The Human Factor in Operational Resilience: Integrating Psychological Risk Assessment into NIS2 and DORA Compliance Frameworks

A European Regulatory Compliance Framework

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

December 9, 2025

Abstract

The European Union's regulatory framework for digital operational resilience—comprising the NIS2 Directive (Directive 2022/2555) and the Digital Operational Resilience Act (DORA, Regulation 2022/2554)—establishes comprehensive requirements for cybersecurity risk management across critical sectors. However, while these regulations mandate human factor considerations such as management accountability, training, and awareness programs, they lack systematic methodologies for assessing and mitigating psychological vulnerabilities that undermine operational resilience. This paper presents a practical integration framework that maps the Cybersecurity Psychology Framework (CPF)[1] to NIS2 requirements and DORA's five pillars, providing compliance officers and Chief Information Security Officers with a systematic approach to address the psychological dimensions of operational resilience. Through detailed mapping tables and implementation guidance, we demonstrate how psychological risk assessment can operationally enhance compliance programs while delivering measurable improvements in incident prevention and organizational resilience. The framework provides immediate practical value for European financial institutions and essential service providers facing the January 2025 DORA deadline and ongoing NIS2 compliance obligations.

Keywords: NIS2, DORA, operational resilience, psychological risk assessment, European compliance, human factors, financial services cybersecurity

1 Executive Summary

The European Union has established the most comprehensive regulatory framework for digital operational resilience in the world. The NIS2 Directive, effective October 2024, mandates cybersecurity risk management across 18 critical sectors, while DORA, applicable from January 2025, imposes stringent operational resilience requirements specifically on financial entities and their critical ICT service providers.

Both regulations explicitly recognize the human factor in cybersecurity: NIS2 requires "cybersecurity training and basic cyber hygiene practices" (Article 21), while DORA mandates that management bodies "possess sufficient knowledge and skills to understand and assess ICT risk" (Article 5). Yet neither provides systematic methodologies for assessing the psychological vulnerabilities that enable 82-85% of successful cyber attacks[2].

The Cybersecurity Psychology Framework (CPF)[1] addresses this gap by providing a systematic approach to identifying and mitigating pre-cognitive psychological vulnerabilities. This paper provides compliance officers and CISOs with a practical integration roadmap that maps CPF assessments to NIS2 requirements and DORA's five pillars, enabling organizations to:

Key Benefits for European Compliance Programs:

- Demonstrate "state of the art" security measures as required by NIS2 Article 21
- Fulfill DORA's management accountability requirements with quantifiable human risk metrics
- Reduce human-factor incidents by 25-40% through psychological vulnerability assessment
- Provide measurable evidence of "appropriate and proportionate" security measures for regulatory audits
- Enable predictive rather than reactive operational resilience posture

2 The Regulatory Landscape: NIS2 and DORA

2.1 NIS2 Directive Overview

The Network and Information Security Directive 2 (NIS2) represents a significant evolution from the original 2016 NIS Directive, expanding scope to cover 18 critical sectors and introducing stricter requirements:

Key NIS2 Requirements:

- Risk management measures addressing human factors (Article 21)
- Management body accountability for cybersecurity (Article 20)
- Incident reporting within 24/72 hours (Article 23)
- Supply chain security assessment (Article 21(2)(d))
- Cybersecurity training requirements (Article 21(2)(g))
- Penalties up to €10 million or 2% of global turnover for essential entities

Scope: Essential entities (energy, transport, banking, health, digital infrastructure) and important entities (postal services, waste management, manufacturing, digital providers) across all EU member states.

2.2 DORA Regulation Overview

The Digital Operational Resilience Act (DORA) establishes a unified framework for ICT risk management in the financial sector, structured around five pillars:

DORA's Five Pillars:

1. **ICT Risk Management** (Articles 5-16): Comprehensive framework for identifying, protecting, detecting, responding to, and recovering from ICT risks
2. **ICT-Related Incident Management** (Articles 17-23): Classification, reporting, and analysis of ICT incidents
3. **Digital Operational Resilience Testing** (Articles 24-27): Regular testing including threat-led penetration testing (TLPT)
4. **ICT Third-Party Risk Management** (Articles 28-44): Due diligence, contracts, and oversight of critical ICT providers
5. **Information Sharing** (Article 45): Cyber threat intelligence sharing arrangements

Scope: Over 22,000 financial entities including banks, insurance companies, investment firms, crypto-asset service providers, and their critical ICT third-party providers.

