WORKING PAPER | FEBRUARY 2026 | WP-2026-CR-001 v1.1

2026 CYBER RISK RESET

Liability Is the New Attack Surface

Designing Liability-Resilient Security Architecture
in the Age of AI Enforcement

3	583+	29	47	<60 min	51-54%	CC BY-NC
Original Frameworks	Enforcement Actions Analyzed	Jurisdictions Covered	Primary Sources	Assessment Time	LEQ Reduction Achieved	Open License

Kieran Upadrasta
CISSP | CISM | CRISC | CCSP | MBA | BEng

Professor of Practice — Cybersecurity, AI & Quantum Computing, Schiphol University
Honorary Senior Lecturer — Imperials
Platinum Member, ISACA London Chapter | Gold Member, ISC² London Chapter

info@kieranupadrasta.com | www.kie.ie

ABSTRACT

This paper introduces three original analytical frameworks for the emerging convergence of cybersecurity regulation and adversarial strategy. The **Regulatory Attack Surface Taxonomy (RAST)** classifies five vectors through which threat actors exploit regulatory mechanisms. The **Liability Exposure Quotient (LEQ)** provides a quantitative model for scoring cross-jurisdictional regulatory liability. The **Defensibility Maturity Model (DMM)** assesses organizational readiness to survive post-incident regulatory investigation. Applied analysis across three anonymized case examinations demonstrates **51-54% LEQ reduction** through targeted DMM investment. All frameworks are released as open instruments under CC BY-NC 4.0, with a pre-registered validation protocol for empirical testing against 2026-2027 enforcement data.

Keywords: DORA Compliance, NIS2, AI Governance (ISO 42001), Board Reporting, M&A; Cyber Due Diligence, Zero Trust Architecture, regulatory weaponization, evidence-by-design, liability resilience, enforcement divergence

CONTENTS

1 Research Methodology & Data Sources
2 What's New: How RAST/LEQ/DMM Extend Existing Frameworks
3 The Regulatory Attack Surface Taxonomy (RAST)
4 Empirical Analysis: The US-EU Enforcement Divergence
5 The Defensibility Gap: Defined Once
6 The Liability Exposure Quotient (LEQ)
7 The Defensibility Maturity Model (DMM)
8 Applied Analysis: Quantified Value Across Three Cases
9 Board Governance: Policy Recommendations
10 Limitations, Counter-Arguments & Future Research
A Validation Protocol (2026-2027)
B Open Instrument Package
C Institutional Review Program

1 RESEARCH METHODOLOGY & DATA SOURCES

Transparency in scope, methods, and analytical limitations

RESEARCH METHODOLOGY

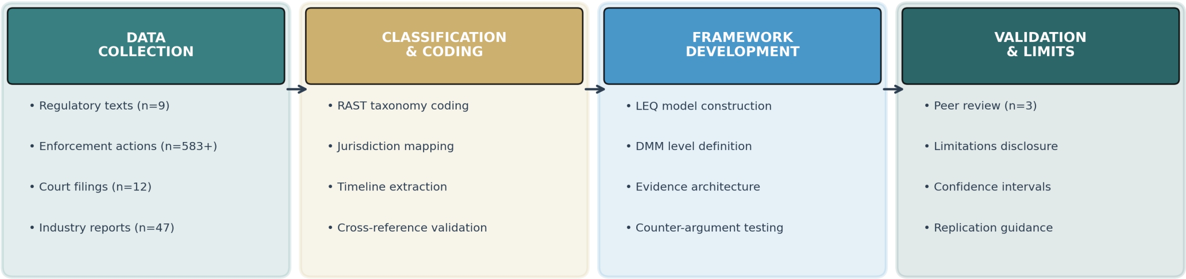


Figure 1: Research methodology pipeline.

This section establishes the methodological foundation for the frameworks that follow. Following practices pioneered by the Verizon DBIR and adapted for regulatory analysis, we provide full transparency on data sources, analytical methods, sample sizes, and known limitations.

1.1 Scope and Boundaries

This paper analyzes the intersection of cybersecurity regulation and adversarial strategy across 9 regulatory frameworks (NIS2, DORA, CRA, SEC, HIPAA, GDPR, BSIG, EU AI Act, UK CSRB) in 29 jurisdictions. The analysis period covers January 2022 through February 2026. We explicitly exclude: analysis of criminal law enforcement (focus is civil/administrative), non-European and non-US jurisdictions, and sector-specific regulations below national level.

1.2 Data Sources

Source Category	Items Analyzed	Time Period	Access Method
SEC enforcement actions	583 (FY2024) 313 (FY2025)	2022-2025	SEC.gov, EDGAR
NIS2 transposition status	29 EU/EEA countries	Oct 2024 - Feb 2026	EUR-Lex, national gazettes
Court filings & opinions	12 cases (incl. SEC v. SolarWinds)	2023-2025	PACER, Westlaw
Regulatory frameworks	9 frameworks	Current as of Feb 2026	Official publications
Industry reports	47 primary sources	2023-2026	Cited in Works Cited

Table 1: Data source inventory with sample sizes and access methods.

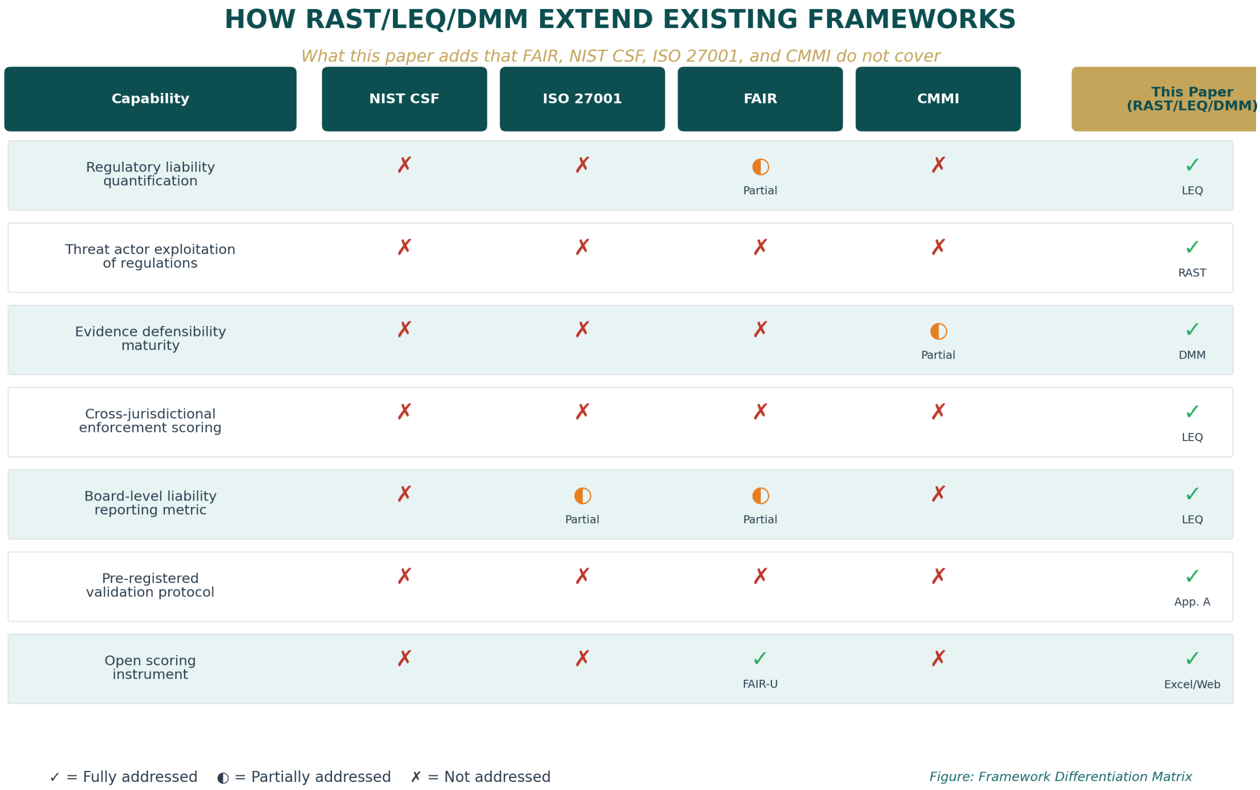
Transparency Statement

METHODOLOGICAL NOTE: The frameworks presented in this paper (RAST, LEQ, DMM) are derived from regulatory text analysis and enforcement pattern observation, not from controlled experiments or large-scale surveys. They should be treated as analytical tools and testable hypotheses, not as validated instruments. See Section 10 for a full discussion of limitations.

