Cybersecurity Risk Assessments

Identify your security risks and protect against future attacks

Security is no longer "nice to have." It's an imperative. And we're here to help simplify security complexity and protect you from attack.

With all the disparate solutions in today's cybersecurity vendor landscape and ever-mounting security threats, defining an impenetrable security strategy is challenging, even for the most mature of organizations. At OneNeck® IT Solutions, we believe that security is a never-ending journey, but like any journey, it has a clear starting point — and that starting point is understanding your current state with a vulnerability assessment, and then prioritizing steps to mitigate your risk. This is no easy task and makes partnering with a trusted IT security services provider a crucial business decision.

At OneNeck, our security assessment services address the broad scope of security and compliance needs that businesses face. Our team is made up of security experts who stay current on the emerging threats so they can help you understand your risk and articulate a security roadmap that will keep you safe from breach. Our scalable security assessments are based on industry standard controls and proven best practices, including:

- ISO 27001 ISMS: The ISO 2700 family of standards helps organizations keep their information assets secure. This includes assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. While there are more than a dozen standards in this family, ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS), which entails a risk management process applied to the people, processes and IT systems in an organization.
- CIS Top 20: The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace.
- ISO 27002: This standard gives guidelines for organizational information security standards and information security management practices including

OneNeck® IT SOLUTIONS a TDS® Company

the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

- NIST SP 800-171: Created by the federal government, NIST 800-171 is a framework that specifies how your information systems and policies need to be setup in order to protect Controlled Unclassified Information (CUI). To comply with CUI requirements, your organization must fully understand what CUI it stores, processes or sends in the course of doing business with the federal government, and you must also be prepared to provide adequate documentation describing your technical solutions, policies and evidence of being able to detect and respond to incidents.
- NIST SP 800-53: NIST 800-53 is a publication that recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security. It subdivides security controls into common, custom and hybrid categories. Common controls are those often used throughout an organization. Custom controls are those intended to be used by an individual application or device. Hybrid controls start with a standard control and are customized per the requirements of a particular device or application.
- PCI DSS 3.2: The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)

.

Baseline Security Risk Assessment

Security risk assessments are essential for discovering risk and defining appropriate mitigation strategies that fit your company's objectives. In our baseline security assessment, our security experts assess your current security posture and identify which devices, programs and applications are putting at risk right now. As a result, this baseline snapshot gives you the visibility you need to develop a security strategy that will help you manage risk and prevent future breaches.

Security Audit & Gap Analysis

In this more in-depth assessment, OneNeck's security experts not only evaluate your current security posture based on applicable controls, but will deliver an actionable roadmap based on industry-standard controls and frameworks that will serve as a guide in mitigating your risk. The recommendations report will help you prioritize your security projects based on critical vulnerabilities and long-term target-maturity initiatives.

Vulnerability Assessment & Penetration Testing

A vulnerability assessment, along with penetration testing, provides your organization with a truly comprehensive application evaluation, more than one single test alone could provide. This assessment is divided into two steps:

- Vulnerability Assessment: The vulnerability assessment portion of the engagement discovers what vulnerabilities may exist in your environment which leave you open to attack.
- Penetration Testing: In the penetration testing phase, our security experts attempt to exploit the vulnerabilities to determine if unauthorized access or other malicious activity is possible, and then measure the severity of each.

OneNeck Has You Covered

Clearly understanding where you are and what vulnerabilities exist can save significant time, money and distress down the road when under attack. Don't go it alone. We're here to help you stay safe from emerging risks that leave you exposed, while allowing you to maintain a balance of productivity and operational effectiveness.

About OneNeck® IT Solutions

OneNeck IT Solutions provides world-class, hybrid IT solutions for thousands of businesses around the globe. From cloud and hosting solutions to managed services, ERP application management, professional services, IT hardware and top-tier data centers in Arizona, Colorado, Iowa, Minnesota, Oregon and Wisconsin, OneNeck has the expertise to help customers navigate the cloud to get the right application on the right cloud at the right time.

OneNeck is a wholly owned subsidiary of Telephone and Data Systems, Inc. [NYSE: TDS]. A Fortune 1000® company, TDS provides wireless; wireline and cable broadband, TV and voice; and hosted and managed services to approximately six million customers nationwide.

Part #6.3.1_SSASAM_0208_v1

OneNeck® IT SOLUTIONS
a TDS® Company

Call 855.ONENECK | Visit OneNeck.com