CPF-201 Training Blueprint

Assessment Methodology Course Design
40 Hours — 80 Slides

CPF3 Training Development
Giuseppe Canale, CISSP
g.canale@cpf3.org

January 2025

Abstract

This training blueprint defines the instructional design for CPF-201: Assessment Methodology, the 40-hour course required for CPF Assessor and CPF Auditor certifications. Building on CPF-101 foundations, this course provides systematic training in conducting privacy-preserving psychological vulnerability assessments using all 100 CPF indicators. Participants master data collection methods, ternary scoring application, privacy-preserving techniques including differential privacy, and professional report writing. This blueprint enables modular slide generation for instructor-led or self-paced delivery, ensuring consistent competence development across certified assessors globally.

Contents

1 Course Overview

1.1 Course Identification

Code: CPF-201 — **Title:** Assessment Methodology — **Duration:** 40 hours — **Slides:** 80 total — **Format:** Instructor-led with extensive hands-on practice

1.2 Target Audience

Cybersecurity professionals and psychologists pursuing CPF Assessor or CPF Auditor certification who have completed CPF-101. Prerequisites include CPF-101 completion with passing score, bachelor's degree, and minimum 2 years relevant experience.

1.3 Learning Objectives

Upon completion, participants will: (1) Plan comprehensive CPF assessments with appropriate scope and privacy protections, (2) Apply systematic data collection methods across behavioral observation, interviews, documents, surveys, and technical logs, (3) Execute ternary scoring for all 100 indicators with inter-rater reliability, (4) Implement differential privacy (epsilon 0.1) and aggregation requirements (minimum 10 individuals), (5) Produce professional assessment reports with actionable recommendations.

1.4 Course Structure

Module 1 - Assessment Planning (6h): Scope definition, stakeholder engagement, resource planning, privacy impact assessment, scheduling.

Modules 2-3 - Data Collection (14h): Behavioral observation, interviews, documents, surveys, logs, triangulation.

Modules 4-5 - Scoring and Analysis (12h): Ternary scoring, evidence evaluation, convergence detection, inter-rater reliability.

Module 6 - Privacy Techniques (6h): Differential privacy, aggregation units, temporal delays, anonymization, secure handling.

Module 7 - Report Writing (8h): Report structure, executive summaries, visualization, stakeholder communication, recommendations.

1.5 Assessment Method

Formative: 7 module exercises. Summative: Practical examination (4 hours complete assessment of realistic scenario) + Written examination (100 questions, 3 hours). Both required, 70% passing for each.

1.6 Materials Provided

CPF-201 Participant Workbook (100 pages), Complete Field Kit Library (all 100 indicators), Assessment Templates, Data Collection Instruments, Scoring Worksheets, Privacy Tools, Report Templates, 3 Case Study Organizations with complete data sets.

2 Module Structures

2.1 Module 1: Assessment Planning

2.1.1 Overview

Duration: 6 hours — **Slides:** 12

Learning Objectives: Define assessment scope with boundaries; engage stakeholders maintaining privacy; plan resources; conduct privacy impact assessments; develop realistic schedules; identify assessment risks.

Key Concepts: Scope definition, stakeholder engagement, resource planning, privacy impact assessment, timeline development, risk management.

2.1.2 Content Outline

1. Scope Definition (90 min): Organizational unit identification, population sizing for aggregation (minimum 10 per unit), inclusion/exclusion criteria, temporal scope, domain prioritization, boundary documentation, scope creep prevention.

2. Stakeholder Engagement (60 min): Executive sponsor identification, privacy officer involvement (mandatory), HR/legal consultation, department manager engagement, employee communication (what they need vs don't need to know), union considerations, confidentiality maintenance.

3. Resource Planning (75 min): Personnel requirements (assessor time, SME access), technology needs (survey platforms, secure storage), budget estimation, timeline realistic estimation, dependency identification, contingency planning.

4. Privacy Impact Assessment (90 min): PIA template for CPF, data minimization analysis, aggregation unit verification (minimum 10), differential privacy parameter selection (epsilon 0.1), temporal delay planning (72 hours), data flow mapping, privacy risk assessment, mitigation strategies.

5. Schedule Development (45 min): Phase breakdown (planning, collection, analysis, reporting), milestone identification, realistic timeframes (4-8 weeks medium org), data collection windows (avoid holidays/deadlines), analysis time allocation (40% of total), buffer for delays.

6. Assessment Risk Management (30 min): Common risks (stakeholder resistance, data access delays, aggregation too small, scope creep, timeline pressure), mitigation strategies, contingency plans, go/no-go criteria, escalation procedures.

2.1.3 Teaching Methods

Lecture: Scope framework, stakeholder mapping, PIA template, schedule visualization.

Exercises: (1) Scope Definition - given org description, define scope with boundaries (30 min), (2) Aggregation Calculation - calculate units for various structures (30 min), (3) Privacy Impact Assessment - complete PIA for sample org (45 min), (4) Schedule Development - create timeline with milestones (30 min).

Discussion: "Biggest planning challenge?", "Balance thoroughness with timeline?", "Stakeholder resistance scenarios?"

Case Study: Healthcare 500 employees, 5 departments, union environment - plan complete assessment.

2.1.4 Slide Breakdown

Slide 1.1: "Assessment Scope Definition" - Unit identification, population sizing, criteria, temporal scope, prioritization.

Slide 1.2: "Aggregation Units for Privacy" - Minimum 10 requirement, calculation for different structures, handling small units.

Slide 1.3: "Stakeholder Engagement Map" - Sponsor, privacy officer, HR/legal, managers, employees, union, communication matrix.

Slide 1.4: "Privacy-Preserving Communication" - What stakeholders need vs what compromises assessment, avoiding Hawthorne effect.

Slide 1.5: "Resource Planning Framework" - Personnel, technology, budget template, timeline formula.

Slide 1.6: "Privacy Impact Assessment Template" - PIA structure, data minimization, aggregation verification, differential privacy parameters, data flow.

Slide 1.7: "Data Flow Mapping" - Collection to analysis to reporting to storage to destruction, security each stage.

Slide 1.8: "Differential Privacy Parameter Selection" - Epsilon 0.1 explained, privacy-utility tradeoff, when to adjust, calculation examples.

Slide 1.9: "Assessment Schedule Structure" - Typical phases (planning 10%, collection 30%, analysis 40%, reporting 20%), milestones, timeframes.

Slide 1.10: "Timeline Estimation by Org Size" - Table: Small (50-250) 3-4 weeks, Medium (250-1000) 5-8 weeks, Large (1000+) 10-16 weeks.

Slide 1.11: "Assessment Risk Management" - Common risks table with mitigation strategies, contingency plans.

Slide 1.12: "Planning Exercise: Healthcare Organization" - 500 employees, 5 departments, union, complete planning exercise instructions.

2.1.5 Materials Needed

Workbook Module 1 (pages 1-20), Planning Template, Aggregation Calculator, PIA Template, Schedule Template (Gantt), Healthcare case study (5 pages).

2.1.6 Assessment Items

Quiz: Q1: Minimum aggregation unit $\rightarrow$ 10 correct. Q2: PIA mandatory for $\rightarrow$ all assessments correct. Q3: Typical analysis time $\rightarrow$ 40% correct. Q4: Standard epsilon $\rightarrow$ 0.1 correct. Q5: Mandatory stakeholder $\rightarrow$ privacy officer correct.

