CPF-101 Training Blueprint

Framework Fundamentals 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-101: Framework Fundamentals, the foundational 40-hour course required for all CPF professional certifications. The document provides module-level outlines enabling systematic slide generation, exercise development, and assessment creation. Each module includes learning objectives, content structure, teaching methods, slide breakdowns, required materials, and assessment items. This blueprint serves as the reference document for creating instructor-led presentations, self-paced learning materials, and certification examination items.

Contents

1 Course Overview

1.1 Course Identification

Code: CPF-101 — **Title:** Framework Fundamentals — **Duration:** 40 hours (5 days intensive or 10 half-days) — **Slides:** 80 total — **Format:** Instructor-led or self-paced

1.2 Target Audience

Cybersecurity professionals, information security practitioners, security auditors, and risk management professionals pursuing CPF Assessor, Practitioner, or Auditor certification. Prerequisites include bachelor's degree (or equivalent) and 2+ years experience in cybersecurity or psychology.

1.3 Learning Objectives

Upon completion, participants will: (1) Explain pre-cognitive psychological mechanisms underlying 82-85% of security incidents, (2) Identify theoretical foundations from psychoanalysis and cognitive psychology, (3) Describe all 10 CPF domains and 100 indicators, (4) Articulate privacy protection requirements, (5) Apply ternary scoring methodology to scenarios, (6) Map CPF to ISO 27001 and NIST CSF 2.0.

1.4 Course Structure

Part I - Foundations (12h, Modules 1-3): Introduction to Cybersecurity Psychology (4h), Psychoanalytic Foundations (4h), Cognitive Psychology Foundations (4h).

Part II - CPF Domains (20h, Modules 4-13): Ten 2-hour modules covering Authority [1.x], Temporal [2.x], Social Influence [3.x], Affective [4.x], Cognitive Overload [5.x], Group Dynamics [6.x], Stress Response [7.x], Unconscious Process [8.x], AI-Specific Bias [9.x], Critical Convergent States [10.x].

Part III - Application (8h, Modules 14-15): Privacy and Ethics (4h), Integration and Application (4h).

1.5 Assessment Method

Formative: Module quizzes (3-5 questions each), 15 practical exercises, 5 case studies. Summative: 100-question written examination (60 multiple-choice, 30 scenario-based, 10 case analysis), 3 hours, 70% passing score. Certification requires 90% attendance and signed ethics agreement.

1.6 Materials Provided

CPF-101 Participant Workbook (80 pages), CPF Taxonomy Quick Reference Card, Field Kit Example (Indicator 1.1 complete), Case Study Packet (5 scenarios), Assessment Template, CPF framework papers (taxonomy, CPF-27001 requirements, certification scheme).

2 Module Structures

2.1 Module 1: Introduction to Cybersecurity Psychology

2.1.1 Overview

Duration: 4 hours — **Slides:** 6

Learning Objectives: Articulate why traditional security awareness fails to prevent 82-85% of incidents; explain neuroscience evidence for pre-cognitive decision-making; describe CPF architecture (10 domains, 100 indicators, ternary scoring); map CPF integration with ISO 27001 and NIST CSF; analyze major breach through CPF lens.

Key Concepts: Pre-cognitive processing, System 1 vs System 2, human factor gap, framework architecture, integration strategy.

2.1.2 Content Outline

1. Human Factor Gap (45 min): Global spending vs increasing breaches, Verizon DBIR statistics, failure of rational actor model, why awareness training provides false confidence, real-world examples (Target, Anthem, SolarWinds).

2. Pre-Cognitive Processing (60 min): Neuroscience evidence (Libet 1983, Soon 2008), amygdala activation 300-500ms before conscious awareness, fMRI decision studies, Damasio somatic markers, evolutionary hardwiring creates vulnerabilities, implications for security training, video demonstration.

3. CPF Architecture (60 min): 10x10 structure overview, brief introduction to all 10 domains, ternary scoring (Green/Yellow/Red), privacy-first design (aggregation, differential privacy, temporal delays), assessment methodology overview.

4. Integration with Frameworks (45 min): ISO 27001:2022 mapping (Clause 7.2 Competence, 7.3 Awareness, Annex A enhancement), NIST CSF 2.0 integration (Identify/Protect/Detect/Respond/Re CPF as psychological intelligence layer, complementary relationship.

5. Case Study: Target Breach (30 min): Technical narrative, CPF psychological analysis (authority vulnerability, alert fatigue, group dynamics, temporal pressure), how assessment could predict convergence, preventive interventions, discussion.

2.1.3 Teaching Methods

Lecture: Statistics/charts for human factor gap, neuroscience video with fMRI images, animated framework diagram, ISO/NIST comparison tables.

Exercises: (1) Awareness Failure Analysis - share failed training examples (15 min), (2) Pre-Cognitive Decision Experiment - live authority/urgency demonstration (10 min), (3) Framework Navigation - speed drill with Quick Reference Card (20 min).

Discussion: "Think of an incident - could awareness training have prevented it?", "What does 300-500ms pre-conscious decision mean for your program?", "Explain CPF to CISO in 60 seconds."

Case Study: Target breach presented chronologically, groups identify vulnerabilities, connect to CPF domains, synthesize convergent state prediction.

2.1.4 Slide Breakdown

Slide 1.1: "The Human Factor Crisis" - Spending vs breach trends chart, Verizon statistics, human silhouette vs fortress visual.

Slide 1.2: "Pre-Cognitive Decision-Making" - Timeline diagram (0ms→300ms→500ms→800ms), Libet/Soon results, brain diagram (amygdala vs prefrontal cortex).

Slide 1.3: "CPF Framework Architecture" - 10x10 grid with domain names/icons, 100 indicators, ternary scoring callout, privacy-first design.

Slide 1.4: "Ternary Scoring System" - Three-column comparison (Green/Yellow/Red), example indicator 1.1, category/CPF score formulas.

Slide 1.5: "Integration with ISO 27001 and NIST CSF" - Split diagram showing enhancement points, "CPF complements not replaces" message.

Slide 1.6: "Target Breach Through CPF Lens" - Timeline, technical story, CPF analysis overlay (4 domains identified), exercise prompt.

2.1.5 Materials Needed

Workbook Module 1 (pages 1-15), Taxonomy Quick Reference Card, neuroscience video (5 min), Target case study handout (2 pages), Exercise Worksheets 1.1 and 1.3, whiteboard/digital collaboration tool.

2.1.6 Assessment Items

Quiz (5 questions): Q1: Verizon DBIR human factor % → 82-85% correct. Q2: Amygdala activation timing → 300-500ms correct. Q3: Total CPF indicators → 100 correct. Q4: Yellow score meaning → moderate vulnerability/monitoring correct. Q5: ISO clause CPF enhances → 7.2 Competence correct.

Exercise Rubric (Framework Navigation): Speed 5 indicators ¡2 min (2 pts), accuracy domain/number (3 pts), comprehension explanation (3 pts), application scenario (2 pts). Total 10 pts (7+ pass).

2.2 Module 2: Psychoanalytic Foundations

2.2.1 Overview

Duration: 4 hours — **Slides:** 7

Learning Objectives: Explain Bion's basic assumptions (baD/baF/baP) in security contexts; apply Klein's object relations (splitting, projection) to organizational blind spots; identify Jung's shadow and collective unconscious in threat perception; describe Winnicott's transitional space relevance to digital security; analyze security postures through psychoanalytic lens.

Key Concepts: Basic assumptions, object relations, splitting, projection, shadow, collective unconscious, transitional space, social defense systems.

2.2.2 Content Outline

1. Bion's Basic Assumptions (75 min): Bion "Experiences in Groups" (1961), three defensive postures under anxiety. baD (Dependency): Omnipotent leader/technology seeking, se-

curity tool magical thinking, [6.6] indicator. baF (Fight-Flight): External enemy focus, fortress mentality, insider threat blindness, [6.7] indicator. baP (Pairing): Future salvation hope, continuous tool shopping, [6.8] indicator. Recognition in security teams, vulnerability creation.

2. Kleinian Object Relations (60 min): Klein contributions, Splitting mechanism (all good/all bad division, insiders idealized vs attackers demonized, insider threat invisibility, [6.9] organizational splitting), Projection mechanism (organizational vulnerabilities attributed externally, learning blocked, [8.1] shadow projection), Menzies Lyth social defense systems (ritualistic checkbox compliance, [6.10] collective defenses), pattern identification.

3. Jungian Psychology (60 min): Shadow concept (disowned aspects projected, black hat hackers embody organizational aggression, security team attacker identification, red team as shadow expression, [8.1][8.2] indicators), Archetypes (Hero CISO, Trickster hacker, Wise consultant, Shadow insider threat, [8.8] archetypal activation), Collective unconscious (shared industry denials, "too small to target" myth, [8.9] patterns), shadow work for vulnerability reduction.

4. Winnicott Transitional Space (30 min): Transitional objects/spaces concept, digital environments as transitional (neither real nor imaginary, reduced reality testing, omnipotent online fantasies, digital identity confusion, social media guard lowering, [8.10] dream logic, [8.7] symbolic equation), exploitation mechanisms, design implications.

