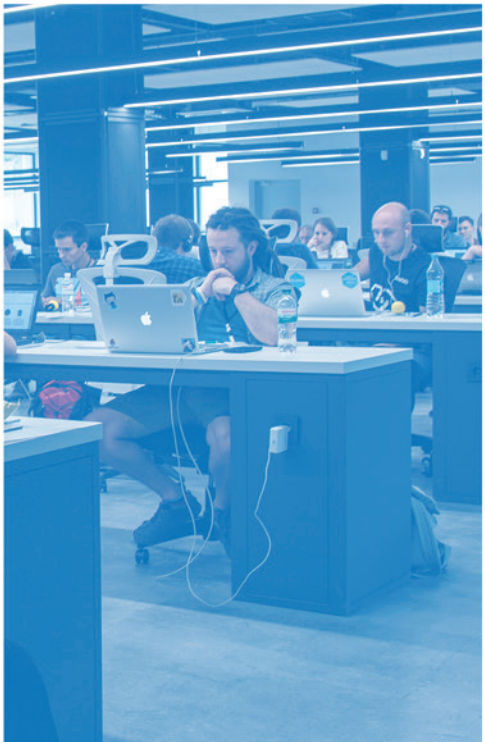
ardalyst

Planning Your Journey to Cyber Maturity



ardalyst

Roadmap to Cyber Maturity: What to Ask

Enhancing a company's cybersecurity program is not a "one size fits all" prospect. It's important to find a provider that will work collaboratively with your team to assess your current environment and develop a plan that best meets your unique needs and business goals.

Here are some questions to consider as you prepare your organization to meet compliance requirements and mature your cybersecurity program.

What are the elements of a mature cybersecurity program?

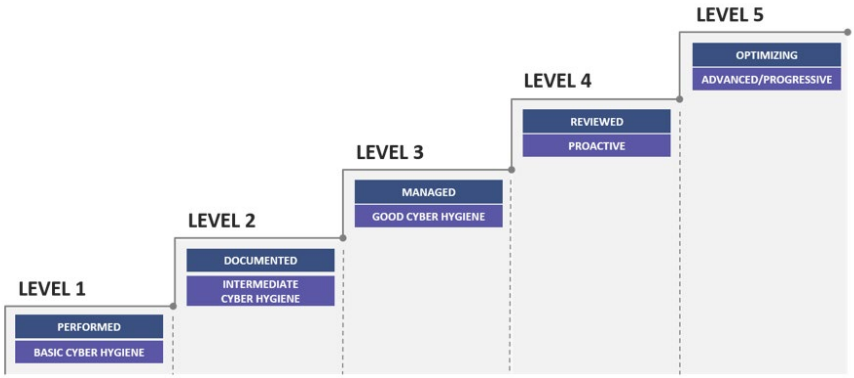


Figure 1. A cyber security maturity model.
(Image courtesy of the Office of the Undersecretary of Defense (Acquisitions & Sustainment)

Figure 1 illustrates a model for thinking about cybersecurity maturity. A comprehensive and mature cybersecurity program requires a wide range of capabilities. To focus your cybersecurity strategy and achieve your compliance and maturity goals, we suggest viewing the problem through the following lenses:

- **Govern your organization.** Ensure your organization is doing the right things to develop and maintain up-to-date policies and procedures that help you maintain compliance with changing regulations.
- **Harden your systems.** Implement capabilities that reduce your vulnerabilities and make it difficult for the adversary to access and compromise your environment.
- **Defend against threats.** Leverage tools that increase your knowledge of threats and help your organization rapidly identify and respond to them.
- **Operate support capabilities.** Use system administration and helpdesk capabilities in a security-aware and compliant manner.
- **Transform your environment.** Migrate and develop applications on a modernized, protected environment.
- **Validate your program.** Assess the effectiveness of your overall program to ensure you are prepared for inspections.

How much and how fast is right for me?

With each step toward optimal maturity, your investment increases, the investment in people, processes and technology increases. It's not necessary to go "all in" right away. A practical, no-pressure approach helps you identify what capabilities are best purchased at the best time with the right investment.

Instead of buying more capability or capacity than you can use or afford, ensure your cyber portfolio is completely customizable based on immediate and future priorities. Prioritize your timeline, within your budget and meet your needs.

Maintaining an in-house security operations center is expensive and time-consuming, so consider outsourcing to a vendor. A good provider can assess your business operations, technology and processes, determine your compliance needs and help you create a plan with simple, immediate steps to enhance your security. You can slowly build maturity over time as your business expands.

What do I look for in a vendor?

When choosing a provider, companies generally have three options for outsourcing their cybersecurity maturity along the spectrum of program vs point solutions. Look for a provider who will work with your team to determine which of the following is best for you.

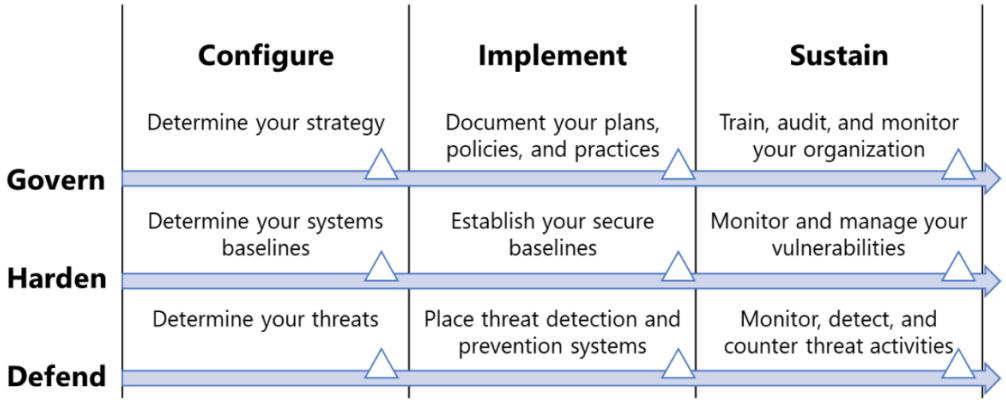


Figure 2. An example of the services you can expect if you choose to hire a provider to configure, implement or fully sustain your environment, using Ardalyst's Govern, Harden and Defend services.

Configure your systems: Hire a provider with in-depth knowledge of cyber defense and regulatory requirements to tailor capabilities to your specific needs, set up and configure the architecture, then turn it over to your in-house IT team to implement and maintain.

Implement your cybersecurity program: Hire a provider with in-depth knowledge of cyber defense and regulations to set up, configure and implement some of the capabilities before turning it over to your in-house team to maintain.

Sustain and manage your cybersecurity program: Hire a provider to supply ongoing services, essentially outsourcing the managed defense and response requirements, leaving your in-house team free to continue focusing on the activities that support your business continuity.

What kind of architecture do I need?

You have options. Several factors go into choosing the right architecture.

For example, the federal government's Cybersecurity Maturity Model Certification (CMMC) states that an organization can achieve certification for the entire company or a smaller enclave of the company, depending on the number of users handling controlled unclassified information (CUI). This is especially good for smaller companies

who only have a handful of employees handling CUI and don't want to spend the money to put every employee on a platform that protects information they aren't using.

All Commercial	All GCC-High	Hybrid

• Best for organizations that do not store or access CUI but are required to be NIST 800-171 or CMMC Level 1 or 2.
• Latest features
• Lower price
• Highest risk
  • Spillage with one accident
  • Hold your own key, training
  • Missing contractual obligations to support
	• Best where organization needs DFARS compliance.
	• Microsoft goal is feature parity with commercial and working to reduce 12-month lag
	• 40% higher price
	• Lowest risk
	  • US Persons
	  • Exceeds FEDRAMP requirements
	  • Supports DFARS cloud language
		• When organizations needs to meet specific compliance requirements, but only some users need to access CUI.
		• Still high risk with accidental spillage, need significant policy enforcement
		• Dual tenants/ branding challenges
		• Organizational friction
		• Better with Managed Services, as far more complicated Policies, Monitoring, and Management requirements

Table 1. Three different architecture configurations using Microsoft 365.

Table 1 provides an example of three different architecture configurations using Microsoft Office 365. Microsoft O365 is one example of a platform that provides embedded and automated security as well as tools that enhance your business operations. Sometimes basic cyber hygiene is as simple as migrating to a new platform.

CMMC doesn't necessarily apply to companies that don't work with the government, but it establishes a model for any organization that wants to mature their cybersecurity posture and protect their proprietary information and their customers. Your vendor should have a wide knowledge of regulations and can help determine what works best for you.

How will I continue to assess and mature my environment in the future?

What you need tomorrow might not be what you need today. Find a provider who will evaluate your program and work with you to evolve and mature your systems, ensuring they remain defensive against changing adversary tactics, techniques and procedures (TTPs).

Access to a provider that offers advanced threat intelligence and adversary emulation/simulation services to continuously validate your environment is key. A team that understands existing threats and possesses the expertise to test your environment for vulnerabilities to those threats will help you harden your network, enhance your IT team, and build on that foundation for future growth.

Ardalyst is a cyber defense company headquartered in Annapolis, Maryland, dedicated to helping customers transform their organization's people, process and technologies into resilient capabilities integrated through business systems, cloud capa-bilities and cybersecurity best practices. Our name is a mashup of the words "ardent" and "catalyst." We are passionate change agents who believe in a future where organizations can thrive in the digital world by replacing uncertainty with understanding.