Exercise Rubric: Scope defined with boundaries (3 pts), aggregation units correct $\geq$10 (3 pts), PIA completed (2 pts), realistic schedule (2 pts). Total 10 pts (7+ pass).

2.2 Module 2: Data Collection Methods - Part 1

2.2.1 Overview

Duration: 8 hours — **Slides:** 16

Learning Objectives: Conduct behavioral observations; design and execute interviews; analyze documents; extract relevant data; triangulate multiple sources.

Key Concepts: Behavioral observation, structured interviews, document analysis, triangulation, avoiding Hawthorne effect, evidence quality.

2.2.2 Content Outline

1. Behavioral Observation (120 min): Types (direct, indirect, participant, non-participant), when to use each, CPF-relevant behaviors (email responses, protocol compliance, group decisions, stress responses), observation protocols (what/how to record, objectivity), avoiding Hawthorne effect, ethical considerations (consent, privacy, no covert), structured templates by domain, practice sessions.

2. Interview Methodologies (150 min): Interview types (structured, semi-structured), design principles (open questions, avoid leading, focus on behaviors not attitudes), domain-specific interview guides (all 100 indicators have questions), interview logistics (duration 30-60 min optimal, setting, recording consent), conducting effective interviews (rapport, active listening, probing, time management), challenging scenarios (defensive interviewees, authority figures, language barriers), aggregation considerations (interview many, report patterns), practice interviews with feedback.

3. Document Review (90 min): Document types relevant to CPF (policies, procedures, training materials, incident reports, audit findings, emails, meeting minutes, org charts, performance reviews), systematic analysis (what to look for by domain, evidence extraction, noting gaps), document request protocols (what to request, justifying necessity, handling sensitive), privacy considerations (anonymize examples, secure handling), evidence quality assessment (primary vs secondary, recency, completeness).

4. Triangulation (30 min): Multiple sources strengthen findings, triangulation methods (data, methodological, investigator), when findings conflict (investigate, weight by quality), documenting triangulation, examples by domain.

2.2.3 Teaching Methods

Lecture: Observation techniques with video examples, interview demonstrations, document analysis framework.

Exercises: (1) Observation Practice - video of org scenario, participants observe/record, compare (45 min), (2) Mock Interviews - pairs conduct structured interviews using Field Kits, feedback (60 min), (3) Document Analysis - given policies, extract CPF evidence (45 min).

Discussion: "Hawthorne effect experiences?", "Most challenging interview scenarios?", "Document access barriers?"

Role Play: Defensive interviewee scenario, practice de-escalation techniques.

2.2.4 Slide Breakdown

Slide 2.1: "Behavioral Observation Overview" - Types (direct, indirect, participant, non-participant), when to use, CPF-relevant behaviors by domain.

Slide 2.2: "Observation Protocols" - What to record (behaviors not interpretations), how to record (templates), objectivity, timestamping.

Slide 2.3: "Avoiding Hawthorne Effect" - Minimize intrusion, natural settings, vague purpose explanation.

Slide 2.4: "Observation Ethics" - Consent requirements, privacy protection, no covert observation, professional boundaries.

Slide 2.5: "Interview Design Principles" - Open vs closed questions, avoiding leading, focus on behaviors, example transformations.

Slide 2.6: "Structured Interview Template" - Domain-by-domain guide structure, Field Kit questions as foundation, timing allocation.

Slide 2.7: "Conducting Effective Interviews" - Building rapport, active listening, probing follow-ups, managing time, concluding professionally.

Slide 2.8: "Interview Challenging Scenarios" - Defensive interviewees (de-escalation), authority figures (maintaining equality), language barriers, emotional responses.

Slide 2.9: "Interview Aggregation for Privacy" - Interview many, identify patterns not individuals, anonymize examples, protecting identity.

Slide 2.10: "Document Types for CPF" - Policies, procedures, training, incidents, audits, emails, minutes, org charts, reviews - what each reveals by domain.

Slide 2.11: "Systematic Document Analysis" - Domain-by-domain framework, evidence extraction, gap identification, source quality weighting.

Slide 2.12: "Document Request Protocols" - What to request (justify necessity), handling sensitive documents (NDAs, secure viewing), privacy considerations.

Slide 2.13: "Evidence Quality Assessment" - Quality hierarchy (policies ¿ procedures ¿ emails ¿ anecdotes), recency weighting, completeness evaluation.

Slide 2.14: "Triangulation for Robust Findings" - Multiple sources strengthen conclusions, triangulation types, conflict resolution.

Slide 2.15: "Triangulation by Domain Example" - Authority [1.x]: Combine policy + interview + observation shows triangulation in action.

Slide 2.16: "Module 2 Practice Exercises" - Observation video instructions, mock interview pairs, document analysis exercise, deliverables.

2.2.5 Materials Needed

Workbook Module 2 (pages 21-40), Observation video (15 min org scenario), Observation templates, Interview guides all 10 domains, Mock interview scripts, Sample documents packet (20 pages), Document analysis worksheets.

2.2.6 Assessment Items

Quiz: Q1: Avoid Hawthorne effect → minimize intrusion, vague purpose correct. Q2: Structured interview duration → 30-60 min correct. Q3: Source quality hierarchy → policies ¿ procedures ¿ emails ¿ anecdotes correct. Q4: Triangulation strengthens by → multiple sources correct. Q5: Interview aggregation → many individuals, report patterns correct.

Exercise Rubric (Mock Interview): Appropriate questions from Field Kit (2 pts), open non-leading questions (2 pts), active listening (2 pts), behavioral focus (2 pts), professional conclusion (2 pts). Total 10 pts (7+ pass).

2.3 Module 3: Data Collection Methods - Part 2

2.3.1 Overview

Duration: 6 hours — **Slides:** 12

Learning Objectives: Design privacy-preserving surveys; analyze technical logs for behavioral indicators; combine multiple methods; manage collection logistics; ensure data quality.

Key Concepts: Survey design, technical log analysis, phishing simulation results, SIEM data, multi-method integration, data quality.

2.3.2 Content Outline

1. Survey Design (120 min): When surveys appropriate (attitudes correlate with behaviors, anonymous aggregated data), design principles (clear questions, Likert scales, avoid bias), CPF domain-specific survey items, privacy-preserving methodology (anonymous responses, aggregate analysis, minimum response rate 70%+ for aggregation), survey platforms (requirements: anonymity, encryption, GDPR-compliant), administration logistics (timing, communication, incentives, follow-up), response rate optimization, data cleaning and validation.

2. Technical Log Analysis (90 min): Log types relevant to CPF (email logs for authority/urgency patterns, authentication logs for password behaviors, security tool logs for alert fatigue, help desk tickets for stress/confusion, VPN logs for off-hours work, SIEM logs for incident response), what logs reveal by domain, log access permissions and privacy (aggregated patterns only, no individual tracking), technical skills required (basic SQL, log parsing, pattern recognition), automated analysis tools, combining technical and behavioral data.

3. Phishing Simulation Data (45 min): Simulation results as CPF data source (click rates, reporting rates), mapping results to indicators (authority [1.x], temporal [2.x], social influence [3.x]), privacy considerations (aggregated only, no individual targeting), limitations (artificial scenario), combining with other sources.