5. Exercise: Psychoanalytic Case Analysis (15 min): Healthcare ransomware case, groups identify basic assumption, splitting evidence, projections, shadow elements, collective defenses. Presentations, facilitator maps to CPF indicators [6.x] and [8.x].

2.2.3 Teaching Methods

Lecture: Bion organizational diagrams, Klein splitting/projection visuals, Jung archetypal images, Winnicott physical vs digital space comparison.

Exercises: (1) Basic Assumption ID - 3 vignettes, identify baD/baF/baP (20 min), (2) Splitting in Security Culture - list trusted/threatening entities, discuss blind spots (15 min), (3) Shadow Recognition - anonymous reflection "what org refuses to acknowledge" (15 min).

Discussion: "Seen silver bullet thinking?", "How does org describe attackers?", "What security rituals provide false comfort?"

Media: Group dynamics video clip (5 min), Jung shadow animation, splitting diagram.

2.2.4 Slide Breakdown

Slide 2.1: "Bion's Basic Assumptions Overview" - Three postures with icons (crown, sword/shield, hope), Bion quote, unconscious not deliberate.

Slide 2.2: "Basic Assumptions in Security" - Three-column table (baD/baF/baP with behaviors, examples, vulnerabilities, CPF indicators).

Slide 2.3: "Kleinian Splitting and Projection" - Split diagram good/bad, splitting mechanism (insiders trusted, insider threats invisible), projection mechanism (blame external, no learning), Klein quote, indicators [6.9][8.1].

Slide 2.4: "Jung's Shadow in Security" - Light/dark silhouette, shadow concept, security manifestations (black hats, red teams, identification), collective shadow (industry denials), Jung quote, indicators [8.1][8.2][8.9].

Slide 2.5: "Archetypes in Security" - Four archetypal images (Hero CISO, Trickster hacker,

Wise consultant, Shadow insider), descriptions with vulnerabilities, unconscious patterns note, indicator [8.8].

Slide 2.6: "Winnicott's Transitional Space" - Physical vs digital comparison table, security implications (omnipotence, identity confusion, dream logic, symbolic equations), Winnicott quote, indicators [8.10][8.7], social media example.

Slide 2.7: "Psychoanalytic Case Analysis Exercise" - Healthcare ransomware brief, analysis framework (basic assumption, splitting, projection, shadow, defenses), group task instructions, expected findings, debrief question.

2.2.5 Materials Needed

Workbook Module 2 (pages 16-30), Exercise 2.1 three vignettes worksheet, Exercise 2.2 splitting template, Exercise 2.3 anonymous shadow cards, healthcare case handout (2 pages), archetypal images, group dynamics video (5 min), whiteboard.

2.2.6 Assessment Items

Quiz (5 questions): Q1: baD characteristic → seeking omnipotent protector correct. Q2: Splitting definition → unconscious all good/bad division correct. Q3: Shadow projection indicator → [8.1] correct. Q4: Transitional space relevance → neither real nor imaginary, reduced reality testing correct. Q5: Continuous tool shopping basic assumption → baP correct.

Exercise Rubric (Splitting): List 3+ trusted and threatening entities (2 pts), recognize idealization/demonization (3 pts), identify 2+ blind spots (3 pts), suggest addressing splitting (2 pts). Total 10 pts (7+ pass).

2.3 Module 3: Cognitive Psychology Foundations

2.3.1 Overview

Duration: 4 hours — **Slides:** 7

Learning Objectives: Explain Kahneman's dual-process theory (System 1/2) implications for security; apply Cialdini's six influence principles to social engineering; analyze Miller's cognitive load impact on security tasks; identify heuristics/biases enabling exploitation; evaluate organizational structures through cognitive lens.

Key Concepts: System 1/2, heuristics, cognitive biases, influence principles (reciprocity, commitment, social proof, authority, liking, scarcity), cognitive load, working memory.

2.3.2 Content Outline

1. Kahneman Dual-Process (75 min): "Thinking Fast and Slow" (2011), System 1 (fast, automatic, unconscious, pattern recognition, emotional, heuristics, always on), System 2 (slow, deliberate, conscious, effortful, analytical, limited capacity, depletes). Security decision problem (most decisions ¡1 sec System 1, verification requires 10-30 sec System 2, time pressure = System 1 dominance, attackers exploit System 1). Key heuristics (availability, representativeness, anchoring, confirmation, optimism bias). CPF indicators leverage System 1 vulnerabilities.

2. Cialdini Six Principles (75 min): "Influence" (2007), each principle = attack vector. (1) Reciprocity: Obligation to return favors, quid pro quo attacks, [3.1] exploitation. (2) Commit-

ment/Consistency: Align with prior commitments, gradual escalation foot-in-door, [3.2] traps. (3) Social Proof: Look to others, "everyone clicked" manipulation, [3.3] manipulation, [3.8] conformity. (4) Authority: Deference to authority, CEO fraud, fake IT, Domain [1.x] entire. (5) Liking: Comply with liked people, rapport building, [3.4] trust override. (6) Scarcity: Value limited things, urgency attacks, [3.5] scarcity decisions. Recognition of combined principles in attacks (BEC = Authority + Scarcity + Commitment).

3. Miller Cognitive Load (45 min): "Magical Number 7±2" (1956), working memory limits (7±2 items now 4±1, 15-30 sec duration, easily overwhelmed). Security task load (intrinsic complexity, extraneous unnecessary complexity, germane learning, total = sum of three, overload = errors/heuristics/System 1). Overload manifestations (alert fatigue, decision fatigue, multitasking degradation, complexity errors). Domain [5.x] all 10 indicators relate to capacity limits. Design principle: reduce extraneous load.

4. Decision Under Uncertainty (30 min): Prospect Theory (Kahneman/Tversky 1979), Loss aversion (losses larger than gains, ransomware effectiveness, [4.1] fear paralysis, [2.3] deadline risk), Framing effects (presentation changes decisions, protection vs restriction framing), Sunk cost fallacy (continue based on past investment, ineffective tool persistence, [4.4] legacy attachment).

5. Exercise: Cognitive Exploitation Analysis (15 min): Three social engineering emails, tasks (identify Cialdini principles, System 1 or 2 target, cognitive load manipulation, countermeasures based on cognitive psychology), group discussion how each fools System 1, facilitator connects to CPF indicators.

2.3.3 Teaching Methods

Lecture: Dual-process with optical illusions and rapid decisions, Cialdini with advertising examples then security, Cognitive load with digit span test, Decision-making with framing exercise.

Exercises: (1) System 1 vs 2 Speed Test - 20 emails 3 sec each then unlimited, compare accuracy (15 min), (2) Cialdini Mapping - 6 scenarios map principles, discuss combinations (20 min), (3) Cognitive Load Simulation - security task with distractions, experience overload (15 min).

Discussion: "Clicked something you shouldn't - System 1 or 2?", "Most dangerous Cialdini principle?", "How many daily security decisions? Cognitive cost?"

Media: Kahneman TED excerpt (5 min), Cialdini Candid Camera demonstrations (10 min), cognitive load animation (3 min).

2.3.4 Slide Breakdown

Slide 3.1: "Thinking Fast and Slow" - Split-screen System 1 vs 2 table (speed, mode, energy, method, security role, vulnerability/limitation), key insight most decisions System 1 timeframe, Kahneman quote, brain diagram.

Slide 3.2: "Heuristics and Biases" - Five heuristics with definitions, security examples, vulnerabilities (availability, representativeness, anchoring, confirmation, optimism).

Slide 3.3: "Cialdini's Six Principles Overview" - Six-box grid with icons, principle names, one-line descriptions, "Each = attack vector" message.

Slide 3.4: "Six Principles in Social Engineering" - Detailed table (principle, mechanism, security example, CPF indicator) for all six, note on combined principles, BEC example.

Slide 3.5: "Cognitive Load Theory" - Working memory capacity visual (7±2 now 4±1), three load types diagram (intrinsic, extraneous, germane), security overload manifestations (alert

fatigue, decision fatigue, multitasking, complexity), Miller quote, Domain [5.x] note.

Slide 3.6: "Decision-Making Under Uncertainty" - Loss aversion explanation with ransomware example, framing effects demonstration, sunk cost fallacy with tool persistence, indicators [4.1][2.3][4.4].

Slide 3.7: "Cognitive Exploitation Exercise" - Three email examples displayed, analysis framework (Cialdini principles, System target, load manipulation, countermeasures), group task instructions, discussion prompt.

2.3.5 Materials Needed

Workbook Module 3 (pages 31-45), Exercise 3.1 20-email test set, Exercise 3.2 six scenario cards, Exercise 3.3 distraction simulation setup, three phishing emails for analysis, Kahneman video (5 min), Cialdini clips (10 min), cognitive load animation (3 min), whiteboard.