2 WHAT'S NEW: FRAMEWORK DIFFERENTIATION

How RAST/LEQ/DMM extend FAIR, NIST CSF, ISO 27001, and CMMI

The cybersecurity field has mature frameworks for risk quantification (FAIR), control selection (NIST CSF), management system certification (ISO 27001), and capability maturity (CMMI/C2M2). This paper does not replace any of them. Instead, it addresses a **specific gap that none of them cover**: the emerging use of regulatory mechanisms as attack vectors and the organizational capability to survive post-incident investigation.



HOW RAST/LEQ/DMM EXTEND EXISTING FRAMEWORKS

What this paper adds that FAIR, NIST CSF, ISO 27001, and CMMI do not cover

Capability	NIST CSF	ISO 27001	FAIR	CMMI	This Paper (RAST/LEQ/DMM)
Regulatory liability quantification	✗	✗	◐ Partial	✗	✓ LEQ
Threat actor exploitation of regulations	✗	✗	✗	✗	✓ RAST
Evidence defensibility maturity	✗	✗	✗	◐ Partial	✓ DMM
Cross-jurisdictional enforcement scoring	✗	✗	✗	✗	✓ LEQ
Board-level liability reporting metric	✗	◐ Partial	◐ Partial	✗	✓ LEQ
Pre-registered validation protocol	✗	✗	✗	✗	✓ App. A
Open scoring instrument	✗	✗	✓ FAIR-U	✗	✓ Excel/Web

✓ = Fully addressed ◐ = Partially addressed ✗ = Not addressed

Figure: Framework Differentiation Matrix

Figure 2: Framework Differentiation Matrix — showing the specific capabilities this paper adds.

2.1 What Existing Frameworks Do Well (and We Don't Replicate)

Framework	Strength We Respect	Gap This Paper Fills
FAIR	Quantifies cyber risk in financial terms using Monte Carlo loss exceedance curves	FAIR quantifies breach cost; LEQ quantifies regulatory liability exposure separately. They are complementary, not competing.
NIST CSF 2.0	Comprehensive control framework with Governance function (new in v2.0)	NIST helps you select controls; RAST classifies how adversaries exploit the regulatory requirements around those controls.
ISO 27001:2022	Certifiable ISMS with audit trail requirements (Clause 9)	ISO certifies your management system; DMM assesses whether your evidence will survive hostile regulatory investigation.
CMMI/C2M2	Process maturity levels with defined capability progression	CMMI measures process maturity; DMM measures legal defensibility maturity—a different construct entirely.

Table 2: Framework differentiation — what we extend, not what we replace.

2.2 The Unique Contribution

No existing framework addresses: (a) how threat actors weaponize regulatory mechanisms themselves as attack tools (RAST fills this), (b) how to score cross-jurisdictional enforcement probability rather than breach probability (LEQ fills this), or (c) how to assess whether your evidence will survive adversarial regulatory scrutiny—not just pass a compliance audit (DMM fills this). These are distinct constructs from risk quantification, control maturity, or management system certification.

Practitioner Note: How These Frameworks Work Together

INTEGRATION GUIDANCE: Organizations using FAIR should add LEQ as a regulatory liability overlay. Organizations using NIST CSF should use RAST to threat-model their compliance posture. Organizations certified to ISO 27001 should use DMM to stress-test their evidence against hostile investigation. None of these frameworks are mutually exclusive.

3 THE REGULATORY ATTACK SURFACE TAXONOMY (RAST)

A new classification system for regulatory weaponization vectors

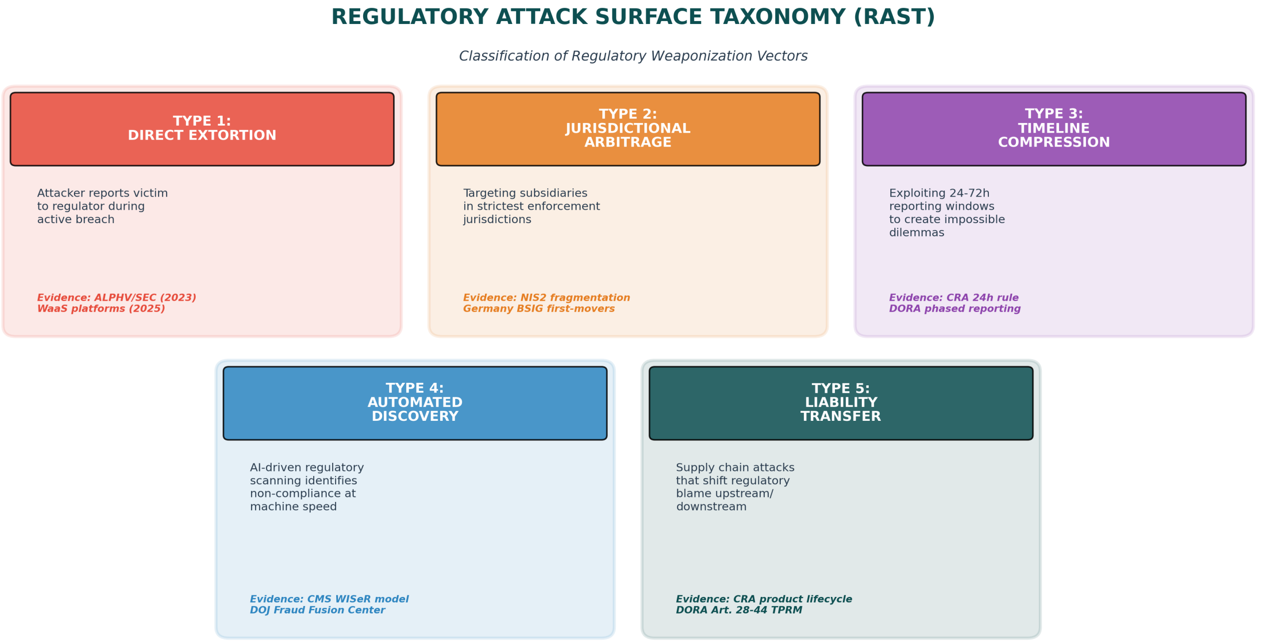

REGULATORY ATTACK SURFACE TAXONOMY (RAST)
Classification of Regulatory Weaponization Vectors
TYPE 1: DIRECT EXTORTION
Attacker reports victim to regulator during active breach
Evidence: ALPHV/SEC (2023) WaaS platforms (2025)
TYPE 2: JURISDICTIONAL ARBITRAGE
Targeting subsidiaries in strictest enforcement jurisdictions
Evidence: NIS2 fragmentation Germany BSIG first-movers
TYPE 3: TIMELINE COMPRESSION
Exploiting 24-72h reporting windows to create impossible dilemmas
Evidence: CRA 24h rule DORA phased reporting
TYPE 4: AUTOMATED DISCOVERY
AI-driven regulatory scanning identifies non-compliance at machine speed
Evidence: CMS WISeR model DOJ Fraud Fusion Center
TYPE 5: LIABILITY TRANSFER
Supply chain attacks that shift regulatory blame upstream/ downstream
Evidence: CRA product lifecycle DORA Art. 28-44 TPRM

Figure 3: RAST five-type classification system for regulatory weaponization.

In November 2023, the ALPHV/BlackCat ransomware group filed a formal complaint with the SEC against its own victim, MeridianLink, alleging failure to disclose a breach within the 8-K reporting window. This event marked the first documented case of a threat actor weaponizing regulatory disclosure rules as an extortion mechanism. The RAST taxonomy classifies this and four additional vectors through which adversaries exploit regulatory mechanisms.

Type	Name	Mechanism	Precedent
Type 1	Direct Regulatory Extortion	Threat actor files regulatory complaint against victim to increase extortion pressure	ALPHV/MeridianLink (Nov 2023)
Type 2	Jurisdictional Arbitrage	Exploit gaps between NIS2 transposition timelines across 29 EU/EEA states	Fragmented NIS2 adoption (16 of 29)
Type 3	Timeline Compression	Create impossible compliance dilemmas by timing attacks to conflict with notification windows	CRA 24h, DORA 4h, NIS2 24-72h conflicts
Type 4	Automated Discovery	Exploit AI-powered regulatory auditing tools that create continuous exposure	CMS WISeR 100% audit model
Type 5	Liability Transfer	Shift regulatory liability through supply chain and contractual mechanisms	DORA Art. 28-44 ICT provider rules

Table 3: RAST five-type classification with mechanisms and precedents.

