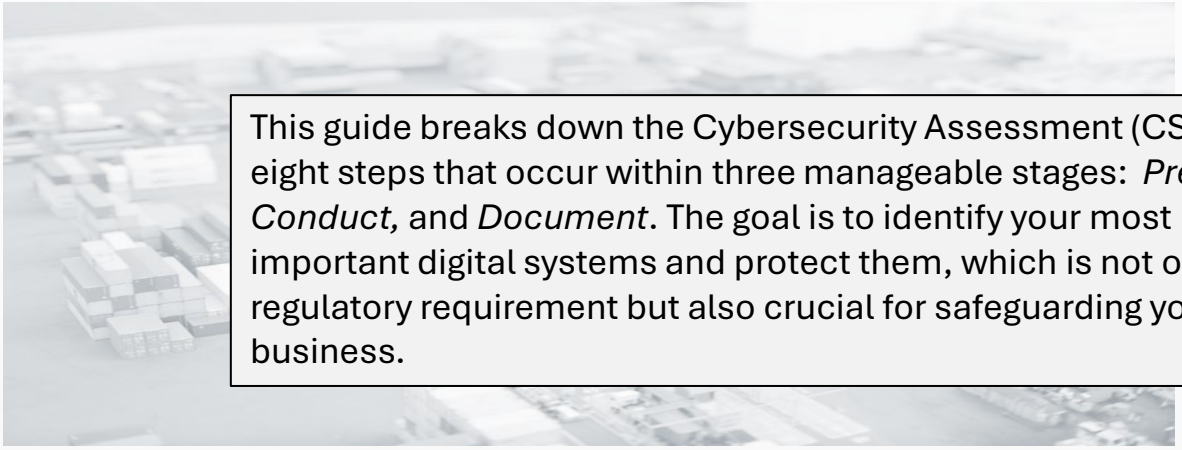
Conducting your Cybersecurity Assessment

A guide for small businesses



This guide breaks down the Cybersecurity Assessment (CSA) into eight steps that occur within three manageable stages: *Prepare*, *Conduct,* and *Document*. The goal is to identify your most important digital systems and protect them, which is not only a regulatory requirement but also crucial for safeguarding your business.

Stage 1 – PREPARE

This first stage is about understanding your business and technology.

1 Get on the Same Page

- Gather your team to agree on the goals of the assessment.
- Discuss your business's tolerance for risk and any limitations you have (e.g., budge or technical constraints).
- List any assumptions you're making, such as which systems you believe are already secure.

2 Identify Your Essential Functions

- Create a master list of all functions that are absolutely necessary for your business to operate.
- Consider what would happen if these functions were interrupted. This includes operational (e.g., vessel navigation, cargo handling), business (e.g., billing), and administrative tasks. Consider also downstream/supply chain impacts to your customers or the region.

3 Create a Full Tech Inventory

- Make a complete list of all your Information Technology (IT) and Operational Technology (OT). Examples include but are not limited to:
  - **Hardware**: Computers, servers navigation equipment, crane controls, engine monitors.
  - **Software**: Billing applications, cargo-handling software, operating systems.
  - **Networks**: Internal networks, connections to the internet, and any external services you rely on.

Stage 2 – CONDUCT

In this stage, you'll analyze the items from your inventory to find potential weaknesses. This is a "risk-filtering" process, starting broad and narrowing down to what is most critical.

4 Identify Threats & Vulnerabilities

- Use a combination of manual reviews and automated tools to get a complete picture of vulnerabilities.
- **Internal Review:** Look at your own history. Have you had security incidents or near-misses before? What went wrong? Talk to employees who use the systems daily; they often know where real-world weaknesses are.
- **External Review:** Consult public resources for known threats. Review vendor security bulletins for your equipment and software. Check for alerts from government agencies like the Cybersecurity and Infrastructure Security Agency (CISA).
- **Use Automated Tools:** Automated scanners can find technical vulnerabilities that are not visible to the naked eye. Many powerful tools are available for free or at a low cost.

5 Determine Likelihood & Impact

For each vulnerability, ask two questions:

- **Likelihood**: How likely is it that a threat will exploit this weakness?
- **Impact**: If that happens, what would be the impact on your essential business functions?

6 Create a Full Tech Inventory

- Using your risk analysis, highlight all the systems from your inventory that support your essential functions (from Step 2).
- Also include any systems that are connected to those essential systems. These become your "priority assets".

7 Classify "Critical IT/OT"

- This is the final and most important filter. Review your list of priority systems and ask:
  - Could the failure or compromise of this system, device or something it's logically or physically connected to lead to an operational disruption or Transportation Security Incident (TSI)?
  - If the answer is "Yes" or even "Maybe", you must designate that system as Critical IT/OT. These systems will require the highest level of protection in your Cybersecurity Plan.

Stage 3 – DOCUMENT

This final stage involves creating your report and formalizing your findings.

8

Document Your Assessment

- Create the official CSA report. This report should detail all your findings, including:
  - A summary of your asset inventory
  - The vulnerabilities and risks you identified (including outputs from your scans)
  - Your final list of Critical IT/OT systems
- This document is the foundation for creating your Cybersecurity Plan (CSP), where you will outline the specific actions you'll take to protect your assets in accordance with 33 CFR 101 Subpart F.

Below is a list of potential tools that can be used to assist in conducting the CSA. The Coast Guard does not endorse the use of any specific tool. CISA maintains a list of No-Cost Cybersecurity Services and Tools that can be found on their agency website.

Category	Possible Options for Free Tools	What it does
Vulnerability Scanners	Nessus Essentials https://www.tenable.com/products/nessus/nessus-essentials OpenVAS https://www.greenbone.net/en/openvas-free/	These tools scan your computers, servers, and other devices for thousands of known vulnerabilities, such as missing patches, weak configurations, and outdated software.
Network Scanners	Nmap https://nmap.org/	Helps you discover devices on your network and identify open ports that could be exposed to attackers.
Web Application Scanners	Zed Attack Proxy (ZAP) https://www.zaproxy.org/	If you have any web-based applications (like a customer portal), this tool specifically checks them for common web vulnerabilities.
Guided Tools	CISA's Cybersecurity Evaluation Tool (CSET) https://www.cisa.gov/downloading-and-installing-cset	Free desktop application that walks you through a process to help you evaluate your practices against recognized standards.