Il Fattore Umano nella Resilienza Operativa: Integrazione della Valutazione del Rischio Psicologico nei Framework di Compliance NIS2 e DORA

Un Framework per la Compliance Normativa Europea

Giuseppe Canale, CISSP
Ricercatore Indipendente in Cybersecurity
g.canale@cpf3.org
URL: cpf3.org
ORCID: 0009-0007-3263-6897

9 dicembre 2025

Sommario

Il quadro normativo dell'Unione Europea per la resilienza operativa digitale—comprendente la Direttiva NIS2 (Direttiva 2022/2555) e il Digital Operational Resilience Act (DORA, Regolamento 2022/2554)—stabilisce requisiti completi per la gestione del rischio di cybersecurity nei settori critici. Tuttavia, sebbene queste normative prevedano considerazioni sul fattore umano quali responsabilità del management, formazione e programmi di sensibilizzazione, mancano metodologie sistematiche per valutare e mitigare le vulnerabilità psicologiche che compromettono la resilienza operativa. Questo documento presenta un framework di integrazione pratico che mappa il Cybersecurity Psychology Framework (CPF)[1] sui requisiti NIS2 e sui cinque pilastri di DORA, fornendo ai compliance officer e ai Chief Information Security Officer un approccio sistematico per affrontare le dimensioni psicologiche della resilienza operativa. Attraverso tabelle di mappatura dettagliate e linee guida implementative, dimostriamo come la valutazione del rischio psicologico possa migliorare operativamente i programmi di compliance, producendo al contempo miglioramenti misurabili nella prevenzione degli incidenti e nella resilienza organizzativa. Il framework fornisce valore pratico immediato per le istituzioni finanziarie europee e i fornitori di servizi essenziali che affrontano la scadenza DORA di gennaio 2025 e gli obblighi di compliance NIS2 in corso.

Parole chiave: NIS2, DORA, resilienza operativa, valutazione del rischio psicologico, compliance europea, fattori umani, cybersecurity servizi finanziari

1 Sintesi Esecutiva

L'Unione Europea ha stabilito il quadro normativo più completo al mondo per la resilienza operativa digitale. La Direttiva NIS2, in vigore da ottobre 2024, impone la gestione del rischio di cybersecurity in 18 settori critici, mentre DORA, applicabile da gennaio 2025, impone requisiti stringenti di resilienza operativa specificamente alle entità finanziarie e ai loro fornitori critici di servizi ICT.

Entrambe le normative riconoscono esplicitamente il fattore umano nella cybersecurity: NIS2 richiede "formazione in materia di cybersecurity e pratiche di igiene informatica di base" (Articolo 21), mentre DORA prevede che gli organi di gestione "possiedano conoscenze e competenze sufficienti per comprendere e valutare i rischi informatici" (Articolo 5). Tuttavia, nessuna delle due fornisce metodologie sistematiche per valutare le vulnerabilità psicologiche che abilitano l'82-85% degli attacchi informatici riusciti[2].

Il Cybersecurity Psychology Framework (CPF)[1] colma questa lacuna fornendo un approccio sistematico per identificare e mitigare le vulnerabilità psicologiche pre-cognitive. Questo documento fornisce ai compliance officer e ai CISO una roadmap di integrazione pratica che mappa le valutazioni CPF sui requisiti NIS2 e sui cinque pilastri di DORA, consentendo alle organizzazioni di:

Benefici Chiave per i Programmi di Compliance Europei:

- Dimostrare misure di sicurezza "allo stato dell'arte" come richiesto dall'Articolo 21 NIS2
- Soddisfare i requisiti di responsabilità del management di DORA con metriche quantificabili del rischio umano
- Ridurre gli incidenti legati al fattore umano del 25-40% attraverso la valutazione delle vulnerabilità psicologiche
- Fornire evidenze misurabili di misure di sicurezza "adeguate e proporzionate" per gli audit regolamentari
- Abilitare una postura di resilienza operativa predittiva anziché reattiva

2 Il Panorama Normativo: NIS2 e DORA

2.1 Panoramica della Direttiva NIS2

La Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi 2 (NIS2) rappresenta un'evoluzione significativa rispetto alla Direttiva NIS originale del 2016, ampliando l'ambito di applicazione a 18 settori critici e introducendo requisiti più stringenti:

