

---

# Bridging the Human Factor Gap in SOC 2 Compliance: Integrating the Cybersecurity Psychology Framework with AICPA Trust Services Criteria

---

A SOC 2 COMPLIANCE ENHANCEMENT FRAMEWORK

Giuseppe Canale, CISSP

Independent Cybersecurity Researcher

[g.canale@cpf3.org](mailto:g.canale@cpf3.org)

URL: [cpf3.org](http://cpf3.org)

ORCID: [0009-0007-3263-6897](https://orcid.org/0009-0007-3263-6897)

February 21, 2026

## Abstract

The AICPA's Service Organization Control 2 (SOC 2) framework, built upon the Trust Services Criteria (TSC), has become the de facto standard for demonstrating security posture among technology and cloud service providers. Yet while the nine Common Criteria (CC1–CC9) address governance, risk assessment, access controls, and operational integrity, they remain fundamentally oriented toward procedural and technical controls. The human factor—responsible for 68–85% of security breaches according to industry reports—is implicitly referenced across multiple criteria but lacks a systematic assessment methodology. This paper presents a detailed integration framework mapping the Cybersecurity Psychology Framework (CPF)<sup>[1]</sup> to each of the five SOC 2 Trust Services Categories and the nine Common Criteria, providing SOC 2 practitioners, auditors, and CISOs with an actionable approach to strengthening the psychological dimension of their compliance programs. Through category-by-category mapping tables and implementation guidance, we demonstrate how CPF-enhanced controls can materially improve the effectiveness of SOC 2 programs while delivering measurable reductions in human-factor incidents. The framework is designed for immediate adoption by service organizations preparing for SOC 2 Type I or Type II examinations.

**Keywords:** SOC 2, Trust Services Criteria, Common Criteria, AICPA, psychological risk assessment, human factors, cybersecurity compliance, control environment, service organizations

## 1 Executive Summary

SOC 2 has emerged as the predominant assurance framework for service organizations that store, process, or transmit customer data. Developed by the AICPA’s Assurance Services Executive Committee (ASEC), the framework evaluates controls against five Trust Services Categories—Security, Availability, Processing Integrity, Confidentiality, and Privacy—with Security (the Common Criteria, CC1–CC9) required for every examination.

The 2017 Trust Services Criteria (with revised Points of Focus, 2022) provide over 200 points of focus within the Security category alone, addressing governance, communication, risk assessment, monitoring, control activities, access controls, system operations, change management, and risk mitigation. These criteria map to the Committee of Sponsoring Organizations (COSO) internal control framework, grounding SOC 2 in established principles of organizational governance.

However, a critical analysis of the Common Criteria reveals a systematic gap: while criteria such as CC1 (Control Environment) reference organizational integrity and CC3 (Risk Assessment) mandate threat identification, neither the criteria nor their associated points of focus provide methodologies for assessing the *psychological* vulnerabilities that underlie the majority of security incidents. The 2024 Verizon Data Breach Investigations Report confirms that 68% of breaches involve a human element<sup>[3]</sup>, while social engineering attacks continue to increase in sophistication and frequency.

The Cybersecurity Psychology Framework (CPF)<sup>[1]</sup> addresses this gap by providing a systematic, privacy-preserving approach to identifying pre-cognitive psychological vulnerabilities across ten categories, from authority-based susceptibilities to AI-specific biases. This paper provides SOC 2 practitioners with a practical integration framework that maps CPF assessments to each Common Criterion and Trust Services Category, enabling organizations to:

### Key Benefits for SOC 2 Programs:

- Strengthen CC1 Control Environment by quantifying psychological dimensions of organizational integrity
- Enhance CC3 Risk Assessment with human-factor threat identification methodologies
- Improve CC6 Logical and Physical Access Controls through social engineering resistance metrics
- Elevate CC7 System Operations with stress-aware incident response capabilities
- Provide auditors with measurable evidence of human-factor control effectiveness
- Differentiate SOC 2 reports through demonstrably comprehensive human risk management