2.3.6 Assessment Items

Quiz (5 questions): Q1: System 1 characteristics → fast, automatic, unconscious correct. Q2: Cialdini reciprocity principle → obligation to return favors correct. Q3: Miller working memory capacity → 7 ± 2 (or 4 ± 1) correct. Q4: Which Domain addresses cognitive overload → [5.x] correct. Q5: Loss aversion explains → ransomware effectiveness correct.

Exercise Rubric (Email Analysis): Identify 2+ Cialdini principles (3 pts), determine System 1/2 target correctly (2 pts), explain cognitive load manipulation (3 pts), suggest effective countermeasure (2 pts). Total 10 pts (7+ pass).

2.4 Module 4: Domain [1.x] Authority-Based Vulnerabilities

2.4.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Understand Milgram obedience research and cybersecurity implications; identify 10 authority indicators; apply ternary scoring to authority compliance scenarios; recommend top 3 remediation strategies.

Key Concepts: Authority deference, diffusion of responsibility, CEO fraud, BEC, verification protocols.

2.4.2 Content Outline

1. Psychological Foundation (20 min): Milgram experiments 65% obedience, neuroscience amygdala hijack, evolution authority deference survival mechanism, System 1 vs 2 in authority contexts.

2. Ten Authority Indicators (30 min): Overview table 1.1-1.10, Deep-dive 1.1 (unquestioning compliance, observables, assessment questions, G/Y/R scoring), Deep-dive 1.3 (impersonation susceptibility, email authentication gaps, verification failures, multi-channel), patterns across remaining indicators.

3. Attack Vectors and Incidents (30 min): BEC $43B FBI losses, Target breach via vendor authority case, spear phishing with authority claims, IT support social engineering, technical failure points (MFA bypass, privilege escalation).

4. Assessment and Solutions (30 min): Observable indicators in organizations, ternary scoring decision tree, Top 3 solutions (dual-channel verification protocol, authority challenge training, simulation testing program), implementation priorities (high/medium/long-term).

5. Exercise (10 min): Case scenario CFO wire transfer email, students assess score/rationale/solutions, group discussion and feedback.

2.4.3 Teaching Methods

Lecture: Milgram with historical footage, neuroscience diagrams, attack flow visuals.

Exercise: CFO fraud scenario, individual assessment then group comparison.

Discussion: "Seen authority bypass in your org?", "How verify unusual executive requests?"

2.4.4 Slide Breakdown

Slide 4.1: "Why We Obey: Authority Vulnerability" - Milgram visual, neuroscience diagram, evolution context, 65% stat, 300-500ms activation, transition to CEO fraud.

Slide 4.2: "10 Authority Indicators" - Table 1.1-1.10 with brief descriptions, highlight 1.1 and 1.3 for deep-dive, indicator icons.

Slide 4.3: "Attack Vectors in Action" - BEC $43B stat, Target breach timeline, spear phishing examples, attack flow diagram, real email snippet (redacted).

Slide 4.4: "Assessment and Solutions" - Observable checklist, scoring decision tree G/Y/R, top 3 solutions with icons/timelines, exercise prompt CFO scenario.

2.4.5 Materials Needed

Field Kit 1.1 and 1.3 (reference), Taxonomy section [1.x], Target case study, CFO exercise handout.

2.4.6 Assessment Items

Quiz: Q1: Milgram obedience % $\rightarrow$ 65% correct. Q2: Indicator for security bypass for superiors $\rightarrow$ 1.4 correct. Q3: Primary authority mechanism $\rightarrow$ amygdala hijack before rational processing correct.

Exercise Rubric: Vulnerability ID (2 pts), ternary score with justification (3 pts), relevant solution (3 pts), implementation priority understanding (2 pts). Total 10 pts (7+ pass).

2.5 Module 5: Domain [2.x] Temporal Vulnerabilities

2.5.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Explain time pressure effects on security decisions; identify 10 temporal indicators; recognize deadline-driven attack patterns; apply temporal vulnerability scoring.

Key Concepts: Urgency exploitation, time pressure degradation, deadline attacks, present bias, hyperbolic discounting.

2.5.2 Content Outline

1. Psychological Foundation (20 min): Time pressure cognitive degradation (Kahneman/Tversky), present bias (immediate rewards overweighted), hyperbolic discounting (future threats discounted), System 2 shutdown under time pressure.

2. Ten Temporal Indicators (30 min): Overview table 2.1-2.10, Deep-dive 2.1 (urgency-induced bypass, "act now" attacks, scoring), Deep-dive 2.3 (deadline-driven risk acceptance, end-of-quarter pressure, scoring), temporal patterns.

3. Attack Vectors and Incidents (30 min): Deadline attacks (tax season, end-of-quarter), time-of-day exploitation (shift changes, late hours), weekend/holiday vulnerabilities, temporal social engineering case examples.

4. Assessment and Solutions (30 min): Temporal vulnerability observables, scoring criteria, Top 3 solutions (cooling-off periods for urgent requests, shift-change security protocols, temporal anomaly detection), implementation.

5. Exercise (10 min): Urgent invoice payment scenario with time pressure, assess temporal vulnerabilities, recommend controls.

2.5.3 Teaching Methods

Lecture: Time pressure experiments, present bias demonstrations, temporal attack timelines.

Exercise: Urgent payment scenario under simulated time pressure.

Discussion: "When are security decisions worst?", "End-of-quarter security compromises?"

2.5.4 Slide Breakdown

Slide 5.1: "Time Pressure and Security" - Cognitive degradation under time constraints, present bias explanation, hyperbolic discounting, System 2 shutdown.

Slide 5.2: "10 Temporal Indicators" - Table 2.1-2.10, highlight 2.1 and 2.3, temporal vulnerability patterns.

Slide 5.3: "Temporal Attack Vectors" - Deadline attacks (tax, quarter-end), time-of-day windows, weekend/holiday exploitation, case examples with timelines.

Slide 5.4: "Assessment and Solutions" - Temporal observables, scoring decision tree, top 3 solutions (cooling-off, shift protocols, anomaly detection), exercise prompt.

2.5.5 Materials Needed

Field Kit 2.1 and 2.3, Taxonomy [2.x], urgent payment exercise handout.

2.5.6 Assessment Items

Quiz: Q1: Present bias definition → immediate rewards overweighted correct. Q2: Indicator for urgency bypass → 2.1 correct. Q3: Temporal vulnerability amplifier → time pressure, deadlines correct.

Exercise Rubric: Temporal vulnerability ID (3 pts), urgency pressure analysis (2 pts), scoring with justification (3 pts), temporal controls recommendation (2 pts). Total 10 pts (7+ pass).

2.6 Module 6: Domain [3.x] Social Influence Vulnerabilities

2.6.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Apply Cialdini principles to security contexts; identify 10 social influence indicators; analyze social engineering attack patterns; design social influence countermeasures.

Key Concepts: Reciprocity, commitment/consistency, social proof, liking, scarcity, unity principle, peer pressure, conformity.

2.6.2 Content Outline

1. Psychological Foundation (20 min): Cialdini six principles review (from Module 3), social influence as evolutionary mechanism, compliance psychology, combination effects in attacks.

2. Ten Social Indicators (30 min): Overview table 3.1-3.10, Deep-dive 3.1 (reciprocity exploitation, quid pro quo, scoring), Deep-dive 3.3 (social proof manipulation, "everyone clicked" attacks, scoring), social influence patterns across indicators.

3. Attack Vectors and Incidents (30 min): Social engineering campaigns (pretext building, rapport establishment), peer pressure attacks (fake IT broadcasts), conformity exploitation (everyone updating passwords), unity principle (fake team requests), real-world social engineering cases.

4. Assessment and Solutions (30 min): Social influence observables, scoring criteria, Top 3 solutions (social proof verification protocols, peer validation systems, influence awareness training), implementation priorities.

5. Exercise (10 min): Social engineering email combining multiple Cialdini principles, identify which principles used, assess vulnerability score, recommend defenses.

2.6.3 Teaching Methods

Lecture: Cialdini principles demonstrations, social engineering video examples, influence combination analysis.

Exercise: Multi-principle phishing email analysis, group identification of techniques.

Discussion: "Most effective Cialdini principle in your experience?", "How resist social proof in security?"

2.6.4 Slide Breakdown

Slide 6.1: "Social Influence Mechanisms" - Six Cialdini principles visual review, evolutionary basis, compliance psychology, combination attack effects.

Slide 6.2: "10 Social Influence Indicators" - Table 3.1-3.10, highlight 3.1 and 3.3, social influence vulnerability patterns.

Slide 6.3: "Social Engineering Attack Patterns" - Campaign examples (pretext, rapport, pressure), conformity exploitation scenarios, unity principle fake requests, real-world cases.

Slide 6.4: "Assessment and Solutions" - Social observables checklist, scoring decision tree, top

3 solutions (verification protocols, peer validation, awareness training), exercise prompt multi-principle email.

2.6.5 Materials Needed

Field Kit 3.1 and 3.3, Taxonomy [3.x], social engineering video clips (5 min), multi-principle exercise handout.