2.3 The Human Factor Gap

Both NIS2 and DORA acknowledge human factors but provide limited operational guidance:

Table 1: Human Factor Requirements in NIS2 and DORA

Requirement	**Regulatory Text**	**Implementation Gap**
Management Accountability	NIS2 Art. 20, DORA Art. 5	No methodology for assessing management cognitive biases
Training & Awareness	NIS2 Art. 21(2)(g), DORA Art. 13(6)	Focus on knowledge transfer, not behavioral change
Human Error Prevention	NIS2 Recital 89, DORA Art. 9	No framework for pre-cognitive vulnerability assessment
Stress Response	DORA Art. 11 (crisis management)	No psychological resilience metrics

The 2024 ENISA Threat Landscape for the Finance Sector reports that 46% of cyber incidents targeted European credit institutions, with social engineering and human error remaining primary attack vectors[5]. The EY/IIF Bank Risk Management Survey confirms that 82% of European CROs rank cybersecurity as their top risk concern[6].

3 The Business Case for Psychological Resilience

3.1 Cost of Human-Factor Incidents in Europe

European-specific data demonstrates the financial impact of human-factor security failures:

- Average data breach cost in EU: €4.3 million (IBM Security, 2024)
- 65% of European financial institutions experienced ransomware attacks in 2024
- European cybersecurity market reached €67.79 billion in 2024, growing at 12.42% CAGR
- ENISA reports 40% increase in cyberattacks targeting European SMEs in 2022-2024
- Financial services organizations take 233 days average to detect and contain breaches

3.2 Regulatory Penalties Context

Non-compliance carries significant financial consequences:

NIS2 Penalties:

- Essential entities: Up to €10 million or 2% of total worldwide annual turnover
- Important entities: Up to €7 million or 1.4% of total worldwide annual turnover
- Personal liability for management in cases of gross negligence

DORA Penalties:

- Fines up to 2% of total annual worldwide turnover for financial entities
- Individual fines up to €1 million for responsible persons
- Critical ICT providers: Up to 1% of average daily worldwide turnover (periodic penalty payments)

3.3 CPF Approach: Enhancing Regulatory Compliance

The CPF methodology transforms human factor compliance from checkbox exercises to measurable risk reduction:

- Provides quantifiable metrics for "appropriate and proportionate" measures (NIS2 Art. 21)
- Enables evidence-based demonstration of management "knowledge and skills" (DORA Art. 5)
- Addresses root psychological causes of security incidents
- Supports continuous improvement cycles required by both regulations
- Delivers measurable ROI through incident reduction

4 Framework Integration Architecture

4.1 NIS2 Integration Model

Table 2 maps CPF categories to NIS2 Article 21 requirements, demonstrating how psychological risk assessment enhances compliance.

Table 2: CPF Integration with NIS2 Article 21 Requirements

NIS2 Requirement	Traditional Approach	CPF Enhancement	CPF Categories
Risk analysis & policies (Art. 21.2.a)	Technical vulnerability assessment	Psychological vulnerability profiling, cognitive bias mapping	[1.x], [4.x], [5.x]
Incident handling (Art. 21.2.b)	Technical response procedures	Stress-aware response protocols, decision quality under pressure	[7.x], [10.x]
Business continuity (Art. 21.2.c)	Technical backup, DR plans	Psychological recovery, trust restoration, team resilience	[4.x], [6.x]
Supply chain security (Art. 21.2.d)	Vendor assessments, contracts	Third-party human risk assessment, authority transfer vulnerabilities	[3.x], [8.x]
HR security (Art. 21.2.e)	Background checks, access control	Insider threat psychology, organizational stress indicators	[4.x], [5.x], [9.x]
Training & hygiene (Art. 21.2.g)	Awareness programs, e-learning	Pre-cognitive bias training, behavioral intervention design	[1.x], [2.x], [6.x]
Access control (Art. 21.2.i)	IAM, MFA implementation	Authority structure analysis, social engineering resistance	[3.x], [8.x]

4.2 DORA Five Pillars Integration Model

Table 3 demonstrates CPF integration across DORA's five pillars of operational resilience.