## 2 SOC 2 and the Trust Services Criteria: An Overview

### 2.1 SOC 2 Framework Structure

SOC 2 is a reporting framework—not a certification—in which a CPA firm opines on the design and operating effectiveness of controls relevant to the Trust Services Criteria. Two report types exist:

- **Type I:** Evaluates control design and implementation at a specific point in time

- **Type II:** Evaluates control design and operating effectiveness over a period (typically 3–12 months)

The framework comprises five Trust Services Categories:

1. **Security (Common Criteria, CC1–CC9):** Required for all SOC 2 examinations. Ensures information and systems are protected against unauthorized access, disclosure, and damage.
2. **Availability (A1):** Optional. Ensures systems are available for operation and use as committed.
3. **Processing Integrity (PI1):** Optional. Ensures system processing is complete, valid, accurate, timely, and authorized.
4. **Confidentiality (C1):** Optional. Ensures confidential information is protected as committed.
5. **Privacy (P1):** Optional. Ensures personal information is collected, used, retained, disclosed, and disposed of in conformity with commitments.

## 2.2 The Nine Common Criteria

The Security category contains nine Common Criteria series (CC1–CC9), which form the backbone of every SOC 2 examination:

Table 1: SOC 2 Common Criteria Overview

Series	Category	Focus Area
CC1	Control Environment	Integrity, ethical values, governance, organizational structure, authority, accountability, HR policies
CC2	Communication & Information	Quality information generation, internal and external communication of policies and objectives
CC3	Risk Assessment	Objective specification, risk identification, fraud risk assessment, change impact analysis
CC4	Monitoring Activities	Ongoing evaluation of controls, communication of deficiencies
CC5	Control Activities	Design and implementation of controls, technology general controls, policy deployment
CC6	Logical & Physical Access	Authentication, access management, encryption, physical security
CC7	System Operations	Monitoring, anomaly detection, incident response, backup and recovery
CC8	Change Management	Authorization, testing, approval, and documentation of changes
CC9	Risk Mitigation	Business disruption mitigation, vendor risk management

## 2.3 COSO Foundation

The Common Criteria are mapped to the 17 principles of the COSO Internal Control—Integrated Framework (2013). This mapping is significant because COSO Principle 1 (“The organization demonstrates a commitment to integrity and ethical values”) and Principle 4 (“The organization demonstrates a commitment to attract, develop, and retain competent individuals”) explicitly reference human behavioral dimensions. CPF provides the operational methodology to assess these dimensions systematically.

## 2.4 The Human Factor Gap in SOC 2

Despite the COSO foundation’s attention to organizational behavior, a detailed examination of the Trust Services Criteria reveals persistent gaps in human factor assessment:

Table 2: Human Factor Gaps in SOC 2 Trust Services Criteria

Common Criterion	Crite-	What TSC Addresses	What TSC Misses
CC1: Control Environment	Governance structures, HR policies, ethical codes	Governance structures, HR policies, ethical codes	Unconscious group dynamics, authority bias patterns, psychological safety metrics
CC2: Communication	Policy communication, reporting channels	Policy communication, reporting channels	Cognitive barriers to information processing, psychological resistance to security messaging
CC3: Risk Assessment	Threat identification, fraud risk	Threat identification, fraud risk	Pre-cognitive vulnerability assessment, social engineering susceptibility profiling
CC6: Access Controls	Authentication, authorization, encryption	Authentication, authorization, encryption	Social engineering resistance, authority-based bypass susceptibility
CC7: System Operations	Monitoring, incident response	Monitoring, incident response	Decision quality under stress, alert fatigue psychology, cognitive load during incidents
CC9: Risk Mitigation	Business continuity, vendor management	Business continuity, vendor management	Psychological dependency on vendors, trust transference vulnerabilities

## 3 The Business Case for CPF-Enhanced SOC 2

### 3.1 The Economics of Human-Factor Breaches

Industry data underscores the financial impact of inadequate human-factor controls:

- The average cost of a data breach reached \$4.88 million globally in 2024, with breaches involving social engineering among the costliest[4]
- Organizations with comprehensive security awareness and training programs experienced 23% lower breach costs

