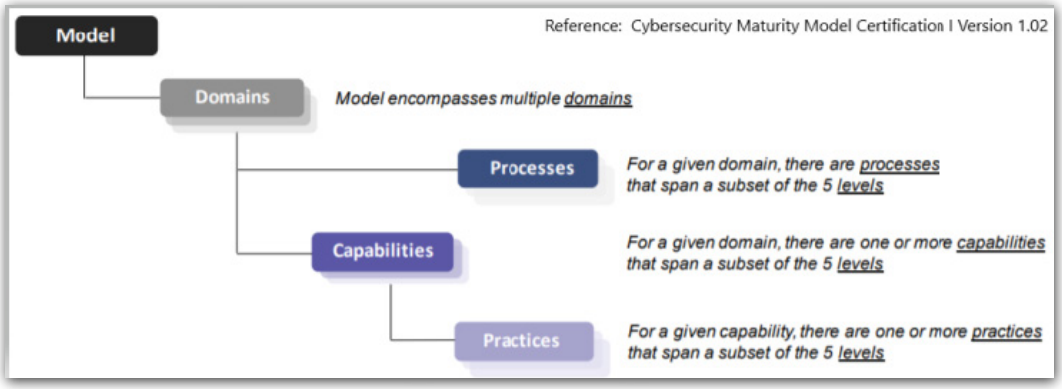
Cybersecurity Risk Assessment–
Cybersecurity Maturity Model Certification (CMMC) Framework

The Cybersecurity Maturity Model Certification (CMMC) framework consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other reference. The model framework organizes these processes and practices into a set of domains and maps them across five levels. In order to provide additional structure, the framework also aligns the practices to a set of capabilities within each domain.



The Rofori Cybersecurity Risk Assessment — CMMC is a cloud-based solution that helps to reduce risk through assessment and scoring, based on your alignment to the CMMC Framework. In accordance with the CMMC Framework, the Rofori Cybersecurity Risk Assessment lays out the entire framework in an easy-to-use environment that a user can manage an organization's security program. The Risk Assessment enables users to maintain and update the security posture over the course of time in a collaborative environment. Multiple individuals can access this system to continuously update their respective function in an organization and all can quickly see where the organization's vulnerabilities are within a specific CMMC level as well as compare the organization's compliance to other levels of the CMMC automatically.

Practice	Name	Description	Date	Implemented	Docs	Risk Inh	Risk Res	Notes	
AC.1.001	Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).		Yes	1	L	VL		Edit
AC.2.005	Access Control	Provide privacy and security notices consistent with applicable CUI rules.		Yes		M	M		Edit
AC.2.006	Access Control	Limit use of portable storage devices on external systems		Yes		L	VL		Edit
AC.1.002	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.		Yes		L	L		Edit
AC.2.007	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.		Yes	1	VL	VL		Edit
AC.3.017	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.		Yes		L	VL		Edit

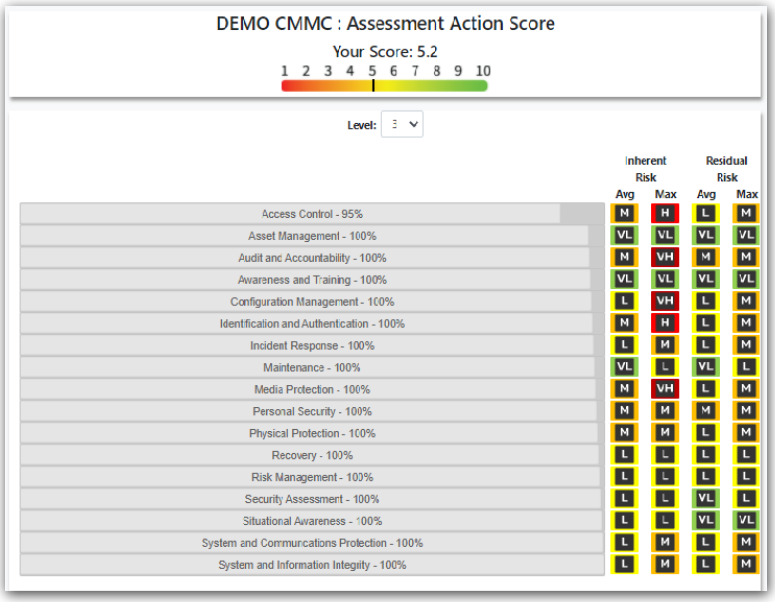
References (7)