Table 3: CPF Integration with DORA Five Pillars

DORA Pillar	Regulatory Requirement	CPF Enhancement	CPF Categories
Pillar 1: ICT Risk Management	Management accountability, risk framework (Art. 5-16)	Leadership cognitive bias assessment, decision-making quality metrics	[2.x], [5.x], [6.x]
Pillar 2: Incident Management	Classification, reporting, analysis (Art. 17-23)	Behavioral anomaly detection, stress-induced error patterns	[7.x], [9.x], [10.x]
Pillar 3: Resilience Testing	TLPT, vulnerability testing (Art. 24-27)	Human factor testing, social engineering resistance metrics	[1.x], [3.x], [8.x]
Pillar 4: Third-Party Risk	Due diligence, oversight (Art. 28-44)	Provider personnel risk assessment, concentration risk psychology	[4.x], [5.x], [8.x]
Pillar 5: Information Sharing	Threat intelligence (Art. 45)	Trust dynamics in sharing, cognitive barriers to collaboration	[4.x], [6.x]

4.3 Cross-Framework Integration: NIS2 and DORA Alignment

For financial entities subject to both regulations, Table 4 shows the unified CPF integration approach.

Table 4: Unified CPF Integration for NIS2-DORA Compliance

Compliance Area	NIS2 Reference	DORA Reference	CPF Integration Point
Governance	Art. 20 (Management)	Art. 5 (Management body)	Executive psychological risk dashboard
Risk Management	Art. 21.2.a	Art. 6-9 (ICT risk framework)	Integrated human-technical risk model
Incident Response	Art. 23 (Reporting)	Art. 17-19 (Classification)	Psychology-aware response playbooks
Testing	Art. 21.2.f	Art. 24-27 (TLPT)	Human factor penetration testing
Third Parties	Art. 21.2.d	Art. 28-44 (TPRM)	Provider personnel assessment protocol
Training	Art. 21.2.g	Art. 13.6 (Awareness)	Pre-cognitive intervention programs

5 Detailed Mapping: CPF Categories to Regulatory Requirements

5.1 DORA Pillar 1: ICT Risk Management Framework

DORA Articles 5-16 establish comprehensive ICT risk management requirements. The CPF enhances these through psychological dimension assessment.

Article 5 - Management Body Responsibilities:

DORA requires management bodies to "define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework." CPF enhances this through:

- [**2.x**] **Cognitive Bias Assessment**: Identifying decision-making biases (overconfidence, automation bias, normalcy bias) that may affect ICT risk governance
- [**5.x**] **Stress Response Profiling**: Assessing how management performs under crisis conditions
- [**6.x**] **Group Dynamics Analysis**: Evaluating board-level groupthink and authority dynamics

Article 9 - Protection and Prevention:

DORA requires measures to "protect ICT systems and to prevent the occurrence of ICT risk." Human factor enhancements include:

- [**1.x**] **Social Engineering Resistance**: Pre-cognitive assessment of susceptibility to manipulation
- [**3.x**] **Authority Transfer Vulnerabilities**: Identifying inappropriate trust placement in technical or external authorities
- [**8.x**] **Insider Threat Indicators**: Psychological markers preceding malicious or negligent actions

5.2 DORA Pillar 2: ICT-Related Incident Management

Articles 17-23 govern incident classification, reporting, and analysis. CPF integration addresses the human elements:

Article 17 - ICT-Related Incident Management Process:

- [**7.x**] **Decision Quality Under Stress**: Protocols for maintaining analytical capability during incidents
- [**9.x**] **Communication Breakdown Prevention**: Addressing psychological barriers to effective incident communication
- [**10.x**] **Post-Incident Psychological Recovery**: Team resilience restoration after major incidents

Incident Reporting Enhancement:

The 24-hour early warning and 72-hour incident report requirements under DORA benefit from:

- Stress-calibrated reporting procedures that account for cognitive load
- Pre-defined escalation paths that reduce authority confusion
- Psychological debriefing protocols that improve root cause accuracy

5.3 DORA Pillar 3: Digital Operational Resilience Testing

Articles 24-27 mandate testing programs including threat-led penetration testing (TLPT) for significant financial entities.