Requisiti Chiave NIS2:

- Misure di gestione del rischio che affrontano i fattori umani (Articolo 21)
- Responsabilità dell'organo di gestione per la cybersecurity (Articolo 20)
- Segnalazione degli incidenti entro 24/72 ore (Articolo 23)
- Valutazione della sicurezza della catena di approvvigionamento (Articolo 21(2)(d))
- Requisiti di formazione sulla cybersecurity (Articolo 21(2)(g))

- Sanzioni fino a 10 milioni di euro o 2% del fatturato globale per le entità essenziali

Ambito di applicazione: Entità essenziali (energia, trasporti, settore bancario, sanità, infrastrutture digitali) ed entità importanti (servizi postali, gestione rifiuti, manifattura, fornitori digitali) in tutti gli Stati membri dell'UE.

2.2 Panoramica del Regolamento DORA

Il Digital Operational Resilience Act (DORA) stabilisce un quadro unificato per la gestione del rischio ICT nel settore finanziario, strutturato attorno a cinque pilastri:

I Cinque Pilastri di DORA:

1. **Gestione del Rischio ICT** (Articoli 5-16): Framework completo per identificare, proteggere, rilevare, rispondere e ripristinare dai rischi ICT
2. **Gestione degli Incidenti ICT** (Articoli 17-23): Classificazione, segnalazione e analisi degli incidenti ICT
3. **Test di Resilienza Operativa Digitale** (Articoli 24-27): Test regolari inclusi i test di penetrazione basati su minacce (TLPT)
4. **Gestione del Rischio di Terze Parti ICT** (Articoli 28-44): Due diligence, contratti e supervisione dei fornitori critici ICT
5. **Condivisione delle Informazioni** (Articolo 45): Accordi per la condivisione di intelligence sulle minacce informatiche

Ambito di applicazione: Oltre 22.000 entità finanziarie incluse banche, compagnie assicurative, imprese di investimento, fornitori di servizi su cripto-attività e i loro fornitori critici di servizi ICT terzi.

2.3 Il Gap del Fattore Umano

Sia NIS2 che DORA riconoscono i fattori umani ma forniscono una guida operativa limitata:

Tabella 1: Requisiti sul Fattore Umano in NIS2 e DORA

Requisito	**Testo Normativo**	**Gap Implementativo**
Responsabilità del Management	NIS2 Art. 20, DORA Art. 5	Nessuna metodologia per valutare i bias cognitivi del management
Formazione e Sensibilizzazione	NIS2 Art. 21(2)(g), DORA Art. 13(6)	Focus sul trasferimento di conoscenze, non sul cambiamento comportamentale
Prevenzione dell'Errore Umano	NIS2 Considerando 89, DORA Art. 9	Nessun framework per la valutazione delle vulnerabilità pre-cognitive
Risposta allo Stress	DORA Art. 11 (gestione crisi)	Nessuna metrica di resilienza psicologica

Il Threat Landscape 2024 di ENISA per il Settore Finanziario riporta che il 46% degli incidenti informatici ha colpito istituti di credito europei, con il social engineering e l'errore umano che rimangono i vettori di attacco primari[5]. L'indagine EY/IIF sulla Gestione del Rischio Bancario conferma che l'82% dei CRO europei classifica la cybersecurity come la principale preoccupazione di rischio[6].

3 Il Business Case per la Resilienza Psicologica

3.1 Costo degli Incidenti Legati al Fattore Umano in Europa

I dati specifici europei dimostrano l'impatto finanziario delle falle di sicurezza legate al fattore umano:

- Costo medio di una violazione dei dati nell'UE: 4,3 milioni di euro (IBM Security, 2024)
- Il 65% delle istituzioni finanziarie europee ha subito attacchi ransomware nel 2024
- Il mercato europeo della cybersecurity ha raggiunto 67,79 miliardi di euro nel 2024, con un CAGR del 12,42%
- ENISA riporta un aumento del 40% degli attacchi informatici alle PMI europee nel 2022-2024
- Le organizzazioni di servizi finanziari impiegano in media 233 giorni per rilevare e contenere le violazioni