4. Multi-Source Integration (45 min): Data source selection matrix (which sources for which domains), collection sequencing (surveys early for attitudes, observations later for behaviors, interviews last for depth), data management during collection (secure storage, version control, access logs), quality assurance (completeness checks, consistency verification, early analysis for gaps), adjusting plan mid-assessment.

2.3.3 Teaching Methods

Lecture: Survey design with examples, log analysis demonstrations, multi-source integration framework.

Exercises: (1) Survey Design - create survey items for selected domain, peer review (45 min), (2) Log Analysis - given sample logs, extract CPF patterns (60 min), (3) Multi-Source Planning - design data collection plan for medium org using all methods (45 min).

Discussion: "Survey response rate challenges?", "Log access restrictions?", "Most valuable data source by domain?"

Demonstration: Live log analysis showing pattern extraction, SQL queries, visualization techniques.

2.3.4 Slide Breakdown

Slide 3.1: "Survey Design for CPF" - When surveys appropriate, design principles, domain-specific items, privacy-preserving methodology.

Slide 3.2: "CPF Survey Items by Domain" - Sample questions for each 10 domains, Likert interpretation, aggregation requirements.

Slide 3.3: "Privacy-Preserving Surveys" - Anonymous collection, no IP tracking, aggregate analysis, minimum response rate 70%+, platform requirements.

Slide 3.4: "Survey Administration Logistics" - Timing selection, communication strategy, incentives (appropriate not coercive), response rate optimization.

Slide 3.5: "Technical Log Types for CPF" - Email logs, authentication logs, security tool logs, help desk tickets, VPN logs, SIEM logs.

Slide 3.6: "What Logs Reveal by Domain" - Table: Domain — Relevant Logs — Patterns to Extract — Privacy Considerations, all 10 domains.

Slide 3.7: "Log Analysis Privacy Requirements" - Aggregated patterns only, no individual tracking/profiling, access permissions, secure handling, retention limits.

Slide 3.8: "Log Analysis Technical Skills" - Basic SQL, log parsing tools, pattern recognition, statistical analysis, visualization, automation.

Slide 3.9: "Phishing Simulation as CPF Data" - Simulation results (click rates, reporting), mapping to indicators (authority, temporal, social), privacy (aggregated), limitations (artificial), combining sources.

Slide 3.10: "Multi-Source Data Integration" - Data source selection matrix (which sources per domain), collection sequencing logic, data management (secure storage, version control).

Slide 3.11: "Data Quality Assurance" - Completeness checks (all domains covered, sufficient data per indicator), consistency verification (triangulation reveals contradictions), early analysis for gaps.

Slide 3.12: "Module 3 Practice Exercises" - Survey design exercise, log analysis with sample data, multi-source collection planning, deliverables.

2.3.5 Materials Needed

Workbook Module 3 (pages 41-55), Survey design template, Sample survey items library (all 10 domains), Survey platform comparison, Sample log files (email metadata, authentication, help desk - anonymized, 50 entries each), Log analysis tools guide (SQL basics, parsing scripts), Multi-source planning template.

2.3.6 Assessment Items

Quiz: Q1: Survey minimum response rate → 70%+ correct. Q2: Log analysis primary privacy requirement → aggregated patterns only correct. Q3: Logs reveal stress patterns through → help desk ticket analysis correct. Q4: Phishing simulation maps to → authority, temporal, social influence correct. Q5: Data source sequencing → surveys early, observations mid, interviews late correct.

Exercise Rubric (Log Analysis): Correct pattern extraction (3 pts), appropriate domain mapping (2 pts), privacy-preserving approach (3 pts), statistical summary (2 pts). Total 10 pts (7+ pass).

2.4 Module 4: Scoring and Analysis - Part 1

2.4.1 Overview

Duration: 6 hours — **Slides:** 12

Learning Objectives: Apply ternary scoring consistently; evaluate evidence for indicator scoring; justify scoring decisions; achieve inter-rater reliability; score indicators across all 10 domains; calculate category and CPF scores.

Key Concepts: Ternary scoring (Green/Yellow/Red), evidence-based rating, scoring justification, inter-rater reliability, category scores, CPF score calculation.

2.4.2 Content Outline

1. Ternary Scoring Review (45 min): Three-level rationale (simplicity, actionability, reduces subjectivity), Green (0) definition and criteria (minimal vulnerability, standard monitoring), Yellow (1) definition and criteria (moderate vulnerability, increased monitoring, preventive intervention), Red (2) definition and criteria (critical vulnerability, immediate intervention), mapping evidence to scores (Field Kit criteria per indicator), avoiding common errors (central tendency bias, leniency/severity bias, halo effect).

2. Evidence-Based Rating (90 min): Evidence collection per indicator (minimum sources: observation + interview OR document + log), evidence quality weighting (recent ¿ old, direct ¿ indirect, multiple ¿ single), scoring decision tree by indicator (Field Kits provide criteria), documentation requirements (evidence summary, scoring rationale, confidence level), handling insufficient evidence (score unknown/NA, investigate further, conservative estimate with low confidence notation).

3. Indicator-by-Indicator Scoring Practice (120 min): Domain [1.x] Authority indicators 1.1-1.10 scoring practice (case studies with evidence, participants score, discuss, compare with expert), Domain [2.x] Temporal indicators 2.1-2.10 practice, continued through all 10 domains (abbreviated - full practice 1-2 indicators per domain, discussion of patterns for remaining), group scoring exercise (same evidence, individual scores, discussion of differences, calibration).

4. Category and CPF Score Calculation (45 min): Category Score formula (sum of 10 indicators per category, range 0-20), CPF Score formula (sum of 10 category scores, range 0-200), score interpretation (thresholds: Level 1 100-149, Level 2 70-99, Level 3 40-69, Level 4 0-39), score trending over time (baseline vs follow-up), score presentation (tables, charts, dashboards).

2.4.3 Teaching Methods

Lecture: Ternary scoring principles, evidence evaluation framework, calculation methodology.

Exercises: (1) Scoring Calibration - 20 indicators with evidence, participants score, compare with expert and peers, discuss discrepancies (90 min), (2) Evidence Quality Assessment - rate evidence quality for given indicators, justify (30 min), (3) Score Calculation - given indicator scores, calculate category and CPF scores, interpret (30 min).

Discussion: "Hardest indicators to score?", "What evidence most convincing?", "How handle scoring disagreements?"

Group Activity: Scoring same evidence individually, then discuss differences, calibrate, rescore.

2.4.4 Slide Breakdown

Slide 4.1: "Ternary Scoring System" - Three-level rationale, Green (0) definition/criteria, Yellow (1) definition/criteria, Red (2) definition/criteria, mapping evidence.

Slide 4.2: "Scoring Criteria Consistency" - Field Kits provide indicator-specific criteria, importance of following strictly, examples of application, avoiding subjective drift.

Slide 4.3: "Common Scoring Errors" - Central tendency bias (over-using Yellow), leniency bias (too many Greens), severity bias (too many Reds), halo effect (one domain influences others), how to recognize and correct.

Slide 4.4: "Evidence-Based Rating Process" - Evidence collection per indicator (minimum sources), quality weighting (recent, direct, multiple sources), decision tree logic, documentation requirements.

Slide 4.5: "Evidence Quality Weighting" - Quality hierarchy: Direct observation ¿ interviews ¿ documents ¿ logs ¿ surveys, recency weighting, multiple source bonus, confidence levels (high/medium/low).

