

Cybersecurity Risk Assessment



- Systematic process for identifying, analyzing, and evaluating digital asset risks



- Converts uncertainty into prioritized, business-aligned decisions



- Output: evidence-based risk register linking threats and controls



- Mandatory under NIS2, DORA, ISO 27001, HIPAA, NYDFS



- Goal: build a repeatable, continuously maintained assessment capability



Core Concepts and Terminology

- Foundational terms: asset, threat source, threat event, vulnerability, likelihood, impact
- Risk is a function of likelihood of occurrence and potential adverse impact
- Threats exploit vulnerabilities to cause harm
- Risk assessment identifies and prioritizes; risk analysis estimates; risk management decides treatment
- Qualitative use ordinal bands vs quantitative dollar-denominated loss estimates



Risk Assessment Frameworks and Standards



NIST SP 800-30

nine-step, prescriptive,
threat-catalog-driven,
government-aligned



ISO/IEC 27005

flexible five-step
cycle for ISO 27001
certification



FAIR v3.0

Risk = Threat Event
Frequency × Vulnerability ×
Loss Magnitude



- ✓ NIST SP 800-30: nine-step, prescriptive, threat-catalog-driven, government-aligned
- ✓ ISO/IEC 27005: flexible five-step cycle for ISO 27001 certification
- ✓ FAIR v3.0: Risk = Threat Event Frequency × Vulnerability × Loss Magnitude
- ✓ FAIR output: probability distribution of financial loss, not a color
- ✓ Select by regulatory needs, maturity, and governance vs. financial justification
- ✓ Mature teams layer: ISO/NIST for process, FAIR for top 10–15 risks

Scoping and Asset Identification

- Define assessment boundary, system scope, data flows, and exclusions
- Inventory hardware, software, data, people, processes, and third parties
- Classify data by sensitivity, criticality, and regulatory requirements
- Value assets by business impact, not just replacement cost
- Name an owner for every critical asset



Threat and Vulnerability Identification

- Threat sources: adversarial, accidental, structural, environmental
- Vulnerabilities: CVEs, misconfigurations, control gaps, policy flaws
- STRIDE models threats using data flow diagrams
- Attack trees map step-by-step attacker paths with AND/OR logic
- Use MITRE ATT&CK and CISA advisories for real-world intelligence



ANALYZING LIKELIHOOD AND IMPACT

Combining Threat Event Probability with Adverse Impact Probability

WHAT WE ASSESS

- Combine the likelihood of a threat event with the likelihood and magnitude of adverse impact
- Assess impact across four dimensions: Financial, Operational, Reputational, Regulatory
- Use a 5x5 risk matrix calibrated to our risk appetite
- Matrices struggle with extreme-impact, low-probability events—supplement with scenario analysis

LIKELIHOOD
(Inherent)

5x5 RISK MATRIX						
		IMPACT (Inherent)				
		1 Very Low	2 Low	3 Moderate	4 High	5 Very High
5 Almost Certain	Medium	Medium	High	Very High	Very High	
4 Likely	Medium	Medium	High	High	Very High	
3 Possible	Low	Medium	Medium	High	High	
2 Unlikely	Low	Low	Medium	Medium	High	
1 Rare	Low	Low	Low	Medium	Medium	
		Low	Medium	High	Very High	

SCALE DEFINITIONS

LIKELIHOOD SCALE			
Score	Band	Description	Indicative Frequency
5	Almost Certain	Expected to occur in most circumstances	> 1 per year
4	Likely	Will probably occur in many circumstances	0.1 – 1 per year
3	Possible	Might occur at some time	0.01 – 0.1 per year
2	Unlikely	Could occur but not expected	0.001 – 0.01 per year
1	Rare	May occur only in exceptional circumstances	< 0.001 per year

