-certification@cpf-cert.org
Web Portal: https://apply.cpf-cert.org

C.3 Recertification Application Template

CPF Recertification Application

Current Certification:

- Certification Type: _____
- Certificate Number: _____
- Original Certification Date: _____
- Current Expiration Date: _____

Personal Information:

- Full Name: _____
- Email: _____ Phone: _____
- Has your contact information changed? ☐ Yes ☐ No
- If yes, provide updated information: _____

Continuing Professional Education (CPE):

CPE Summary (3-Year Cycle):

- Year 1 Credits: _____ (Required: _____)
- Year 2 Credits: _____ (Required: _____)
- Year 3 Credits: _____ (Required: _____)
- Total CPE Credits: _____ (Required: _____)

CPE Documentation:

☐ Complete CPE log attached (with dates, activities, credits)

☐ Supporting certificates/documentation attached

☐ All activities comply with CPE policy

Professional Experience (Past 3 Years):

For Assessors:

- Number of CPF Assessments Conducted: _____
- Assessment Summary Attached: ☐ Yes ☐ No

For Practitioners:

- Updated Portfolio Attached: ☐ Yes ☐ No
- Number of Implementation Projects: _____

For Auditors:

- Total Audit Days: _____ (Required: 45)
- Number of Lead Auditor Roles: _____ (Required: 5)
- Audit Summary Attached: ☐ Yes ☐ No

Ethics Attestation:

I attest that during the past certification period:

☐ I have complied with the CPF Code of Ethics

☐ I have maintained confidentiality requirements

☐ I have practiced within my competence boundaries

☐ I have maintained privacy-preserving practices

☐ I have no unresolved ethics complaints

☐ I am not subject to any professional discipline

I agree to continue adhering to the CPF Code of Ethics for the next certification period.

Signature: _____ Date: _____

Recertification Fee:

- CPF Assessor: $400
- CPF Practitioner: $300
- CPF Auditor: $500
- Late Recertification (within 90 days): Add $100

Payment Method: ☐ Credit Card ☐ Bank Transfer ☐ Check

Required Attachments:

- ☐ Complete CPE log with supporting documentation
- ☐ Experience documentation (assessments, portfolio, or audits)
- ☐ Professional references (if requested)
- ☐ Recertification fee payment confirmation

Submit completed application with all required attachments to:

CPF Certification Body
Recertification Department
Email: recertification@cpf-cert.org
Web Portal: https://recertify.cpf-cert.org

Note: Applications should be submitted 90-180 days before expiration to ensure timely processing.

Document Control

Version History:

Version	Date	Changes
1.0	January 2025	Initial release

Review Schedule:

- Annual review: January of each year
- Major revision: As needed based on industry changes, research advances, or stakeholder feedback
- Next scheduled review: January 2026

Approval:

Document Owner: CPF Certification Scheme Committee

Approved by: _____ Date: _____

Distribution:

- All approved CPF certification bodies
- CPF training providers
- Public version available at: https://cpf3.org/certification-scheme

Contact Information:

CPF Certification Body
Website: https://cpf3.org
Email: info@cpf3.org

Certification Questions: certification@cpf-cert.org
Technical Support: support@cpf-cert.org

End of Document