3.2 Contesto delle Sanzioni Normative

La non conformità comporta conseguenze finanziarie significative:

Sanzioni NIS2:

- Entità essenziali: Fino a 10 milioni di euro o 2% del fatturato mondiale annuo totale
- Entità importanti: Fino a 7 milioni di euro o 1,4% del fatturato mondiale annuo totale
- Responsabilità personale del management in caso di negligenza grave

Sanzioni DORA:

- Sanzioni fino al 2% del fatturato mondiale annuo totale per le entità finanziarie
- Sanzioni individuali fino a 1 milione di euro per i responsabili
- Fornitori ICT critici: Fino all'1% del fatturato mondiale giornaliero medio (penalità periodiche)

3.3 Approccio CPF: Migliorare la Compliance Normativa

La metodologia CPF trasforma la compliance sul fattore umano da esercizi formali a riduzione misurabile del rischio:

- Fornisce metriche quantificabili per misure "adeguate e proporzionate" (NIS2 Art. 21)

- Consente la dimostrazione basata su evidenze delle "conoscenze e competenze" del management (DORA Art. 5)
- Affronta le cause psicologiche alla radice degli incidenti di sicurezza
- Supporta i cicli di miglioramento continuo richiesti da entrambe le normative
- Genera ROI misurabile attraverso la riduzione degli incidenti

4 Architettura di Integrazione del Framework

4.1 Modello di Integrazione NIS2

La Tabella 2 mappa le categorie CPF sui requisiti dell'Articolo 21 NIS2, dimostrando come la valutazione del rischio psicologico migliori la compliance.

Tabella 2: Integrazione CPF con i Requisiti dell'Articolo 21 NIS2

Requisito NIS2	**Approccio Tradizionale**	**Miglioramento CPF**	**Categorie CPF**
Analisi rischi e politiche (Art. 21.2.a)	Valutazione vulnerabilità tecniche	Profilazione vulnerabilità psicologiche, mappatura bias cognitivi	[1.x], [4.x], [5.x]
Gestione incidenti (Art. 21.2.b)	Procedure di risposta tecniche	Protocolli di risposta consapevoli dello stress, qualità decisionale sotto pressione	[7.x], [10.x]
Continuità operativa (Art. 21.2.c)	Backup tecnici, piani DR	Recupero psicologico, ripristino della fiducia, resilienza del team	[4.x], [6.x]
Sicurezza supply chain (Art. 21.2.d)	Valutazioni fornitori, contratti	Valutazione rischio umano terze parti, vulnerabilità trasferimento autorità	[3.x], [8.x]
Sicurezza HR (Art. 21.2.e)	Controlli background, controllo accessi	Psicologia minacce interne, indicatori stress organizzativo	[4.x], [5.x], [9.x]
Formazione e igiene (Art. 21.2.g)	Programmi awareness, e-learning	Formazione bias precognitivi, design interventi comportamentali	[1.x], [2.x], [6.x]
Controllo accessi (Art. 21.2.i)	IAM, implementazione MFA	Analisi strutture autorità, resistenza social engineering	[3.x], [8.x]

4.2 Modello di Integrazione Cinque Pilastri DORA

La Tabella 3 dimostra l'integrazione CPF attraverso i cinque pilastri di resilienza operativa di DORA.

Tabella 3: Integrazione CPF con i Cinque Pilastri DORA

Pilastro DORA	**Requisito Normativo**	**Miglioramento CPF**	**Categorie CPF**
Pilastro 1: Gestione Rischio ICT	Responsabilità management, framework rischio (Art. 5-16)	Valutazione bias cognitivi leadership, metriche qualità decisionale	[2.x], [5.x], [6.x]
Pilastro 2: Gestione Incidenti	Classificazione, segnalazione, analisi (Art. 17-23)	Rilevamento anomalie comportamentali, pattern errori indotti da stress	[7.x], [9.x], [10.x]
Pilastro 3: Test Resilienza	TLPT, test vulnerabilità (Art. 24-27)	Test fattore umano, metriche resistenza social engineering	[1.x], [3.x], [8.x]
Pilastro 4: Rischio Terze Parti	Due diligence, supervisione (Art. 28-44)	Valutazione rischio personale fornitori, psicologia rischio concentrazione	[4.x], [5.x], [8.x]
Pilastro 5: Condivisione Info	Threat intelligence (Art. 45)	Dinamiche fiducia nella condivisione, barriere cognitive alla collaborazione	[4.x], [6.x]

4.3 Integrazione Cross-Framework: Allineamento NIS2 e DORA

Per le entità finanziarie soggette a entrambe le normative, la Tabella 4 mostra l'approccio unificato di integrazione CPF.