IMPACT SCALE (Across 4 Dimensions)					
Score	Band	Financial (USD)	Operational	Reputational	Regulatory
5	Very High	> \$100M	Severe disruption > 30 days	Severe market impact	Critical breach / License at risk
4	High	\$10M – \$100M	Major disruption 7 – 30 days	Major negative attention	Material fine / Legal action likely
3	Moderate	\$1M – \$10M	Moderate disruption 1 – 7 days	Notable concern	Reportable incident
2	Low	\$100K – \$1M	Minor disruption < 1 day	Limited interest	Minor violation / Low fine
1	Very Low	< \$100K	Negligible impact	No noticeable impact	No regulatory impact

ASSESSMENT APPROACH

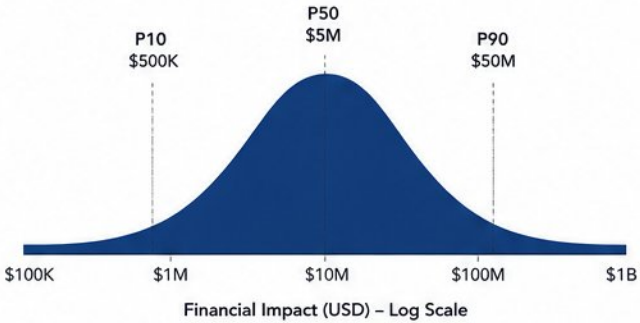
- 

QUALITATIVE (Descriptive Bands)
Use defined bands to ensure consistency and clarity. Focus on informed judgment.
- 

SEMI-QUANTITATIVE (Numeric Bins)
Use numeric bins for impact to improve comparability without implying false precision.
- 

QUANTITATIVE (Dollar Distributions)
For financial impact, model a range of possible outcomes (e.g., P10 / P50 / P90) rather than a single point estimate.

EXAMPLE: FINANCIAL IMPACT DISTRIBUTION



MATRIX LIMITATIONS & COMPLEMENTARY PRACTICES

- 

Risk matrices are less effective for extreme-impact, low-probability events.
- Use complementary practices:
- Scenario analysis and stress testing
 - Expert elicitation
 - Early warning indicators
 - Resilience and response planning
 - Review and challenge assumptions regularly

CALIBRATION TO RISK APPETITE

- 

Align risk appetite with strategy, capital, and stakeholder expectations.
- 

Set thresholds for Low / Medium / High on the matrix based on what we are willing to accept.
- 

Ensure consistent application, document rationale, and avoid false precision.
- 

Review and recalibrate as the business, threats, and external environment change.

Risk Evaluation and Prioritization



- Compare scored risks against defined risk appetite and tolerance thresholds



- Prioritize by severity, exploitability, asset criticality, control effectiveness, and business impact