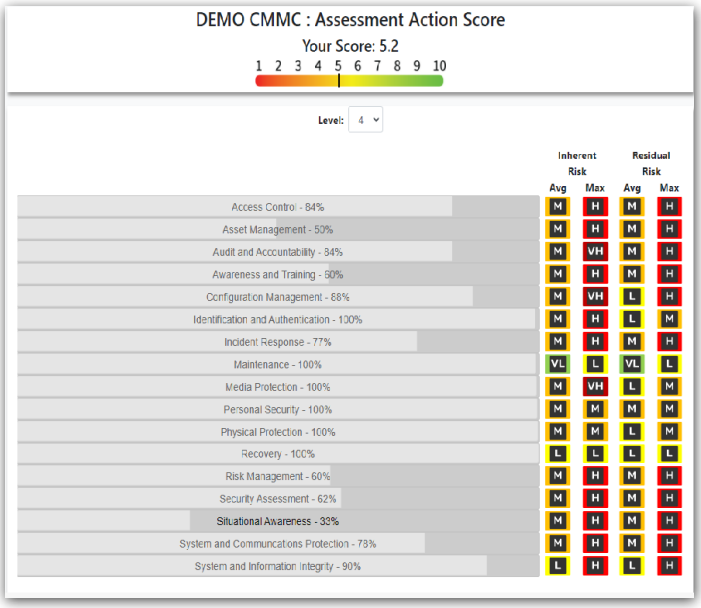
Reference Publication	Reference Location
FAR Clause 52.204-21	b.1.i
NIST SP 800-171 Rev 1	3.1.1
CIS Controls v7.1	1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11
NIST CSF v1.1	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4
CERT RMM v1.2	TM:SG4.SP1
NIST SP 800-53 Rev 4	AC-2, AC-3, AC-17
AU ACSC Essential Eight	N/A

Clarification/Example

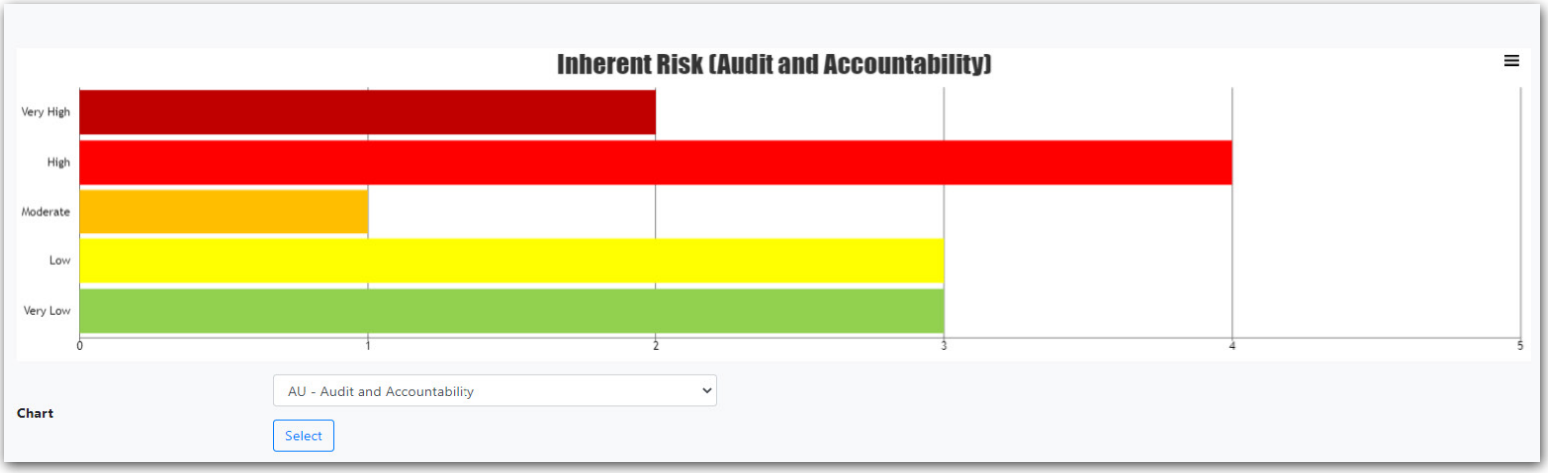
Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network. **Example 1)** You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately. **Example 2)** A coworker from the marketing department tells you their boss warts to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

The Rofori Cybersecurity Risk Assessment's inherent and residual risk feature, nested with the CMMC Framework enables an or-ganization to assess risk prior to and after mitigation measures are implemented. This feature serves as a core capability that ena-bles an organization's ability to manage risk priorities and risk tolerance. The dashboard enables individuals at all levels of the organization to quickly see the organizational risk in accordance with their preferred cybersecurity standard. The current inherent and residual risk calculation is promptly displayed helping you understand your most critical risks within your organization and serves as a means to focus on implementing proper remediation to protect what is most important. Additionally, the Rofori Cybersecurity Risk Assessment—CMMC Framework enables you to quickly measure your compliance with other CMMC levels in the event your organization needs to focus compliance in a different manner to support a future government contract. The Risk Assessment will take what it understands of your existing compliance and quickly compare you to another while automatically calculating the Inherent and Residual risks.





The Rofori Cybersecurity Risk Assessment was designed for easy implementation and delivery of risk status at-a-glance, in the form of a drill-down dashboard status display providing detailed visibility to your cybersecurity assessment status, as determined by your implementation response.



Experience how the Rofori Cybersecurity Risk Assessment can make you more aware of the cyber risk in your business operations and help prioritize remediations to reduce your cyber risk exposure