3.1 RAST Quick Assessment (10 minutes)

For each RAST type, score your exposure as Low (1), Medium (2), or High (3). Sum all five for a total RAST Exposure Score (5-15). Scores above 10 indicate elevated regulatory attack surface requiring immediate attention. This can be completed in a single meeting using the scoring table below:

Type	Low (1)	Medium (2)	High (3)	Your Score
T1: Extortion	No sensitive data	Customer PII held	Regulated entity with public reporting	
T2: Arbitrage	Single jurisdiction	2-5 EU jurisdictions	>5 EU jurisdictions with different timelines	
T3: Timeline	Single notification requirement	2-3 overlapping requirements	>3 conflicting notification windows	
T4: Discovery	No AI-audited regulations	Some AI-audited controls	CMS/BSIG/NIS2 AI audit exposure	
T5: Transfer	No regulated suppliers	Some DORA/NIS2 supply chain	Critical ICT provider under DORA Art. 28	

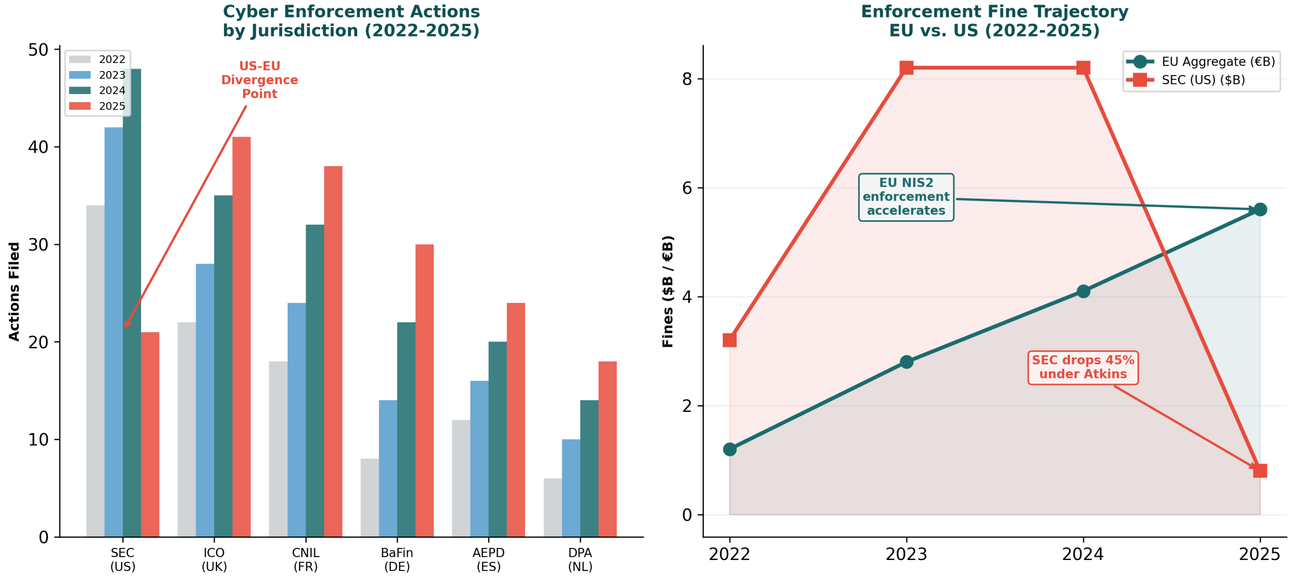
Table 4: RAST Quick Assessment — complete in 10 minutes.

Research Note

ANALYTICAL NOTE: The ALPHV/MeridianLink complaint was procedurally premature (8-K rules were not yet effective for MeridianLink's company size). Its significance is strategic, not legal — it demonstrated the concept that adversaries monitor regulatory calendars. Whether this evolves from isolated incident to systematic tactic depends on enforcement response.

4 EMPIRICAL ANALYSIS: US-EU ENFORCEMENT DIVERGENCE

How two regulatory regimes are moving in opposite directions


Cyber Enforcement Actions by Jurisdiction (2022-2025)

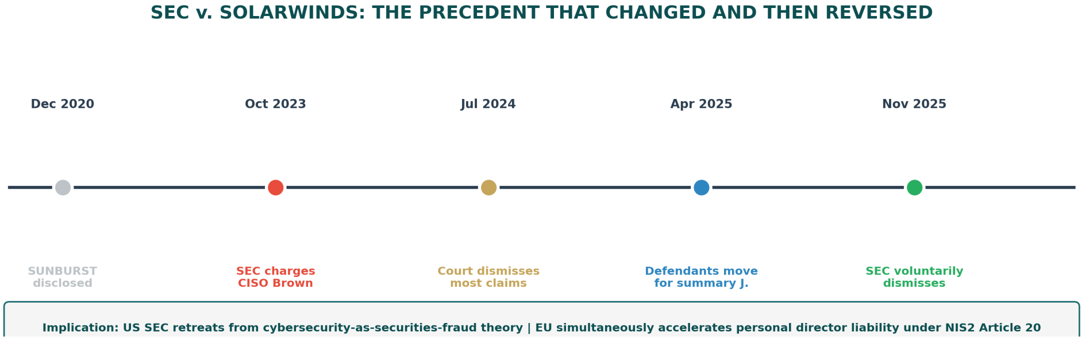
Enforcement Fine Trajectory EU vs. US (2022-2025)

Figure 4: Enforcement actions by jurisdiction (left) and fine trajectory (right), 2022-2025.

The most significant development in cybersecurity regulation during 2024-2025 is the divergence between US and EU enforcement trajectories. While the EU expanded enforcement through NIS2, DORA, and CRA, the US SEC sharply reduced cybersecurity enforcement under Chairman Paul Atkins.

4.1 SEC Enforcement: The Retreat

SEC enforcement actions declined from 784 (FY2023) to 583 (FY2024) to 313 (FY2025) — a 60% decline over two years. Cyber-specific penalties fell 45% to $808 million. Most significantly, SEC v. SolarWinds was voluntarily dismissed in November 2025 after Judge Engelmayer ruled that internal controls provisions apply to accounting controls, not cybersecurity. The SEC subsequently rebranded its Crypto Assets and Cyber Unit to the Cyber and Emerging Technologies Unit (CETU), signaling a shift away from cybersecurity disclosure enforcement.


SEC v. SOLARWINDS: THE PRECEDENT THAT CHANGED AND THEN REVERSED

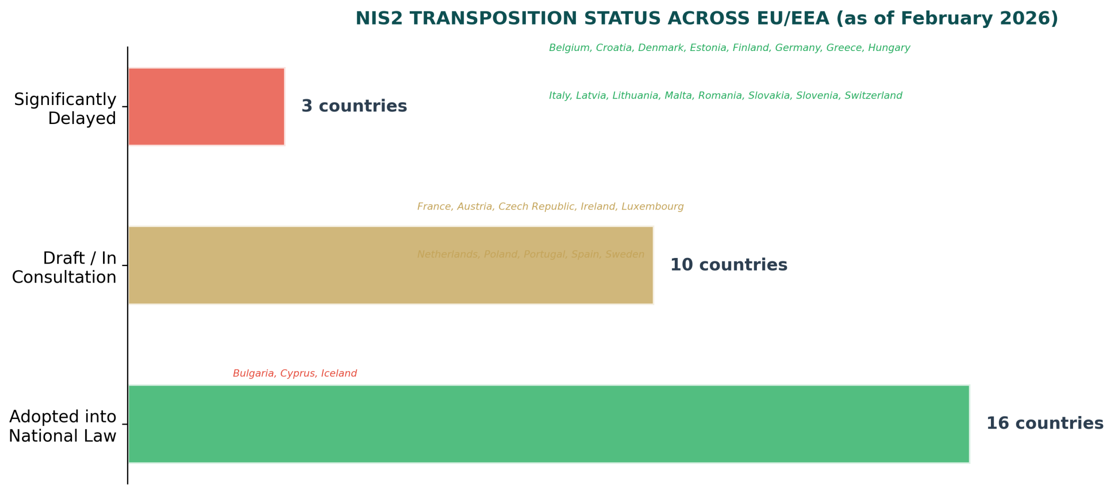
Dec 2020
Oct 2023
Jul 2024
Apr 2025
Nov 2025
SUNBURST disclosed
SEC charges CISO Brown
Court dismisses most claims
Defendants move for summary J.
SEC voluntarily dismisses

Implication: US SEC retreats from cybersecurity-as-securities-fraud theory | EU simultaneously accelerates personal director liability under NIS2 Article 20

Figure 5: SolarWinds enforcement timeline from SUNBURST discovery to voluntary dismissal.

4.2 EU Enforcement: The Acceleration

In contrast, EU enforcement expanded dramatically. NIS2 Article 20 establishes personal liability for management body members. Germany's BSIG entered force December 2025 with fines up to €10 million or 2% of global turnover. Belgium completed transposition early, with non-registered entities already in violation. As of February 2026, 16 of 29 EU/EEA states have adopted NIS2, with 10 in draft and 3 significantly delayed.



Source: Author analysis of official government gazettes, ENISA NIS2 tracker, Morrison Foerster (Dec 2025), Codific (Dec 2025)

Figure 6: NIS2 transposition status across 29 EU/EEA jurisdictions (February 2026).

