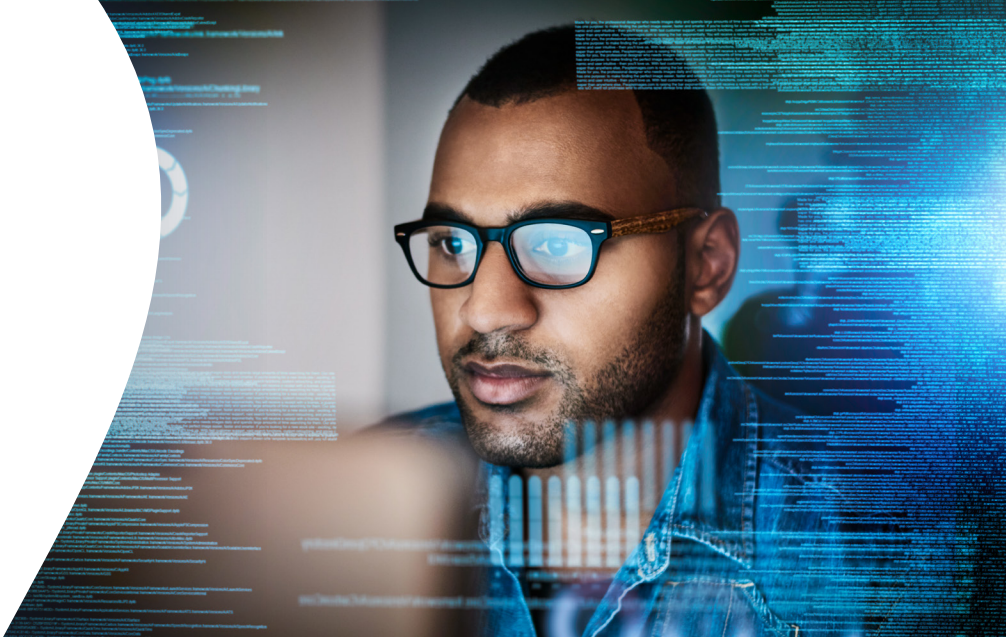
CDW Professional Services

Our assessments elevate the security of your IT environment.



Cybersecurity Capability Assessments

In 2022, there were more than 1,800 publicly disclosed data breaches in the United States, impacting more than 422 million individuals. These breaches occur in a myriad of ways — intentional and unintentional, technical and nontechnical, malicious and benign — and are driven by a complex web of technology and business challenges, including aging or misaligned technology, poor policies and practices, complex infrastructures, and lack of security awareness in the organization. With CDW's Cybersecurity Capability Assessments, organizations gain the insights needed to remediate these issues, reduce incident likelihood and severity, and build strong, sustainable cybersecurity programs.

CDW's Cybersecurity Capability Assessments can help you achieve:

Operational Efficiencies | **Reduced Risk** | **Reliability**

Finding the Right Solution

Cybersecurity Capability Assessments from CDW give organizations practical guidance for addressing key risks and improving their overall risk posture. Our assessments use industry-recognized security frameworks, including the NIST CSF, NIST 800-53, CIS Top 18 Critical Security Controls, ISO 27001/2 and PCI DSS, and are designed to identify critical cybersecurity risks and opportunities for improvement. By leveraging the established Capability Maturity Model (CMM), we can objectively evaluate your program and provide realistic maturity rankings across industry standards. Our approach focuses on three main stages to provide you with a holistic view of your cybersecurity program.

Phase 1: Project Planning
CDW guides your organization toward a maturity strategy that provides a clear scope and objectives, and establishes a communication method and cadence for status reporting. Leveraging this information, we coordinate with your organization to set up document and interview requests.

Phase 2: Program Analysis
CDW conducts both on-site and remote discovery sessions with key stakeholders and subject matter experts within your organization. We then build a current state gap analysis of your policies, procedures and technologies against industry standards. Using the Capability Maturity Model, we evaluate each domain within your security program to understand the confidentiality, integrity and availability of business systems, and identify and document areas for process improvement.

Phase 3: Remediation Strategy
CDW establishes achievable target cyber maturity goals for your program, provides future state recommendations for improvement and delivers a roadmap for short-term and long-term cyber maturity.

CDW + CYBERSECURITY MATURITY

Our Cybersecurity Capability Assessments help organizations build a strong, sustainable cybersecurity program due to our:

- **Broad Security Expertise:** Our team brings expertise in a broad range of security disciplines, enabling us to holistically assess the people, processes and technology that drive your security program.
- **Full Lifecycle Support:** From new program design to the configuration of your existing security environment, CDW has the experts and services to improve all security domains.
- **Risk Reduction:** Cybersecurity Capability Assessments can provide clear, practical guidance for addressing key risks and reducing your exposed attack surface.
- **Ongoing Support:** We provide ongoing support to implement new policies, procedures and technologies and execute on project roadmaps.

CDW's full lifecycle of Services can support your organization no matter where you are on your journey

Design → Orchestrate → Manage

On-Premises → On-Journey → Cloud-Based

CDW

Services Overview

The following deliverables and outcomes are included in Cybersecurity Capability Assessments:

Cybersecurity Capability Assessments	Available
Deliverables	
A documented mapping of your current program against industry frameworks	✓
A report on identified process inefficiencies and opportunities for improvement	✓
Summary for executive audiences	✓
Established target cyber maturity goals	✓
Long- and short-term roadmaps to maturity	✓
Outcomes	
Measure the overall condition of the IT infrastructure, current business processes and utilized technologies	✓
Identify and understand process inefficiencies and areas in need of improvement	✓
Align cybersecurity priorities to your organizational objectives and policies	✓
Allocate resources more efficiently	✓
Make well-informed decisions regarding the level of risk associated with the current IT environment	✓

Cybersecurity Capability Assessments Areas of Focus

The following domains are covered within CDW's Cybersecurity Capability Assessments:

- Threat and Vulnerability Management
- Audit Logging
- Anti-Virus and Malware Management
- Secure Systems Development
- Incident Identification and Response
- Patch Management
- Data Loss Prevention
- Security Awareness Training
- Logical Access and IAM
- Data Encryption
- Data Classification
- Compliance Management
- Configuration Management
- Risk Management and Assessment
- Third-Party Management

To learn more about CDW's Cybersecurity Capability Assessments, contact your account manager or call 800.800.8239.