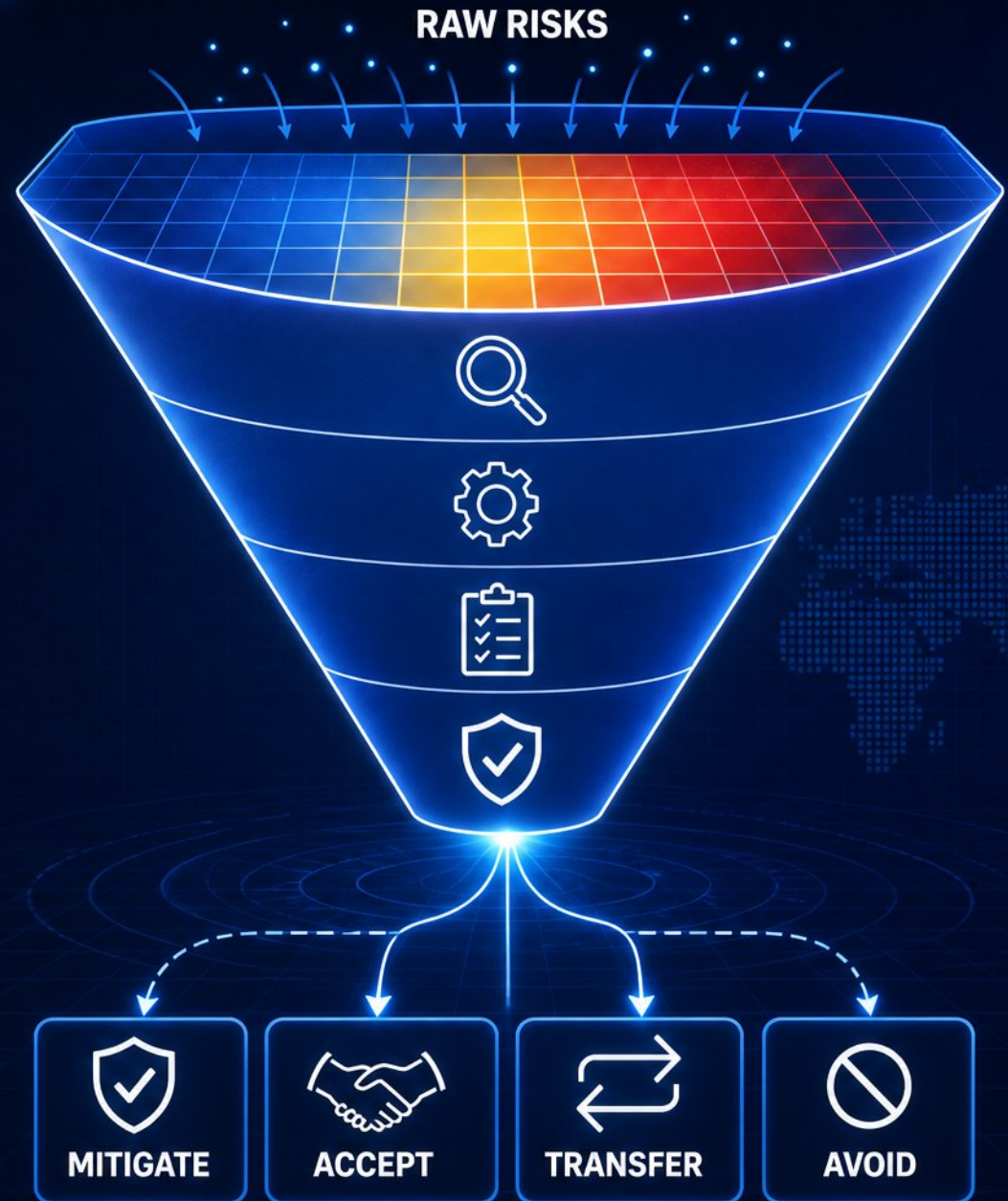
- Choose treatment: mitigate, accept, transfer, or avoid—assign owners and rationale



- Translate findings to financial exposure, operational disruption, and regulatory consequence



- Document decisions; quick wins first, then high-risk complex items



Reporting and Documentation



Risk assessment report: scope, methodology, findings, register, recommendations



Risk register: asset, threat, vulnerability, likelihood, impact, owner, status



Inherent vs. residual: document both to show control value



Audience-specific: business terms for executives, details for IT



Treatment plans: actions, owner, timeline, resources, verification method



Continuous Monitoring and Review

- ✓ - Assessment is a recurring process, not a one-time project
- ✓ - KRIs signal risk deterioration early
- ✓ - Incidents and system changes trigger reassessment
- ✓ - Automated monitoring maintains situational awareness
- ✓ - Annual full reassessment at minimum



Practical Implementation and Tooling



- Define methodology, templates, scoring criteria, roles, and cadence first



- Use GRC platforms, scanners, inventory tools, and risk registers



- Automate CVSS mapping to asset classification for risk scoring



- Start with NIST CSF 2.0 and spreadsheets; mature to platforms



- Assign named risk owners and review dates for every entry



Common Pitfalls and Lessons Learned



- Checklist mindset misses real business impact and threat scenarios.



- Scope gaps: legacy systems, shadow IT, AI tools, third parties.



- Compliance does not equal security; breaches still occur.