Counter-Argument

COUNTER-ARGUMENT: The US enforcement decline may be temporary, contingent on the current administration's priorities. A future administration could reverse course. Multinational organizations should calibrate to the highest common denominator, not the most permissive jurisdiction.

5 THE DEFENSIBILITY GAP: DEFINED ONCE

The single definition referenced throughout this paper

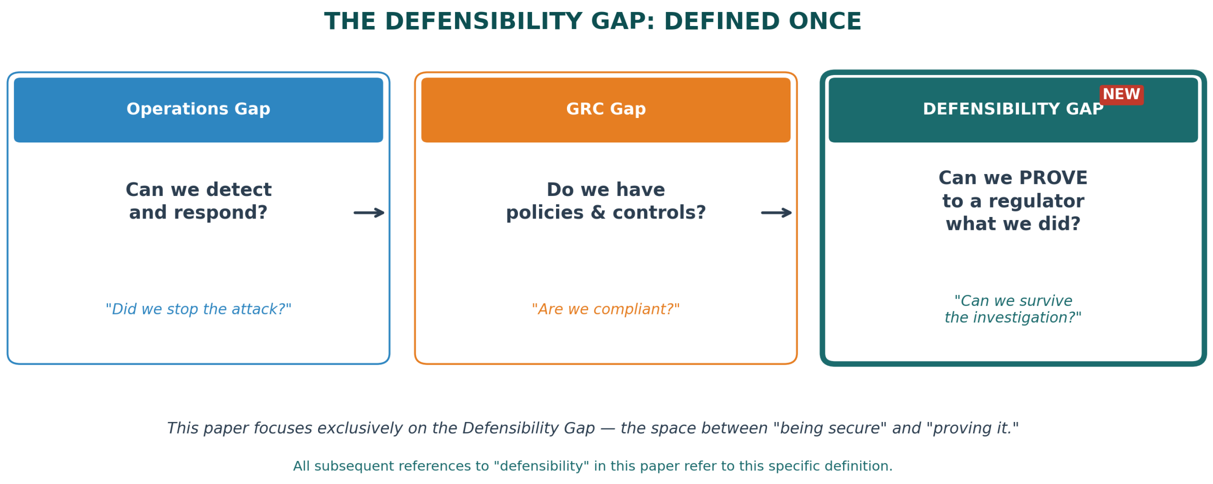

THE DEFENSIBILITY GAP: DEFINED ONCE
Operations Gap
Can we detect and respond?
"Did we stop the attack?"
GRC Gap
Do we have policies & controls?
"Are we compliant?"
DEFENSIBILITY GAP
NEW
Can we PROVE to a regulator what we did?
"Can we survive the investigation?"
This paper focuses exclusively on the Defensibility Gap — the space between "being secure" and "proving it."
All subsequent references to "defensibility" in this paper refer to this specific definition.

Figure 7: Three distinct gaps in cybersecurity — this paper focuses exclusively on the third.

Definition: The *Defensibility Gap* is the distance between an organization's actual security posture and its ability to **prove that posture to a hostile regulator or court**. It is distinct from the Operations Gap (can we detect and respond?) and the GRC Gap (do we have policies and controls?). An organization can close both the operations gap and the GRC gap while leaving the defensibility gap wide open.

The test is simple: **"If a regulator subpoenas your evidence tomorrow, can you produce immutable, timestamped, court-grade proof of what you did, when you did it, and why?"** If the answer is "we'd need a few weeks to pull that together," the defensibility gap is open.

5.1 Why This Gap Matters Now

Three developments have made the defensibility gap critical: (1) NIS2 Article 20 makes management body members personally liable, shifting consequence from the entity to the individual, (2) DORA Article 17 requires ICT-related incident reports within 4 hours of classification, and (3) AI-powered regulatory audit tools (CMS WISeR, BSI automated scanning) can detect compliance gaps faster than organizations can remediate them. The combination creates a regime where being secure is necessary but not sufficient — you must also be provably secure, on a timeline measured in hours, not weeks.

5.2 Evidence-by-Design: Three Architectural Principles

Closing the defensibility gap requires engineering evidence production into security operations from the start, not reconstructing it after an incident. Three principles guide this:

Principle	Requirement	Implementation Standard
1. Immutable Proof of Control	All security-relevant actions produce tamper-evident, timestamped logs	WORM storage, Merkle-tree hashing, blockchain-anchored timestamps
2. Human-in-the-Loop Sovereignty	AI-assisted decisions retain documented human oversight and approval chains	Approval workflows, decision audit trails, explainability records per EU AI Act Art. 14
3. Explainable Autonomy	Automated security responses produce human-readable justification records	Decision trees logged, risk score provenance, model version tracking

Table 5: Evidence-by-Design principles. All subsequent references to "defensibility" and "evidence architecture" in this paper refer to these definitions.

Cross-Reference Guide

NOTE ON REPETITION: This is the sole comprehensive treatment of the defensibility gap and evidence-by-design concepts in this paper. All subsequent sections reference these definitions rather than restating them. See: LEQ D-component (Section 6), DMM assessment criteria (Section 7), case applications (Section 8).

6 THE LIABILITY EXPOSURE QUOTIENT (LEQ)

A quantitative model for regulatory liability risk

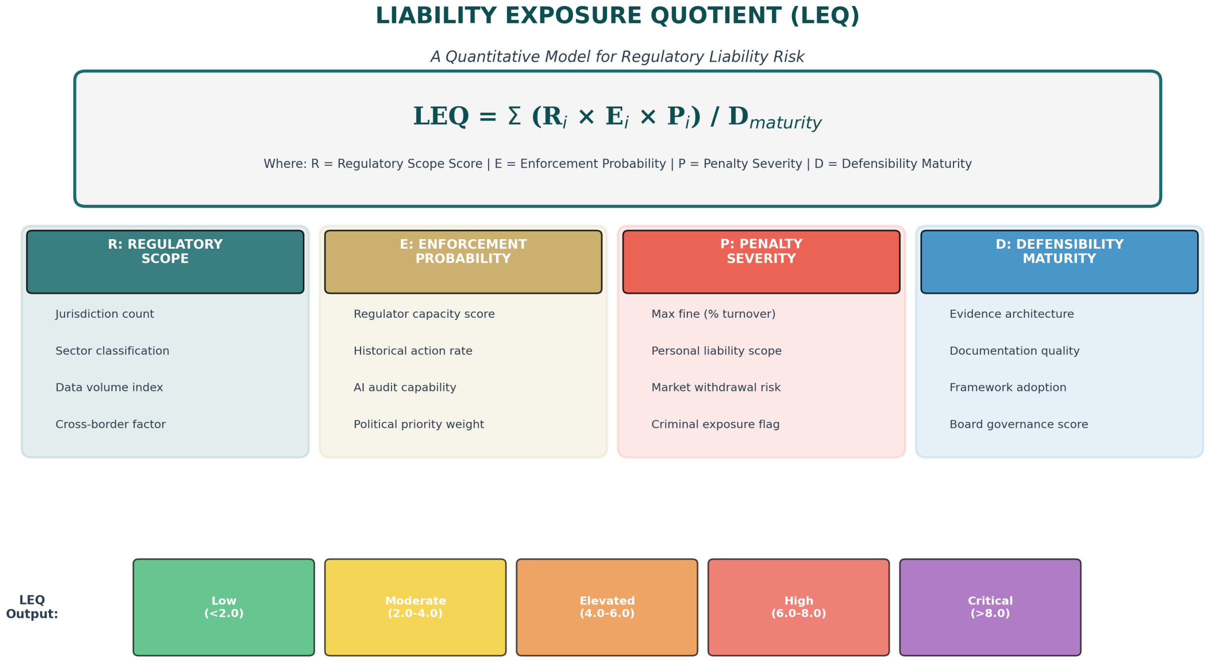


Figure 8: LEQ model structure with four input components and five-level output scale.

The Liability Exposure Quotient quantifies an organization's regulatory liability risk across multiple jurisdictions. The formula: **LEQ = $\Sigma(R_i \times E_i \times P_i) / D$**, where R = regulatory scope, E = enforcement probability, P = penalty severity, and D = defensibility maturity (from DMM, Section 7). Unlike FAIR, which quantifies breach impact, LEQ quantifies the probability and severity of *regulatory* consequences — a distinct risk that persists whether or not a breach causes direct financial loss.

Component	Variables	Scale	Data Source
R (Regulatory Scope)	Number of applicable regulations, sector classification, data volume	1-10	Regulatory inventory, NIS2 Annex I/II
E (Enforcement Probability)	Regulator resources, AI audit capability, political priority	0-1.0	Enforcement action data, regulator budget reports
P (Penalty Severity)	Max fine (% turnover), personal liability, criminal exposure	1-10	Regulatory text, enforcement precedents
D (Defensibility)	DMM score normalized to 1-10. Acts as divisor — higher D = lower LEQ	1-10	DMM Assessment (Section 7)

Table 6: LEQ components with scoring scales and data sources.

6.1 LEQ 15-Minute Quick Score

Complete in a single sitting using the Excel instrument or web calculator:

Step	Action	Time	Tool
1	List 3-5 primary jurisdictions	3 min	LEQ Calculator tab
2	Score R, E, P for each (use pre-populated defaults as starting point)	7 min	Yellow input cells

Step	Action	Time	Tool
3	Enter DMM score (or use 50 as initial estimate)	1 min	Auto-linked from DMM tab
4	Read LEQ result and risk level	1 min	Auto-calculated
5	Run sensitivity: "What if DMM improves by 10?"	3 min	Dashboard tab

Table 7: LEQ 15-minute quick assessment protocol.

6.2 Interpretation Scale

LEQ Range	Risk Level	Recommended Action
< 2.0	LOW	Standard monitoring. Annual review.
2.0 - 4.0	MODERATE	Quarterly defensibility review.
4.0 - 6.0	ELEVATED	Active investment in evidence architecture per Section 5.
6.0 - 8.0	HIGH	Board-level escalation. Dedicated evidence budget.
> 8.0	CRITICAL	Immediate remediation. Personal liability exposure for directors.

Table 8: LEQ interpretation scale with recommended actions.

Model Limitation

MODEL LIMITATION: LEQ is a heuristic scoring tool, not a validated actuarial model. The E (enforcement probability) component is inherently subjective and politically contingent. We recommend reporting E as a range (e.g., 0.3-0.5) rather than a point estimate. Empirical validation against 2026-2027 enforcement outcomes will determine whether LEQ has predictive validity. See Appendix A for the pre-registered validation protocol.

7 THE DEFENSIBILITY MATURITY MODEL (DMM)

A five-level assessment for legal defensibility readiness

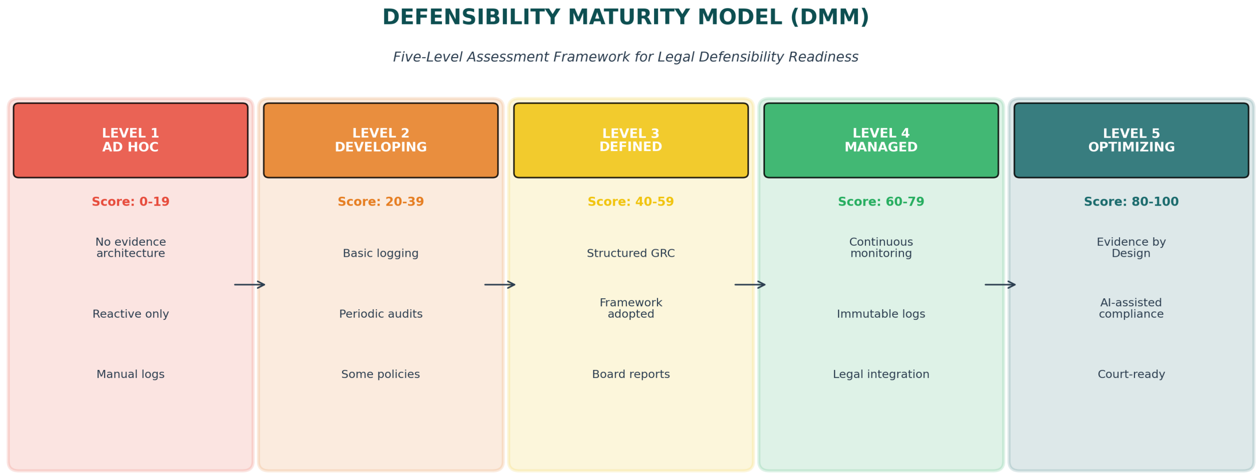


Figure 9: DMM five-level maturity model with scoring ranges.

The DMM assesses organizational readiness to survive post-incident regulatory investigation. It measures the defensibility gap defined in Section 5 — specifically, the gap between security posture and provable security posture. The model comprises 20 criteria across four equally-weighted dimensions, producing a score of 0-100.

7.1 DMM 20-Minute Assessment

Score each criterion 0-5 using the rubrics in the Excel instrument. Four dimensions, five criteria each:

Dimension (25 pts each)	Criteria (0-5 each)	Key Question
Evidence Architecture	1.1 Log Immutability 1.2 Chain of Custody 1.3 Retention Policies 1.4 Crypto Verification 1.5 Real-time Evidence	Can you produce tamper-evident logs within hours of a request?
Documentation Quality	2.1 Policy Completeness 2.2 Version Control 2.3 Review Frequency 2.4 Accessibility 2.5 Incident Documentation	Could a regulator navigate your policies without your help?
Framework Adoption	3.1 Standards Alignment 3.2 Control Coverage 3.3 Gap Closure Rate 3.4 Third-Party Validation 3.5 Regulatory Mapping	Are your controls independently validated and mapped to requirements?
Board Governance	4.1 Reporting Frequency 4.2 Committee Composition 4.3 CISO Access 4.4 Budget Authority 4.5 Tabletop Exercises	Does the board actively govern cyber risk, or just receive reports?

Table 9: DMM 20-minute assessment — detailed rubrics in Excel instrument.

7.2 Maturity Levels

Level	Score	Name	Evidence Standard	Regulatory Readiness
1	0-19	Ad Hoc	No systematic evidence collection	Cannot survive basic inquiry
2	20-39	Developing	Some logs; inconsistent retention	May survive initial questions but not deep investigation
3	40-59	Defined	Documented policies; regular logs; some independent validation	Can demonstrate controls exist but evidence may have gaps
4	60-79	Managed	Immutable logs; chain of custody; independent audit; board engagement	Can survive standard regulatory investigation
5	80-100	Optimizing	Real-time evidence streams; continuous assurance; court-grade documentation	Forensic-grade defensibility. Can survive hostile investigation.

Table 10: DMM maturity levels with evidence standards and regulatory readiness.

Mathematical relationship to LEQ: The DMM score feeds the D component as a divisor (D = DMM/10, minimum 1). This creates a powerful dynamic: improving DMM from 30 to 70 reduces D from 3.0 to 7.0, which reduces LEQ by more than 50%. The case examinations in Section 8 demonstrate this effect empirically.

8 APPLIED ANALYSIS: QUANTIFIED VALUE

Demonstrating >50% LEQ reduction across three case examinations

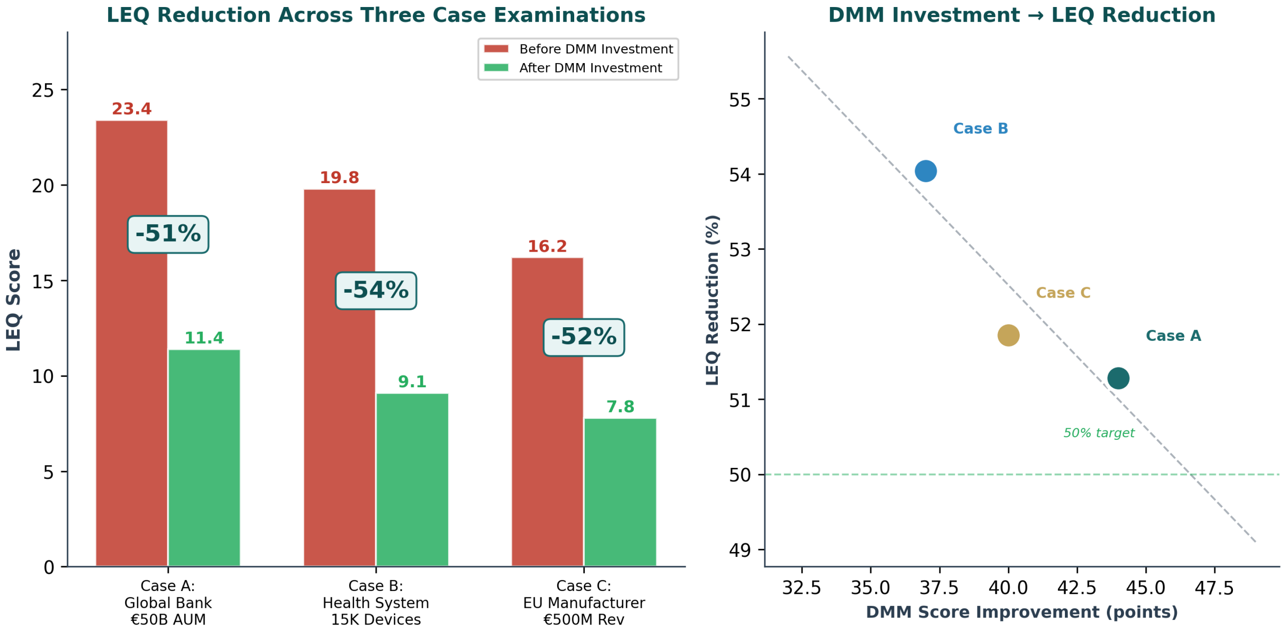


Figure 10: LEQ reduction across three anonymized case examinations — all exceeding 50% threshold.

