# Security Risk Assessment

Solution brief

Know where the risks are.

**Your business is built on a digital foundation. With a rapid evolution in the digital workplace, from a distributed workforce to online customer engagement, organizations may be exposing themselves to new cyber threats. How confident are you that you clearly understand the risks you face?**

Organizations today are highly reliant on their information, systems and networks to support customers and employees. Meanwhile, attackers both inside and outside the company continually search for ways to compromise these assets and steal financial and proprietary data. As your industry threat profile and attack surfaces change, it can be difficult to know if your people, processes and technology are up to the task.

Verizon's Security Risk Assessment is designed to provide you with an objective, repeatable, standards-based assessment of your information security risk through a detailed analysis of key business systems. Our methodology employs a standards-based approach combined with underlying data analysis from the industry-recognized Data Breach Investigations Report. The outcome is a clear understanding of information security risks associated with your sensitive data and a prioritized set of recommendations for reducing the risk of compromise.

## Address your risk in one assessment.

The Security Risk Assessment employs a NIST-based risk methodology (NIST 800-30) where risk is calculated based on a) the likelihood of a breach of the business system, and b) the business impact such a breach would have on the customer. The likelihood of a specific business system being compromised is determined using threat, vulnerability, and information security control analyses, and a risk rating for each business system in scope is assigned.

The assessment also includes an analysis of information security controls in order to identify vulnerabilities in people, processes and technology, using one of six commonly used industry security standards:

- ISO 27002: The primary international standard that provides a common baseline upon which most other security requirement documents have been developed
- NIST CSF: A more focused and simplified set of security control requirements
- NIST 800-53: A catalog of security controls to support implementation of security programs around public institutions and private corporations
- NIST 800-171: a catalog of security controls to support the protection of Confidential Unclassified Information (CUI) in non-federal (e.g., defense contractor) information systems and organizations
- HIPAA/HITECH: used within the healthcare community as the baseline standard for implementing and mainlining data protections around Protected Health Information (PHI)
- PCI DSS: The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard provided by the Payment Card Industry Security Standards Council and establishes the requirements for the information security controls required of organizations that handle payment cards

The security framework used for assessment is determined by the organization.

verizon

## Applicable to every organization.

The Security Risk Assessment is relevant to public and private institutions in both regulated and unregulated industries, and for companies of all sizes.

The standard assessment is offered in three sizes:

| Size | Employees | Location | Business Units | Business systems evaluated |
|---|---|---|---|---|
| Small | <1000 | one US HQ/DC location (no int'l) | one primary | Up to 5 |
| Medium | <10,000 | one US HQ/DC location (no int'l) | Up to 3 primary | Up to 10 |
| Large | 10,000 - 50,000 | one US HQ/DC location (int'l remote only) | Up to 4 primary | Up to 15 |

Customized risk assessments are also available on request. Regardless of scale, each assessment follows four phases:

**Phase 1:** We work with you to identity the relevant documentation and individuals that are required to perform the assessment.

**Phase 2:** We review provided documentation, interview identified individuals and collect information on your business systems and security protections.

**Phase 3:** We analyze your information security protection maturity, performance, and scope relative to the selected security standard. Using a threat and business impact analysis of the identified business systems, we develop an information security risk rating for each.

**Phase 4:** We provide a report on our findings as well as detailed, prioritized recommendations designed to help you improve information security protections and avoid or reduce information security risk to identified business systems.

## An optional roadmap to implementation.

Not sure what to do with the final report? We can help you with a detailed roadmap for implementing our recommendations. If you select this option, we will work with you to determine the recommendations to be included in the roadmap, and then develop detailed project definitions, timing, costs and staffing projections for each project. This can give you a clear path to peace of mind.

## Why Verizon.

As an award-winning leader in cybersecurity, we keep up with the rapidly changing nature of cyber threats by processing billions of security events each year, analyzing evolving threats at our global security operations centers, performing forensic investigations for companies around the world, and sharing our knowledge through industry-recognized content like the annual Data Breach Investigations Report.

We differ from other security service providers because our substantial risk and incident experience lets us understand the real-world threats you face and the potential vulnerabilities in each system. And, our years of practical experience in developing and implementing security programs across all industries helps you know that our priority is your long-term success.

## Learn more.

For more information on Verizon's Security Risk Assessment, contact your account representative.

For the 2020 Data Breach Investigations Report, go to: enterprise.verizon.com/resources/reports/dbir

verizon