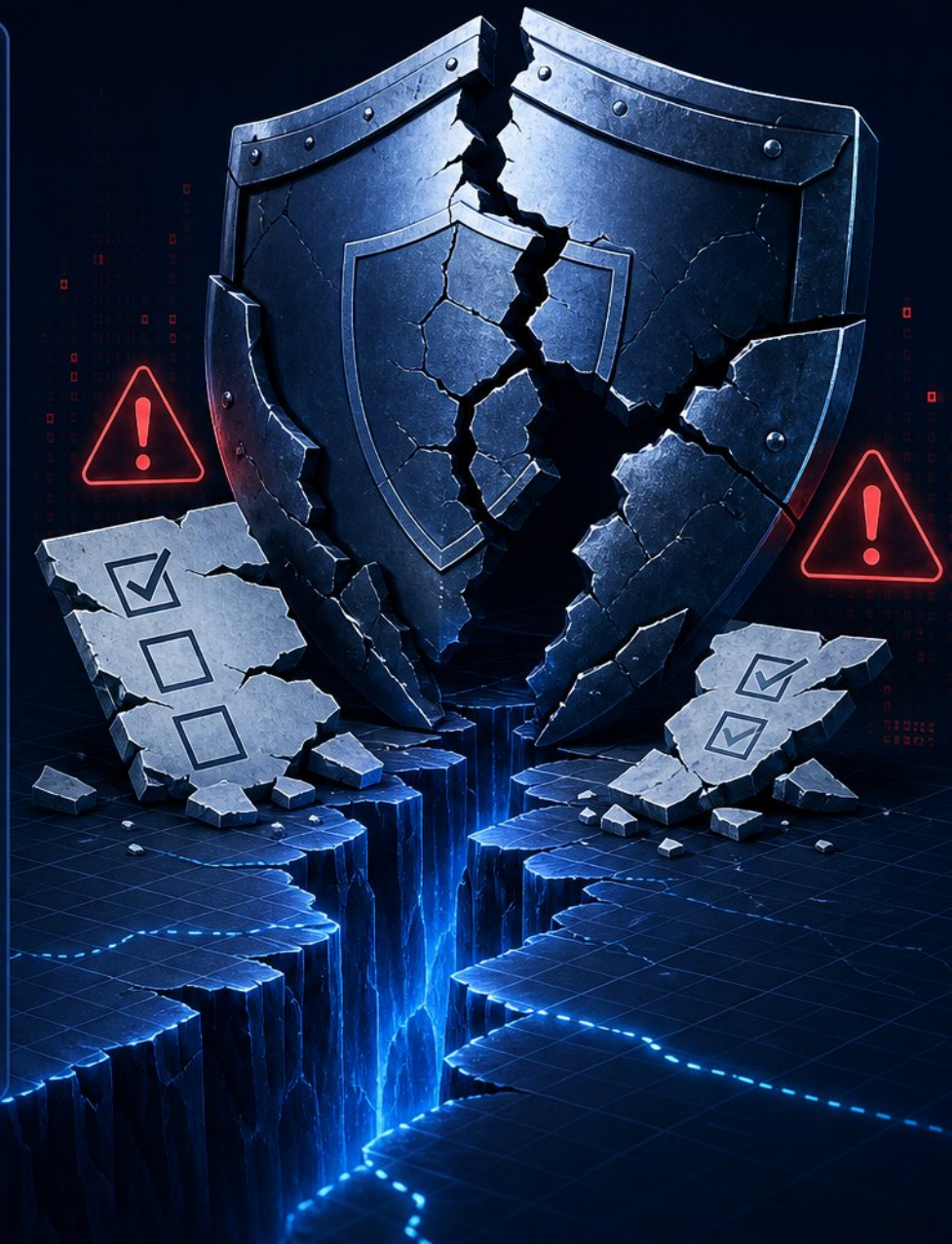
- Sugarcoating results hides threats behind a green dashboard.



- CISA: leadership miscalculated likelihood and impact of known risks.



- NYDFS: generic assessments fail regulatory scrutiny.



