

# **MxD Cyber Marketplace**





**MxD Cyber**  
**MARKETPLACE**

Welcome to the MxD Cyber Marketplace, your one-stop shop for all cybersecurity needs for manufacturers of all sizes.

 **ENTER THE CYBER MARKETPLACE**

# MxD Cyber Marketplace



## Assessments

Low-cost self-paced assessments:

- Cybersecurity: CMMC, NIST SP800-171, NIST CSF, etc.
- Others: PCI, HIPAA, etc.

Guided recommendations on tools and services to address gaps

- Address knowledge gap

Additional support materials

- Security policy templates, POA&M, SSP, etc.



## Tools and Services

Focused on 17 CMMC domains:

- Access Control, Awareness and Training, Configuration Management, Incident Response, System Information Integrity, etc.

Cost and usability optimized for multiple tiers

- Different budgets and skills

Future expansion to include digital tools and services specific for SMM needs

## ASSESSMENT QUESTIONS AND GUIDANCE

### i. Basic Questions

1. Do you have an inventory of hardware, cloud instances, virtual and physical servers, network devices, & wireless access points?

MW +

Evidence Notes (2)

No

Yes

#### 1.1. Do you use an active and/or passive discovery tool?

Active discovery means scanning the network to be able to find devices, such as a ping sweep, NMAP or a more enterprise tool. Passive discovery means scanning the network traffic logs for new devices. Scan firewall, dns, dhcp and web logs to check for new devices.

\*Please select all answers that apply

+ (multiple selection icon)

Evidence Notes (4)

None

Passive

Active

Settings Generate Report

Assessment Marketplace Reports



TITLE

NIST 800-171 In progress

CREATED

Oct 15, 2021 10:09 PM (6 months ago)

PROGRESS

113 / 114 questions answered

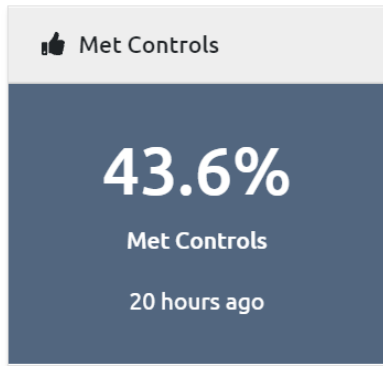
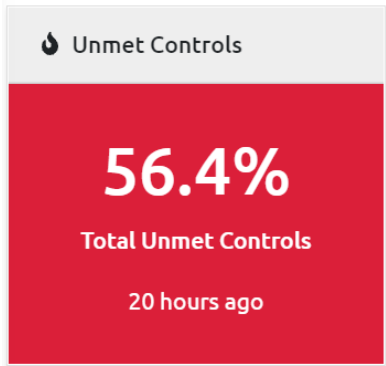


DESCRIPTION

NIST 800-171r2 provides organizations with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

# ASSESSMENT

## ASSESSMENT RESULTS AND TOP RECOMMENDATIONS



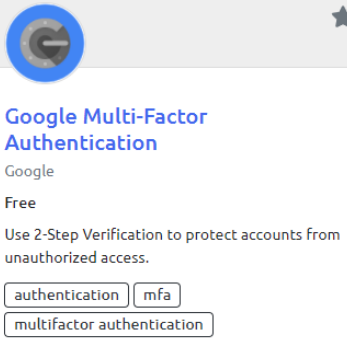
Assessment results show manufacturers their progress to meeting their desired controls and the platform highlights top control gaps along with recommended solutions

