Formal Cybersecurity Assessments

A security assessment is a thorough, proactive study of an organization's systems that helps identify security challenges and implement solutions. Assessments help identify and prevent security issues, meet national standards, and gain voter trust. They can also justify a budget and guide procurements of security resources, tools, and services.

Formal cybersecurity assessments are a fundamental aspect of managing cybersecurity risk. Assessments can take many forms, but good ones are based on a highly-accepted risk framework, like ISO 27000 series, the NIST Cybersecurity Framework, and the CIS Controls.

Most importantly, you need to be prepared to do something about the results of your assessments. Most will provide some prioritization of results. Once you have these results, develop a plan of action and milestones to get issues addressed.

Risk assessments are a common form of assessment that can be sorted into two categories:

1. Self-assessments: In-house risk assessments are generally faster and less expensive while still providing useful insight into your cybersecurity posture.
2. Independent assessments: Because they are conducted by outside assessment specialists, independent assessments usually cost more and take longer, but they are more objective and thorough. Where time and resources permit, they are preferable even when an organization has deep cybersecurity experience.

Goals

1. Understand and determine the type and extent of cybersecurity assessment your organization should undergo (Level 1 maturity)
2. Use the results to improve your cybersecurity posture (Level 1 maturity)
3. Implement a risk assessment program (Level 2 maturity)

Actions

For Formal Cybersecurity Assessments, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Choose a type of assessment.
2. Perform a security assessment.
3. Receive results of the assessment.
4. Do something about the results.

Keep it simple. If you haven't implemented the critical actions for the Level 1 maturity yet, start with those. If you have, consider stepping up to vulnerability scanning or a risk and vulnerability assessment. Review the CISA's CyHy site or contact CISA at vulnerability_info@cisa.dhs.gov for more information.

Whatever you choose to do, figure out how often you should do it, stick to it, and add to it when resources permit.

Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Consider a more robust assessment program. While conducting large assessments can provide significant information about your systems and put you in a great position to harden them, they can be expensive and resource-intensive.
2. Focus on automated or structured tools and services for understanding your systems. There are many options available to you.
   - Review the options CISA offers through its resource hub with your technical staff and decide which services make sense for you and how often you should use them.
3. Consider implementing the CIS Controls and CIS Benchmarks.
   - Tools available to election offices include CIS-CAT, which can automate much of the process of implementing appropriate safeguards.

Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Implementing sophisticated controls and undergoing both internal and independent assessments. All of the tools mentioned above are still in play for you, but you should be implementing them as part of a well-crafted overall plan. Build this into your program documentation, track progress, and seek new ways to conduct regular, automated, or continuous monitoring of your risk framework.

Cost-Effective Tools

- CISA's Cyber Hygiene Services: CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Types of scans and assessments include vulnerability scanning, web application scanning, phishing campaign assessments, and remote penetration testing.
- CIS Controls: see the CIS Controls best practice
- CIS Benchmarks: Secure configurations for more than a hundred of the most common software applications.
- CIS-CAT Pro: a tool freely available to EI-ISAC members to support implementation of the CIS Controls

Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls, though assessments can be conducted against the CIS Controls using the tools listed above.

Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices