Security Program Assessment

Solution brief

Know where the gaps are.

Your business is built on a digital foundation. Today, that core is stressed as your ways of working, from a distributed workforce to online customer engagement, are undergoing rapid evolution. How confident are you that your existing security program is up to the challenge?

Organizations today are highly reliant on their information, systems and networks to support customers and employees. Attackers both inside and outside the company continually search for ways to compromise these assets and potentially deliver you a devastating blow. Your information security programs are intended to ensure that you are protected from these threats, but it can be difficult to know if they have remained relevant in a time of rapid change.

Verizon's Security Program Assessment is designed to provide you with an objective, repeatable, standards-based assessment of the programs and practices that protect the confidentiality, integrity and availability of your information and environments. We look at the three dimensions of security control effectiveness: maturity of the solution, performance of the solution to the controls expectation, and scope of application of the solution.

Our methodology provides you a detailed review compared with your preferred information security control framework, and the outcome is a clear understanding of your program maturity, the gaps that could be exploited, and a prioritized set of recommendations to reduce the risk of compromise.

Address compliance and risk in one assessment.

The Security Program Assessment evaluates your security program against commonly used industry security standards for data protection:

- 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 standard used for assessment is determined by the organization.

verizon

Applicable to every organization.

The Security Program Assessment is relevant to public and private institutions in both regulated and unregulated industries, and for companies of all sizes. Small businesses and start-ups leverage assessments to help define their security programs while mature global conglomerates can use them to measure the standardization of their programs.

The standard assessment is offered in three sizes:

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

Customized program 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 security program.

Phase 3: We analyze your security program's maturity, performance, and scope relative to your requirements. We also develop compliance and maturity scores from this analysis and identify potential risks and gaps in your program.

Phase 4: We provide a report on our findings as well as recommendations designed to help you reduce risks and achieve better alignment with your selected framework.

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 security controls that are effective, and not effective. 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 Program Assessment, contact your account representative.

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

verizon