SERVICE BRIEF

Risk Assessments

Drive risk reduction with quantitative and qualitative results

As critical business operations have become more reliant on a digital workforce, cybersecurity has risen in stature with executives and boards of directors. In order for this audience to best understand relevance of the state of cyber, it’s become increasingly important for cyber risk be addressed from both a quantitative and qualitative perspective, similar to other areas of enterprise risk. Traditional risk assessments rely heavily on reviewing gaps against select controls and are only qualitative in nature, not tying results back to financial and quantitative metrics that business leaders are most interested in. They also often overlook procedural and personnel activities that affect increased risks.

Delivered through a scientific and repeatable methodology that not only looks at existing or desired controls, Optiv risk assessments analyze procedural and personnel risks to provide qualitative and quantitative results. These findings deliver a holistic view of cyber risk throughout your organization. Results and documentation are designed to be easily understood at executive and board levels to highlight potential losses that can affect your organization’s bottom line while also providing you an actionable path to prioritize future investments and activities to reduce overall enterprise risk.

Optiv Solutions

Delivered through a scientific and repeatable methodology that not only looks at existing or desired controls, Optiv risk assessments analyze procedural and personnel risks to provide qualitative and quantitative results. These findings deliver a holistic view of cyber risk throughout your organization. Results and documentation are designed to be easily understood at executive and board levels to highlight potential losses that can affect your organization’s bottom line while also providing you an actionable path to prioritize future investments and activities to reduce overall enterprise risk.

How We Do It?

Phase 1
Review of your existing programs, risk appetite and asset valuations

Phase 2
Data gathering via Review, Interview, Inspect, Observe and Test (RIIOT) methodology.

Phase 3
Evaluation of threats, vulnerabilities, impacts and likelihood

Phase 4
Risk analysis

Phase 5
Results delivery

As organizations continue to rely more on digitization, cyber risks are more ingrained with overall business risk.
Why Clients Choose Optiv

Averaging more than 15 years of experience each, Optiv’s Risk Management and Transformation team brings a wealth of knowledge to every client engagement. Many are former CISOs, CROs, and CIOs with in-depth familiarity of numerous industries.

Risk Expertise:

15+ Years
Average industry experience for the Risk Management team

Risk Standards Expertise
ISO31000, ISO27005, FAIR, OCTAVE, NIST 800-30, NIST 800-37, NIST 800-39, NIST IR 8062 and more

Inspired Thought Leaders
40+ textbooks, 100s panels, 1,000+ articles, ExecRank Top 100 and more

Industry Expertise
Healthcare, Finance, Manufacturing, Critical Infrastructure, Retail, Aerospace and Defense, Energy and more

Case Study

CUSTOMER PROFILE
Public Insurance Company

DESIRED OUTCOMES
Document the risks being faced by the client’s public key infrastructure (PKI) and recommend mitigations to manage those risks.

SOLUTION
Optiv’s Risk Management and Transformation team perform a health check of the public key infrastructure (PKI) environment, documenting the organizational risks associated with operating a PKI environment. The impact of confidentiality, integrity, or availability risks were reviewed in a collaborative format with the client. Key controls were then mapped against those risks and areas for risk reduction or acceptance were identified. Findings and recommendations were then presented to the board for review and next steps.

CLIENT BENEFITS:
• Third-party recommendations on how to reduce risk
• Alignment on unmitigated and mitigated risks
• Clear prioritization of risks

Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

Secure your security.™

©2020 Optiv Security Inc. All Rights Reserved.