- The mean time to identify and contain breaches involving human factors exceeds 250 days
- SaaS and technology companies—the primary SOC 2 audience—face disproportionate social engineering risk due to privileged access to customer data

### **3.2 Competitive Differentiation Through Comprehensive Human Risk Management**

SOC 2 reports are increasingly table stakes for technology vendors. In a market where most competitors hold clean SOC 2 Type II reports, differentiation comes from the *depth and quality* of controls. CPF-enhanced SOC 2 programs provide:

- Demonstrable sophistication in human risk management beyond standard awareness training
- Quantifiable metrics for control effectiveness in the human factor domain
- Evidence of proactive, predictive security posture rather than reactive compliance
- Enhanced trust with enterprise customers who evaluate vendor SOC 2 reports

### **3.3 Auditor Perspective**

SOC 2 auditors evaluate whether controls are suitably designed and, for Type II, operating effectively. CPF integration provides:

- Additional points of focus that demonstrate comprehensive risk coverage
- Measurable evidence that control environment integrity extends beyond written policies
- Quantitative data supporting management representations about security culture
- Clear audit trail for human-factor risk management activities

## **4 Framework Integration Architecture**

### **4.1 CPF Mapping to Common Criteria (CC1–CC9)**

Table 3 presents the comprehensive mapping of CPF categories to each of the nine Common Criteria, identifying enhancement opportunities and specific CPF indicators.

Table 3: CPF Integration with SOC 2 Common Criteria  
(CC1–CC9)

<b>Common Criterion</b>	<b>Standard Controls</b>	<b>SOC 2</b>	<b>CPF Enhancement</b>	<b>CPF Categories</b>	<b>Cate-</b>
CC1: Control Environment	Code of conduct, board oversight, organizational structure, HR policies		Psychological safety assessment, authority gradient analysis, group dynamics profiling, unconscious bias identification in governance	[1.x], [6.x], [8.x]	
CC2: Communication & Information	Security policies, internal/external communication, reporting mechanisms		Cognitive load analysis of security communications, psychological barriers to reporting, information processing capacity assessment	[5.x], [4.x], [3.x]	
CC3: Risk Assessment	Risk identification, fraud risk assessment, change analysis		Pre-cognitive vulnerability profiling, social engineering susceptibility mapping, psychological threat modeling	[1.x], [2.x], [3.x], [9.x]	
CC4: Monitoring Activities	Control effectiveness evaluation, deficiency communication		Behavioral pattern monitoring, psychological indicator trending, cognitive drift detection	[5.x], [7.x], [10.x]	
CC5: Control Activities	Policy deployment, technology controls, segregation of duties		Human factor effectiveness of controls, cognitive ergonomics of security processes, compliance fatigue monitoring	[2.x], [5.x], [4.x]	
CC6: Logical & Physical Access	Authentication, network segmentation, encryption, physical controls		Social engineering resistance assessment, authority-based bypass susceptibility, insider threat psychology indicators	[1.x], [3.x], [8.x]	
CC7: System Operations	Anomaly detection, incident response, backup, disaster recovery		Stress-aware incident response protocols, decision quality under pressure, alert fatigue mitigation, cognitive load management during incidents	[7.x], [5.x], [10.x]	

Common Criterion	Standard Controls	SOC 2	CPF Enhancement	CPF Categories	Category
CC8: Change Management	Change authorization, testing, approval, documentation		Psychological resistance to change, cognitive bias in change evaluation, security regression under organizational transition	[4.x], [6.x], [8.x]	
CC9: Risk Mitigation	Business disruption mitigation, vendor risk management		Psychological dependency assessment, trust transference vulnerabilities in vendor relationships, concentration risk psychology	[3.x], [4.x], [9.x]	

## 4.2 CPF Mapping to Optional Trust Services Categories

Beyond the mandatory Common Criteria, CPF integration extends to the four optional Trust Services Categories.