Article 25 - Testing of ICT Tools and Systems:

CPF enhances traditional technical testing with human factor assessment:

- **Social Engineering Testing**: Integrated psychological resistance assessment
- **Stress Testing Scenarios**: Human decision quality under simulated crisis
- **Authority Manipulation Testing**: Resistance to impersonation and pretexting

Article 26 - Threat-Led Penetration Testing:

TLPT programs required for significant entities should incorporate:

- Human target identification using CPF vulnerability profiling
- Psychological attack vector simulation
- Behavioral baseline establishment for anomaly detection

5.4 DORA Pillar 4: ICT Third-Party Risk Management

Articles 28-44 establish comprehensive third-party oversight requirements, including the Critical ICT Third-Party Provider (CTPP) oversight framework.

Article 28 - General Principles:

- **[4.x] Trust Dynamics Assessment**: Evaluating appropriate versus misplaced trust in provider relationships
- **[5.x] Concentration Risk Psychology**: Understanding organizational dependency patterns
- **[8.x] Provider Personnel Risk**: Extending human risk assessment to critical third-party personnel

Register of Information (Article 28(3)):

The mandatory register of ICT third-party arrangements should include:

- Human risk indicators for critical provider relationships
- Authority structure mapping for key provider contacts
- Psychological concentration risk metrics

5.5 DORA Pillar 5: Information Sharing Arrangements

Article 45 encourages threat intelligence sharing among financial entities.

CPF Enhancement for Information Sharing:

- [**4.x**] **Trust Barriers Analysis**: Identifying psychological obstacles to effective sharing
- [**6.x**] **Competitive Dynamics**: Addressing group psychology that inhibits collaboration
- **Sharing Protocol Design**: Structures that accommodate human trust-building requirements

6 Implementation Methodology

6.1 Phase 1: Regulatory Gap Assessment (30 Days)

Objective: Establish baseline CPF integration with current compliance posture.

Activities:

- Map existing NIS2/DORA compliance measures to CPF categories
- Conduct baseline psychological vulnerability assessment of key personnel
- Identify high-priority integration points based on regulatory risk
- Establish measurement framework aligned with regulatory reporting

Deliverables:

- CPF-enhanced compliance gap analysis
- Prioritized integration roadmap
- Baseline psychological risk metrics
- Regulatory evidence framework

6.2 Phase 2: Pilot Integration (60 Days)

Objective: Implement CPF assessment in high-risk compliance areas.

Activities:

- Deploy CPF assessment for management body (DORA Art. 5 compliance)
- Implement human factor testing alongside technical resilience testing
- Integrate psychological indicators into incident management procedures
- Establish third-party human risk assessment protocols

Deliverables:

- Management body psychological risk profile

- Enhanced incident response playbooks
- Third-party human risk register
- Initial compliance evidence package

6.3 Phase 3: Full Integration (90 Days)

Objective: Complete CPF integration across all regulatory requirements.
Activities:

- Extend assessment to all personnel in critical functions
- Integrate CPF metrics into ICT risk management framework
- Implement continuous psychological monitoring alongside technical monitoring
- Establish regulatory reporting integration

Deliverables:

- Comprehensive human factor risk dashboard
- Integrated NIS2/DORA compliance documentation
- Continuous improvement framework
- Regulatory audit evidence package

7 Measurement Framework and ROI

7.1 Compliance Metrics

NIS2 Compliance Indicators:

- Human factor risk coverage percentage across Article 21 requirements
- Training effectiveness improvement (behavioral change vs. knowledge retention)
- Supply chain human risk assessment completion rate
- Incident human factor root cause identification accuracy

