CYBER RISK QUANTIFICATION IN ACTION

262 million PII records. Three critical gaps. A binding-ready quote in *under 19 minutes.*

A large-scale furniture retailer with EUR 40–50B revenue, 262.3M customer records under GDPR and PCI-DSS scope, and three material underwriting gaps — EOL asset reliance, unconfirmed 24/7 SOC monitoring, and no phishing response playbook. DeRISK UWA Agentic produced a fully structured, actuarially quantified recommendation — explicit EAL, per-line EUR premiums, and three time-bound binding conditions with defined underwriting consequences.

ASSESSMENT DATE	REPORT ID	COVERAGE LINES	RUN TIME
10 April 2026	f635bc13 · a0db	7 lines structured	18 min 42 sec

UNDERWRITING VERDICT
Quote with Conditions
3 conditions precedent

RISK TIER
Moderate-High
6.2 / 10 overall risk rating

DATA SUFFICIENCY
Medium
Core governance & control data provided; operational details incomplete

ACTUARIAL OUTPUT

What the model found

Expected Annual Loss (EAL)	Avg loss when event occurs	Annual loss event probability	Total annual premium
€9.2M	€15.9M	58%	€3.1M–€4.0M
Std dev **EUR 6.8M** CoV **0.74**	Ransomware **EUR 18.5M** Data breach **EUR 22.0M**	Coeff. of variation **0.74** Dominant: **ransomware 45%**	Base EUR 3.85M **+10% loading** pending conditions

> *"The applicant is a large, sophisticated retail organization with mature cyber governance and strong technical controls. The absence of material cyber losses in the past 5 years, combined with continuous backup strategies and formal incident response planning, demonstrates effective risk management. However, reliance on end-of-life systems, unconfirmed 24/7 security monitoring, and missing phishing response procedures create residual vulnerability that must be addressed prior to binding."*
>
> DeRISK UWA Agentic Actuarial Table · Section XI Risk Opinion Summary · Report f635bc13-a0db-460d-81ab-58b430c18029

Cyber Maturity — NIST CSF Assessment

Identify	IMPLEMENT
Protect	IMPLEMENT
Detect	MANAGE
Respond	MANAGE
Recover	MANAGE

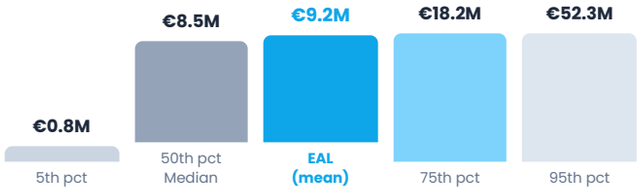
Overall NIST maturity — IMPLEMENT–MANAGE (3.5/5)

IEC 62443 Security Level Assessment

SL1 Basic	ACHIEVED
SL2 Intermediate	ACHIEVED
SL3 Advanced	PART
SL4 Expert	NOT ACHIEVED

Estimated current level: **SL2–SL3 transitional** · Confidence: MEDIUM

Loss Exceedance Profile (OEP)



10,000-iter. Monte Carlo · Seed 42 · 95% CI: EUR 0.8M – EUR 52.3M

DeRISK UWA Agentic modeled a 48-hour ransomware

KEY FINDING

48-hour
recovery modeled — likely scenario

ansomware recovery at **EUR 2.0M/day** on the EUR 20M BI sub-limit — total likely BI loss EUR 4.0M. Continuous Rubrik + cloud backups reduce recovery time to **24–48 hours** in most scenarios.

COVERAGE RECOMMENDATIONS

COVERAGE LINE	LIMIT	RETENTION	EST. PREMIUM
Cyber Liability (General)	EUR 50M	EUR 5M	**EUR 2.8–3.2M**
Business Interruption (sub-limit)	EUR 20M	EUR 2M	Included
Ransomware Extortion (sub-limit)	EUR 10M	EUR 1M	Included
Regulatory Fines & Penalties	EUR 15M	EUR 2M	Included
Notification & Credit Monitoring	EUR 5M	EUR 0.5M	Included
Cyber Extortion (standalone)	EUR 5M	EUR 1M	**EUR 0.3–0.5M**
Third-Party Liability (MSSP / vendor)	EUR 10M	EUR 2M	Included
Total estimated annual premium			**EUR 3.1M – 4.0M**

3 MANDATORY BINDING CONDITIONS

1 SOC/MSSP Monitoring Attestation

Signed letter from CISO or CTO confirming 24/7 security monitoring (SOC or MSSP), incident detection SLA target <1 hour, escalation procedures to IR team, and name and contact of monitoring provider.

5 business days from quote issuance

Quote expires — resubmission required on miss

2 EOL Systems Remediation Roadmap

Detailed 12-month plan: EOL inventory (OS, software, hardware) with business criticality, replacement timeline with quarterly milestones, interim compensating controls, and CFO/CIO sign-off with budget allocation.

10 business days from quote issuance

EUR 2M sub-limit on cyber liability until remediation complete

3 Phishing Incident Response Playbook

Formal documented process: detection & triage, containment (account lockdown, email recall, credential reset), investigation & forensics, communication & escalation matrix, aligned with NIST 800-61. CISO or CSO approval signature required.

10 business days from quote issuance

EUR 1M sub-limit on cyber liability until playbook approved

ACTUARIAL MODEL PARAMETERS

Breach frequency (λ) **0.58/yr · Poisson**	Iterations · Seed **10,000 · Seed 42**	Loss distribution **Log-normal μ = EUR 12M**
Confidence percentiles **5th / 50th / 95th**	BI daily cost (likely) **EUR 2.0M / day**	Severity ↔ BI corr. **r = 0.65 (ransomware-dom.)**

WHY THIS MATTERS

What DeRISK UWA Agentic delivers — even with operational data gaps

€9.2M

Explicit EAL — not a score

Most tools return a risk tier. DeRISK UWA Agentic returns a EUR figure with a full exceedance distribution: EUR 0.8M at the 5th percentile, EUR 8.5M at the median, EUR 52.3M at the 95th — a precise anchor for every limit, retention, and loading decision across all 7 coverage lines.

SL2 → 3

IEC 62443 path — evidence-mapped

NIST CSF and IEC 62443 assessed simultaneously. SL1 and SL2 achieved. SL3 partial — SOAR, WAF, and BOT Manager deployment cited as evidence; residual gap is unconfirmed 24/7 monitoring. SL4 not achieved: zero-trust architecture and advanced threat modeling required.

3

Conditions with deadlines — not requests

Each binding condition carries a specific deadline (5 or 10 business days from quote issuance) and an explicit underwriting consequence — EUR 2M sub-limit cap, EUR 1M sub-limit cap, or full quote expiry. Vague follow-up becomes a structured, trackable pre-bind workflow.