



Compliance • Risk Reduction • Cost Recovery • Guaranteed



Covered Entities should undertake a cybersecurity risk analysis on a regular basis to account for ongoing developments in cybersecurity technologies.

The benefits of using a standardized approach to assess and improve cybersecurity preparedness... firms adopting a standardized approach are better able to track their progress over time, and share information and best practices with other financial institutions and with regulators.

Still relying on outdated risk management models? It's time to get real compliance - and millions in risk reduction and cost recovery - guaranteed.

Despite significant increases in cybersecurity spending, companies are losing more than ever.

REDUCE RISK

- Identifies sources and impacts of specific risks traced back to their contributing threats and vulnerabilities.
- Highest-impact risks can be identified and targeted to their origins resulting in measurable risk reduction.
- Provides for measurable risk reduction with frequent retargeting and calibration.

OPTIMIZE CYBER SPEND

- Provides insurance-grade analysis of current cyber spending in relation to risks being mitigated.
- Enhances visibility and understanding of what value current spending is yielding.
- Ability to identify priorities and optimize overall cybersecurity programs and budgets.

GAIN COMPLIANCE

- Documents organizations risk status and the contributing factors to your current risk.
- Isolates origins of specific risks, their associated costs, all in accordance with regulator-approved frameworks (NIST 800-53, ISO 27001 & NIST CSF)
- Provides documentation in support of risk-related compliance filings.

COST RECOVERY

- Identifies ongoing cost of digital risk - the remaining risk after all current risk mitigation efforts.
- Tracks incremental effectiveness of mitigation efforts attained.
- Provides the ability to compare effectiveness of proposed cybersecurity strategies and approaches.