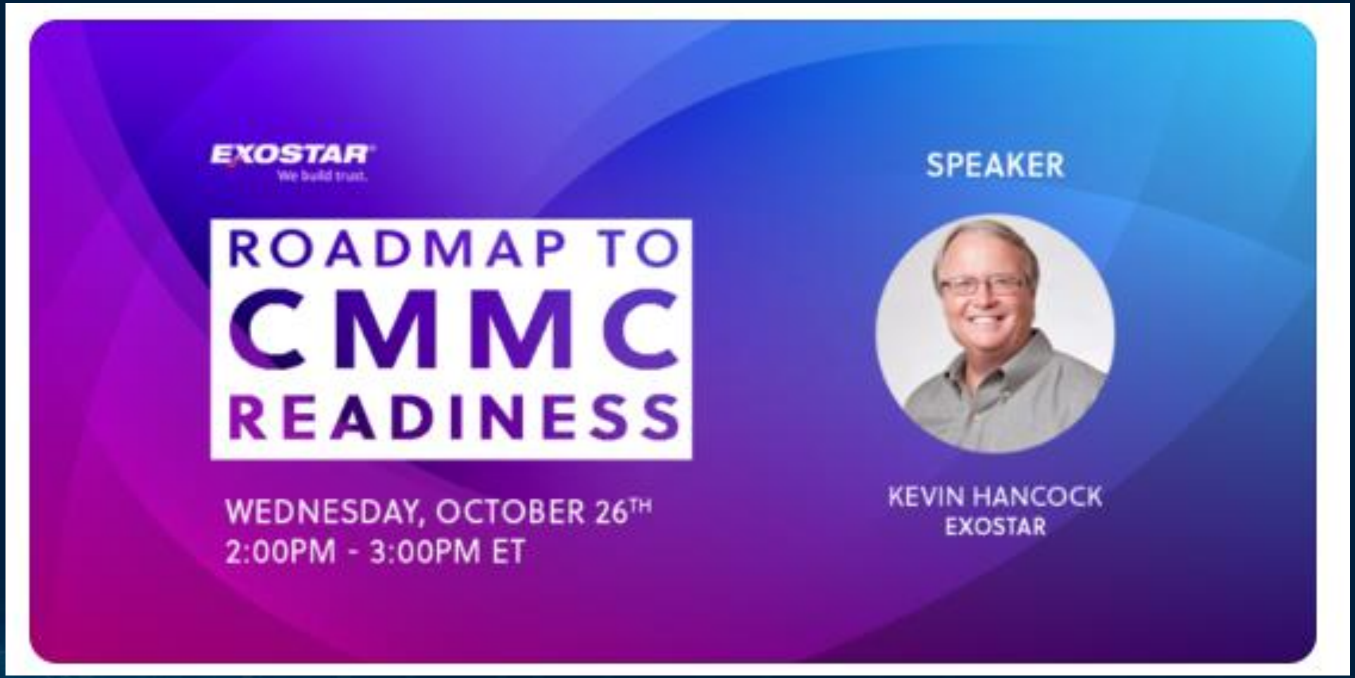
EXOSTAR®
We build trust.



EXOSTAR
We build trust.

ROADMAP TO CMMC READINESS

WEDNESDAY, OCTOBER 26TH
2:00PM - 3:00PM ET

SPEAKER

KEVIN HANCOCK
EXOSTAR

How Exostar Can Help

Kevin Hancock
October 26, 2022

Housekeeping

EXOSTAR®
We build trust.

- Today’s webinar is scheduled to last 45 min to 1 hour including Q&A.
- All participants will be muted to enable the speakers to present without interruption.
- A large portion of today’s event is dedicated to answering pressing questions from the audience. Speakers will be answering questions that have been submitted prior to today’s event.
- In case of outage, please wait for a minute and refresh the page.
- For your convenience, there is a link in the YouTube description to a glossary of commonly used terms, acronyms and initializations that will be referenced during today’s webinar.
- This webinar is being recorded and will be available on-demand via the Exostar Resource Library (www.Exostar.com/Resources) post-event as well as at this same YouTube link.
- To speak with one of our industry experts or request a copy of this slide deck, please reach out to us at cmmc-team@Exostar.com or use the live chat feature at www.Exostar.com.