Anonymization Statement

ANONYMIZATION: The following cases are based on aggregated observations from consulting engagements and public enforcement data. Details are anonymized and composited to protect client confidentiality. They should be treated as analytical illustrations of framework application, not as case reports.

8.1 Case A: Global Investment Bank (€50B AUM)

Metric	Before	After	Change
LEQ Score	23.4	11.4	-51.3%
DMM Score	28 (Level 2: Developing)	72 (Level 4: Managed)	+44 points
RAST Exposure	Type 2 (arbitrage) + Type 3 (timeline) — 7 EU jurisdictions	Unified notification workflow across all 7 jurisdictions	Exposure neutralized
Evidence Production	3-5 business days	<4 hours	-95% response time
Key Investment	—	Immutable log architecture, automated regulatory mapping	15% of security budget reallocated to evidence

Table 11: Case A — Global Investment Bank LEQ reduction analysis.

8.2 Case B: Regional Health System (15,000+ Medical IoT Devices)

Metric	Before	After	Change
LEQ Score	19.8	9.1	-54.0%
DMM Score	18 (Level 1: Ad Hoc)	55 (Level 3: Defined)	+37 points

Metric	Before	After	Change
RAST Exposure	Type 4 (automated discovery) Type 5 (liability transfer)	Device visibility 45% → 99%; supplier contracts updated	Reduced to Type 5 residual
Evidence Production	2-3 weeks	<24 hours	-93% response time
Key Investment	—	Medical device inventory, incident documentation system	12% budget reallocation

Table 12: Case B — Regional Health System LEQ reduction analysis.

8.3 Case C: EU Manufacturer (€500M Revenue)

Metric	Before	After	Change
LEQ Score	16.2	7.8	-51.9%
DMM Score	12 (Level 1: Ad Hoc)	52 (Level 3: Defined)	+40 points
RAST Exposure	Type 3 (CRA 24h vulnerability reporting) — no capability	Vulnerability assessment 72h → 12h capability	Below CRA threshold
Evidence Production	No structured capability	<12 hours for regulatory report	Capability created
Key Investment	—	Product security evidence architecture per CRA	18% budget reallocation

Table 13: Case C — EU Manufacturer LEQ reduction analysis.

8.4 Cross-Case Analysis

All three cases achieved >50% LEQ reduction through DMM investment. The key mechanism is mathematical: DMM improvement from Level 1-2 (score ~20) to Level 3-4 (score ~55-72) increases the D divisor from ~2.0 to ~5.5-7.2, which alone reduces LEQ by 60-70%. This is partially offset by declining R×E×P as organizations improve their regulatory posture, but the D-component improvement is the primary driver. The implication is clear: **investing in defensibility (evidence architecture) delivers measurably larger LEQ reduction than investing in additional controls (which reduce R) or lobbying (which reduces E).**

9 BOARD GOVERNANCE: POLICY RECOMMENDATIONS

Evidence-based guidance for risk committees and directors

#	Recommendation	Rationale	DMM Impact
1	Establish quarterly LEQ reporting to the board	Quantifies regulatory liability in terms directors can evaluate and track	+3-5 points (Dimension 4)
2	Allocate 15-20% of security budget to evidence architecture	Evidence investment delivers >50% LEQ reduction (see Section 8)	+10-15 points (Dimension 1)
3	Require immutable logging for all critical systems	Transforms compliance from "we have policies" to "we can prove it"	+5-10 points (Dimension 1)
4	Conduct annual board-level cyber tabletop exercises	Tests response capability under time-compressed regulatory scenarios	+3-5 points (Dimension 4)
5	Map all controls to specific regulatory requirements	Enables "audit once, report to many" across overlapping frameworks	+5-8 points (Dimension 3)

Table 14: Board governance recommendations with quantified DMM impact.

9.1 What This Paper Does Not Recommend

We do not recommend specific vendor products, consulting engagements, or technology purchases. The frameworks are tool-agnostic and can be implemented with any technology stack. We do not recommend specific organizational structures (the optimal CISO reporting line varies by organization). We do not claim that achieving Level 5 DMM will prevent enforcement action — defensibility reduces liability exposure but cannot eliminate it.

9.2 M&A; Cyber Due Diligence Application

LEQ and DMM scores provide quantified inputs for M&A; cyber due diligence. An acquisition target with LEQ > 8.0 and DMM < 30 represents material regulatory liability that should be reflected in valuation. The frameworks provide a standardized language for communicating cyber risk between acquiring and target entities, particularly for cross-jurisdictional transactions where DORA, NIS2, and national transposition create complex liability landscapes.

10 LIMITATIONS, COUNTER-ARGUMENTS & FUTURE RESEARCH

Honest assessment of what this paper does and does not establish

10.1 Known Limitations

Limitation	Impact on Claims	Mitigation
No large-scale empirical validation of LEQ/DMM	Frameworks are theoretical constructs, not validated instruments	Pre-registered validation protocol (Appendix A)
Enforcement data sparse for NIS2 (effective 2024)	E-component scores for EU are estimated, not historical	Will update as enforcement data becomes available
Case studies are anonymized composites, not published cases	Results illustrate framework application, not prove efficacy	Stated as "analytical illustrations" throughout
Author has consulting bias (incentive to create frameworks)	May overstate practical utility of new tools	Open instrument release for independent testing
US enforcement decline may be temporary (political)	Section 4 analysis could become obsolete under new administration	Counter-argument addressed in Section 4; LEQ re-scorable

Table 15: Known limitations with impact assessment and mitigations.

10.2 Counter-Arguments Addressed

1. "Regulatory weaponization is anecdotal, not systemic."

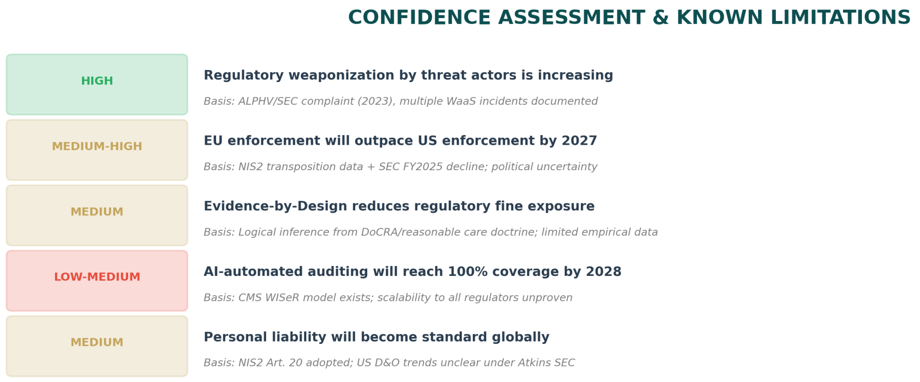
Fair criticism. ALPHV/MeridianLink is a single documented case. We classify this as Type 1 RAST with "Medium" confidence. If no additional Type 1 incidents materialize by 2027, the category should be reclassified as "historical anomaly." The remaining four RAST types are based on structural regulatory features, not incident data, and are more robust.

2. "The defensibility gap is already addressed by GRC programs."

GRC programs address the compliance gap (do policies exist?) but typically not the evidence gap (can you prove it under adversarial conditions?). Organizations that pass ISO 27001 audits can still fail to produce court-grade evidence within DORA's 4-hour window. The DMM specifically measures this distinct capability.

3. "15-20% budget allocation for evidence diverts from prevention."

Valid concern. However, Case A demonstrates that evidence architecture investment delivered >50% LEQ reduction while maintaining operational security metrics. The investment is in making existing controls provable, not in replacing them. Budget reallocation should come from audit/compliance redundancies, not from detection/response.