2.6.6 Assessment Items

Quiz: Q1: Reciprocity principle definition → obligation to return favors correct. Q2: Social proof indicator → 3.3 correct. Q3: Most dangerous combination → multiple answers acceptable (Authority + Scarcity, Social Proof + Liking).

Exercise Rubric: Identify 3+ Cialdini principles (3 pts), explain influence mechanism (2 pts), vulnerability scoring with justification (3 pts), defense recommendations (2 pts). Total 10 pts (7+ pass).

2.7 Module 7: Domain [4.x] Affective Vulnerabilities

2.7.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Explain emotion-driven security decisions; identify 10 affective indicators; recognize emotional manipulation attacks; apply affective vulnerability assessment.

Key Concepts: Fear exploitation, anger-induced risk, trust transference, attachment, shame hiding, emotional contagion.

2.7.2 Content Outline

1. Psychological Foundation (20 min): Emotion primacy over cognition (LeDoux), affective heuristic (Slovic), emotional contagion (Hatfield), amygdala hijack in security contexts, emotional states alter risk perception.

2. Ten Affective Indicators (30 min): Overview table 4.1-4.10, Deep-dive 4.1 (fear-based paralysis, ransomware FUD, scoring), Deep-dive 4.5 (shame-based security hiding, incident non-reporting, scoring), affective patterns.

3. Attack Vectors and Incidents (30 min): Fear-based attacks (ransomware, scare tactics), anger manipulation (provocative content), trust exploitation (fake support), shame prevention of reporting, emotional contagion in breaches, case examples.

4. Assessment and Solutions (30 min): Affective vulnerability observables, scoring criteria, Top 3 solutions (psychological safety for reporting, emotional regulation training, FUD resistance protocols), implementation.

5. Exercise (10 min): Ransomware scenario with fear manipulation, assess emotional vulnerabilities, design psychological safety interventions.

2.7.3 Teaching Methods

Lecture: Emotion neuroscience, affective heuristic demonstrations, emotional attack examples.

Exercise: Ransomware fear scenario, individual then group analysis of emotional manipulation.

Discussion: "Fear-based security decisions made?", "How create psychological safety for incident reporting?"

2.7.4 Slide Breakdown

Slide 7.1: "Emotion and Security Decisions" - Emotion primacy (LeDoux), affective heuristic explanation, amygdala hijack diagram, emotional risk perception alteration.

Slide 7.2: "10 Affective Indicators" - Table 4.1-4.10, highlight 4.1 and 4.5, emotional vulnerability patterns.

Slide 7.3: "Emotional Manipulation Attacks" - Fear-based (ransomware FUD), anger manipulation, trust exploitation, shame reporting prevention, emotional contagion effects, case examples.

Slide 7.4: "Assessment and Solutions" - Affective observables, scoring decision tree, top 3 solutions (psychological safety, emotional regulation, FUD resistance), exercise prompt ransomware scenario.

2.7.5 Materials Needed

Field Kit 4.1 and 4.5, Taxonomy [4.x], ransomware exercise handout, emotional contagion video (3 min).

2.7.6 Assessment Items

Quiz: Q1: Affective heuristic definition → decisions based on emotional state correct. Q2: Fear paralysis indicator → 4.1 correct. Q3: Shame-based hiding indicator → 4.5 correct.

Exercise Rubric: Fear manipulation identification (3 pts), emotional vulnerability assessment (2 pts), scoring with justification (3 pts), psychological safety intervention design (2 pts). Total 10 pts (7+ pass).

2.8 Module 8: Domain [5.x] Cognitive Overload Vulnerabilities

2.8.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Apply Miller cognitive load theory to security; identify 10 overload indicators; recognize capacity exploitation attacks; design cognitive load reduction interventions.

Key Concepts: Working memory limits, alert fatigue, decision fatigue, multitasking degradation, cognitive tunneling.

2.8.2 Content Outline

1. Psychological Foundation (20 min): Miller 7 ± 2 working memory (now 4 ± 1), cognitive load types (intrinsic, extraneous, germane), capacity overload consequences, System 2 depletion, security task complexity.

2. Ten Overload Indicators (30 min): Overview table 5.1-5.10, Deep-dive 5.1 (alert fatigue desensitization, SOC overload, scoring), Deep-dive 5.2 (decision fatigue errors, repeated security choices, scoring), overload patterns.

3. Attack Vectors and Incidents (30 min): Alert fatigue exploitation (noise before attack), decision fatigue timing (end-of-day attacks), multitasking vulnerability windows, complexity-induced errors, Target SOC alert fatigue case.

4. Assessment and Solutions (30 min): Overload vulnerability observables, scoring criteria, Top 3 solutions (alert consolidation and tuning, decision simplification, cognitive load budgets), implementation.

5. Exercise (10 min): SOC analyst overload scenario with 50+ alerts, assess cognitive vulnerabilities, design alert reduction strategy.

2.8.3 Teaching Methods

Lecture: Working memory demonstrations (digit span), alert fatigue visualization, decision fatigue experiments.

Exercise: SOC overload simulation, experience cognitive capacity limits.

Discussion: "How many security decisions daily?", "Alert fatigue in your SOC?"

2.8.4 Slide Breakdown

Slide 8.1: "Cognitive Load and Capacity Limits" - Miller 7±2 (4±1) visual, three load types diagram, overload consequences, System 2 depletion, security complexity impact.

Slide 8.2: "10 Cognitive Overload Indicators" - Table 5.1-5.10, highlight 5.1 and 5.2, overload vulnerability patterns.

Slide 8.3: "Cognitive Exploitation Attacks" - Alert fatigue exploitation examples, decision fatigue timing attacks, multitasking windows, complexity errors, Target SOC case with 40+ ignored alerts.

Slide 8.4: "Assessment and Solutions" - Overload observables (alert counts, decision frequency), scoring decision tree, top 3 solutions (consolidation, simplification, load budgets), exercise prompt SOC scenario.

2.8.5 Materials Needed

Field Kit 5.1 and 5.2, Taxonomy [5.x], SOC overload exercise with 50-alert scenario, digit span test materials.

2.8.6 Assessment Items

Quiz: Q1: Miller working memory capacity → 7±2 or 4±1 correct. Q2: Alert fatigue indicator → 5.1 correct. Q3: Decision fatigue indicator → 5.2 correct.

Exercise Rubric: Cognitive overload identification (3 pts), capacity limit analysis (2 pts), vulnerability scoring with justification (3 pts), alert reduction strategy (2 pts). Total 10 pts (7+ pass).

2.9 Module 9: Domain [6.x] Group Dynamic Vulnerabilities

2.9.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Apply Bion basic assumptions to security teams; identify 10 group dynamic indicators; recognize collective vulnerability patterns; design group-level interventions.

Key Concepts: Groupthink, risky shift, diffusion of responsibility, social loafing, bystander effect, basic assumptions (baD/baF/baP).

2.9.2 Content Outline

1. Psychological Foundation (20 min): Bion basic assumptions review (from Module 2), groupthink (Janis), risky shift phenomenon, diffusion of responsibility (Latané), collective unconscious in security teams.

2. Ten Group Indicators (30 min): Overview table 6.1-6.10, Deep-dive 6.1 (groupthink security blind spots, consensus pressure, scoring), Deep-dive 6.3 (diffusion of responsibility, "someone else will check", scoring), group patterns.

3. Attack Vectors and Incidents (30 min): Organizational disruption attacks (exploiting group dynamics), collective decision failures, bystander effect in incident response, group-level social engineering, NASA Challenger as groupthink parallel.

4. Assessment and Solutions (30 min): Group vulnerability observables, scoring criteria, Top 3 solutions (red team dissent roles, responsibility assignment, group decision protocols), implementation.

5. Exercise (10 min): Security committee decision scenario with groupthink pressure, identify group vulnerabilities, design dissent mechanisms.

2.9.3 Teaching Methods

Lecture: Groupthink video examples, risky shift demonstrations, basic assumptions in teams.

Exercise: Committee decision with groupthink, experience consensus pressure.

Discussion: "Groupthink in your security team?", "How encourage dissent safely?"

2.9.4 Slide Breakdown

Slide 9.1: "Group Psychology in Security" - Bion basic assumptions brief review, groupthink concept (Janis), risky shift, diffusion of responsibility, collective vulnerabilities.

Slide 9.2: "10 Group Dynamic Indicators" - Table 6.1-6.10, highlight 6.1 and 6.3, group vulnerability patterns.

Slide 9.3: "Group-Level Attack Vectors" - Organizational disruption techniques, collective decision failures, bystander effect in IR, group social engineering, Challenger groupthink parallel.

Slide 9.4: "Assessment and Solutions" - Group observables (meeting dynamics, decision patterns), scoring decision tree, top 3 solutions (dissent roles, responsibility assignment, decision protocols), exercise prompt committee scenario.

2.9.5 Materials Needed

Field Kit 6.1 and 6.3, Taxonomy [6.x], groupthink video (5 min), committee exercise handout.

2.9.6 Assessment Items

Quiz: Q1: Groupthink definition → consensus pressure prevents critical evaluation correct. Q2: Groupthink indicator → 6.1 correct. Q3: Diffusion of responsibility indicator → 6.3 correct.