Speaker

Kevin Hancock has over 20 years experience leading Sales Engineering, Customer Success, and Professional Services Teams across a broad technology spectrum that has focused on Secure Collaboration between Enterprises. It includes Agile Development and DevOps tools and practices; Zero Trust Networking; and Identity and Access Management just to name a few. Focusing on driving adoption, managing change, and helping customers learn, Kevin joined Exostar in May 2021 as Director, Sales Engineering.

Agenda

EXOSTAR®
We build trust.

Purpose

Provide a roadmap for CMMC Compliance and how Exostar can assist customers on their journey.

- Latest CMMC News
- CMMC Destination
- Define the System
- Assess your current state
- Remediate your policies and environment
- Cloud Solutions and Shared Responsibility
- Assessment and Ongoing Updates

Current State

EXOSTAR®
We build trust.

CMMC 2.0 Rulemaking

- March 2023 Interim Rule
- May 2023 DFARS Clauses

Joint Surveillance Voluntary Program

- Starting Aug. 2022
- C3PAO Voluntary Assessments (3 being completed)
- Draft of CMMC Assessment Process

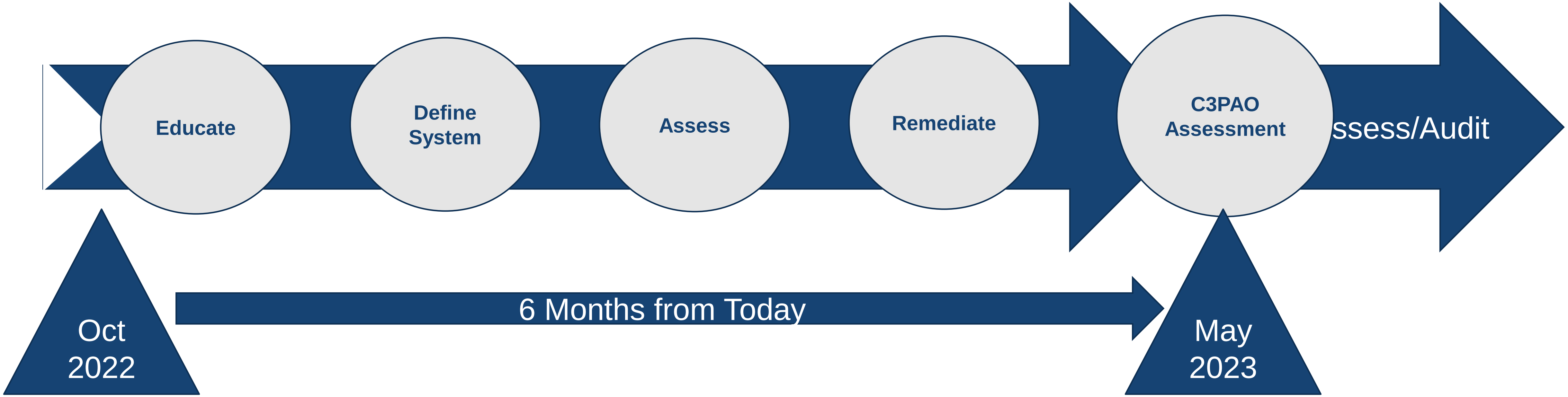
Cyber Accreditation Body

- Name and domain change from CMMC AB to Cyber AB
- https://cyberab.org/

Training

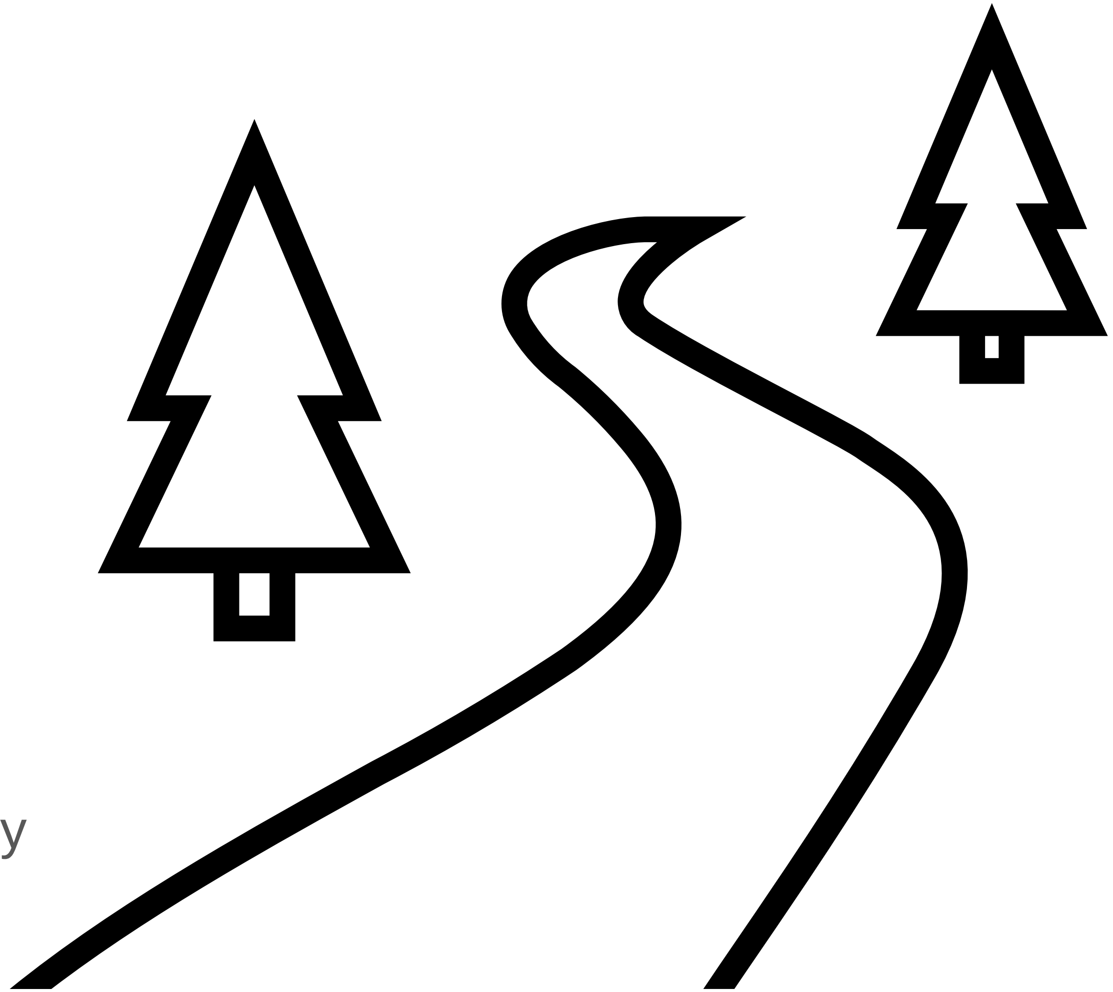
- CCP Training is Ongoing
- Pilot Test available in Q4 2022
- CCA Training to follow shortly after

CMMC 2.0 Implementation (Estimate)