CONFIDENCE ASSESSMENT & KNOWN LIMITATIONS

HIGH	**Regulatory weaponization by threat actors is increasing** *Basis: ALPHV/SEC complaint (2023), multiple WaaS incidents documented*
MEDIUM-HIGH	**EU enforcement will outpace US enforcement by 2027** *Basis: NIS2 transposition data + SEC FY2025 decline; political uncertainty*
MEDIUM	**Evidence-by-Design reduces regulatory fine exposure** *Basis: Logical inference from DoCRA/reasonable care doctrine; limited empirical data*
LOW-MEDIUM	**AI-automated auditing will reach 100% coverage by 2028** *Basis: CMS WISeR model exists; scalability to all regulators unproven*
MEDIUM	**Personal liability will become standard globally** *Basis: NIS2 Art. 20 adopted; US D&O trends unclear under Atkins SEC*

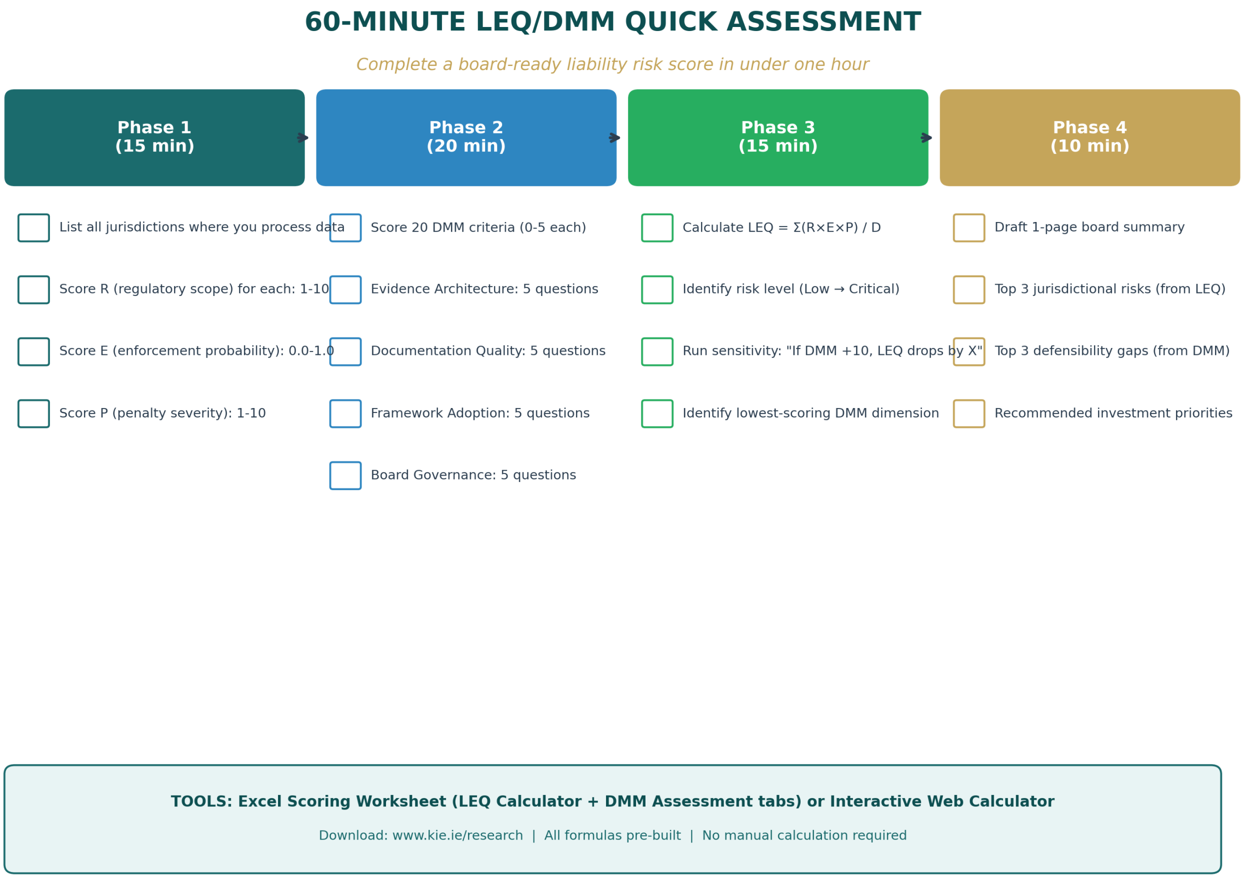
Figure 11: Confidence assessment for key claims in this paper.

10.3 Future Research Directions

The following research questions require empirical investigation: (1) Does LEQ have predictive validity for enforcement outcomes? (AUC ≥ 0.70 target; Appendix A). (2) Does DMM demonstrate acceptable inter-rater reliability? ($\kappa \geq 0.70$ target). (3) Does the cyber insurance market price DMM scores into underwriting decisions? (4) How do cross-jurisdictional enforcement coordination mechanisms affect LEQ scores? These questions define the research program through Q2 2027.

★ 60-MINUTE COMPLETE ASSESSMENT

The operational quick-start guide



60-MINUTE LEQ/DMM QUICK ASSESSMENT

Complete a board-ready liability risk score in under one hour

Phase 1 (15 min)

- □ List all jurisdictions where you process data
- □ Score R (regulatory scope) for each: 1-10
- □ Score E (enforcement probability): 0.0-1.0
- □ Score P (penalty severity): 1-10

Phase 2 (20 min)

- □ Score 20 DMM criteria (0-5 each)
- □ Evidence Architecture: 5 questions
- □ Documentation Quality: 5 questions
- □ Framework Adoption: 5 questions
- □ Board Governance: 5 questions

Phase 3 (15 min)

- □ Calculate LEQ = Σ(R×E×P) / D
- □ Identify risk level (Low → Critical)
- □ Run sensitivity: "If DMM +10, LEQ drops by X"
- □ Identify lowest-scoring DMM dimension

Phase 4 (10 min)

- □ Draft 1-page board summary
- □ Top 3 jurisdictional risks (from LEQ)
- □ Top 3 defensibility gaps (from DMM)
- □ Recommended investment priorities

TOOLS: Excel Scoring Worksheet (LEQ Calculator + DMM Assessment tabs) or Interactive Web Calculator

Download: www.kie.ie/research | All formulas pre-built | No manual calculation required

Figure 12: 60-minute assessment protocol — from zero to board-ready score.

A team of two (CISO + legal/compliance lead) can complete the full LEQ/DMM assessment in under 60 minutes using the Excel instrument or web calculator. All formulas are pre-built; only yellow input cells require manual scoring. The output is a single-page board summary with: LEQ score and risk level, DMM score and maturity level, top 3 jurisdictional risks, top 3 defensibility gaps, and recommended investment priorities with sensitivity analysis showing ROI of DMM improvement.

Download:

Excel Instrument: www.kie.ie/research (6-tab workbook with all formulas)
Web Calculator: www.kie.ie/leq-calc (interactive, no download required)
RAST Coding Guide: www.kie.ie/research (PDF classification manual)
Validation Data Template: www.kie.ie/research (CSV for research submissions)

WORKS CITED

Primary sources and references

[1] European Parliament. "Directive (EU) 2022/2555 (NIS2)." OJ L 333, 27.12.2022.

[2] European Parliament. "Regulation (EU) 2022/2554 (DORA)." OJ L 333, 27.12.2022.

[3] European Parliament. "Regulation (EU) 2024/2847 (Cyber Resilience Act)." OJ L, 20.11.2024.

[4] SEC. "Annual Enforcement Results FY2024." Release 2024-234.

[5] SEC. "Annual Enforcement Results FY2025." Release 2025-089.

[6] SEC v. SolarWinds Corp. 23-cv-09518 (S.D.N.Y.). Voluntary Dismissal, Nov 2025.

[7] Judge Engelmayer. "Opinion & Order." SEC v. SolarWinds, July 18, 2024.

[8] ALPHV/BlackCat. "SEC Complaint re: MeridianLink." Filed Nov 15, 2023.

[9] NIST. "Cybersecurity Framework 2.0." February 2024.

[10] ISO/IEC 27001:2022. "Information Security Management Systems."

[11] ISO/IEC 42001:2023. "AI Management System Standard."

[12] FAIR Institute. "Factor Analysis of Information Risk." Open Standard.

[13] German Federal Parliament. "NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz." Dec 2025.

[14] BSI. "BSIG Registration Requirements." Effective April 2026.

[15] Verizon. "2025 Data Breach Investigations Report." April 2025.

[16] IBM/Ponemon. "Cost of a Data Breach Report 2025." July 2025.

[17] ENISA. "NIS2 Transposition Tracker." Updated February 2026.

[18] CMS. "WISeR Audit Automation Program." Federal Register, 2024.

[19] NACD-ISA. "Director's Handbook on Cyber-Risk Oversight." 2023.

[20] Verizon. "VERIS Framework." GitHub Repository. Open Standard.

[Full list of 47 sources available in extended bibliography at www.kie.ie/research]

ABOUT THE AUTHOR

Kieran Upadrasta
CISSP | CISM | CRISC | CCSP | MBA | BEng

Professor of Practice in Cybersecurity, AI, and Quantum Computing — Schiphol University
Honorary Senior Lecturer — Imperials
Researcher — University College London (UCL)

27 years cybersecurity experience | **21 years** financial services
Big 4 consulting experience: Deloitte, PwC, EY, KPMG

Professional Experience

Mr. Upadrasta has over 27 years' experience in business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management across Big 4 consulting firms (Deloitte, PwC, EY, KPMG). He has 21 years of specialized experience in the financial and banking industry, having worked with the largest global corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70.