Slide 4.6: "Scoring Documentation Requirements" - Evidence summary for each indicator, scoring rationale (why this score), confidence level notation, dissenting opinions if team assessment.

Slide 4.7: "Handling Insufficient Evidence" - Options: Score unknown/NA, investigate further (if possible), conservative estimate with low confidence, documenting limitations, when to defer scoring.

Slide 4.8: "Indicator Scoring Practice: Authority [1.x]" - Case study with evidence for indicators 1.1-1.10, participants score individually, discussion of rationale, expert scoring comparison.

Slide 4.9: "Scoring Calibration Activity" - 20 indicators from various domains with evidence packets, individual scoring, peer comparison, discussion of discrepancies, recalibration.

Slide 4.10: "Category Score Calculation" - Formula: Sum of 10 indicators, range 0-20, interpretation (0-5 low, 6-10 moderate, 11-15 high, 16-20 critical), example calculations.

Slide 4.11: "CPF Score Calculation" - Formula: Sum of 10 category scores, range 0-200, interpretation (compliance level thresholds), trending over time (baseline vs follow-up), presentation formats.

Slide 4.12: "Score Interpretation and Communication" - Compliance level mapping (Level 1-4), what scores mean for organization, presenting scores to stakeholders (executive-friendly formats), actionability by score range.

2.4.5 Materials Needed

Workbook Module 4 (pages 56-70), Field Kit Library (all 100 for reference), Scoring Calibration Packet (20 indicators with evidence, 30 pages), Evidence Quality Assessment Worksheet, Score Calculation Templates, Scoring practice case studies (3 organizations with complete evidence sets), Expert scoring answer key.

2.4.6 Assessment Items

Quiz: Q1: Ternary scoring levels → Green (0), Yellow (1), Red (2) correct. Q2: Minimum evidence sources per indicator → observation + interview OR document + log correct. Q3: Evidence quality hierarchy → direct observation ¿ interviews ¿ documents ¿ logs ¿ surveys

correct. Q4: Category Score range → 0-20 correct. Q5: CPF Score range → 0-200 correct.

Exercise Rubric (Scoring Calibration): Scores within 1 point of expert on 15/20 indicators (5 pts), appropriate evidence weighting (2 pts), scoring rationale documented (2 pts), confidence levels noted (1 pt). Total 10 pts (7+ pass).

2.5 Module 5: Scoring and Analysis - Part 2

2.5.1 Overview

Duration: 6 hours — **Slides:** 12

Learning Objectives: Detect convergent vulnerability states; perform statistical analysis on indicator data; achieve inter-rater reliability in team assessments; identify vulnerability patterns and trends; perform longitudinal analysis; validate scoring consistency.

Key Concepts: Convergence index, statistical analysis, inter-rater reliability, pattern recognition, trending, longitudinal assessment, scoring validation.

2.5.2 Content Outline

1. Convergence Index Analysis (90 min): Convergence concept review (multiple vulnerabilities aligned = exponential risk), Convergence Index calculation (identifying simultaneous Red/Yellow indicators across domains), mathematical approach (multiplication not addition), Domain interaction patterns (which domains commonly converge: authority + temporal + social influence = BEC perfect storm), Swiss cheese model application (Reason's model, holes aligning), Critical convergent states from Domain [10.x] (perfect storm 10.1, cascade failures 10.2, Swiss cheese 10.4), Real-world examples (Target breach: authority + cognitive overload + group dynamics + temporal), Convergence visualization (network diagrams, heat maps), Early warning thresholds (3+ Red across domains triggers alert).

2. Statistical Analysis Methods (75 min): Descriptive statistics (mean, median, mode by category, standard deviation, distribution), Correlation analysis (which indicators co-occur, domain interdependencies), Trend analysis (comparison over time if longitudinal data), Confidence intervals for aggregated data, Statistical significance testing (comparing groups or time periods), Visualization techniques (box plots, scatter plots, heat maps, radar charts), Using software (Excel sufficient for basic, R/Python for advanced), Interpreting outputs for non-technical stakeholders.

3. Inter-Rater Reliability (60 min): Why reliability matters (consistency across assessors, certification credibility), Reliability coefficient calculation (Cohen's Kappa, percent agreement), Acceptable thresholds (Kappa ¿ 0.7 for certification), Calibration exercises (multiple raters score same evidence, compare, discuss discrepancies, rescore), Common disagreement sources (interpretation, applying criteria, domain knowledge gaps), Improving reliability (training, detailed rubrics, calibration sessions, expert review), Documenting reliability (report Kappa coefficients, describe calibration).

4. Pattern Recognition and Trending (60 min): Common vulnerability patterns by organization type (healthcare: stress + cognitive overload, finance: authority + temporal, tech: AI bias + cognitive overload), Industry benchmarking (typical scores by sector if data available), Organizational structure influences (hierarchical: authority vulnerabilities, flat: group dynamic vulnerabilities), Temporal patterns (time-of-day, day-of-week, seasonal variations), Longitudinal assessment methodology (baseline vs follow-up, intervention effectiveness), Trending visualization (line charts, before-after comparisons), Pattern documentation in reports.

2.5.3 Teaching Methods

Lecture: Convergence mathematics, statistical methods demonstrations, reliability calculation examples, pattern recognition frameworks.

Exercises: (1) Convergence Detection - given indicator scores, identify convergent states and calculate index (45 min), (2) Inter-Rater Reliability - groups of 3 score same evidence, calculate Kappa, discuss (60 min), (3) Pattern Analysis - examine three organizations' data, identify patterns, document (45 min).

Discussion: "Convergence examples in your experience?", "Statistical skills needed - gaps?", "Most common vulnerability patterns by industry?"

Software Demo: Live demonstration of statistical analysis in Excel and/or R, visualization creation, output interpretation.

2.5.4 Slide Breakdown

Slide 5.1: "Convergence Index Concept" - Multiple vulnerabilities aligned = exponential risk, multiplication not addition, Swiss cheese holes aligning, Reason model visual.

Slide 5.2: "Convergence Calculation Method" - Identify simultaneous Red/Yellow across domains, calculate interaction effects, example: Authority (Red) + Temporal (Red) + Social (Yellow) = critical convergence.

Slide 5.3: "Common Convergent Patterns" - Domain interaction matrix (which domains commonly converge), BEC perfect storm (authority + temporal + social), APT convergence, real-world examples.

Slide 5.4: "Convergence Visualization" - Network diagrams showing domain connections, heat maps of indicator scores, convergence alert thresholds (3+ Red across domains).

Slide 5.5: "Statistical Analysis Overview" - Descriptive statistics (mean, median, SD), correlation analysis (domain interdependencies), trend analysis (time series), confidence intervals, significance testing.

Slide 5.6: "Visualization Techniques" - Box plots by category, scatter plots for correlations, heat maps for scores, radar charts for domain comparison, choosing appropriate visuals.

Slide 5.7: "Statistical Tools" - Excel for basic analysis (functions, charts), R/Python for advanced, when each appropriate, learning resources.

Slide 5.8: "Inter-Rater Reliability Importance" - Consistency across assessors, certification credibility, professional standards, what good reliability means for CPF.

Slide 5.9: "Reliability Calculation" - Cohen's Kappa formula, percent agreement calculation, interpretation (Kappa ¿ 0.7 acceptable, ¿ 0.8 excellent), example calculations.