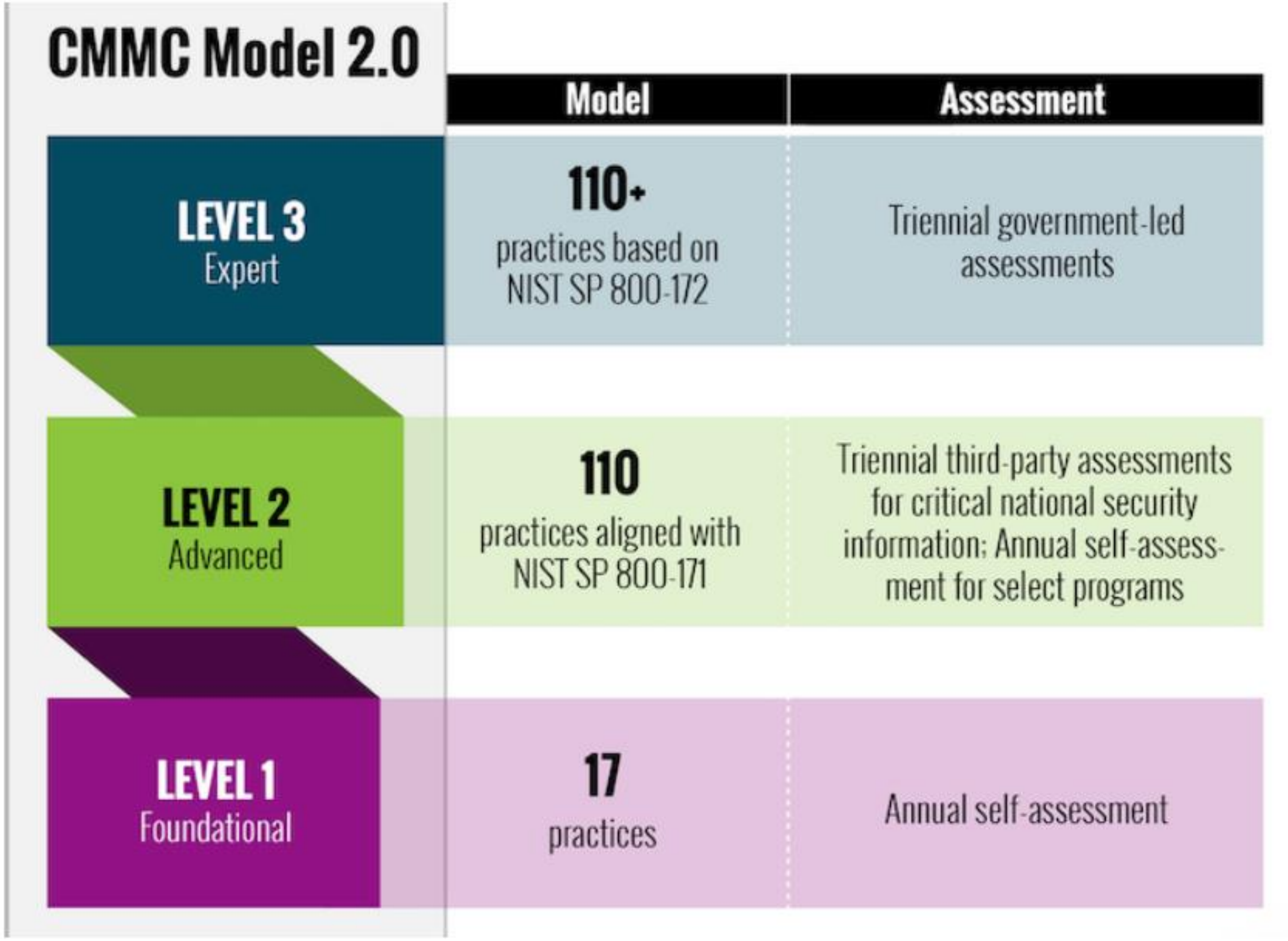


Practical Roadmap

1. Choose your destination (CMMC Level)
2. Identify the system, individuals and existing resources
3. Perform an initial assessment and identify gaps
4. Start the Journey
   a) Tools to help
   b) Cloud Services
   c) Partners
5. Consolidate policies, procedures, control systems, logs, etc.
6. Perform self assessment or engage with 3rd party to do readiness assessment
7. Engage C3PAO for assessment