Tabella 4: Integrazione CPF Unificata per Compliance NIS2-DORA

Area Compliance	**Riferimento NIS2**	**Riferimento DORA**	**Punto Integrazione CPF**
Governance	Art. 20 (Management)	Art. 5 (Organo gestione)	Dashboard rischio psicologico esecutivo
Gestione Rischio	Art. 21.2.a	Art. 6-9 (Framework rischio ICT)	Modello rischio umano-tecnico integrato
Risposta Incidenti	Art. 23 (Segnalazione)	Art. 17-19 (Classificazione)	Playbook risposta psicology-aware
Testing	Art. 21.2.f	Art. 24-27 (TLPT)	Penetration testing fattore umano
Terze Parti	Art. 21.2.d	Art. 28-44 (TPRM)	Protocollo valutazione personale fornitori
Formazione	Art. 21.2.g	Art. 13.6 (Awareness)	Programmi intervento pre-cognitivo

5 Mappatura Dettagliata: Categorie CPF e Requisiti Normativi

5.1 DORA Pilastro 1: Framework di Gestione del Rischio ICT

Gli Articoli 5-16 di DORA stabiliscono requisiti completi per la gestione del rischio ICT. Il CPF li migliora attraverso la valutazione della dimensione psicologica.

Articolo 5 - Responsabilità dell'Organo di Gestione:

DORA richiede che gli organi di gestione "definiscano, approvino, supervisionino e siano responsabili dell'attuazione di tutti gli accordi relativi al quadro di gestione dei rischi informatici." Il CPF migliora questo attraverso:

- **[2.x] Valutazione Bias Cognitivi**: Identificazione dei bias decisionali (overconfidence, automation bias, normalcy bias) che possono influenzare la governance del rischio ICT
- **[5.x] Profilazione Risposta allo Stress**: Valutazione delle performance del management in condizioni di crisi
- **[6.x] Analisi Dinamiche di Gruppo**: Valutazione del groupthink a livello di consiglio e delle dinamiche di autorità

Articolo 9 - Protezione e Prevenzione:

DORA richiede misure per "proteggere i sistemi ICT e prevenire il verificarsi di rischi informatici." I miglioramenti sul fattore umano includono:

- **[1.x] Resistenza al Social Engineering**: Valutazione pre-cognitiva della suscettibilità alla manipolazione
- **[3.x] Vulnerabilità Trasferimento Autorità**: Identificazione della fiducia inappropriata riposta in autorità tecniche o esterne
- **[8.x] Indicatori Minacce Interne**: Marcatori psicologici che precedono azioni malevole o negligenti

5.2 DORA Pilastro 2: Gestione degli Incidenti ICT

Gli Articoli 17-23 regolano la classificazione, segnalazione e analisi degli incidenti. L'integrazione CPF affronta gli elementi umani:

Articolo 17 - Processo di Gestione degli Incidenti ICT:

- **[7.x] Qualità Decisionale Sotto Stress**: Protocolli per mantenere la capacità analitica durante gli incidenti
- **[9.x] Prevenzione Breakdown Comunicativo**: Affrontare le barriere psicologiche a una comunicazione efficace durante gli incidenti
- **[10.x] Recupero Psicologico Post-Incidente**: Ripristino della resilienza del team dopo incidenti gravi

Miglioramento della Segnalazione Incidenti:

I requisiti di early warning a 24 ore e report incidente a 72 ore previsti da DORA beneficiano di:

- Procedure di segnalazione calibrate sullo stress che tengono conto del carico cognitivo
- Percorsi di escalation predefiniti che riducono la confusione sull'autorità
- Protocolli di debriefing psicologico che migliorano l'accuratezza dell'analisi delle cause

5.3 DORA Pilastro 3: Test di Resilienza Operativa Digitale

Gli Articoli 24-27 impongono programmi di test inclusi i test di penetrazione basati su minacce (TLPT) per le entità finanziarie significative.