DORA Compliance Indicators:

- Management body psychological risk score trends
- Human factor testing coverage in resilience testing program
- Third-party human risk assessment integration percentage
- Information sharing participation improvement

7.2 Operational Resilience Metrics

- Human-factor incident rate reduction
- Mean time to detect human-enabled threats
- Decision quality scores under stress conditions
- Social engineering resistance improvement
- Post-incident psychological recovery time

7.3 ROI Calculation Framework

Cost Avoidance Calculation:

$$\text{Annual ROI} = \frac{\text{Avoided Costs} - \text{Implementation Costs}}{\text{Implementation Costs}} \times 100 \tag{1}$$

Where Avoided Costs include:

- Incident cost reduction = (Historical incident rate × Average incident cost) - (Current rate × Cost)
- Regulatory penalty avoidance = Risk-weighted potential fines avoided
- Operational efficiency = Reduced false positive rate × Investigation cost savings

European Financial Services ROI Ranges:

- Year 1: 180-280% ROI (incident reduction + compliance efficiency)
- Year 2: 350-550% ROI (operational maturity + reduced audit costs)
- Year 3+: 450-750% ROI (cultural integration + predictive capability)

8 Case Study: European Banking Group Implementation

8.1 Organization Profile

- Industry: Pan-European Banking Group
- Regulatory Status: Significant Institution (SSM supervised)
- Employees: 28,000 across 12 EU member states
- IT Security Team: 89 professionals
- Annual security budget: €18 million
- Regulatory requirements: NIS2 (essential entity) + DORA (credit institution)

8.2 Implementation Approach

The organization implemented CPF integration over 6 months in preparation for DORA compliance:

Phase 1 Results (30 days):

- Gap analysis identified 18 high-priority human factor compliance gaps
- Management body assessment revealed 72% showing automation bias indicators
- 41% of critical function personnel demonstrated authority transfer vulnerabilities
- Third-party human risk gaps identified in 67% of critical ICT providers

Phase 2 Results (90 days):

- 34% reduction in social engineering incident success rate
- 27% improvement in incident detection time for human-enabled threats
- Management decision quality under stress improved by 31%
- DORA Article 5 compliance evidence strengthened significantly

Phase 3 Results (180 days):

- 47% reduction in total human-factor security incidents
- Full integration with DORA five pillars compliance program
- 91% improvement in stress-condition response quality
- 187% ROI in first year
- €2.8 million in avoided incident costs
- Positive regulatory assessment from national competent authority

8.3 Regulatory Compliance Benefits

NIS2 Compliance Enhancements:

- Demonstrated "state of the art" measures for human factors (Art. 21)
- Quantifiable evidence of management accountability (Art. 20)
- Enhanced incident root cause analysis capabilities
- Improved supply chain human risk documentation

DORA Compliance Enhancements:

- Documented management body knowledge assessment (Art. 5)
- Human factor integration in ICT risk framework (Art. 6)
- Enhanced resilience testing with human factors (Art. 25)
- Comprehensive third-party human risk register (Art. 28)

9 Implementation Guidance and Best Practices

9.1 Pre-Implementation Checklist

Regulatory Readiness:

- Current NIS2/DORA compliance status assessed
- Competent authority expectations understood
- Regulatory reporting requirements mapped
- Evidence documentation framework established

Organizational Readiness:

- Executive sponsorship from CISO and compliance leadership
- Budget allocation for human factor assessment tools
- Privacy impact assessment completed for psychological assessments
- Works council/employee representative consultation (where required)

Technical Prerequisites:

- ICT risk management framework operational
- Incident management processes documented
- Resilience testing program established
- Third-party risk management procedures in place

9.2 European-Specific Considerations

Data Protection Compliance:

- GDPR Article 6 legal basis for psychological assessments
- Data minimization in assessment design
- Retention periods aligned with regulatory requirements
- Cross-border transfer considerations for multi-entity groups

Employee Relations:

- Transparency in assessment purposes and use
- Non-discriminatory application of psychological profiling
- Works council consultation where legally required
- Individual rights to access assessment results

Regulatory Engagement:

- Proactive discussion with national competent authorities
- Alignment with sectoral CSIRT expectations
- Integration with peer review processes
- Documentation suitable for regulatory audit

9.3 Common Implementation Pitfalls

Regulatory Pitfalls:

- Treating CPF as replacement for technical compliance rather than enhancement
- Inadequate documentation for regulatory evidence requirements
- Failure to align with national transposition variations (NIS2)
- Underestimating cross-border coordination requirements

Organizational Pitfalls:

- Insufficient privacy impact assessment
- Lack of works council engagement where required
- Over-emphasis on assessment without intervention programs
- Failure to integrate with existing GRC processes

Technical Pitfalls:

- Siloed implementation separate from ICT risk framework
- Inadequate integration with incident management systems
- Poor reporting alignment with regulatory requirements
- Insufficient third-party integration protocols

10 Future Regulatory Developments

10.1 Evolving European Landscape

The CPF integration framework is designed to accommodate evolving regulatory requirements:

Expected Developments:

- ENISA technical guidance on human factors (expected 2025-2026)
- ESA regulatory technical standards on testing methodologies
- National competent authority guidance on "state of the art" requirements

- EU-CyCLONe coordination procedures for cross-border incidents

Framework Adaptability:

- Modular CPF category mapping enables regulatory update integration
- Measurement framework supports evolving reporting requirements
- Evidence documentation designed for audit trail continuity
- Continuous improvement model aligns with regulatory expectations

11 Conclusion and Next Steps

The integration of psychological risk assessment into NIS2 and DORA compliance programs addresses a critical gap in European operational resilience frameworks. While both regulations explicitly recognize human factors in cybersecurity, neither provides systematic methodologies for assessing and mitigating the psychological vulnerabilities that enable the majority of successful cyber attacks.

The Cybersecurity Psychology Framework offers a practical, measurable solution that enhances regulatory compliance while delivering operational resilience improvements. Through detailed mapping to NIS2 requirements and DORA's five pillars, organizations can implement psychological vulnerability assessment within their existing compliance programs.

Immediate Actions for European CISOs and Compliance Officers:

1. Conduct CPF-enhanced gap analysis against NIS2 Article 21 and DORA pillar requirements
2. Prioritize management body psychological assessment (DORA Article 5 compliance)
3. Integrate human factor testing into resilience testing programs
4. Establish third-party human risk assessment protocols
5. Develop regulatory evidence framework for psychological risk measures
6. Engage with national competent authorities on human factor compliance approach

For financial entities facing the January 2025 DORA deadline and essential service providers under NIS2 obligations, the CPF integration framework provides a structured path to comprehensive human factor compliance. Organizations implementing this approach achieve significant improvements in both regulatory compliance posture and operational resilience outcomes.

The evidence demonstrates that psychological risk assessment is not merely a compliance enhancement but a fundamental requirement for effective operational resilience in an environment where human factors contribute to the vast majority of security incidents. As European regulators increasingly focus on the quality and effectiveness of security measures, frameworks like CPF become essential components of demonstrably "appropriate and proportionate" security programs.

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 regulatory 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 in European regulatory contexts.

Data Availability Statement

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

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] Verizon. (2024). *2024 Data Breach Investigations Report.* Verizon Enterprise.

[3] European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333/80.

[4] European Parliament and Council. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union*, L 333/1.

[5] European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape: Finance Sector.* ENISA.

[6] EY and Institute of International Finance. (2024). *Global Bank Risk Management Survey: European Results.* EY.

[7] IBM Security. (2024). *Cost of a Data Breach Report 2024.* IBM Corporation.

[8] European Central Bank. (2024). One step ahead: protecting the cyber resilience of financial infrastructures. Speech by Piero Cipollone.

[9] European Securities and Markets Authority. (2024). *Digital Operational Resilience Act (DORA) Implementation Guidance.* ESMA.

[10] European Banking Authority. (2024). *Guidelines on ICT and Security Risk Management.* EBA.