Exercise Rubric: Groupthink identification (3 pts), consensus pressure analysis (2 pts), vulnerability scoring with justification (3 pts), dissent mechanism design (2 pts). Total 10 pts (7+ pass).

2.10 Module 10: Domain [7.x] Stress Response Vulnerabilities

2.10.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Explain stress physiology impact on security; identify 10 stress response indicators; recognize stress exploitation attacks; design stress resilience interventions.

Key Concepts: Acute vs chronic stress, fight/flight/freeze/fawn responses, cortisol impairment, stress contagion, burnout.

2.10.2 Content Outline

1. Psychological Foundation (20 min): Selye stress physiology, HPA axis activation, cortisol effects on cognition/memory, acute vs chronic stress, four F responses (fight/flight/freeze/fawn), stress contagion mechanisms.

2. Ten Stress Indicators (30 min): Overview table 7.1-7.10, Deep-dive 7.1 (acute stress impairment, incident response degradation, scoring), Deep-dive 7.2 (chronic stress burnout, SOC analyst exhaustion, scoring), stress patterns.

3. Attack Vectors and Incidents (30 min): Stress induction attacks (create chaos then exploit), burnout exploitation windows, incident response under acute stress, stress contagion during breaches, healthcare ransomware stress cases.

4. Assessment and Solutions (30 min): Stress vulnerability observables, scoring criteria, Top 3 solutions (stress inoculation training, burnout prevention programs, incident stress management), implementation.

5. Exercise (10 min): Incident response scenario under simulated stress, assess stress vulnerabilities, design resilience protocols.

2.10.3 Teaching Methods

Lecture: Stress physiology diagrams, cortisol effects, four F response explanations.

Exercise: Incident response with time pressure and incomplete information, experience stress impairment.

Discussion: "Stress level during last incident?", "Burnout in your security team?"

2.10.4 Slide Breakdown

Slide 10.1: "Stress and Security Performance" - Selye stress physiology, HPA axis diagram, cortisol cognitive effects, acute vs chronic comparison, four F responses.

Slide 10.2: "10 Stress Response Indicators" - Table 7.1-7.10, highlight 7.1 and 7.2, stress vulnerability patterns.

Slide 10.3: "Stress Exploitation Attacks" - Stress induction techniques, burnout exploitation timing, IR under acute stress, stress contagion effects, healthcare ransomware cases.

Slide 10.4: "Assessment and Solutions" - Stress observables (incident performance, team exhaustion), scoring decision tree, top 3 solutions (inoculation training, burnout prevention, stress management), exercise prompt IR scenario.

2.10.5 Materials Needed

Field Kit 7.1 and 7.2, Taxonomy [7.x], stressful IR exercise scenario, stress physiology diagrams.

2.10.6 Assessment Items

Quiz: Q1: Four F responses → fight/flight/freeze/fawn correct. Q2: Acute stress indicator → 7.1 correct. Q3: Chronic stress/burnout indicator → 7.2 correct.

Exercise Rubric: Stress vulnerability identification (3 pts), stress impairment analysis (2 pts), vulnerability scoring with justification (3 pts), resilience protocol design (2 pts). Total 10 pts (7+ pass).

2.11 Module 11: Domain [8.x] Unconscious Process Vulnerabilities

2.11.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Apply psychoanalytic concepts to security; identify 10 unconscious indicators; recognize unconscious exploitation; design shadow-aware interventions.

Key Concepts: Shadow projection, unconscious identification, transference, countertransference, defense mechanisms, archetypes.

2.11.2 Content Outline

1. Psychological Foundation (20 min): Psychoanalytic unconscious review (from Module 2), Jung shadow, Klein projection, transference/countertransference, defense mechanisms in security, archetypal patterns.

2. Ten Unconscious Indicators (30 min): Overview table 8.1-8.10, Deep-dive 8.1 (shadow projection onto attackers, external attribution, scoring), Deep-dive 8.4 (transference to authority figures, security leader idealization, scoring), unconscious patterns.

3. Attack Vectors and Incidents (30 min): Symbolic attacks exploiting unconscious, transference manipulation, archetypal activation (hero/trickster), defense mechanism exploitation, unconscious identification with attackers.

4. Assessment and Solutions (30 min): Unconscious vulnerability observables, scoring criteria, Top 3 solutions (shadow work facilitation, transference awareness training, defense mechanism recognition), implementation.

5. Exercise (10 min): Organizational breach post-mortem with external blame, identify unconscious defenses, design shadow integration.

2.11.3 Teaching Methods

Lecture: Unconscious mechanisms review, shadow examples, transference in organizations.

Exercise: Breach post-mortem analysis for projection and shadow.

Discussion: "What does org refuse to acknowledge?", "Idealization of security leaders?"

2.11.4 Slide Breakdown

Slide 11.1: "The Unconscious in Security" - Psychoanalytic unconscious concept, shadow projection mechanism, transference/countertransference, defense mechanisms, archetypes.

Slide 11.2: "10 Unconscious Process Indicators" - Table 8.1-8.10, highlight 8.1 and 8.4, unconscious vulnerability patterns.

Slide 11.3: "Unconscious Exploitation" - Symbolic attack examples, transference manipulation, archetypal activation (hero/trickster exploitation), defense mechanism use, identification with attackers.

Slide 11.4: "Assessment and Solutions" - Unconscious observables (external blame patterns, idealization), scoring decision tree, top 3 solutions (shadow work, transference awareness, defense recognition), exercise prompt breach post-mortem.

2.11.5 Materials Needed

Field Kit 8.1 and 8.4, Taxonomy [8.x], breach post-mortem exercise with external blame narrative.

2.11.6 Assessment Items

Quiz: Q1: Shadow projection definition → disowned aspects projected onto others correct. Q2: Shadow projection indicator → 8.1 correct. Q3: Transference indicator → 8.4 correct.

Exercise Rubric: Unconscious defense identification (3 pts), projection/shadow analysis (2 pts), vulnerability scoring with justification (3 pts), shadow integration design (2 pts). Total 10 pts (7+ pass).

2.12 Module 12: Domain [9.x] AI-Specific Bias Vulnerabilities

2.12.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Explain AI-human interaction psychology; identify 10 AI bias indicators; recognize AI vulnerability exploitation; design AI-aware security controls.

Key Concepts: Anthropomorphization, automation bias, algorithm aversion, AI authority transfer, uncanny valley, hallucination acceptance.

2.12.2 Content Outline

1. Psychological Foundation (20 min): Human-AI interaction psychology, anthropomorphization tendency, automation bias (over-reliance), algorithm aversion (under-trust), AI authority transfer, uncanny valley effects, emerging AI psychology research.

2. Ten AI Indicators (30 min): Overview table 9.1-9.10, Deep-dive 9.1 (anthropomorphization of AI systems, emotional attachment, scoring), Deep-dive 9.2 (automation bias override, uncritical AI acceptance, scoring), AI vulnerability patterns.

3. Attack Vectors and Incidents (30 min): AI social engineering (chatbot manipulation), deepfake exploitation (voice/video), AI recommendation poisoning, automation bias attacks (malicious ML), hallucination exploitation, adversarial ML cases.

4. Assessment and Solutions (30 min): AI vulnerability observables, scoring criteria, Top 3 solutions (AI literacy training, human-in-loop requirements, AI output verification protocols), implementation.

5. Exercise (10 min): AI-generated phishing scenario with chatbot pretext, assess AI-specific vulnerabilities, design verification controls.

2.12.3 Teaching Methods

Lecture: AI psychology research, anthropomorphization demonstrations, automation bias examples.

Exercise: AI chatbot phishing scenario, experience anthropomorphization pressure.

Discussion: "Trust AI security tools how much?", "Experienced AI hallucinations?"

2.12.4 Slide Breakdown

Slide 12.1: "AI-Human Interaction Psychology" - Anthropomorphization tendency, automation bias vs algorithm aversion, AI authority transfer, uncanny valley, emerging research.

Slide 12.2: "10 AI-Specific Bias Indicators" - Table 9.1-9.10, highlight 9.1 and 9.2, AI vulnerability patterns.

Slide 12.3: "AI Exploitation Attacks" - AI social engineering (chatbot), deepfakes (voice/video examples), recommendation poisoning, automation bias attacks, hallucination exploitation, adversarial ML cases.

Slide 12.4: "Assessment and Solutions" - AI observables (AI tool trust levels, verification practices), scoring decision tree, top 3 solutions (AI literacy, human-in-loop, verification protocols), exercise prompt chatbot phishing.

2.12.5 Materials Needed

Field Kit 9.1 and 9.2, Taxonomy [9.x], AI chatbot phishing exercise, deepfake video examples (3 min).

2.12.6 Assessment Items

Quiz: Q1: Anthropomorphization definition → attributing human intentions to AI correct. Q2: Automation bias indicator → 9.2 correct. Q3: AI authority transfer indicator → 9.4 correct.