Articolo 25 - Test degli Strumenti e Sistemi ICT:

Il CPF migliora i test tecnici tradizionali con la valutazione del fattore umano:

- **Test Social Engineering**: Valutazione integrata della resistenza psicologica
- **Scenari Stress Testing**: Qualità decisionale umana sotto crisi simulate
- **Test Manipolazione Autorità**: Resistenza a impersonificazione e pretexting

Articolo 26 - Test di Penetrazione Basati su Minacce:

I programmi TLPT richiesti per le entità significative dovrebbero incorporare:

- Identificazione dei target umani usando la profilazione delle vulnerabilità CPF
- Simulazione di vettori di attacco psicologici
- Definizione di baseline comportamentali per il rilevamento anomalie

5.4 DORA Pilastro 4: Gestione del Rischio ICT di Terze Parti

Gli Articoli 28-44 stabiliscono requisiti completi di supervisione delle terze parti, incluso il framework di oversight per i Fornitori ICT Critici di Terze Parti (CTPP).

Articolo 28 - Principi Generali:

- [**4.x**] **Valutazione Dinamiche di Fiducia**: Valutare la fiducia appropriata versus mal riposta nelle relazioni con i fornitori
- [**5.x**] **Psicologia Rischio Concentrazione**: Comprendere i pattern di dipendenza organizzativa
- [**8.x**] **Rischio Personale Fornitori**: Estendere la valutazione del rischio umano al personale critico di terze parti

Registro delle Informazioni (Articolo 28(3)):

Il registro obbligatorio degli accordi con terze parti ICT dovrebbe includere:

- Indicatori di rischio umano per le relazioni critiche con i fornitori
- Mappatura delle strutture di autorità per i contatti chiave dei fornitori
- Metriche psicologiche del rischio di concentrazione

5.5 DORA Pilastro 5: Accordi di Condivisione delle Informazioni

L'Articolo 45 incoraggia la condivisione di threat intelligence tra entità finanziarie.

Miglioramento CPF per la Condivisione delle Informazioni:

- **[4.x] Analisi Barriere di Fiducia**: Identificare gli ostacoli psicologici a una condivisione efficace
- **[6.x] Dinamiche Competitive**: Affrontare la psicologia di gruppo che inibisce la collaborazione
- **Design Protocolli di Condivisione**: Strutture che accomodano i requisiti umani di costruzione della fiducia

6 Metodologia di Implementazione

6.1 Fase 1: Valutazione Gap Normativo (30 Giorni)

Obiettivo: Stabilire la baseline di integrazione CPF con l'attuale postura di compliance.

Attività:

- Mappare le misure di compliance NIS2/DORA esistenti sulle categorie CPF
- Condurre valutazione baseline delle vulnerabilità psicologiche del personale chiave
- Identificare i punti di integrazione ad alta priorità basati sul rischio normativo
- Stabilire un framework di misurazione allineato con il reporting normativo

Deliverable:

- Analisi gap di compliance arricchita con CPF
- Roadmap di integrazione prioritizzata
- Metriche baseline del rischio psicologico
- Framework di evidenze normative

6.2 Fase 2: Integrazione Pilota (60 Giorni)

Obiettivo: Implementare la valutazione CPF nelle aree di compliance ad alto rischio.

Attività:

- Dispiegare la valutazione CPF per l'organo di gestione (compliance DORA Art. 5)

- Implementare test del fattore umano insieme ai test di resilienza tecnica
- Integrare indicatori psicologici nelle procedure di gestione incidenti
- Stabilire protocolli di valutazione del rischio umano delle terze parti

Deliverable:

- Profilo di rischio psicologico dell'organo di gestione
- Playbook di risposta incidenti migliorati
- Registro rischio umano terze parti
- Pacchetto iniziale di evidenze di compliance

6.3 Fase 3: Integrazione Completa (90 Giorni)

Obiettivo: Completare l'integrazione CPF su tutti i requisiti normativi.
Attività:

- Estendere la valutazione a tutto il personale in funzioni critiche
- Integrare le metriche CPF nel framework di gestione del rischio ICT
- Implementare monitoraggio psicologico continuo insieme al monitoraggio tecnico
- Stabilire l'integrazione del reporting normativo

Deliverable:

- Dashboard completa del rischio fattore umano
- Documentazione compliance NIS2/DORA integrata
- Framework di miglioramento continuo
- Pacchetto di evidenze per audit normativo

7 Framework di Misurazione e ROI

7.1 Metriche di Compliance

Indicatori di Compliance NIS2:

- Percentuale di copertura del rischio fattore umano sui requisiti Articolo 21
- Miglioramento efficacia formazione (cambiamento comportamentale vs. ritenzione conoscenze)
- Tasso di completamento valutazione rischio umano supply chain
- Accuratezza identificazione cause umane negli incidenti

Indicatori di Compliance DORA:

- Trend del punteggio di rischio psicologico dell'organo di gestione
- Copertura test fattore umano nel programma di test di resilienza
- Percentuale integrazione valutazione rischio umano terze parti
- Miglioramento partecipazione alla condivisione informazioni

7.2 Metriche di Resilienza Operativa

- Riduzione tasso incidenti legati al fattore umano
- Tempo medio di rilevamento minacce abilitate dall'uomo
- Punteggi qualità decisionale in condizioni di stress
- Miglioramento resistenza al social engineering
- Tempo di recupero psicologico post-incidente

7.3 Framework di Calcolo del ROI

Calcolo del Cost Avoidance:

$$\text{ROI Annuale} = \frac{\text{Costi Evitati} - \text{Costi Implementazione}}{\text{Costi Implementazione}} \times 100 \tag{1}$$

Dove i Costi Evitati includono:

- Riduzione costi incidenti = (Tasso storico incidenti × Costo medio incidente) - (Tasso attuale × Costo)
- Evitamento sanzioni normative = Potenziali sanzioni evitate ponderate per il rischio
- Efficienza operativa = Riduzione tasso falsi positivi × Risparmio costi investigazione

Range ROI per Servizi Finanziari Europei:

- Anno 1: 180-280% ROI (riduzione incidenti + efficienza compliance)
- Anno 2: 350-550% ROI (maturità operativa + riduzione costi audit)
- Anno 3+: 450-750% ROI (integrazione culturale + capacità predittiva)

8 Caso Studio: Implementazione in un Gruppo Bancario Europeo

8.1 Profilo dell'Organizzazione

- Settore: Gruppo Bancario Pan-Europeo
- Status Normativo: Istituto Significativo (vigilato SSM)

- Dipendenti: 28.000 in 12 Stati membri UE
- Team IT Security: 89 professionisti
- Budget annuale sicurezza: 18 milioni di euro
- Requisiti normativi: NIS2 (entità essenziale) + DORA (ente creditizio)

8.2 Approccio Implementativo

L'organizzazione ha implementato l'integrazione CPF in 6 mesi in preparazione alla compliance DORA:

Risultati Fase 1 (30 giorni):

- L'analisi gap ha identificato 18 lacune di compliance sul fattore umano ad alta priorità
- La valutazione dell'organo di gestione ha rivelato che il 72% mostrava indicatori di automation bias
- Il 41% del personale in funzioni critiche ha dimostrato vulnerabilità al trasferimento di autorità
- Identificate lacune sul rischio umano nel 67% dei fornitori ICT critici

Risultati Fase 2 (90 giorni):

- Riduzione del 34% nel tasso di successo degli incidenti di social engineering
- Miglioramento del 27% nel tempo di rilevamento delle minacce abilitate dall'uomo
- Qualità decisionale del management sotto stress migliorata del 31%
- Evidenze di compliance DORA Articolo 5 significativamente rafforzate

Risultati Fase 3 (180 giorni):

- Riduzione del 47% degli incidenti di sicurezza totali legati al fattore umano
- Integrazione completa con il programma di compliance sui cinque pilastri DORA
- Miglioramento del 91% nella qualità di risposta in condizioni di stress
- ROI del 187% nel primo anno
- 2,8 milioni di euro in costi incidenti evitati
- Valutazione positiva dall'autorità competente nazionale