Slide 5.10: "Improving Inter-Rater Reliability" - Calibration exercises (multiple raters, compare, discuss), detailed rubrics (Field Kits provide), training and practice, expert review, documentation.

Slide 5.11: "Vulnerability Pattern Recognition" - Common patterns by organization type (healthcare, finance, tech), industry benchmarking, organizational structure influences (hierarchical, flat, matrix).

Slide 5.12: "Longitudinal Analysis" - Baseline vs follow-up methodology, intervention effectiveness evaluation, trending visualization (line charts, before-after), temporal pattern detection (seasonal, time-of-day).

2.5.5 Materials Needed

Workbook Module 5 (pages 71-85), Convergence detection worksheets with scenario data, Statistical analysis software guide (Excel functions), Sample datasets (3 organizations with complete indicator scores), Inter-rater reliability calculator, Pattern recognition case studies (healthcare, finance, tech organizations), Visualization examples gallery.

2.5.6 Assessment Items

Quiz: Q1: Convergence risk calculation → multiplication not addition correct. Q2: Acceptable Kappa coefficient → ¿ 0.7 correct. Q3: Convergence alert threshold → 3+ Red indicators across domains correct. Q4: Statistical visualization for domain comparison → radar chart correct. Q5: Longitudinal assessment compares → baseline vs follow-up correct.

Exercise Rubric (Inter-Rater Reliability): Scores same evidence independently (2 pts), calculates Kappa correctly (2 pts), Kappa ¿ 0.7 achieved after calibration (3 pts), documents calibration process (2 pts), reflects on disagreement sources (1 pt). Total 10 pts (7+ pass).

2.6 Module 6: Privacy-Preserving Techniques

2.6.1 Overview

Duration: 6 hours — **Slides:** 12

Learning Objectives: Implement differential privacy with epsilon 0.1; maintain minimum aggregation units throughout assessment; apply temporal delay mechanisms; anonymize data appropriately; secure data handling and storage; conduct privacy audits.

Key Concepts: Differential privacy, epsilon parameter, noise injection, aggregation units, temporal delay, anonymization, encryption, secure destruction.

2.6.2 Content Outline

1. Differential Privacy Implementation (120 min): Differential privacy concept review (mathematical privacy guarantee), Epsilon parameter explained (privacy budget, epsilon 0.1 = strong privacy), Noise injection mechanisms (Laplace, Gaussian), When to apply noise (aggregated scores, statistical summaries, never raw individual data), Calculating noise amount (based on epsilon, data sensitivity, query function), Practical implementation (tools, libraries, manual calculation), Privacy-utility tradeoff (lower epsilon = more privacy but less accuracy, 0.1 balances well), Verification methods (check outputs satisfy epsilon-DP), Common errors (noise too little, applied to wrong data, epsilon too high).

2. Minimum Aggregation Units (60 min): 10-individual requirement rationale (prevents identification even with background knowledge), Calculating aggregation units (by department, role, location, ensuring each $\geq$10), Handling edge cases (small departments: combine with similar, exclude if can't aggregate, document decisions), Dynamic aggregation (adjusting units as data collected, ensuring ongoing compliance), Verification throughout assessment (periodic checks units maintained), Reporting aggregation (clearly state unit definitions, sample sizes), What to do when aggregation not possible (report limitation, suggest future assessment with larger scope).

3. Temporal Delay Mechanisms (45 min): 72-hour minimum delay rationale (prevents real-time surveillance, allows anonymization review), Implementation workflows (data collection

→ cleaning → 72-hour hold → analysis → reporting), Exceptions (are there any? No - delay mandatory), Communicating delays to stakeholders (set expectations upfront, explain privacy rationale), Delay verification (timestamp logs, audit trails), Longer delays when appropriate (higher sensitivity data, additional review needed).

4. Data Anonymization Techniques (60 min): Anonymization vs pseudonymization (CPF requires anonymization, no linkage back to individuals), Removing direct identifiers (names, employee IDs, email addresses, photos), Removing indirect identifiers (unique combinations of attributes), k-anonymity concepts (groups of k indistinguishable individuals, k $\geq$ 10 for CPF), Data suppression (removing unique values), Data generalization (age ranges instead of exact age, department instead of specific role), Anonymization validation (attempt re-identification, red team privacy), Secure handling during anonymization.

5. Secure Data Handling and Destruction (45 min): Encryption requirements (AES-256 at rest, TLS 1.3 in transit), Access controls (role-based, least privilege, multi-factor authentication), Audit logging (all data access logged, logs reviewed regularly), Secure storage (encrypted databases, backup encryption, physical security for printed materials), Data retention limits (5 years maximum, earlier destruction if appropriate), Secure destruction procedures (crypto-shredding for encrypted data, DOD 5220.22-M for physical media, certificate of destruction), Breach response planning (what if privacy compromised, notification procedures).

2.6.3 Teaching Methods

Lecture: Differential privacy mathematics (simplified), anonymization techniques, secure handling procedures.

Exercises: (1) Differential Privacy Calculation - calculate noise for given epsilon and data, apply noise, verify privacy (45 min), (2) Aggregation Unit Design - given organizational chart, define aggregation units ensuring all $\geq$10 (30 min), (3) Anonymization Practice - anonymize sample dataset, validate k-anonymity (45 min), (4) Privacy Audit - audit sample assessment for privacy compliance (30 min).

Discussion: "Differential privacy implementation challenges?", "Aggregation unit edge cases encountered?", "Data handling gaps in your organization?"

Software Demo: Differential privacy library demonstration (Python), anonymization tools, encryption implementation.

2.6.4 Slide Breakdown

Slide 6.1: "Differential Privacy Explained" - Mathematical privacy guarantee concept, epsilon parameter (privacy budget), epsilon 0.1 rationale (strong privacy), noise injection visualization.

Slide 6.2: "Noise Injection Mechanisms" - Laplace mechanism, Gaussian mechanism, when to apply each, calculating noise amount (formula simplified), practical tools.

Slide 6.3: "Differential Privacy Implementation" - Step-by-step workflow (aggregate data → calculate noise → inject noise → verify epsilon-DP), common errors (noise to wrong data, epsilon too high), verification methods.

Slide 6.4: "Privacy-Utility Tradeoff" - Graph showing epsilon vs accuracy, epsilon 0.1 balance point, when to adjust (rarely, with justification), communicating tradeoffs to stakeholders.

Slide 6.5: "Minimum Aggregation Units: 10 Individuals" - Rationale (prevents identification with background knowledge), calculation by department/role/location, edge case handling (combine, exclude, document).

Slide 6.6: "Aggregation Unit Verification" - Periodic checks throughout assessment, dynamic adjustment as data collected, reporting units clearly (definitions, sample sizes), what to do if can't aggregate.

Slide 6.7: "Temporal Delay: 72-Hour Minimum" - Rationale (prevents real-time surveillance), implementation workflow (collection → hold → analysis), no exceptions (delay mandatory), stakeholder communication.

Slide 6.8: "Data Anonymization Requirements" - Anonymization vs pseudonymization (CPF requires full anonymization), removing direct identifiers, removing indirect identifiers (unique attribute combinations).

Slide 6.9: "k-Anonymity for CPF" - Concept: k indistinguishable individuals, $k \geq 10$ for CPF, techniques (suppression, generalization), validation (attempt re-identification).