Executive and Board Communication



- Quarterly updates plus one annual deep dive; ad-hoc for material incidents



- Translate technical findings into financial exposure and operational disruption



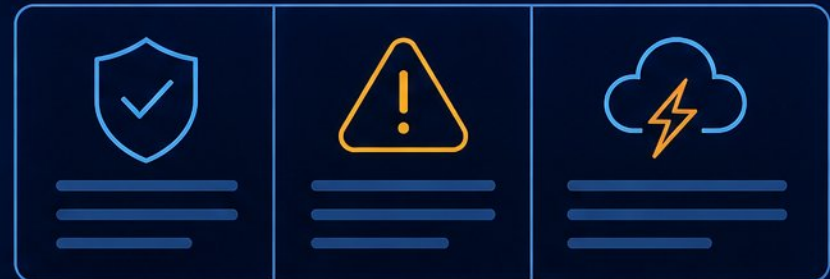
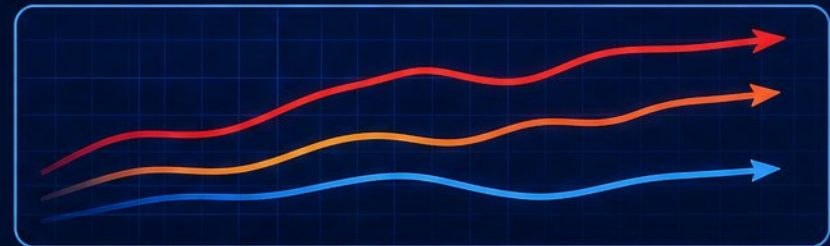
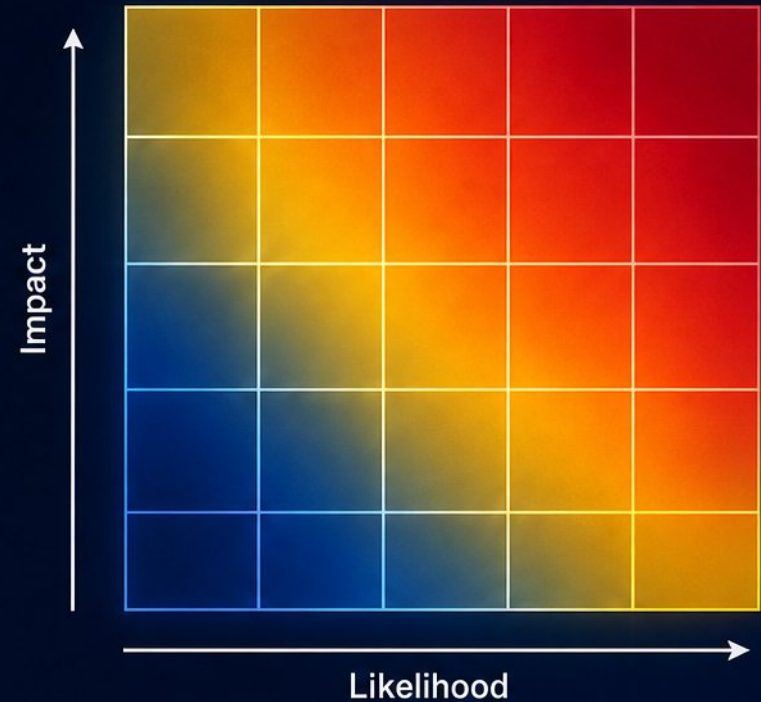
- Dashboards align to risk appetite; use trends and heat maps, not raw vulnerability lists



- Boards ask about appetite alignment, investment rationale, and incident readiness



- Escalate material incidents based on financial impact within 24 hours



ent

A hooded figure in a dark blue hoodie is centered against a dark blue background filled with faint, glowing binary code (0s and 1s). The figure's face is obscured by the hood. At the bottom, there are two glowing arcs: a blue one on the left and a red one on the right. The word "ent" is written in large, white, sans-serif font on the left side of the image.

-
- The diagram illustrates the progression of a cyber threat. At the top, four circular icons are connected by dashed arrows: a globe with a building, a server rack with a globe, a bug, and a factory. Below the second icon, three red dashed arrows point to three hexagonal icons: a network diagram, a shield with a red 'X', and a person with a padlock. Below these hexagons are the labels 'Limited network controls', 'Overreliance on EDR', and 'Weak identity management'. A red trail of footprints leads from the bottom left towards the right, ending near the factory icon.



Action Plan and Course Summary



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/df641021/public