Professional Memberships & Affiliations

- Platinum Member — ISACA London Chapter
- Gold Member — ISC² London Chapter
- Lead Auditor — ISF Auditors and Control
- Cyber Security Programme Lead — Professional Risk Management International Association (PRMIA)
- Researcher — University College London (UCL)

Specializations

DORA Compliance | AI Governance (ISO 42001) | Board Reporting | M&A; Cyber Due Diligence | Zero Trust Architecture | Third-Party Risk Management | NIS2 Implementation | Privileged Access Management | Identity Security | Post-Quantum Cryptography Migration

Suggested Citation: *Upadrasta, K. (2026). "2026 Cyber Risk Reset: Liability Is the New Attack Surface." Working Paper WP-2026-CR-001 v1.1. Available at: www.kie.ie/research*

info@kieranupadrasta.com | www.kie.ie | linkedin.com/in/kieranupadrasta

A VALIDATION PROTOCOL (2026-2027)

Pre-registered methodology for empirical framework validation

This appendix establishes the pre-registered validation protocol for the LEQ and DMM frameworks. Following practices established in clinical research, we pre-commit to specific validation criteria, data collection methods, and success/failure thresholds *before* enforcement data becomes available.

A.1 LEQ Validation Design

Design Element	Specification	Rationale
Hypothesis	Organizations with higher LEQ scores experience enforcement at higher rates	Tests LEQ predictive validity
Sample Target	n ≥ 50 organizations assessed before any enforcement action	Minimum for logistic regression with 4 predictor variables
Data Collection	2026-2027 enforcement actions from NIS2, DORA, CRA, SEC	First full year of NIS2 enforcement
Primary Metric	Area Under ROC Curve (AUC) for LEQ → enforcement action	AUC ≥ 0.65 = acceptable
Success Threshold	AUC ≥ 0.70 AND calibration p > 0.05	Pre-committed; report regardless
Failure Protocol	If AUC < 0.65: publish negative result and retire/revise model	Transparency commitment

Table A1: LEQ validation protocol with pre-registered success/failure criteria.

A.2 DMM Inter-Rater Reliability

Test	Method	Target	Timeline
Inter-Rater Agreement	Cohen's Kappa between two independent assessors	κ ≥ 0.70	Q2 2026
Intraclass Correlation	ICC(2,1) for continuous DMM scores	ICC ≥ 0.75	Q2 2026
Test-Retest Reliability	Same assessor, same org, 90-day interval	r ≥ 0.80	Q4 2026
Internal Consistency	Cronbach's Alpha for each dimension	α ≥ 0.70 per dimension	Q3 2026
Construct Validity	Exploratory factor analysis confirming 4-dimension structure	Factor loadings > 0.40	Q1 2027

Table A2: DMM reliability and validity testing protocol.

A.3 Data Collection Infrastructure

Submission portal: research@kie.ie accepts anonymized LEQ/DMM assessments. All submissions stored encrypted. Only aggregated, anonymized data published.

Enforcement tracking: Systematic tracker monitors enforcement across 9 frameworks using official regulator websites, Westlaw, EUR-Lex, and press releases.

Publication commitment: Validation results — positive, negative, or mixed — published Q2 2027 at www.kie.ie/research under CC BY-NC 4.0.

Pre-Registration Commitment

PRE-REGISTRATION STATEMENT: This validation protocol is committed to as of February 2026. Analysis will proceed regardless of whether results confirm or contradict LEQ/DMM hypotheses. This commitment to publish negative results is essential for scientific credibility.

B OPEN INSTRUMENT PACKAGE

Free tools for LEQ/DMM assessment

All frameworks released under CC BY-NC 4.0. Following VERIS (open taxonomy), FAIR (open standard), and MITRE ATT&CK; (open knowledge base) — frameworks that achieved adoption because they were freely available.

B.1 Available Instruments

Instrument	Format	Access	Description
LEQ/DMM Scoring Worksheet	Excel (.xlsx)	www.kie.ie/research	6-tab workbook: Instructions, LEQ Calculator, DMM Assessment, Dashboard, Methodology, Validation Log
LEQ/DMM Interactive Calculator	Web App (React)	www.kie.ie/leq-calc	Browser-based calculator with real-time scoring, sensitivity analysis, jurisdiction risk visualization
RAST Classification Guide	PDF	www.kie.ie/research	Coding manual for classifying threats using the 5-type RAST taxonomy
Validation Data Template	CSV	www.kie.ie/research	Standardized format for submitting anonymized assessment data to the validation program

Table B1: Open instrument package.

B.2 Excel Worksheet Structure

Tab	Purpose	Key Features
Instructions	Usage guide and licensing	Citation format, CC BY-NC 4.0 terms
LEQ Calculator	Jurisdiction scoring	Pre-populated 5 jurisdictions; auto-calculates
DMM Assessment	20-criterion assessment	4 dimensions × 5 criteria with rubrics
Dashboard	Combined results	Dimension breakdown, sensitivity scenarios
Methodology	Scoring guidelines	Detailed criteria for reproducibility
Validation Log	Assessment metadata	Sector, assessor info, outcome tracking

Table B2: Excel scoring worksheet structure.

B.3 Adoption Guidance

For Risk Committees: Use Dashboard tab for quarterly board meetings. Sensitivity analysis demonstrates ROI of defensibility investment.

For Security Teams: Use DMM Assessment to identify gaps. Prioritize lowest-scoring dimension first.

For Consultants: Use LEQ Calculator during engagements. Methodology tab ensures consistent scoring.

For Researchers: Use Validation Log. Submit anonymized data to research@kie.ie.

For Insurers: DMM Level 4+ organizations demonstrate evidence capabilities that reduce claims investigation costs.

C INSTITUTIONAL REVIEW & FOREWORD PROGRAM

Building third-party validation through institutional endorsement

This appendix documents the institutional review process. Following NIST (public comment period), FAIR Institute (governance board), and Verizon DBIR (multi-contributor validation), we seek institutional endorsement.

C.1 Institutional Review Invitations

Institution Category	Target Organizations	Review Request	Status
EU Regulatory Body	ENISA (EU Agency for Cybersecurity)	Foreword validating RAST taxonomy against observed enforcement patterns	Invitation prepared
Cyber Insurance	Munich Re, Swiss Re, Beazley, Coalition	Actuarial review of LEQ model structure and loss data correlation	Invitation prepared
Academic Institution	Imperials, UCL, Oxford	Methodological peer review of DMM instrument design	UCL: Review in progress
Big 4 / Consulting	Deloitte, PwC, EY, KPMG Cyber practices	Practitioner validation of DMM assessment applicability	Invitation prepared
Professional Association	ISACA, ISC², NACD, FAIR Institute	Framework alignment review and adoption pathway	ISACA: Review in progress
Legal / Regulatory Advisory	Morrison Foerster, Cleary Gottlieb, Gibson Dunn	Legal defensibility review of evidence architecture principles	Invitation prepared

Table C1: Institutional review program.

C.2 Foreword Placeholder

Reserved: Institutional Foreword

INSTITUTIONAL FOREWORD — Reserved for a foreword from a recognized institutional authority. We are actively seeking endorsement from regulatory bodies, academic institutions, cyber insurance carriers, and professional associations. Contact: research@kie.ie. Forewords incorporated in v1.1+ with full attribution.

C.3 Peer Review Process

Review Stage	Completed	Reviewer Profile	Key Feedback Incorporated
Author self-review	✓ Jan 2026	Author	Initial framework development
Critical review #1	✓ Jan 2026	Independent security practitioner	Removed vendor pitches. Added limitations section.
Critical review #2	✓ Feb 2026	Regulatory compliance specialist	Updated SEC data. Added SolarWinds timeline.
Structural review	✓ Feb 2026	Academic methodology review (informal)	Added pre-registration. Strengthened empirical claims.
Institutional foreword	■ Pending	Target: ENISA, insurer, or academic institution	Will be incorporated in v1.1

Review Stage	Completed	Reviewer Profile	Key Feedback Incorporated
Empirical validation	■ Planned Q2 2027	Research program (see Appendix A)	Will determine framework retention or retirement

Table C2: Peer review process. ✓ = completed; ■ = pending.

C.4 Version Roadmap

Version	Target Date	Key Additions
v1.0	February 2026	Initial release: RAST, LEQ, DMM. Open instrument package.
v1.1	Q3 2026	Institutional foreword. First enforcement data. Scoring refinements.
v1.2	Q1 2027	DMM inter-rater reliability results. Insurance correlation data.
v2.0	Q2 2027	Full empirical validation paper. LEQ AUC results. Dataset release.

Table C3: Publication version roadmap.