Slide 6.10: "Secure Data Handling" - Encryption (AES-256 at rest, TLS 1.3 in transit), access controls (RBAC, least privilege, MFA), audit logging (all access logged), secure storage.

Slide 6.11: "Data Retention and Destruction" - Retention limit (5 years maximum), earlier destruction when appropriate, secure destruction procedures (crypto-shredding, DOD 5220.22-M), certificate of destruction.

Slide 6.12: "Privacy Audit Checklist" - Verify differential privacy correctly applied, aggregation units $\geq$10 throughout, temporal delay implemented, anonymization complete, encryption proper, access controls in place, audit logs reviewed, retention limits followed.

2.6.5 Materials Needed

Workbook Module 6 (pages 86-100), Differential privacy calculator tool (Excel or Python), Aggregation unit worksheet, Sample dataset for anonymization practice (50 records with identifiers), Anonymization validation guide, Privacy audit checklist, Encryption tool demonstrations, Data destruction procedure template.

2.6.6 Assessment Items

Quiz: Q1: CPF standard epsilon for differential privacy → 0.1 correct. Q2: Minimum aggregation unit size → 10 individuals correct. Q3: Temporal delay minimum → 72 hours correct. Q4: k-anonymity k value for CPF → $k \geq 10$ correct. Q5: Data retention maximum → 5 years correct.

Exercise Rubric (Privacy Audit): Differential privacy correctly verified (2 pts), aggregation units checked and $\geq$10 (2 pts), temporal delay confirmed (1 pt), anonymization validated (2 pts), encryption and access controls verified (2 pts), documentation complete (1 pt). Total 10 pts (7+ pass).

2.7 Module 7: Report Writing and Communication

2.7.1 Overview

Duration: 8 hours — **Slides:** 16

Learning Objectives: Structure professional assessment reports; write executive summaries; document technical findings; create effective visualizations; tailor communication to stakeholders; provide actionable recommendations; handle sensitive findings professionally.

Key Concepts: Report structure, executive summary, findings documentation, visualization, stakeholder communication, actionable recommendations, professional presentation.

2.7.2 Content Outline

1. Report Structure and Components (60 min): Standard CPF report template (Executive Summary, Methodology, Findings by Domain, Convergence Analysis, Recommendations, Appendices), Executive Summary requirements (1-2 pages maximum, key findings, overall CPF Score, compliance level, top priorities, written for non-technical executives), Methodology section (scope, data sources, privacy protections applied, limitations), Findings section structure (domain-by-domain, indicator scores with evidence summaries, category scores, narrative explanation), Convergence Analysis section (interactions between domains, critical convergent states, perfect storm conditions), Recommendations section (prioritized by impact/effort, mapped to compliance level progression, specific actionable steps), Appendices (full indicator scores table, methodology details, glossary, references).

2. Executive Summary Writing (75 min): Purpose and audience (busy executives, 5-minute read maximum), Structure (opening context, key findings, CPF Score and meaning, top 3-5 priorities, next steps), Writing style (clear, concise, no jargon, positive framing without minimizing risks), What to include (overall picture, critical findings, opportunities), What to exclude (excessive detail, individual attribution, technical methodology), Strong opening (hook reader, state significance), Effective closing (clear call to action, proposed timeline), Examples of good vs poor summaries, Practice writing exercise.

3. Technical Findings Documentation (90 min): Indicator-by-indicator documentation (score, evidence summary, analysis, confidence level), Evidence presentation (quote snippets not full transcripts, aggregate observations, statistical summaries, protecting individual identities), Scoring justification (why this score, Field Kit criteria applied, alternative interpretations considered), Confidence levels (high/medium/low based on evidence quality and quantity), Domain narrative (synthesize indicators into domain story, patterns and themes, organizational context), Balancing detail with readability (enough for credibility, not overwhelming), Handling conflicting evidence (present both sides, explain resolution, document uncertainty), Visual aids for findings (tables, charts, heat maps, radar charts).

4. Visualization Best Practices (60 min): Choosing appropriate visualizations (bar charts for comparisons, radar charts for domain overview, heat maps for indicator matrices, line charts for trends), CPF-specific visualizations (domain score radar, indicator heat map, convergence network diagram, compliance level progress), Color coding (Green/Yellow/Red consistent with ternary scoring, colorblind-friendly alternatives), Data-ink ratio (maximize information, minimize decoration), Chart titles and labels (clear, standalone, explain what reader should see), Accessibility considerations (contrast, alt text, not relying solely on color), Tools (Excel, PowerPoint, Tableau, R/Python for advanced), Common visualization errors to avoid.

5. Stakeholder Communication (60 min): Identifying stakeholders (executives, security team, privacy officer, HR, managers, auditors, board), Tailoring messages by audience (executives want priorities and ROI, security team wants technical details, HR wants employee impact, board wants risk and compliance), Presentation formats (written report, slide deck, verbal briefing, dashboard), Handling questions and challenges (prepare for skepticism, have evidence ready, professional defensiveness), Sensitive findings (negative results, attribution avoidance, constructive framing), Cultural considerations (organizational culture, communication norms, hierarchy), Follow-up communication (action plan development, progress updates, re-assessment scheduling).

6. Actionable Recommendations (60 min): Recommendation development (based on find-

ings, prioritized, specific and actionable, realistic given org context), Prioritization framework (impact vs effort matrix, quick wins vs long-term investments, compliance level progression), Mapping to compliance levels (what's needed to progress from current to next level), Intervention types (training, technical controls, process changes, cultural initiatives), Resource requirements (personnel, budget, timeline estimates), Success metrics (how to measure effectiveness, baseline and target), Implementation roadmap (phased approach, milestones, dependencies), Solution catalog reference (Field Kits provide solutions, adapt to org context).

2.7.3 Teaching Methods

Lecture: Report structure, executive summary principles, visualization design, stakeholder analysis.

Exercises: (1) Executive Summary Writing - given findings, write 1-page executive summary, peer review (60 min), (2) Visualization Creation - create 5 charts for sample data, critique (45 min), (3) Recommendation Development - prioritize interventions for case organization (45 min), (4) Stakeholder Presentation - present findings to "executive" (role play), Q&A (60 min).

Discussion: "Most challenging report sections?", "How handle negative findings diplomatically?", "Visualization tools preferences?"

Examples: Review 3 sample reports (good, mediocre, poor), identify strengths/weaknesses, discuss improvements.

2.7.4 Slide Breakdown

Slide 7.1: "CPF Report Structure" - Standard template components (Executive Summary, Methodology, Findings, Convergence, Recommendations, Appendices), purpose of each section, typical page counts.

Slide 7.2: "Executive Summary Requirements" - 1-2 pages maximum, audience (busy executives), structure (context, findings, score, priorities, next steps), writing style (clear, concise, no jargon), what to include/exclude.

Slide 7.3: "Executive Summary Examples" - Side-by-side good vs poor examples, annotations showing strengths/weaknesses, key takeaways for effective summaries.

Slide 7.4: "Methodology Section Content" - Scope description, data sources used, privacy protections applied (differential privacy, aggregation, temporal delay), assessment limitations, timeline.

Slide 7.5: "Findings Documentation Framework" - Indicator-by-indicator (score, evidence, analysis, confidence), domain narrative (synthesize into story), balancing detail with readability.