Table 4: CPF Integration with Optional Trust Services Categories

TSC Category	Standard Controls	CPF Enhancement	CPF Categories	Category
Availability (A1)	DR/BCP plans, redundancy, capacity planning	Psychological resilience during outages, decision quality in degraded operations, stress cascade prevention	[7.x], [10.x]	
Processing Integrity (PI1)	Input validation, error handling, output review	Cognitive error patterns, attention degradation, automation bias in validation	[5.x], [9.x]	
Confidentiality (C1)	Data classification, encryption, access restriction	Insider threat psychology, social pressure to share, authority-based data exfiltration	[1.x], [8.x]	[3.x],
Privacy (P1)	Notice, consent, collection, retention, disposal	Privacy fatigue, consent manipulation, psychological aspects of data minimization	[2.x], [5.x]	[4.x],

## 5 Detailed Mapping: CPF Categories to Common Criteria

### 5.1 CC1: Control Environment—Psychological Foundations of Governance

CC1 establishes the organizational foundation for internal controls through COSO Principles 1–5. The control environment encompasses integrity, ethical values, board oversight, organiza-

tional structure, and accountability. CPF enhances each dimension:

#### **COSO Principle 1 – Integrity and Ethical Values:**

Traditional SOC 2 controls include codes of conduct and ethics policies. CPF adds:

- [6.x] **Group Dynamics Assessment:** Identifying whether organizational culture enables genuine ethical behavior or produces performative compliance driven by groupthink
- [8.x] **Shadow Analysis:** Assessing whether ethical blind spots exist due to unconscious organizational projection (e.g., attributing ethical failures only to external actors)
- [1.x] **Authority Gradient Measurement:** Evaluating whether hierarchical dynamics suppress ethical reporting

#### **COSO Principle 4 – Competence and Accountability:**

Beyond skill verification, CPF assesses:

- [5.x] **Cognitive Load Capacity:** Whether personnel can effectively process security requirements alongside operational demands
- [7.x] **Stress Resilience Profiles:** Aggregate stress indicators that predict degraded security performance
- [4.x] **Affective State Monitoring:** Organizational emotional climate indicators that correlate with security incident rates

## **5.2 CC3: Risk Assessment—Integrating Psychological Threat Modeling**

CC3 requires organizations to identify, assess, and manage risks. Traditional SOC 2 risk assessments focus on technical and procedural threats. CPF introduces a psychological threat layer:

#### **Risk Identification Enhancement:**

- [1.x] **Authority-Based Threat Vectors:** Mapping susceptibility to CEO fraud, pretexting, and authority impersonation across organizational roles
- [2.x] **Temporal Vulnerability Windows:** Identifying periods of elevated risk (end of quarter, organizational change, post-incident fatigue)
- [3.x] **Social Influence Susceptibility:** Profiling organizational resistance to social engineering at aggregate level

#### **Fraud Risk Enhancement:**

CC3 explicitly requires fraud risk consideration. CPF strengthens this through:

- [4.x] **Insider Threat Psychology:** Assessing organizational conditions (dissatisfaction, disengagement, grievance) that correlate with insider risk
- [8.x] **Rationalization Patterns:** Identifying unconscious organizational dynamics that enable fraud rationalization
- [6.x] **Bystander Effect Assessment:** Evaluating whether group dynamics inhibit fraud reporting

### 5.3 CC6: Logical and Physical Access—The Social Engineering Dimension

CC6 addresses authentication, access management, and physical security. While technical controls (MFA, encryption, network segmentation) are well understood, the social engineering dimension remains under-assessed:

- [1.x] **Authority Bypass Assessment:** Testing resistance to authority-based access requests (“I’m from IT, I need your credentials”)
- [3.x] **Reciprocity and Liking Exploitation:** Assessing susceptibility to rapport-based social engineering
- [8.x] **Trust Transference Patterns:** Identifying how organizational trust dynamics create access control bypass opportunities
- [9.x] **AI-Assisted Social Engineering:** Evaluating preparedness for deepfake and AI-generated social engineering attacks

### 5.4 CC7: System Operations—Stress-Aware Incident Response

CC7 governs monitoring, detection, incident response, and recovery. The human element is critical during incident response, where decisions are made under extreme time pressure and stress:

#### Incident Detection Enhancement:

- [5.x] **Alert Fatigue Metrics:** Quantifying cognitive desensitization to security alerts and monitoring capacity degradation
- [9.x] **Automation Bias Assessment:** Measuring over-reliance on automated detection tools and corresponding reduction in human analytical vigilance