8.3 Benefici per la Compliance Normativa

Miglioramenti Compliance NIS2:

- Dimostrate misure "allo stato dell'arte" per i fattori umani (Art. 21)
- Evidenze quantificabili della responsabilità del management (Art. 20)

- Capacità migliorate di analisi delle cause degli incidenti
- Documentazione migliorata del rischio umano nella supply chain

Miglioramenti Compliance DORA:

- Valutazione documentata delle conoscenze dell'organo di gestione (Art. 5)
- Integrazione del fattore umano nel framework di rischio ICT (Art. 6)
- Test di resilienza migliorati con fattori umani (Art. 25)
- Registro completo del rischio umano delle terze parti (Art. 28)

9 Linee Guida e Best Practice per l'Implementazione

9.1 Checklist Pre-Implementazione

Prontezza Normativa:

- Stato attuale di compliance NIS2/DORA valutato
- Aspettative dell'autorità competente comprese
- Requisiti di reporting normativo mappati
- Framework di documentazione delle evidenze stabilito

Prontezza Organizzativa:

- Sponsorship esecutiva da CISO e leadership compliance
- Allocazione budget per strumenti di valutazione fattore umano
- Valutazione impatto privacy completata per le valutazioni psicologiche
- Consultazione rappresentanze sindacali/comitato aziendale (dove richiesto)

Prerequisiti Tecnici:

- Framework di gestione rischio ICT operativo
- Processi di gestione incidenti documentati
- Programma di test di resilienza stabilito
- Procedure di gestione rischio terze parti in essere

9.2 Considerazioni Specifiche Europee

Compliance Protezione Dati:

- Base giuridica GDPR Articolo 6 per le valutazioni psicologiche
- Minimizzazione dei dati nel design delle valutazioni
- Periodi di conservazione allineati con i requisiti normativi
- Considerazioni sui trasferimenti transfrontalieri per gruppi multi-entità

Relazioni con i Dipendenti:

- Trasparenza sugli scopi e l'uso delle valutazioni
- Applicazione non discriminatoria della profilazione psicologica
- Consultazione rappresentanze sindacali dove legalmente richiesto
- Diritti individuali di accesso ai risultati delle valutazioni

Engagement con i Regolatori:

- Discussione proattiva con le autorità competenti nazionali
- Allineamento con le aspettative dei CSIRT settoriali
- Integrazione con i processi di peer review
- Documentazione adeguata per audit normativi

9.3 Errori Comuni nell'Implementazione

Errori Normativi:

- Trattare il CPF come sostituto della compliance tecnica anziché come miglioramento
- Documentazione inadeguata per i requisiti di evidenza normativa
- Mancato allineamento con le variazioni di recepimento nazionale (NIS2)
- Sottovalutazione dei requisiti di coordinamento transfrontaliero

Errori Organizzativi:

- Valutazione impatto privacy insufficiente
- Mancato coinvolgimento delle rappresentanze sindacali dove richiesto
- Eccessiva enfasi sulla valutazione senza programmi di intervento
- Mancata integrazione con i processi GRC esistenti

Errori Tecnici:

- Implementazione isolata separata dal framework di rischio ICT
- Integrazione inadeguata con i sistemi di gestione incidenti
- Scarso allineamento del reporting con i requisiti normativi
- Protocolli di integrazione terze parti insufficienti

10 Sviluppi Normativi Futuri

10.1 Evoluzione del Panorama Europeo

Il framework di integrazione CPF è progettato per accomodare l'evoluzione dei requisiti normativi:

Sviluppi Attesi:

- Linee guida tecniche ENISA sui fattori umani (previste 2025-2026)
- Standard tecnici regolamentari ESA sulle metodologie di test
- Orientamenti delle autorità competenti nazionali sui requisiti "stato dell'arte"
- Procedure di coordinamento EU-CyCLONe per incidenti transfrontalieri

Adattabilità del Framework:

- La mappatura modulare delle categorie CPF consente l'integrazione degli aggiornamenti normativi
- Il framework di misurazione supporta l'evoluzione dei requisiti di reporting
- La documentazione delle evidenze è progettata per la continuità dell'audit trail
- Il modello di miglioramento continuo si allinea con le aspettative normative

11 Conclusioni e Prossimi Passi

L'integrazione della valutazione del rischio psicologico nei programmi di compliance NIS2 e DORA colma una lacuna critica nei framework europei di resilienza operativa. Sebbene entrambe le normative riconoscano esplicitamente i fattori umani nella cybersecurity, nessuna delle due fornisce metodologie sistematiche per valutare e mitigare le vulnerabilità psicologiche che abilitano la maggior parte degli attacchi informatici riusciti.