Slide 7.6: "Evidence Presentation" - Quote snippets not full transcripts, aggregate observations (never individual), statistical summaries, protecting identities, visual aids (tables, charts).

Slide 7.7: "Scoring Justification" - Document why this score, Field Kit criteria applied, evidence weighting explained, alternative interpretations considered, confidence levels.

Slide 7.8: "Visualization Types for CPF" - Domain score radar chart, indicator heat map (10x10 grid, color-coded), convergence network diagram, compliance level progress, before-after comparisons.

Slide 7.9: "Visualization Best Practices" - Choose appropriate type for data, color coding consistent (Green/Yellow/Red), colorblind-friendly alternatives, data-ink ratio maximized, clear titles/labels, accessibility.

Slide 7.10: "Visualization Tools" - Excel (sufficient for most), PowerPoint (presentation charts), Tableau (dashboards), R/Python (advanced custom), when to use each, learning resources.

Slide 7.11: "Stakeholder Analysis" - Identify audiences (executives, security, privacy, HR, managers, board), tailor messages (priorities vs details vs impact), presentation formats (report, slides, brief, dashboard).

Slide 7.12: "Handling Sensitive Findings" - Negative results framing (constructive, opportunity-focused), attribution avoidance (systemic not individual), professional diplomacy, prepare for skepticism, evidence ready.

Slide 7.13: "Actionable Recommendations Framework" - Prioritization (impact vs effort matrix), specificity (actionable steps not vague suggestions), realistic given org context, mapped to compliance progression.

Slide 7.14: "Recommendation Prioritization" - Quick wins (high impact, low effort - do first), strategic initiatives (high impact, high effort - plan carefully), fill-ins (low impact, low effort - if resources), avoid (low impact, high effort).

Slide 7.15: "Implementation Roadmap" - Phased approach (immediate 0-30 days, short-term 30-90 days, long-term 90+ days), milestones, dependencies, resource requirements, success metrics.

Slide 7.16: "Report Writing Exercises" - Executive summary writing instructions, visualization creation exercise, recommendation development case, stakeholder presentation role play.

2.7.5 Materials Needed

Workbook Module 7 (pages 101-120), CPF Report Template (blank, 30 pages), Sample Reports (3 complete - good, mediocre, poor), Executive Summary Examples (10 samples), Visualization Gallery (20+ examples with critiques), Stakeholder Analysis Worksheet, Recommendation Prioritization Matrix, Role Play Scenarios (3 stakeholder presentations), Peer Review Rubric.

2.7.6 Assessment Items

Quiz: Q1: Executive summary maximum length → 1-2 pages correct. Q2: Evidence presentation for privacy → aggregate not individual correct. Q3: Recommendation prioritization framework → impact vs effort matrix correct. Q4: Visualization for domain overview → radar chart correct. Q5: Stakeholder tailoring principle → different messages for different audiences correct.

Exercise Rubric (Executive Summary): Appropriate length 1-2 pages (1 pt), clear structure (context, findings, priorities, next steps) (3 pts), executive-appropriate language (no jargon) (2 pts), key findings accurately summarized (2 pts), actionable next steps (2 pts). Total 10 pts (7+ pass).

Final Report Rubric (Practical Exam): Executive summary effective (10 pts), methodology clearly documented (5 pts), findings properly documented per domain (20 pts), evidence appropriately presented (10 pts), scoring justified with confidence levels (15 pts), convergence analysis included (10 pts), recommendations prioritized and actionable (15 pts), visualizations effective (10 pts), professional presentation (5 pts). Total 100 pts (70+ pass).

3 Appendices

3.1 Appendix A: Complete Slide Inventory

Module & **Content** & **Duration**	
Module 1 & Assessment Planning (12 slides) & 6 hours	
Module 2 & Data Collection Part 1 (16 slides) & 8 hours	
Module 3 & Data Collection Part 2 (12 slides) & 6 hours	
Module 4 & Scoring Part 1 (12 slides) & 6 hours	
Module 5 & Scoring Part 2 (12 slides) & 6 hours	
Module 6 & Privacy Techniques (12 slides) & 6 hours	
Module 7 & Report Writing (16 slides) & 8 hours	
Total: 80 slides (12+16+12+12+12+12+16), 40 hours	

3.2 Appendix B: Practical Examination Structure

CPF-201 Practical Examination:

Format: 4-hour hands-on assessment, realistic organizational scenario with complete data set

Scenario: Medium organization (500 employees, 6 departments), evidence includes interview transcripts (anonymized, 20 employees), policy documents (15 pages), technical logs (email, authentication, help desk), survey results (70% response rate), behavioral observations (summarized).

Candidate Tasks:

1. Review all evidence systematically (30 min recommended)
2. Score all 100 indicators using ternary system with justification (120 min)
3. Calculate category and CPF scores (15 min)
4. Identify convergent vulnerability states (20 min)
5. Verify privacy requirements met (aggregation, temporal delay documentation) (15 min)
6. Develop top 5 prioritized recommendations (30 min)
7. Create 2-page executive summary (30 min)
8. Produce 3 visualizations (domain radar, indicator heat map, prioritization matrix) (30 min)

Evaluation Criteria (100 points total):

- Indicator Scoring Accuracy: 70/100 indicators scored correctly (within expert range) = 35 pts
- Scoring Justification: Evidence-based rationale documented = 15 pts
- Category/CPF Score Calculation: Correct mathematics = 5 pts
- Convergence Detection: Critical convergent states identified = 10 pts
- Privacy Compliance: Aggregation/differential privacy verified = 10 pts

- Recommendations: Prioritized, actionable, mapped to findings = 10 pts
- Executive Summary: Effective 2-page summary = 10 pts
- Visualizations: Appropriate and clear = 5 pts

Passing Standard: 70/100 points minimum

Both Practical Exam + Written Exam (100 questions, 70% pass) required for CPF-201 completion and Assessor certification eligibility.

3.3 Appendix C: Field Kit Usage Guide

How to Use Field Kits in CPF-201:

Each of 100 indicators has complete Field Kit with three components:

- Foundation: Psychological theory and research basis
- Operational: Assessment questions, observables, scoring criteria
- Field Kit: Quick reference checklist for assessments

During CPF-201 Training:

- Modules 1-3 (Planning, Data Collection): Reference Field Kits for assessment question examples and data source identification
- Modules 4-5 (Scoring): Use Field Kit scoring criteria extensively for calibration and practice
- Module 6 (Privacy): Field Kits show how privacy applies to each indicator
- Module 7 (Reporting): Field Kits provide solution catalogs for recommendations

Field Kits Referenced by Module:

Module 2 (Interviews): All 100 Field Kits contain interview questions - instructors demonstrate using 1.1, 2.1, 3.1 as examples

Module 3 (Surveys, Logs): Field Kits show relevant data sources - examples 5.1 (logs for alert fatigue), 7.1 (help desk for stress)

Module 4 (Scoring Practice): Intensive use of Field Kits 1.1, 1.3, 2.1, 2.3, 3.1, 3.3, 4.1, 4.5, 5.1, 5.2 (2 per domain for deep practice)

Module 5 (Convergence): Field Kits 10.1, 10.4 specifically address convergent states

Module 7 (Recommendations): All Field Kits contain Solution Catalogs with prioritized interventions

Complete Field Kit Library: All 100 provided to CPF-201 participants as reference materials. During practical exam, candidates may reference Field Kits but must demonstrate competence without excessive reliance.