#### Incident Response Enhancement:

- [7.x] **Decision Quality Under Stress:** Protocols ensuring analytical rigor is maintained during high-pressure incident response
- [10.x] **Cascade Prevention:** Identifying convergent psychological states that amplify incident impact (e.g., simultaneous stress, cognitive overload, and authority confusion)
- [6.x] **Team Dynamics During Crisis:** Assessing and mitigating Bion’s basic assumption group behaviors that emerge during security incidents

### 5.5 CC9: Risk Mitigation—Psychology of Vendor Dependency

CC9 addresses business continuity and third-party risk. CPF enhances vendor risk management through psychological assessment:

- [4.x] **Attachment to Vendors:** Assessing whether emotional attachment to vendor relationships compromises objective risk evaluation
- [3.x] **Social Influence in Vendor Selection:** Identifying how vendor marketing and relationship management exploit psychological vulnerabilities in procurement decisions
- [9.x] **AI Vendor Trust Dynamics:** Evaluating appropriate trust calibration for AI/ML service providers and addressing automation bias in vendor-provided AI tools

## 6 Implementation Methodology for SOC 2 Programs

### 6.1 Phase 1: Readiness Assessment (Weeks 1–4)

**Objective:** Evaluate current SOC 2 control set and identify CPF integration opportunities.

**Activities:**

- Review existing SOC 2 System Description and control narratives for human-factor coverage
- Map current controls to CPF categories, identifying gaps and enhancement opportunities
- Conduct baseline CPF assessment using aggregated organizational data
- Develop CPF integration roadmap aligned with SOC 2 examination timeline
- Identify key stakeholders: CISO, compliance, HR, legal, and external auditor

**Deliverable:** CPF-SOC 2 Gap Analysis Report

### 6.2 Phase 2: Control Design and Enhancement (Weeks 5–12)

**Objective:** Design CPF-enhanced controls for integration into the SOC 2 control framework.

**Priority Control Enhancements:**

Table 5: Priority CPF-Enhanced Controls for SOC 2

CC Series	Enhancement	Implementation	Evidence Type
CC1	Psychological safety assessment	Annual aggregate CPF assessment of control environment	Assessment report
CC3	Human-factor risk register	Quarterly psychological threat landscape review	Risk register entries
CC6	Social engineering resistance program	Bi-annual CPF-based social engineering testing	Test results, trending
CC7	Stress-aware IR playbooks	Incident response procedures incorporating cognitive load management	Updated IR procedures
CC9	Vendor human risk assessment	CPF-informed vendor risk questionnaire	Vendor assessments

### 6.3 Phase 3: Operational Integration (Weeks 13–24)

**Objective:** Embed CPF-enhanced controls into operational processes and begin evidence collection.

**Activities:**

- Deploy CPF assessment instruments with privacy safeguards
- Integrate psychological risk indicators into existing monitoring dashboards

- Conduct first round of CPF-enhanced social engineering testing
- Train incident response teams on stress-aware protocols
- Begin evidence collection for SOC 2 examination period

#### **6.4 Phase 4: Audit Preparation and Evidence (Ongoing)**

**Objective:** Prepare CPF-enhanced evidence for SOC 2 examination.

**Evidence Framework for Auditors:**

- CPF aggregate assessment reports (anonymized, privacy-preserving)
- Trending data showing psychological risk indicator changes over examination period
- Social engineering test results with CPF-informed analysis
- Incident response effectiveness metrics including decision quality measures
- Vendor human-factor risk assessments integrated into third-party management program

### **7 CPF-Enhanced Points of Focus**

The 2022 revised Points of Focus provide guidance on controls that may satisfy each criterion. The following CPF-enhanced Points of Focus extend the AICPA's framework:

#### **7.1 CC1 Enhanced Points of Focus**

- **Psychological Safety Metrics:** The organization assesses and monitors aggregate psychological safety indicators that influence willingness to report security concerns (supports COSO Principle 1)
- **Authority Gradient Assessment:** The organization evaluates hierarchical dynamics that may suppress security-relevant communication or enable authority-based compliance bypass (supports COSO Principle 3)
- **Group Dynamics Monitoring:** The organization monitors team-level dynamics that could produce groupthink in security-relevant decision-making (supports COSO Principle 5)

#### **7.2 CC3 Enhanced Points of Focus**

- **Pre-Cognitive Vulnerability Assessment:** The organization includes psychological vulnerability identification in its risk assessment process, addressing biases and susceptibilities that technical controls cannot mitigate
- **Social Engineering Threat Modeling:** The organization assesses susceptibility to authority, urgency, and social proof manipulation as part of its fraud and threat risk identification
- **Temporal Risk Profiling:** The organization identifies and monitors periods of elevated psychological vulnerability (organizational change, post-incident, high-stress periods)

### 7.3 CC6 Enhanced Points of Focus

- **Social Engineering Resistance Testing:** The organization conducts regular testing of personnel resistance to social engineering attacks informed by CPF vulnerability categories
- **Authority-Based Bypass Assessment:** The organization tests and monitors susceptibility to access requests based on impersonated or real authority
- **AI-Enhanced Attack Preparedness:** The organization assesses readiness for AI-assisted social engineering, including deepfake and synthetic identity attacks

### 7.4 CC7 Enhanced Points of Focus

- **Cognitive Load Management:** The organization designs alert thresholds and monitoring interfaces to account for cognitive processing limitations and prevent alert fatigue
- **Stress-Calibrated Response Procedures:** Incident response procedures include provisions for decision quality assurance under high-stress conditions
- **Post-Incident Psychological Recovery:** The organization includes team psychological resilience restoration in its incident recovery procedures

## 8 Measurement and Metrics Framework

### 8.1 Key Performance Indicators for CPF-Enhanced SOC 2

Table 6: CPF-SOC 2 Key Performance Indicators

Metric	Measurement Method	Target	CC Mapping
Social Engineering Resistance Rate	CPF-informed phishing and pretexting tests	>85% resistance	CC3, CC6
Alert Response Quality	Cognitive load-adjusted alert analysis	<5% false dismissal	CC4, CC7
Incident Decision Quality	Post-incident decision analysis	>90% protocol adherence	CC7
Authority Bypass Susceptibility	CPF authority-based testing	<10% bypass success	CC1, CC6
Vendor Human Risk Score	CPF-informed vendor assessment	All critical vendors assessed	CC9
Psychological Safety Index	Aggregate CPF [6.x] assessment	Green across all teams	CC1, CC2
Security Communication Effectiveness	Cognitive processing assessment of security policies	>80% comprehension	CC2
Change Resistance Index	CPF [4.x], [6.x] assessment during change periods	Monitor trend	CC8

## 8.2 Reporting to Auditors

SOC 2 auditors require evidence that controls are designed suitably and operating effectively. CPF-enhanced reporting should include:

- **Quarterly CPF Dashboards:** Aggregate psychological vulnerability scores trending over the examination period, demonstrating control operating effectiveness
- **Social Engineering Test Reports:** Results of CPF-informed testing campaigns with trend analysis showing improvement
- **Incident Response Quality Reviews:** Post-incident analyses incorporating decision quality metrics
- **Vendor Human Risk Register:** CPF-informed risk assessments integrated into the third-party management program
- **Training Effectiveness Evidence:** Pre/post CPF scores demonstrating that training programs produce measurable behavioral change, not merely knowledge transfer

## 9 SOC 2+ Integration: CPF as Supplementary Subject Matter

SOC 2+ reports expand the standard framework by incorporating additional compliance requirements. CPF can serve as supplementary subject matter in a SOC 2+ examination:

### CPF as SOC 2+ Subject Matter:

- Define CPF-specific control objectives alongside Trust Services Criteria
- Map CPF assessments to additional criteria for human factor risk management
- Provide auditors with supplementary testing procedures for psychological controls
- Deliver a differentiated report that demonstrates comprehensive human risk coverage

This approach is particularly valuable for organizations that serve regulated industries (healthcare, financial services) where human-factor risk management is increasingly scrutinized.