Top 3 Control Gaps	
<p><b>3.1.1</b></p> <p>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</p> <p> 12.5%</p>	<p><b>Recommended Solutions:</b></p> <ul style="list-style-type: none"> <li>Google Multi-Factor Authentication</li> <li>Microsoft Multi-Factor Authentication</li> <li>Okta Multi-Factor Authentication</li> <li>Cisco Meraki Managed Firewall</li> <li>Duo Multi-Factor Authentication</li> <li>Endpoint Monitoring with RMM &amp; Webroot</li> <li>CloudKnox Multi-Cloud Permissions Management Platform</li> </ul>
<p><b>3.1.2</b></p> <p>Limit system access to the types of transactions and functions that authorized users are permitted to execute.</p> <p> 12.5%</p>	<p><b>Recommended Solutions:</b></p> <ul style="list-style-type: none"> <li>Google Multi-Factor Authentication</li> <li>Microsoft Multi-Factor Authentication</li> <li>Okta Multi-Factor Authentication</li> <li>Cisco Meraki Managed Firewall</li> <li>Duo Multi-Factor Authentication</li> <li>Endpoint Monitoring with RMM &amp; Webroot</li> <li>CloudKnox Multi-Cloud Permissions Management Platform</li> </ul>
<p><b>3.1.3</b></p> <p>Control the flow of CUI in accordance with approved authorizations.</p> <p> 12.5%</p>	<p><b>Recommended Solutions:</b></p> <ul style="list-style-type: none"> <li>Tenable Managed Vulnerability Assessment</li> <li>Tenable Vulnerability Assessment as a Service</li> <li>Cisco Meraki Managed Firewall</li> <li>Endpoint Detection &amp; Response</li> </ul>


# MARKETPLACE

## MARKETPLACE PRODUCT LISTING


- My Purchases
- My Quotes
- Favorites
- Recommended
- All**
- Authentication
- Consulting Services
- EDR
- Email
- MSSP
- Pentest
- Software Development Security
- Training
- Vulnerability Management



**Google Multi-Factor Authentication**  
 Google  
 Free  
 Use 2-Step Verification to protect accounts from unauthorized access.  
 authentication mfa  
 multifactor authentication



**Google Multi-Factor Authentication**  
 Google  
 Free

Implemented +
Learn More 

**Description**

Use 2-Step Verification to protect accounts from unauthorized access. 2-Step Verification puts an extra barrier between your business and cybercriminals who try to steal usernames and passwords to access business data. Turning on 2-Step Verification is the single most important action you can take to protect your business.

Users generate one-time verification codes on an app on their mobile device, such as Google Authenticator. The user enters the code to sign in to their computer and other devices, including the mobile device itself. Google Authenticator and other apps don't need an internet connection to generate codes.

Click on Learn More above to access Google's step-by-step instructions.

**Tags**  
 mfa, multifactor authentication, authentication

**MxD's Take**

Multifactor authentication, MFA, or 2FA is one of the most cost effective means to reduce cybersecurity risk. Google makes their Authenticator App freely available for use within G.Suite and through third-party identity providers (IdP) to authenticate users.

**CSF Controls Met**

PR.AC-3	PR.AC-7	PR.AC-6
---------	---------	---------

**HIPAA Controls Met**

164.312(a)	164.312(d)
------------	------------

**800-171 Controls Met**

3.1.1	3.1.2	3.1.14
3.1.15	3.1.18	3.1.20
3.13.9	3.13.12	3.5.3
3.7.5		

Product page includes a more detailed description, links to resources, MxD's take on the product, and the various controls that the product addresses

# MxD Cyber Marketplace

The screenshot displays the MxD Cyber Marketplace dashboard. The interface includes a top navigation bar with the MxD Cyber logo, a 'Dashboard' title, and user information (MxD Enterprise, shopping cart, notifications, and user profile JP). A left sidebar contains navigation menus for ENTERPRISE, VIEW, EXPLORE, and MANAGE. The main content area is divided into several sections:

- Roll-up View / Organization View:** Two tabs at the top of the main content area.
- Last Report:** A card indicating 'No reports Found!' with a 'Get Started' button.
- Your Reports:** A bar chart showing 0% completion.
- Top 3 Control Gaps:** A card indicating 'No control recommendation gaps found!' with a link to 'an assessment'.
- In Progress Assessments:** A table showing two assessments in progress.

CREATED	COMPLETION PERCENT	ASSESSMENT
July 16, 2021 (24 days ago)	0%	HIPAA Readiness Assessment
July 16, 2021 (24 days ago)	50%	NIST Cybersecurity Framework Assessment
2 results		



## CMMC 2.0 Recommendations

- Start Early
- Engage a cross functional team
- Think in binary – Yes/No
- Consider using self-assessment resources
- Leverage a POAM
- It's a Journey, not a Milestone



The logo for MxD, featuring the letters 'M', 'x', and 'D' in a bold, sans-serif font. The 'M' and 'D' are white, while the 'x' is red.

Where Innovative Manufacturers go to forge their future

[www.mxdusa.org](http://www.mxdusa.org)

  @MxDInnovates