Choose your destination



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

Existing Requirements

DFARS 252.204-7012 + Completed a DIBCAC High Assessment	CUI/Critical CUI
DFARS 252.204.7012	CUI
FAR 52.204-12	FCI

Controlled Unclassified Information

*Abbreviated as **CUI** and often pronounced "kyooie" (rhymes with "phooey")*

- *Engineering Drawings*
- *Engineering data*
- *Standards*
- *Specifications*
- *Technical Manuals*
- *Technical Reports*
- *Technical Orders*
- *Blueprints*
- *Plans*
- *Instructions*
- *Source Code*
- *Documentation*
- *Studies*
- *Analysis*
- *Bills of Material*

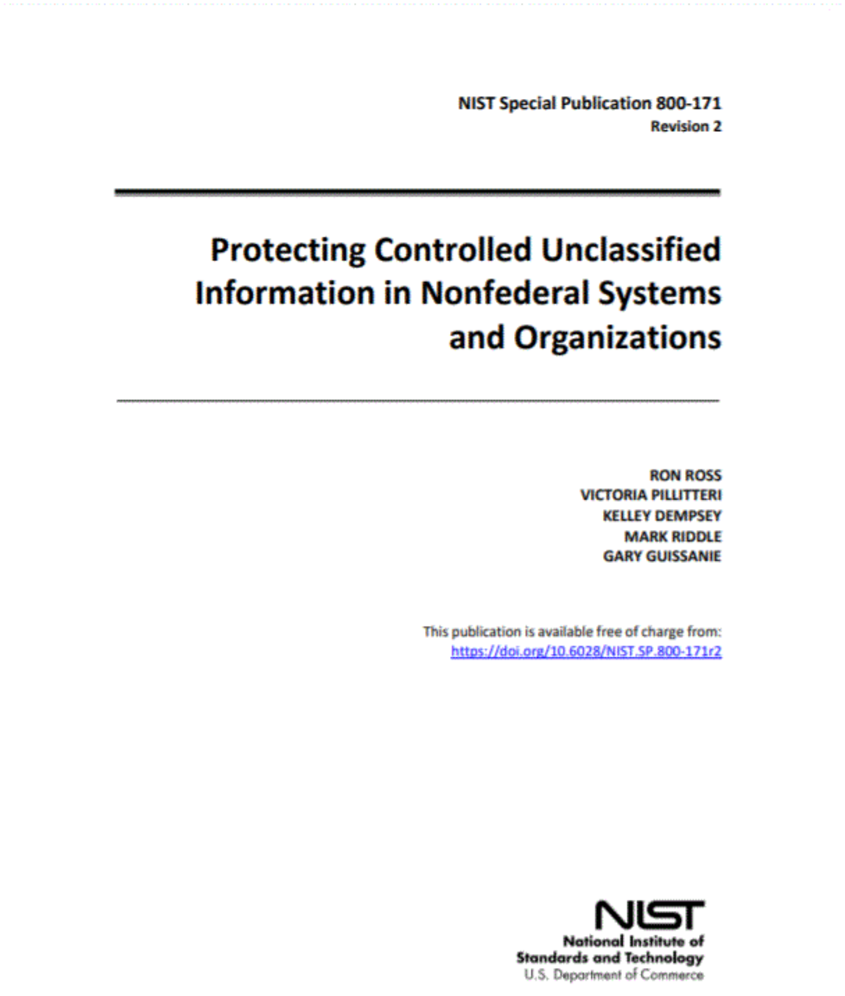
Determining whether or not information qualifies for CUI status falls on the originator.