Exercise Rubric: AI vulnerability identification (3 pts), anthropomorphization analysis (2 pts), vulnerability scoring with justification (3 pts), verification control design (2 pts). Total 10 pts (7+ pass).

2.13 Module 13: Domain [10.x] Critical Convergent States

2.13.1 Overview

Duration: 2 hours — **Slides:** 4

Learning Objectives: Explain vulnerability convergence concept; identify 10 convergent state indicators; recognize perfect storm conditions; design convergence monitoring systems.

Key Concepts: Perfect storm, cascade failures, tipping points, Swiss cheese alignment, black swans, gray rhinos, complexity catastrophe.

2.13.2 Content Outline

1. Psychological Foundation (20 min): System theory emergence, Reason Swiss cheese model, Perrow normal accidents, convergence mathematics (multiplication not addition), tipping point dynamics, complexity theory in security.

2. Ten Convergent Indicators (30 min): Overview table 10.1-10.10, Deep-dive 10.1 (perfect storm conditions, multiple vulnerability alignment, scoring), Deep-dive 10.4 (Swiss cheese alignment, hole alignment critical, scoring), convergence patterns.

3. Attack Vectors and Incidents (30 min): APT perfect storms (multiple vulnerabilities exploited), cascade failure attacks, tipping point breaches, Swiss cheese exploitation, SolarWinds as convergence case, black swan vs gray rhino events.

4. Assessment and Solutions (30 min): Convergent state observables, scoring criteria (exponential not linear), Top 3 solutions (convergence monitoring dashboards, vulnerability correlation analysis, early warning systems), implementation.

5. Exercise (10 min): Multi-domain vulnerability scenario, calculate convergence risk, design monitoring for perfect storm detection.

2.13.3 Teaching Methods

Lecture: Swiss cheese model visual, convergence mathematics demonstration, SolarWinds timeline.

Exercise: Multi-vulnerability scenario, calculate exponential risk.

Discussion: "Experienced perfect storm breach?", "How monitor convergence in your org?"

2.13.4 Slide Breakdown

Slide 13.1: "Vulnerability Convergence" - System emergence concept, Reason Swiss cheese visual, convergence mathematics (multiplication), tipping point dynamics, complexity catastro-

phe.

Slide 13.2: "10 Critical Convergent Indicators" - Table 10.1-10.10, highlight 10.1 and 10.4, convergence vulnerability patterns.

Slide 13.3: "Convergent State Attacks" - APT perfect storms, cascade failures, tipping point breaches, Swiss cheese hole alignment, SolarWinds convergence timeline, black swan vs gray rhino.

Slide 13.4: "Assessment and Solutions" - Convergent observables (multiple simultaneous vulnerabilities), exponential scoring approach, top 3 solutions (monitoring dashboards, correlation analysis, early warning), exercise prompt multi-domain scenario.

2.13.5 Materials Needed

Field Kit 10.1 and 10.4, Taxonomy [10.x], Swiss cheese model visual, multi-vulnerability exercise, SolarWinds case study.

2.13.6 Assessment Items

Quiz: Q1: Convergence risk calculation → multiplication not addition correct. Q2: Perfect storm indicator → 10.1 correct. Q3: Swiss cheese alignment indicator → 10.4 correct.

Exercise Rubric: Multi-vulnerability identification (3 pts), convergence calculation (2 pts), exponential risk scoring (3 pts), monitoring system design (2 pts). Total 10 pts (7+ pass).

2.14 Module 14: Privacy and Ethics

2.14.1 Overview

Duration: 4 hours — **Slides:** 8

Learning Objectives: Articulate privacy-preserving assessment principles; apply differential privacy mathematics; implement minimum aggregation requirements; design temporal delay mechanisms; explain ethical boundaries in psychological assessment.

Key Concepts: Differential privacy, aggregation units, temporal delays, prohibition on individual profiling, ethical assessment, data handling.

2.14.2 Content Outline

1. Privacy-Preserving Principles (60 min): Why privacy matters in psychological assessment, aggregation-only principle (never individual), minimum aggregation unit (10 individuals), differential privacy concept (epsilon = 0.1), temporal delay requirement (72 hours minimum), role-based not individual analysis, prohibition on performance evaluation use.

2. Differential Privacy Mathematics (45 min): Epsilon privacy budget concept, noise injection mechanisms, privacy-utility tradeoff, CPF epsilon = 0.1 rationale, practical implementation examples, verification methods.

3. Data Handling Requirements (45 min): Encryption at rest (AES-256) and in transit (TLS 1.3), access controls and audit trails, retention limits (5 years maximum), secure destruction procedures, cross-border data transfer considerations, GDPR/CCPA compliance mapping.

4. Ethical Boundaries (45 min): CPF is organizational not clinical assessment, no individual diagnosis or therapy, psychological vulnerabilities are normal human characteristics not failures, prohibition on stigmatization or blame, informed consent requirements, opt-out mechanisms while maintaining statistical validity, whistleblower protections.

5. Case Studies: Privacy Violations (30 min): Historical psychological profiling abuses, Cambridge Analytica lessons, employee surveillance concerns, three violation scenarios analysis, discussion of ethical boundaries.

6. Exercise: Privacy Impact Assessment (15 min): Design assessment for 50-person department, ensure aggregation units, calculate differential privacy parameters, implement temporal delays, verify no individual profiling possible.

2.14.3 Teaching Methods

Lecture: Privacy principles with violation examples, differential privacy mathematics with visualizations, ethical framework with case comparisons.

Exercises: (1) Aggregation unit calculation for various org sizes (15 min), (2) Differential privacy parameter selection (15 min), (3) Privacy impact assessment design (15 min).

Discussion: "Tension between assessment and privacy?", "How ensure no individual profiling?", "Ethical concerns with psychological assessment?"

Case Studies: Three privacy violation scenarios, group analysis of what went wrong, design safeguards.

2.14.4 Slide Breakdown

Slide 14.1: "Privacy-First Assessment Principles" - Why privacy matters, aggregation-only principle, minimum 10 individuals, differential privacy epsilon, 72-hour temporal delay, role-based analysis, no performance evaluation use.

Slide 14.2: "Differential Privacy Explained" - Epsilon privacy budget concept, noise injection visual, privacy-utility tradeoff graph, CPF epsilon = 0.1 rationale, implementation example.

Slide 14.3: "Minimum Aggregation Units" - 10-individual requirement, calculation for different org sizes, small organization challenges, aggregation unit examples (departments, roles, locations).

Slide 14.4: "Temporal Delay Mechanisms" - 72-hour minimum rationale, delayed reporting workflow diagram, prevents real-time surveillance, balances timeliness with privacy.

Slide 14.5: "Data Handling Requirements" - Encryption (AES-256, TLS 1.3), access controls and audit, retention limits 5 years, secure destruction, cross-border considerations, GDPR/CCPA mapping.

Slide 14.6: "Ethical Boundaries" - Organizational not clinical assessment, no individual diagnosis, vulnerabilities are normal, prohibition on stigma/blame, informed consent, opt-out mechanisms, whistleblower protections.

Slide 14.7: "Privacy Violation Case Studies" - Cambridge Analytica lessons, employee surveillance concerns, three scenario examples (what went wrong, safeguards needed), discussion prompts.

Slide 14.8: "Privacy Impact Assessment Exercise" - 50-person department scenario, aggregation unit calculation, differential privacy parameters, temporal delay implementation, verification no individual profiling, group exercise instructions.

2.14.5 Materials Needed

Workbook Module 14 (pages 61-75), differential privacy calculator tool, aggregation unit worksheet, three privacy violation case studies (2 pages each), privacy impact assessment template, GDPR/CCPA compliance checklist.

2.14.6 Assessment Items

Quiz (5 questions): Q1: Minimum aggregation unit → 10 individuals correct. Q2: CPF differential privacy epsilon → 0.1 correct. Q3: Temporal delay minimum → 72 hours correct. Q4: Data retention maximum → 5 years correct. Q5: CPF assessment type → organizational not clinical correct.

Exercise Rubric (Privacy Impact Assessment): Correct aggregation unit calculation (2 pts), appropriate differential privacy parameters (2 pts), temporal delay implementation (2 pts), verification no profiling possible (2 pts), complete data handling plan (2 pts). Total 10 pts (7+ pass).

2.15 Module 15: Integration and Application

2.15.1 Overview

Duration: 4 hours — **Slides:** 7

Learning Objectives: Map CPF to ISO 27001:2022 clauses; integrate CPF with NIST CSF 2.0 functions; design organizational implementation strategies; overcome common challenges; apply framework to capstone assessment.

Key Concepts: ISO 27001 integration, NIST CSF mapping, implementation strategy, change management, common challenges, maturity progression.

2.15.2 Content Outline

1. CPF and ISO 27001:2022 Integration (60 min): CPF-27001:2025 standard overview, mapping to ISO clauses (4.1 context, 6.1 risk assessment, 7.2 competence, 7.3 awareness, 8.2 operational planning, 9.1 monitoring, 10.1 improvement), Annex A control enhancement, PVMS as parallel to ISMS, documentation requirements, audit considerations.

