opentext™

OpenText Security Health Check Service

Cost effective review that targets high-impact, strategic cyber-security controls.

👁 **Visibility** into current capabilities for 6 foundational security control areas

👍 **Actionable Recommendations** to address gaps and drive security posture

🛡 **Reduced Risk** through improved procedures

Organizations must be proactive and resilient in mitigating cyber and regulatory risks. As these risks have increased in number and complexity, many organizations have reacted with many new tools and processes, but may have lost sight of the building blocks of a cyber resilient program. Maintaining a complete picture of foundational security controls and capabilities is critical to preventing and responding to cyber-attacks.

A resilient cyber program must maintain a clear understanding of its capabilities. Further, compliance requirements necessitate that businesses assess their risks regularly to ensure that security controls are in place and operating effectively. A Cyber-security Health Check is a great way to achieve these objectives.
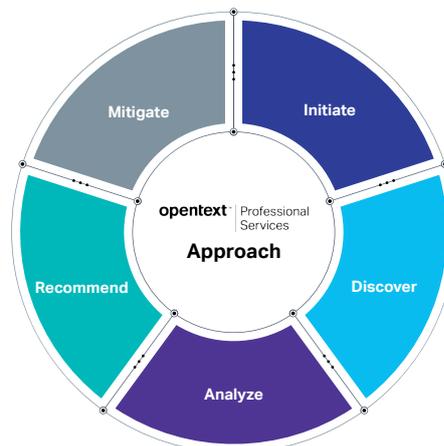
Health Assessment Workflow

opentext™

Visibility—Having a clear line of sight to control activity maturity provides valuable information on an organization's cybersecurity risk posture to support informed decision-making. Having OpenText professional services provide an independent assessment of foundational controls ensures that you are have your bases covered.

Actionable Recommendations—The key deliverable is a security assessment report featuring an executive summary, identified risks and recommendations for improvement. The recommendations will be prioritized by the associated risk impact and ease of implementation.

Reduced Risk—The implementation of recommended action plans are designed to reduce the risk of a cyber incident or regulatory fines.

Inventory and Control of Hardware Assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.
Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of oppotunity for attackers.
Controlled Use of Administrative Privileges	The proesses and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Maintenance, Monitoring and Analysis of Audit Logs	Collect, manage, and analyze udit logs of events that could help detect, understand, or recover from attack.

OpenText Security Health Assessment Process

To talk to a Security Services expert, please contact securityservices@opentext.com

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact Twitter | LinkedIn