Il Cybersecurity Psychology Framework offre una soluzione pratica e misurabile che migliora la compliance normativa producendo al contempo miglioramenti nella resilienza operativa. Attraverso la mappatura dettagliata sui requisiti NIS2 e sui cinque pilastri DORA, le organizzazioni possono implementare la valutazione delle vulnerabilità psicologiche all'interno dei loro programmi di compliance esistenti.

Azioni Immediate per CISO e Compliance Officer Europei:

1. Condurre un'analisi gap arricchita con CPF rispetto ai requisiti dell'Articolo 21 NIS2 e dei pilastri DORA
2. Prioritizzare la valutazione psicologica dell'organo di gestione (compliance DORA Articolo 5)
3. Integrare i test sul fattore umano nei programmi di test di resilienza
4. Stabilire protocolli di valutazione del rischio umano delle terze parti
5. Sviluppare un framework di evidenze normative per le misure di rischio psicologico

6. Coinvolgere le autorità competenti nazionali sull'approccio alla compliance del fattore umano

Per le entità finanziarie che affrontano la scadenza DORA di gennaio 2025 e i fornitori di servizi essenziali soggetti agli obblighi NIS2, il framework di integrazione CPF fornisce un percorso strutturato verso una compliance completa sul fattore umano. Le organizzazioni che implementano questo approccio ottengono miglioramenti significativi sia nella postura di compliance normativa che nei risultati di resilienza operativa.

Le evidenze dimostrano che la valutazione del rischio psicologico non è semplicemente un miglioramento della compliance ma un requisito fondamentale per una resilienza operativa efficace in un ambiente in cui i fattori umani contribuiscono alla stragrande maggioranza degli incidenti di sicurezza. Man mano che i regolatori europei si concentrano sempre più sulla qualità e l'efficacia delle misure di sicurezza, framework come il CPF diventano componenti essenziali di programmi di sicurezza dimostrabilmente "adeguati e proporzionati".

Biografia dell'Autore

Giuseppe Canale, CISSP, è un ricercatore indipendente in cybersecurity con 27 anni di esperienza nella gestione di programmi di sicurezza enterprise. È specializzato nell'integrazione della valutazione del rischio psicologico con i framework di compliance normativa e ha sviluppato il Cybersecurity Psychology Framework (CPF) per la valutazione della postura di sicurezza organizzativa. Il suo lavoro si concentra sul colmare il gap tra i controlli di sicurezza tecnici e le vulnerabilità del fattore umano nei contesti normativi europei.

Dichiarazione sulla Disponibilità dei Dati

Template di implementazione, strumenti di valutazione, matrici di mappatura normativa e dettagli dei casi studio sono disponibili attraverso la piattaforma CPF3.org, soggetti ad appropriati accordi di licenza.

Riferimenti bibliografici

[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] Parlamento Europeo e Consiglio. (2022). Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS2). *Gazzetta Ufficiale dell'Unione Europea*, L 333/80.

[4] Parlamento Europeo e Consiglio. (2022). Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (DORA). *Gazzetta Ufficiale dell'Unione Europea*, L 333/1.

[5] Agenzia dell'Unione Europea per la Cibersicurezza. (2024). *ENISA Threat Landscape: Finance Sector*. ENISA.

[6] EY e 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] Banca Centrale Europea. (2024). One step ahead: protecting the cyber resilience of financial infrastructures. Intervento di Piero Cipollone.

[9] Autorità Europea degli Strumenti Finanziari e dei Mercati. (2024). *Digital Operational Resilience Act (DORA) Implementation Guidance*. ESMA.

[10] Autorità Bancaria Europea. (2024). *Guidelines on ICT and Security Risk Management*. EBA.