3.4 Appendix D: Assessment Case Studies

Three Complete Practice Organizations:

Case Study 1: Regional Hospital (Healthcare)

- Size: 500 employees, 5 departments (Emergency, Surgery, ICU, Administration, IT)
- Scenario: Recent ransomware incident, high stress, 24/7 operations
- Evidence: 20 interview transcripts, policies (15 pages), incident reports (3 months), help desk tickets (200 entries), survey (350 responses)
- Expected Findings: High stress [7.x], cognitive overload [5.x], temporal vulnerabilities [2.x], convergence during shift changes
- Teaching Use: Modules 2-3 data collection practice, Module 4-5 scoring practice, Module 7 reporting practice

Case Study 2: Financial Services Firm (Finance)

- Size: 300 employees, 4 departments (Trading, Risk, Compliance, Operations)
- Scenario: Regulatory pressure, hierarchical culture, end-of-quarter deadline stress
- Evidence: 15 interview transcripts, email log samples (anonymized, 500 entries), policies (20 pages), phishing simulation results (3 campaigns), org chart with authority levels
- Expected Findings: Authority vulnerabilities [1.x], temporal deadline pressure [2.x], social proof in trading floor [3.x], convergence end-of-quarter
- Teaching Use: Module 1 planning (hierarchical culture), Modules 4-5 convergence detection, Module 7 executive communication

Case Study 3: Technology Startup (Tech)

- Size: 150 employees, flat structure, 3 product teams + support functions
- Scenario: Rapid growth, AI tool adoption, informal security practices
- Evidence: 10 interview transcripts, minimal documentation (5 pages), Slack samples (anonymized), AI tool usage logs, informal survey (120 responses)
- Expected Findings: AI-specific biases [9.x], group dynamics in flat structure [6.x], cognitive overload from rapid growth [5.x], unconscious processes [8.x]
- Teaching Use: Module 1 planning (minimal documentation challenges), Module 3 alternative data sources, Module 6 privacy with small aggregation units

All case studies include: Complete evidence packets, expert scoring answer keys (with justification), sample reports, common student errors to anticipate, teaching notes for instructors.

3.5 Appendix E: Inter-Rater Reliability Standards

CPF-201 Reliability Requirements:

Definition: Inter-rater reliability measures consistency between different assessors scoring same evidence.

Calculation Method: Cohen's Kappa coefficient

- Formula: $\kappa = \frac{p_o - p_e}{1 - p_e}$ where p_o = observed agreement, p_e = expected agreement by chance
- Range: -1 to +1, higher = better reliability
- Interpretation: ¡ 0.20 poor, 0.21-0.40 fair, 0.41-0.60 moderate, 0.61-0.80 substantial, 0.81-1.00 almost perfect

CPF Standards:

- Minimum acceptable: Kappa ¿ 0.70 (substantial agreement)
- Target: Kappa ¿ 0.80 (almost perfect agreement)
- Applied to: Indicator-level scores (Green/Yellow/Red), at least 20 indicators tested

Calibration Process:

1. Multiple raters (minimum 3) independently score same evidence
2. Calculate Kappa between all rater pairs
3. If Kappa ¡ 0.70: Discuss discrepancies, identify sources of disagreement
4. Review Field Kit scoring criteria together
5. Re-score independently
6. Recalculate Kappa, verify ¿ 0.70
7. Document calibration process and final Kappa

Common Sources of Disagreement:

- Misinterpretation of Field Kit criteria (solution: review criteria definition)
- Different evidence weighting (solution: discuss quality hierarchy)
- Domain knowledge gaps (solution: additional training)
- Bias (leniency, severity, halo - solution: awareness and calibration)

Documentation Requirements: Professional assessments must document:

- Number of raters involved
- Indicators tested for reliability
- Kappa coefficient calculated

- Calibration process if Kappa initially ¡ 0.70
- Final reliability achieved

Certification Examination: CPF-201 practical exam includes reliability testing. Candidate scores compared to expert panel scores, must achieve Kappa ¿ 0.70 on at least 70/100 indicators to demonstrate competence.

3.6 Appendix F: Privacy Calculation Examples

Differential Privacy Example:

Scenario: Calculating mean score for Domain [1.x] Authority across 50-person department.

Step 1: Calculate true mean: Sum of 50 individual category scores: 450, True mean: 450 / 50 = 9.0

Step 2: Determine sensitivity: Sensitivity = maximum possible change from adding/removing one individual, Category score range: 0-20, Sensitivity = 20 / 50 = 0.4

Step 3: Calculate noise scale: Laplace mechanism: Scale = Sensitivity / epsilon, Scale = 0.4 / 0.1 = 4.0

Step 4: Generate and add noise: Sample from Laplace(0, 4.0): e.g., noise = +1.2, Noisy mean: 9.0 + 1.2 = 10.2

Step 5: Report noisy mean: "Domain [1.x] Authority mean score: 10.2" (This satisfies epsilon-differential privacy with epsilon = 0.1)

Aggregation Unit Example:

Scenario: 200-person organization, 8 departments of varying sizes.

Department Sizes: Executive: 5 (too small), Sales: 30 ✓, Marketing: 15 ✓, Engineering: 60 ✓, Operations: 40 ✓, Finance: 12 ✓, HR: 8 (too small), IT: 30 ✓

Aggregation Strategy: Option 1: Combine Executive + HR = 13 ✓ (administrative functions), Option 2: Exclude Executive and HR, focus on 6 departments ≥10, Option 3: Use role-based aggregation instead (Managers, Individual Contributors across all departments)

Selected Approach: Option 1 (combine small departments by function), results in 7 aggregation units all ≥10.

Documentation: "Assessment used department-based aggregation units. Executive and HR combined due to small sizes (total n=13). All aggregation units maintained minimum 10 individuals."

Document Control

Version History:

Version	Date	Changes
1.0	January 2025	Initial release

Review Schedule: Annual review following course deliveries, practical examination statistics analysis, and Field Kit updates.

Approval:

Document Owner: CPF3 Training Development

Approved by: Giuseppe Canale, CISSP

Date: January 2025

Usage Instructions:

This blueprint enables modular slide generation for CPF-201 using the workflow:

1. Select module from Section 2 (Module Structures)
2. Review module overview, content outline, teaching methods, and slide breakdown
3. Generate slide content using AI assistance with prompt: "Generate slide content for [Module X, Slide Y] based on CPF-201-Training-Blueprint.tex Section 2.X. Include [specified Field Kits]. Output format: [title, bullets, notes, visual suggestions]."
4. Reference Field Kit Library extensively (all 100 indicators available)
5. Implement exercises using case study organizations (Healthcare, Finance, Tech)
6. Conduct practical examination following Appendix B structure
7. Verify inter-rater reliability per Appendix E standards

Relationship to Other Courses:

- Prerequisite: CPF-101 (Framework Fundamentals) must be completed first
- Leads to: CPF Assessor certification (with passing practical and written exams)
- Also prerequisite for: CPF-401 (Audit Techniques) for Auditor certification track
- Parallel track: CPF-301 (Advanced Implementation) for Practitioners focuses on interventions not assessment

Contact Information:

CPF3 Training Development

Website: https://cpf3.org

Email: training@cpf3.org

Assessment Support: assessment@cpf3.org

End of CPF-201 Training Blueprint