## 10 Implementation Considerations

### 10.1 Privacy and Employee Relations

CPF integration within SOC 2 programs must adhere to privacy principles consistent with the Privacy Trust Services Category itself:

- All CPF assessments use aggregated data with a minimum unit of 10 individuals
- Individual profiling is never performed; analysis is role-based and team-based
- Transparent communication to employees about assessment purposes and methods
- Compliance with applicable privacy regulations (CCPA, state privacy laws, GDPR for multinational organizations)
- Data minimization: collect only what is necessary for aggregate risk assessment

## **10.2 Organizational Prerequisites**

### **Executive Sponsorship:**

- CISO and compliance leadership commitment to human-factor enhancement
- Budget allocation for CPF assessment tools and training
- Clear communication that CPF enhances—not replaces—existing SOC 2 controls

### **Auditor Engagement:**

- Early discussion with SOC 2 auditor about CPF-enhanced controls
- Agreement on evidence requirements and testing procedures
- Alignment on how CPF metrics support management assertions

### **Technical Prerequisites:**

- Existing SOC 2 control framework operational and documented
- Risk assessment processes established and regularly performed
- Incident management and change management processes in place
- Vendor management program with established due diligence procedures

## **10.3 Common Implementation Pitfalls**

### **Compliance Pitfalls:**

- Treating CPF as a replacement for required SOC 2 controls rather than an enhancement
- Insufficient evidence documentation for auditor testing
- Misalignment between CPF assessment cadence and SOC 2 examination period
- Overscoping CPF integration in the first examination year

### **Organizational Pitfalls:**

- Inadequate privacy impact assessment before deployment
- Failure to communicate CPF purpose transparently, creating employee anxiety
- Over-emphasis on assessment without corresponding intervention programs
- Treating CPF scores as individual performance metrics rather than organizational indicators

### **Technical Pitfalls:**

- Siloed implementation separate from existing GRC platforms
- Insufficient integration with incident management and risk assessment workflows
- Poor data quality in aggregate assessments due to inadequate participation
- Failure to maintain CPF assessments throughout the full examination period

## 11 Cross-Framework Synergies

Organizations subject to multiple compliance frameworks benefit from CPF's framework-agnostic design. Table 7 illustrates synergies between CPF-enhanced SOC 2 controls and other common frameworks.

Table 7: CPF Cross-Framework Compliance Synergies

Framework	SOC 2 CC Series	Parallel Requirement	CPF	Shared Enhancement
ISO 27001	CC1, CC3	A.5 (Policies), A.8 (HR Security)	Control environment & human risk assessment	
NIST CSF 2.0	CC3, CC7	GV (Govern), RS (Respond)	Risk assessment & incident response	
NIS2	CC1, CC6	Art. 20 (Management), Art. 21.2.g (Training)	Governance & social engineering resistance	
DORA	CC7, CC9	Art. 5 (Management), Art. 28 (Third Parties)	Incident response & vendor risk	
HIPAA	CC6, CC9	§164.308 (Administrative), §164.312 (Technical)	Access controls & risk management	

## 12 Future Directions

### 12.1 Evolving SOC 2 Landscape

The AICPA periodically revises the Trust Services Criteria and Points of Focus. Anticipated developments that align with CPF integration include:

- Increased emphasis on AI governance and AI-related risk assessment
- Enhanced points of focus addressing social engineering and human-factor threats
- Growing auditor expectation for behavioral metrics alongside technical controls
- Expansion of SOC 2+ examinations incorporating human risk management frameworks

### 12.2 CPF Research Agenda

Future work specific to SOC 2 integration will focus on:

- Pilot implementations with SOC 2-certified service organizations
- Correlation analysis between CPF scores and SOC 2 examination findings
- Development of standardized CPF-enhanced testing procedures for SOC 2 auditors
- Longitudinal studies tracking human-factor incident reduction in CPF-enhanced SOC 2 environments

## 13 Conclusion

SOC 2 provides a robust framework for evaluating organizational security controls, grounded in the COSO internal control principles and operationalized through the Trust Services Criteria. However, the framework’s implicit treatment of human factors—despite their role in the majority of security incidents—represents a significant gap that CPF is uniquely positioned to address.