2. CPF and NIST CSF 2.0 Integration (45 min): NIST functions mapping (Identify: CPF assessment identifies human risks, Protect: psychological controls complement technical, Detect: behavioral indicators enable detection, Respond: psychological first aid during incidents, Recover: address psychological trauma post-breach), subcategories enhancement examples, CPF as human-factor intelligence layer.

3. Implementation Strategies (60 min): Phased approach (assessment, pilot, rollout, continuous), stakeholder engagement (executive buy-in, middle management, staff participation), change management considerations, resource planning (personnel, technology, budget), training requirements, communication planning, quick wins identification.

4. Common Challenges and Solutions (30 min): Challenge: "This feels invasive" - Solution: Emphasize privacy protections and aggregation, Challenge: "Too psychological for security team" - Solution: Focus on observables not therapy, Challenge: "We don't have psychologists" - Solution: CPF training creates competence, Challenge: "ROI unclear" - Solution: Incident

reduction metrics, Challenge: "Integration complexity" - Solution: Start small pilot, Challenge: "Resistance to change" - Solution: Demonstrate value through pilot.

5. Maturity Progression (30 min): Level 1 Foundation (CPF Score 100-149), Level 2 Intermediate (70-99), Level 3 Advanced (40-69), Level 4 Exemplary (0-39), progression pathways, capability building over time.

6. Capstone Exercise: Complete Mini-Assessment (45 min): Realistic organizational scenario with multiple indicators across domains, students conduct abbreviated assessment using Quick Reference Card, apply ternary scoring, calculate category and CPF scores, identify convergent states, recommend top 5 interventions, present findings to group.

2.15.3 Teaching Methods

Lecture: ISO/NIST frameworks with CPF overlay diagrams, implementation roadmap visualization, maturity level progression charts.

Exercises: (1) ISO clause mapping exercise - assign CPF domains to ISO clauses (20 min), (2) NIST function enhancement - design CPF integration for one function (20 min), (3) Implementation planning - create 90-day pilot plan (20 min), (4) Capstone mini-assessment (45 min).

Discussion: "Biggest implementation challenge anticipated?", "How gain executive buy-in?", "Integration with existing security program?"

Case Study: Healthcare organization CPF implementation journey (pilot to Level 2 in 18 months), lessons learned, success factors.

2.15.4 Slide Breakdown

Slide 15.1: "CPF and ISO 27001:2022" - CPF-27001:2025 overview, clause mapping table (4.1, 6.1, 7.2, 7.3, 8.2, 9.1, 10.1), Annex A enhancement examples, PVMS parallel to ISMS.

Slide 15.2: "CPF and NIST CSF 2.0" - Five functions with CPF integration points (Identify human risks, Protect with psychological controls, Detect via behavioral indicators, Respond with psychological first aid, Recover addressing trauma), subcategory enhancement examples, human-factor intelligence layer visual.

Slide 15.3: "Implementation Strategy" - Phased approach diagram (assessment, pilot, rollout, continuous), stakeholder engagement pyramid, change management considerations, resource planning checklist, quick wins identification.

Slide 15.4: "Common Challenges and Solutions" - Six challenge-solution pairs table (feels invasive/privacy protections, too psychological/observables focus, no psychologists/training creates competence, ROI unclear/incident metrics, integration complex/start small, resistance/demonstrate value).

Slide 15.5: "Maturity Progression" - Four levels visual (Foundation 100-149, Intermediate 70-99, Advanced 40-69, Exemplary 0-39), characteristics of each level, progression pathways, capability building timeline.

Slide 15.6: "Case Study: Healthcare Implementation" - Organization background, implementation timeline (pilot to Level 2 in 18 months), challenges encountered and solutions, key success factors, lessons learned, measurable outcomes.

Slide 15.7: "Capstone Exercise: Mini-Assessment" - Organizational scenario description (multi-domain vulnerabilities), assessment task instructions (identify indicators, apply scoring, calcu-

late scores, find convergence, recommend interventions), presentation format, evaluation criteria.

2.15.5 Materials Needed

Workbook Module 15 (pages 76-90), ISO 27001:2022 standard (reference), NIST CSF 2.0 document (reference), CPF-27001:2025 requirements document, Quick Reference Card for capstone, capstone scenario packet (5 pages), implementation planning template, healthcare case study handout (3 pages).

2.15.6 Assessment Items

Quiz (5 questions): Q1: ISO clause CPF primarily addresses → 7.2 Competence and 7.3 Awareness correct. Q2: NIST Identify function CPF contribution → human risk identification correct. Q3: CPF Level 2 score range → 70-99 correct. Q4: First implementation phase → assessment correct. Q5: CPF-27001 standard type → organizational PVMS requirements correct.

Capstone Rubric: Indicator identification across domains (3 pts), accurate ternary scoring with justification (3 pts), correct category and CPF score calculation (2 pts), convergent state recognition (1 pt), appropriate intervention recommendations (1 pt). Total 10 pts (7+ pass).

Course Completion Rubric: All 15 module quizzes passed (15 pts), active participation in exercises (10 pts), capstone mini-assessment passed (10 pts), ethics agreement signed (5 pts). Total 40 pts (28+ pass for course completion, separate written exam required for certification).

3 Appendices

3.1 Appendix A: Complete Slide Inventory

Module	Slide	Title	Type	Duration
Module 1	1.1	The Human Factor Crisis	Lecture	10 min
Module 1	1.2	Pre-Cognitive Decision-Making	Lecture	15 min
Module 1	1.3	CPF Framework Architecture	Lecture	15 min
Module 1	1.4	Ternary Scoring System	Lecture	15 min
Module 1	1.5	Integration with ISO 27001 and NIST CSF	Lecture	15 min
Module 1	1.6	Target Breach Through CPF Lens	Case Study	30 min
Module 2	2.1	Bion's Basic Assumptions Overview	Lecture	15 min
Module 2	2.2	Basic Assumptions in Security	Lecture	20 min
Module 2	2.3	Kleinian Splitting and Projection	Lecture	20 min
Module 2	2.4	Jung's Shadow in Security	Lecture	15 min
Module 2	2.5	Archetypes in Security	Lecture	15 min
Module 2	2.6	Winnicott's Transitional Space	Lecture	10 min
Module 2	2.7	Psychoanalytic Case Analysis Exercise	Exercise	15 min
Module 3	3.1	Thinking Fast and Slow	Lecture	20 min
Module 3	3.2	Heuristics and Biases	Lecture	15 min
Module 3	3.3	Cialdini's Six Principles Overview	Lecture	15 min
Module 3	3.4	Six Principles in Social Engineering	Lecture	20 min
Module 3	3.5	Cognitive Load Theory	Lecture	15 min
Module 3	3.6	Decision-Making Under Uncertainty	Lecture	10 min
Module 3	3.7	Cognitive Exploitation Exercise	Exercise	15 min
Module 4	4.1	Why We Obey: Authority Vulnerability	Lecture	20 min
Module 4	4.2	10 Authority Indicators	Lecture	30 min
Module 4	4.3	Attack Vectors in Action	Lecture	30 min
Module 4	4.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 5	5.1	Time Pressure and Security	Lecture	20 min
Module 5	5.2	10 Temporal Indicators	Lecture	30 min
Module 5	5.3	Temporal Attack Vectors	Lecture	30 min
Module 5	5.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 6	6.1	Social Influence Mechanisms	Lecture	20 min
Module 6	6.2	10 Social Influence Indicators	Lecture	30 min
Module 6	6.3	Social Engineering Attack Patterns	Lecture	30 min
Module 6	6.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 7	7.1	Emotion and Security Decisions	Lecture	20 min
Module 7	7.2	10 Affective Indicators	Lecture	30 min
Module 7	7.3	Emotional Manipulation Attacks	Lecture	30 min
Module 7	7.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 8	8.1	Cognitive Load and Capacity Limits	Lecture	20 min
Module 8	8.2	10 Cognitive Overload Indicators	Lecture	30 min
Module 8	8.3	Cognitive Exploitation Attacks	Lecture	30 min
Module 8	8.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 9	9.1	Group Psychology in Security	Lecture	20 min
Module 9	9.2	10 Group Dynamic Indicators	Lecture	30 min
Module 9	9.3	Group-Level Attack Vectors	Lecture	30 min
Module 9	9.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 10	10.1	Stress and Security Performance	Lecture	20 min

