ENTERPRISE RISK MANAGEMENT

Identify, Mitigate and Manage Cyber Security Risk

OVERVIEW

Understanding and evaluating risk means smarter decision-making in business. Once you have perspective on the risks you face, you can modify your security program, optimize current technology usage, plan future investments and address risks more effectively.

Optiv can help you get the answers you need to evaluate opportunities and analyze risk. Our 360 degree view of the security space means we take a comprehensive approach to track, triage and treat potential hazards and threats. We can translate your requirements into in-depth remediation recommendations that take into account the technology, people and processes specific to your organization.

Our Enterprise Risk Management Approach:

1 Identify risk events
2 Assess the probability of each event
3 Make a cost-benefit analysis of response alternatives
4 Choose a response
5 Re-assess probability and impact with company response
6 On-going monitoring of risk events

By 2020, **75 percent** of ENTERPRISE INFORMATION SECURITY BUDGETS will be allocated for rapid detection and response approaches, up from **LESS THAN 10 percent** in 2012.
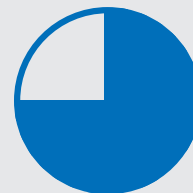
-Gartner

Enterprise Risk and Compliance:

At Optiv, we help organizations move from discrete, compartmentalized efforts to programs that strategically address the big picture. Our experience and unique perspective on the industry translate into in-depth remediation recommendations that take into account the technology, people and processes specific to your organization. Using our proprietary organizational maturity model, we help you evaluate current practices, identify gaps and map your security goals to your business objectives.

Results-driven benefits of working with our risk professionals include:

- Identify, assess and quantify your risks
- Optimize your security spending to focus on what matters to your organization
- Reduce risk and demonstrate compliance

Will *you* be ready?

1. Information Security Risk Management

Goal

Evaluate and document current controls and their intent and actual function.

Overview

Security control assessments provide a line of defense in knowing the strengths and weaknesses of an organization's information system. Our security controls assessment verifies and documents controls and their function. This independent, third-party controls analysis can be customized to meet specific client needs. Post-engagement, clients will receive detailed documentation of the project including controls verification. This record can be used to advance the overall effectiveness of your risk mitigation program.

OUTCOMES

› Identify and Document Your Controls

› Validate that Your Existing Controls are Operating as Intended

› Gain Insight into the Strengths and Weaknesses of Your Current Defense Program

› Facilitate a Cost-Effective Approach to Correcting Deficiencies in a Way that is Consistent with Your Organization's Requirements

2. Security Maturity Assessment

Goal

Assess an organization's current controls and benchmark those controls against leading practices and industry standards.

Overview

During a security maturity assessment, Optiv examines current controls and provides a maturity assessment based on a standards-based proprietary evaluation process. This independent third-party assessment benchmarks current controls and practices against leading methods and industry standards. Understanding how you manage risk relative to leading best practices and your organization's appetite for risk can help you optimize your security investments.

OUTCOMES

› Understand Your Current Risk Posture Relative to Leading Practices, Compliance Requirements and Peer Organizations

› Reconcile Your Current Practices with Your Organization's Appetite for Risk

› Gain Insight into the Strengths and Weaknesses of Your Current Defense Program

› Optimize Your Current Program to More Closely Align with Your Security and Risk Mitigation Goals

› Identify Areas of Operation that Present too High a Risk for Your Organization

3. Security Risk Assessment

Goal

Assess, identify and modify your security posture to identify areas of weakness.

Overview

A comprehensive enterprise security risk assessment identifies and quantifies risk in an environment. A risk assessment also helps your organization ensure that it is compliant with regulatory administrative, physical and technical safeguards. This service also helps reveal areas where your organization's essential information, including protected individual information (PII), protected health information (PHI) and credit card data, could be at risk.

OUTCOMES

› Document Existing Controls and Security Efforts to Demonstrate that a Control System is in Place and Operating Effectively

› Take a Proactive Approach to Securing Your Organization

› Identify and Quantify the Risks to the Organization's Information Assets

› Examine Weaknesses from the Perspective of an Attacker

4. Policy Assessment and Development

Goal

Assess the effectiveness of your current policies and modify existing or develop new policies to more closely align with your business goals.

Overview

Your security policies are an essential component of your overall risk management program. We can help you examine your current policies, determine if they are aligned with your business goals and help modify existing policies or create new ones to optimize your risk approach. We leverage leading practices and our extensive experience developing programs for clients in every industry to quickly advance and customize your program and keep you nimble enough to respond to new and evolving threats.

OUTCOMES

› Improve New or Existing Policies and Align Them to Your Business Goals

› Establish Confidence in Your Current Policies and Controls

› Provide Better Audit Documentation to Support Your Compliance and Regulatory Requirements

› Optimize Your Risk Approach

› Plan for Future Events and Emerging Threats

› Adopt Leading Practices and Industry Standards

› Advance Your Current Program Quickly and Cost-Effectively

› Create a Faster Risk Management Approach

5. Governance, Risk and Compliance (GRC) Consulting and Implementation Services

Goal:

Deploy GRC technology to automate the management of your enterprise governance, risk and compliance programs.

Optiv provides support and expertise for your GRC automation effort. We help create a centralized repository of information that provides an enterprise view of risks and threats. We also identify areas for focus and improvement to mitigate risk throughout your enterprise. This centralized view supports timely decision-making informed by data from across your organization. Our knowledge and hands-on experience with leading GRC automation platforms helps you achieve a rapid time to deployment with early wins to deepen project support.

SERVICES:

› GRC Roadmap and Integration

› Allgress, Archer, Lockpath, RSAM

› GRC Custom Consulting

› GRC Staff Augmentation

OUTCOMES:

› More Efficient Deployment Effort

› GRC Automation Mapped to Your Organization's Business Needs

› Support for Early Deployment Wins as well as Programmatic Development of Your Long-Term GRC Road Map

› Benchmark Your Current GRC Program Maturity

Additional Services:

› Third-Party Risk Management Consulting

› Data Loss Prevention Consulting

› Capabilities Assessments

› Staff Augmentation

Custom Risk Management Consulting

Optiv's enterprise and compliance experts and consultants have delivered high-quality engagements to thousands of clients. We routinely assist organizations by assessing policies, procedures and the human element of complex systems. As part of our commitment to quality and client service, we deliver detailed documentation of our findings along with actionable recommendations to eliminate problems now and in the future. We can help you find solutions for your current needs.

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.