SecurityMetrics

NIST 800-30 RISK ASSESSMENT

NIST 800-30 is a framework to conduct a thorough risk analysis. A thorough risk assessment is an important step to ensure your organization's data is secure.

MEET COMPLIANCE REQUIREMENTS

Achieving and maintaining compliance protects your business from fines and penalties, ultimately keeps clients, partners, or upper management happy. Completing a NIST 800-30 Risk Assessment fulfills aspects of regulatory compliance standards such as PCI DSS, HIPAA, EI3PA, GLBA, FISMA, and SOX.

EFFECTIVELY MANAGE AND MITIGATE RISK

An organization's data is one of its most important assets. A NIST 800-30 Risk Assessment helps you identify threats, vulnerabilities, and risks to your organization and sensitive data. The results of your Risk Assessment guide your remediation efforts and risk management efforts moving forward.

RISK ASSESSMENT PROCESS

1. Prepare for Assessment – Identify the purpose and scope of the assessment. Determine how and where sensitive data is created, transmitted, and stored.
2. Threat Sources and Events – Identify the type of threat sources your organization faces (e.g. adversarial, accidental, structural, environmental) and the events the sources could trigger (e.g. phishing, power outage, etc.).
3. Vulnerabilities and Predisposing Conditions – Through identifying threats you identify vulnerabilities, which can be associated to information systems or environments where those systems operate. This will also identify predisposed conditions to consider during the risk assessment (e.g. architectures and technologies employed, personnel, etc.).
4. Determine Likelihood of Occurrence – Using different tiers, determine the likelihood of threat events occurring and causing adverse impacts.
5. Determine Magnitude of Impact – Once likelihood of occurrence is determined, use tiers to determine the impact of threat events.
6. Risk Determination – Combining the likelihood and the magnitude of the impact of a threat determine the risk to the organization.

CONDUCTING A THOROUGH RISK ASSESSMENT WILL NOT ONLY HELP MEET COMPLIANCE REGULATIONS, BUT GET YOU STARTED ON THE PATH TO EFFECTIVE RISK MANAGEMENT.

7. **Informing Risk Response (Communicate Results)** – Ensure the appropriate people inside the organization understand the appropriate risk-related information to inform and guide decision-making. Often times risk assessment reports are used to communicate within the organization.
8. **Maintain Assessment** – Monitor risk factors identified in the risk assessment and update the risk assessment as threats, vulnerabilities, and risks change.

SIMPLIFYING COMPLIANCE

To simplify your regulatory compliance efforts, when you engage SecurityMetrics for your NIST 800-30 Assessment, you'll also benefit from the following:

- **Compliance Vendor** –Expertise in PCI assessments, forensic incident response, vulnerability scanning, penetration testing, card data discovery, security appliances, PA-DSS application security assessments, P2PE assessments, HIPAA assessments, training, and consulting. SecurityMetrics is one of only a few companies that hold credentials for all aspects of PCI.
- **Open and Ongoing Relationship** – Whenever compliance questions or worries arise, SecurityMetrics' compliance professionals will work with you to address your concerns.
- **Accurate and Understandable Results** – SecurityMetrics gives you the facts on every aspect of your assessment through an easy-to-understand online reporting console.
- **Single Point of Contact** – To keep communication lines open and eliminate confusion, SecurityMetrics assigns a single point of contact for each assessment.
- **Fair, No-Surprise Pricing** – SecurityMetrics strives to offer simple and straightforward pricing with a single bid that won't change.
- **No Long-Term Contracts** – SecurityMetrics never locks you into a long-term contract.

ABOUT SECURITYMETRICS

SecurityMetrics is a global leader in merchant data security and compliance for all business sizes and merchant levels, and has helped secure over 1 million payments systems. SecurityMetrics helps organizations secure their network infrastructure, data communication, other information assets and/or manage PCI DSS compliance. As an Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Payment Application Qualified Security Assessor (PA-QSA), Point-to-Point Encryption auditor, Penetration Tester, and Payment Card Industry Forensic Investigator (PFI), SecurityMetrics has the knowledge and tools available to help businesses achieve lasting security and validate accurate PCI compliance.

securityMETRICS®