Module	Slide	Title	Type	Duration
Module 10	10.2	10 Stress Response Indicators	Lecture	30 min
Module 10	10.3	Stress Exploitation Attacks	Lecture	30 min
Module 10	10.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 11	11.1	The Unconscious in Security	Lecture	20 min
Module 11	11.2	10 Unconscious Process Indicators	Lecture	30 min
Module 11	11.3	Unconscious Exploitation	Lecture	30 min
Module 11	11.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 12	12.1	AI-Human Interaction Psychology	Lecture	20 min
Module 12	12.2	10 AI-Specific Bias Indicators	Lecture	30 min
Module 12	12.3	AI Exploitation Attacks	Lecture	30 min
Module 12	12.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 13	13.1	Vulnerability Convergence	Lecture	20 min
Module 13	13.2	10 Critical Convergent Indicators	Lecture	30 min
Module 13	13.3	Convergent State Attacks	Lecture	30 min
Module 13	13.4	Assessment and Solutions	Lecture/Exercise	40 min
Module 14	14.1	Privacy-First Assessment Principles	Lecture	20 min
Module 14	14.2	Differential Privacy Explained	Lecture	15 min
Module 14	14.3	Minimum Aggregation Units	Lecture	15 min
Module 14	14.4	Temporal Delay Mechanisms	Lecture	10 min
Module 14	14.5	Data Handling Requirements	Lecture	15 min
Module 14	14.6	Ethical Boundaries	Lecture	15 min
Module 14	14.7	Privacy Violation Case Studies	Case Study	20 min
Module 14	14.8	Privacy Impact Assessment Exercise	Exercise	30 min
Module 15	15.1	CPF and ISO 27001:2022	Lecture	30 min
Module 15	15.2	CPF and NIST CSF 2.0	Lecture	30 min
Module 15	15.3	Implementation Strategy	Lecture	30 min
Module 15	15.4	Common Challenges and Solutions	Lecture	15 min
Module 15	15.5	Maturity Progression	Lecture	15 min
Module 15	15.6	Case Study: Healthcare Implementation	Case Study	20 min
Module 15	15.7	Capstone Exercise: Mini-Assessment	Exercise	45 min
Total: 80 slides, 40 hours				

3.2 Appendix B: Exercise Bank Summary

Module 1 Exercises:

- 1.1 Awareness Failure Analysis (15 min): Share failed training examples, identify why conscious interventions didn't work
- 1.2 Pre-Cognitive Decision Experiment (10 min): Live demonstration authority/urgency scenarios, reflect on rapid decisions
- 1.3 Framework Navigation (20 min): Speed drill with Quick Reference Card, locate indicators across domains

Module 2 Exercises:

- 2.1 Basic Assumption Identification (20 min): Three vignettes, identify baD/baF/baP and vulnerabilities
- 2.2 Splitting in Security Culture (15 min): List trusted/threatening entities, discuss blind spots from idealization/demonization

- 2.3 Shadow Recognition (15 min): Anonymous reflection "what org refuses to acknowledge"
- 2.4 Psychoanalytic Case Analysis (15 min): Healthcare ransomware, identify basic assumption, splitting, projections

Module 3 Exercises:

- 3.1 System 1 vs 2 Speed Test (15 min): 20 emails 3 sec each then unlimited time, compare accuracy rates
- 3.2 Cialdini Principle Mapping (20 min): Six scenarios, map influence principles, discuss combinations
- 3.3 Cognitive Load Simulation (15 min): Security task with distractions, experience overload degradation
- 3.4 Cognitive Exploitation Analysis (15 min): Three phishing emails, identify principles/System/load manipulation

Modules 4-13 Domain Exercises (10 min each): Each domain includes scenario-based exercise applying ternary scoring to realistic case with discussion.

Module 14 Exercises:

- 14.1 Aggregation Unit Calculation (15 min): Calculate for various org sizes, ensure privacy requirements
- 14.2 Differential Privacy Parameters (15 min): Select appropriate epsilon, understand privacy-utility tradeoff
- 14.3 Privacy Impact Assessment (30 min): Design assessment for 50-person department, verify no profiling

Module 15 Exercises:

- 15.1 ISO Clause Mapping (20 min): Assign CPF domains to ISO 27001 clauses
- 15.2 NIST Function Enhancement (20 min): Design CPF integration for one NIST function
- 15.3 Implementation Planning (20 min): Create 90-day pilot plan with stakeholders/resources
- 15.4 Capstone Mini-Assessment (45 min): Complete abbreviated assessment with scoring and recommendations

Total: 25 exercises across 40 hours

3.3 Appendix C: Examination Blueprint

CPF-101 Written Examination Structure:

Format: 100 questions, 3 hours, closed-book, computer-based

Question Types:

- 60 Multiple-Choice: Single correct answer from 4 options

- 30 Scenario-Based: Short scenario with question requiring analysis
- 10 Case Analysis: Extended case study with complex multi-step questions

Content Distribution by Module:

Module	Questions	Focus Areas
Module 1	8	Pre-cognitive processes, framework architecture, integration
Module 2	8	Bion, Klein, Jung, Winnicott concepts in security
Module 3	8	Kahneman, Cialdini, Miller, cognitive biases
Modules 4-13	50	5 questions per domain, ternary scoring, attack vectors, solutions
Module 14	12	Privacy requirements, differential privacy, ethics
Module 15	14	ISO/NIST integration, implementation, capstone scenarios
Total	**100**	

Cognitive Level Distribution (Bloom's Taxonomy):

- Knowledge/Recall: 20% (20 questions) - Facts, definitions, terminology
- Comprehension/Application: 40% (40 questions) - Explain concepts, apply to scenarios
- Analysis/Synthesis: 40% (40 questions) - Analyze complex situations, integrate multiple concepts

Passing Standard: 70% (70 correct responses)

Question Development Process:

- Psychometric validation with pilot groups
- Item difficulty distribution: 30% easy, 50% moderate, 20% difficult
- Regular statistical analysis (discrimination index, difficulty index)
- Continuous improvement based on performance data

Retake Policy:

- First retake: 30-day waiting period, 50% fee
- Second retake: 30-day waiting period, 50% fee
- After three failures: Additional training required, 6-month waiting period

3.4 Appendix D: Reference Materials

CPF Framework Documents:

- The Cybersecurity Psychology Framework: Complete taxonomy paper with all 100 indicators

- CPF-27001:2025 Requirements: Organizational PVMS standard
- CPF Certification Scheme: Professional certification pathways and requirements
- Field Kit Example: Indicator 1.1 complete (foundation, operational, field kit)

Foundational Research Papers:

- Milgram, S. (1974). Obedience to Authority
- Bion, W. R. (1961). Experiences in Groups
- Klein, M. (1946). Notes on some schizoid mechanisms
- Jung, C. G. (1969). The Archetypes and the Collective Unconscious
- Winnicott, D. W. (1971). Playing and Reality
- Kahneman, D. (2011). Thinking, Fast and Slow
- Kahneman, D. & Tversky, A. (1979). Prospect Theory
- Cialdini, R. B. (2007). Influence: The Psychology of Persuasion
- Miller, G. A. (1956). The Magical Number Seven, Plus or Minus Two

Security Framework Standards:

- ISO/IEC 27001:2022 Information Security Management Systems
- ISO/IEC 27002:2022 Code of Practice for Information Security Controls
- NIST Cybersecurity Framework 2.0
- ISO 19011:2018 Guidelines for Auditing Management Systems (for Auditor track)

Privacy and Ethics References:

- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- Differential Privacy: A Survey of Results (Dwork, 2008)
- APA Ethical Principles of Psychologists and Code of Conduct

Field Kits Referenced (by module):

- Module 4: Field Kit 1.1 (Unquestioning compliance), 1.3 (Impersonation susceptibility)
- Module 5: Field Kit 2.1 (Urgency bypass), 2.3 (Deadline risk acceptance)
- Module 6: Field Kit 3.1 (Reciprocity exploitation), 3.3 (Social proof manipulation)
- Module 7: Field Kit 4.1 (Fear paralysis), 4.5 (Shame hiding)
- Module 8: Field Kit 5.1 (Alert fatigue), 5.2 (Decision fatigue)
- Module 9: Field Kit 6.1 (Groupthink), 6.3 (Diffusion of responsibility)

- Module 10: Field Kit 7.1 (Acute stress), 7.2 (Chronic burnout)
- Module 11: Field Kit 8.1 (Shadow projection), 8.4 (Transference)
- Module 12: Field Kit 9.1 (Anthropomorphization), 9.2 (Automation bias)
- Module 13: Field Kit 10.1 (Perfect storm), 10.4 (Swiss cheese alignment)

Note: All 100 Field Kits available as separate reference library for certified assessors.

Document Control

Version History:

Version	Date	Changes
1.0	January 2025	Initial release

Review Schedule: Annual review following each course delivery, major revision based on examination statistics, participant feedback, and framework updates.

Approval:

Document Owner: CPF3 Training Development

Approved by: Giuseppe Canale, CISSP

Date: January 2025

Usage Instructions:

This blueprint enables modular slide generation using the following 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 structure: "Generate slide content for [Module X, Slide Y] based on CPF-101-Training-Blueprint.tex Section 2.X. Include [specified materials]. Output format: [title, bullets, notes, visual suggestions]."
4. Reference appropriate Field Kits and Taxonomy sections as specified in Materials Needed
5. Implement exercises from Appendix B with provided rubrics
6. Develop assessment items following Appendix C blueprint

Contact Information:

CPF3 Training Development

Website: https://cpf3.org

Email: training@cpf3.org

End of CPF-101 Training Blueprint