DENEXUS

METHODOLOGY BRIEF May 2026

DeRISK™ CRQ — How We Produce Defensible Financial Loss Numbers

For CFOs, boards, risk officers, and insurance markets: the methodology behind the number, why it can be trusted, and what each audience does with it.

300+	4	3	Full
REAL INDUSTRIAL DEPLOYMENTS CALIBRATION BASIS	OT SECTORS POWER · T&D · MANUFACTURING · DATA CENTERS	FINANCIAL OUTPUTS AEL · VAR · LOSS EXCEEDANCE	AUDIT TRAIL EVERY OUTPUT TRACEABLE TO SOURCE

OT cyber risk has no natural financial unit. Vulnerability counts, maturity scores, and qualitative assessments cannot drive investment decisions, size insurance programs, or satisfy governance requirements. **DeRISK CRQ provides that unit:** a probability-weighted financial loss estimate, built bottom-up from your specific OT environment, auditable at every step, and defensible to any audience that needs to rely on it.

THE THREE FINANCIAL OUTPUTS

Annual Expected Loss

AEL

The probability-weighted average financial loss from OT cyber incidents, annualized across the full scenario distribution. The primary metric for ongoing governance and investment decisions.

ENABLES

Security budget allocation · ROI per remediation dollar · Year-on-year improvement tracking · Board reporting

Value at Risk

VaR

The maximum expected loss at a defined confidence level — expressing tail exposure in a single, defensible figure. Comparable across facilities and communicable to finance and audit committees.

ENABLES

Capital adequacy assessment · Insurance limit sizing · Balance sheet exposure disclosure · Scenario stress-testing

Loss Exceedance Curves

OEP / AEP

The full probability distribution of losses — showing the likelihood of any given loss level being exceeded. Facility-level and portfolio-level curves, both available.

ENABLES

Actuarial pricing · Premium indication · Accumulation modeling · Reinsurance program structuring

WHY THE NUMBER IS DEFENSIBLE

Bottom-up specificity

Every loss estimate is built from your facility's actual data — your assets, your network topology, your CVEs. Facility-level inputs are modeled independently before aggregation to the portfolio. The number reflects your exposure, not a sector average.

Calibrated on real outcomes

The URMS engine is calibrated on 300+ real industrial deployments across US and EU markets — not actuarial tables constructed from surveys. Loss estimates are grounded in observed OT incident mechanics across Power, T&D, Manufacturing, and Data Centers.

Fully traceable audit trail

Every output traces back to the specific facility inputs, model assumptions, and model version that produced it. Assumptions are explicit and versioned. When architecture or threat conditions change, the model can be re-run and the delta explained. The number is a governed artifact — not a static report.

HOW EACH AUDIENCE USES THE OUTPUT

CFO / Finance

Uses AEL to size the security budget and calculate ROI per remediation dollar. Uses VaR to quantify balance sheet exposure and justify insurance spend. Translates cyber risk into financial language that boards and auditors understand.

Board / Audit Committee

Receives a defensible, auditable governance artifact — not a qualitative briefing. AEL and VaR on the board dashboard update as exposure changes. Satisfies directors' duty of oversight with a number that can be challenged and explained.

Chief Risk Officer

Uses CRQ output as the evidence bundle for risk transfer. Loss exceedance curves and bounded scenarios are the submission-ready inputs that underwriting workflows process into actuarial assessments and placement decisions.

Underwriter / Actuary

Receives facility-level loss curves rather than questionnaire narratives. Bounded scenarios and traceable assumptions support premium indication, limit adequacy review, and accumulation modeling across a portfolio of industrial accounts.

To request a methodology walkthrough: **info@denexus.io**