The integration framework presented in this paper demonstrates that CPF-enhanced controls can be mapped systematically to each of the nine Common Criteria and all five Trust Services Categories, providing service organizations with actionable methodologies for strengthening the psychological dimension of their security posture. By introducing enhanced Points of Focus, measurable key performance indicators, and a phased implementation approach, the framework enables immediate adoption within existing SOC 2 compliance programs.

For CISOs and compliance leaders at service organizations, the message is clear: in an environment where SOC 2 reports are increasingly commoditized, differentiation comes from the depth and sophistication of human risk management. CPF provides the theoretical foundation and practical tools to move beyond checkbox compliance toward genuine organizational resilience.

### **Recommended Next Steps for SOC 2 Practitioners:**

1. Conduct a CPF gap analysis against your current SOC 2 control set, prioritizing CC1, CC3, CC6, and CC7
2. Engage your SOC 2 auditor early to discuss CPF-enhanced controls and evidence requirements
3. Implement CPF-informed social engineering testing as a high-impact, quick-win enhancement
4. Develop stress-aware incident response procedures incorporating cognitive load management
5. Establish baseline CPF metrics and begin trending for your next SOC 2 examination period
6. Evaluate SOC 2+ options to include CPF as supplementary subject matter for comprehensive human risk coverage

The evidence is unambiguous: technical controls alone are insufficient. By integrating psychological risk assessment into SOC 2 compliance programs, organizations address the root cause of the majority of security incidents while delivering demonstrably superior assurance to customers, auditors, and stakeholders.

## **Note on AI-Assisted Composition**

This manuscript presents the original theoretical framework and intellectual contributions of the author. In the composition and formatting process, the author utilized a large language model (LLM) as an auxiliary tool for specific tasks:

- **Stylistic Refactoring:** Rephrasing sentences for improved clarity and flow in English.
- **Formatting Assistance:** Aiding in the consistent application of LaTeX syntax for tables and cross-referencing.

## **It is crucial to emphasize that:**

- The core idea, the CPF-SOC 2 integration architecture, the mapping of all indicators to Trust Services Criteria, and the overall analysis are solely the product of the author's expertise and intellectual effort.
- The LLM generated no novel ideas, concepts, or conclusions. Its role was limited to rewording and formatting assistance under the author's strict direction and continuous review.
- The author is entirely responsible for the accuracy, validity, and integrity of the published content.

## **Author Bio**

Giuseppe Canale, CISSP, is an independent cybersecurity researcher with 27 years of experience in enterprise security program management. He specializes in the integration of psychological risk assessment with compliance frameworks and has developed the Cybersecurity Psychology Framework (CPF) for organizational security posture assessment. His work focuses on bridging the gap between technical security controls and human factor vulnerabilities across multiple regulatory and assurance contexts, including European regulatory frameworks (NIS2, DORA) and international compliance standards (SOC 2, ISO 27001).

## **Data Availability Statement**

Implementation templates, assessment tools, mapping matrices, and case study details are available through the CPF3.org platform, subject to appropriate licensing agreements.

## **Conflict of Interest**

The author declares no conflicts of interest.

## **References**

- [1] Canale, G. (2025). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5387222>
- [2] Canale, G. (2025). The Human Factor in Operational Resilience: Integrating Psychological Risk Assessment into NIS2 and DORA Compliance Frameworks. *Preprint*.
- [3] Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Enterprise.
- [4] IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.
- [5] AICPA. (2017). *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*. American Institute of Certified Public Accountants.

- [6] Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal Control—Integrated Framework*. COSO.
- [7] Bion, W. R. (1961). *Experiences in Groups*. London: Tavistock Publications.
- [8] Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.
- [9] Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion*. New York: Collins.
- [10] Milgram, S. (1974). *Obedience to Authority*. New York: Harper & Row.
- [11] Klein, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psycho-analysis*, 27, 99-110.
- [12] SANS Institute. (2023). *Security Awareness Report 2023*. SANS Security Awareness.