What is NIST 800-171

U.S. Government Standard for Protecting Controlled Unclassified Information (CUI)

The security requirements are intended for use by federal agencies in contractual vehicles

Protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

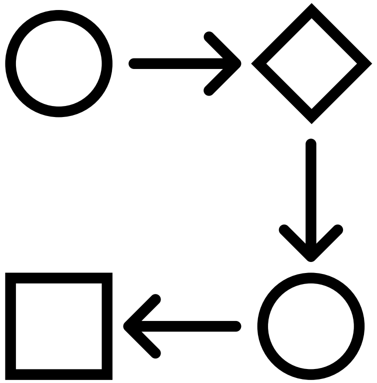
NIST 800-171 Categories

- 3.1 Access Control
- 3.2 Awareness and Training
- 3.3 Audit and Accountability
- 3.4 Configuration Management
- 3.5 Identification and Authentication
- 3.6 Incident Response
- 3.7 Maintenance
- 3.8 Media Protection
- 3.9 Personnel Security
- 3.10 Physical Protection
- 3.11 Risk Assessment
- 3.12 Security Assessment
- 3.13 System and Communications Protection
- 3.14 System and Information Protection

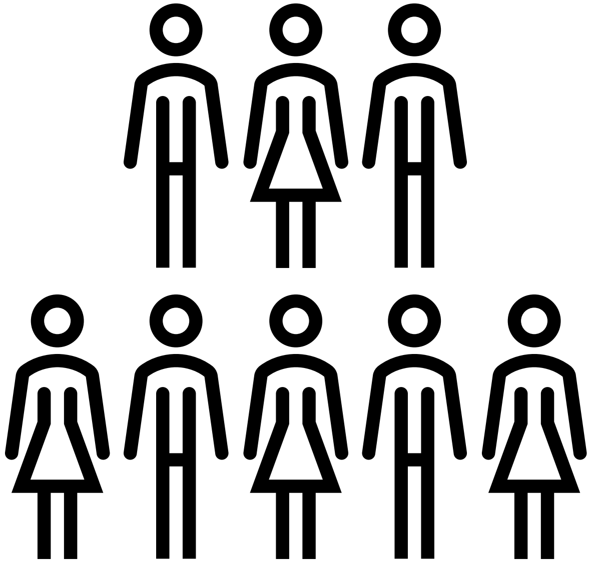
110 Controls within these 14 Categories

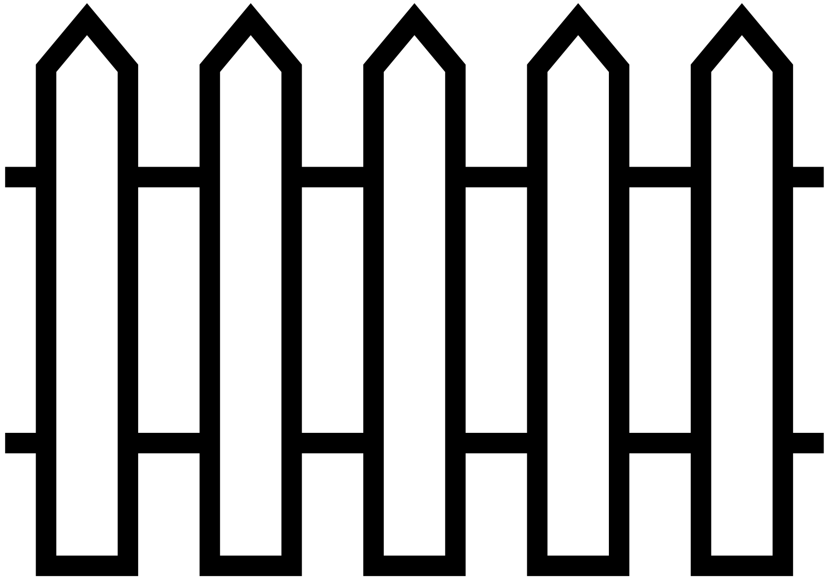
Identify the system

Process

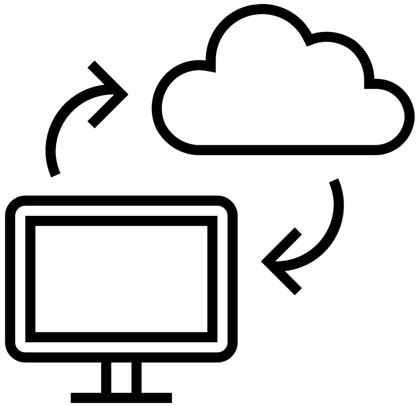


People



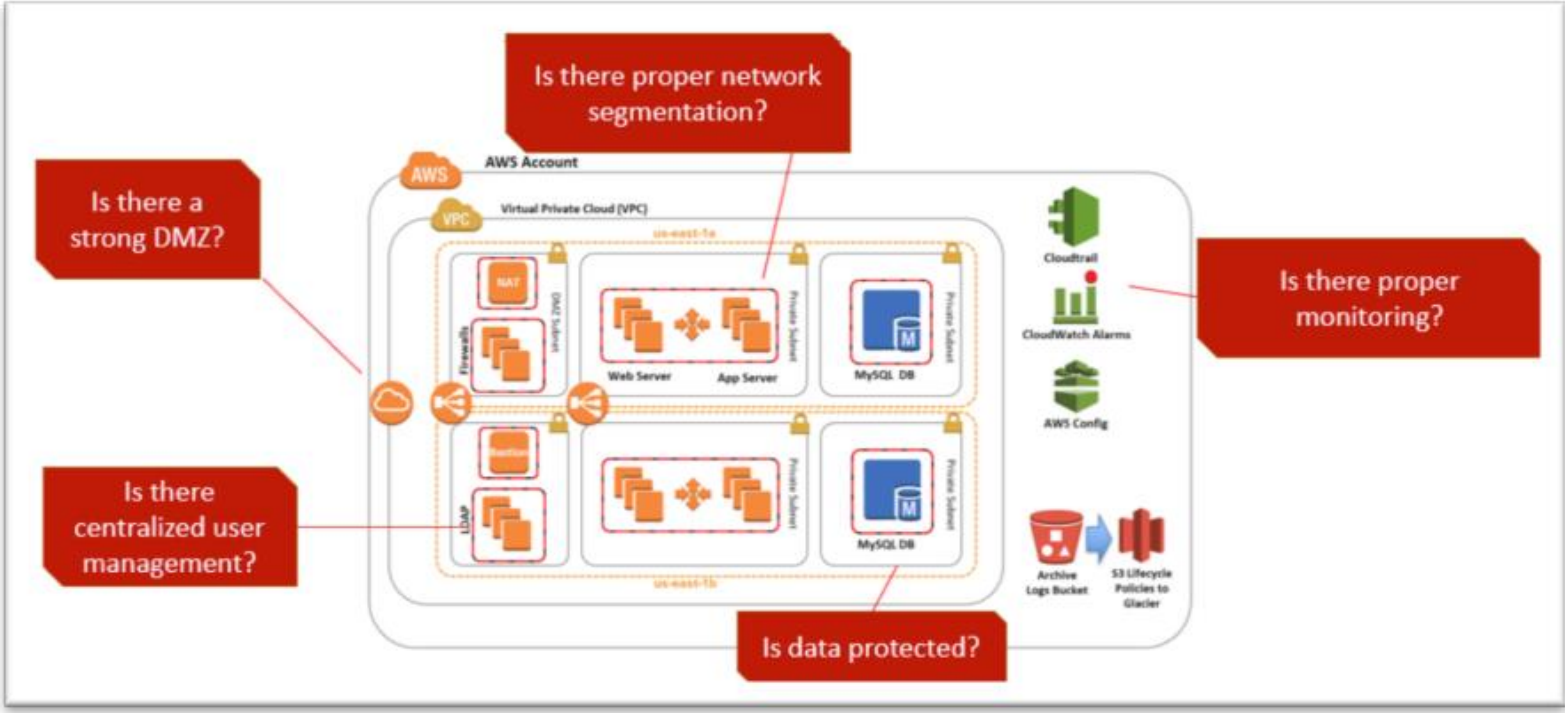


Boundary



Technology

System Diagram and Boundary



Is there proper network segmentation?

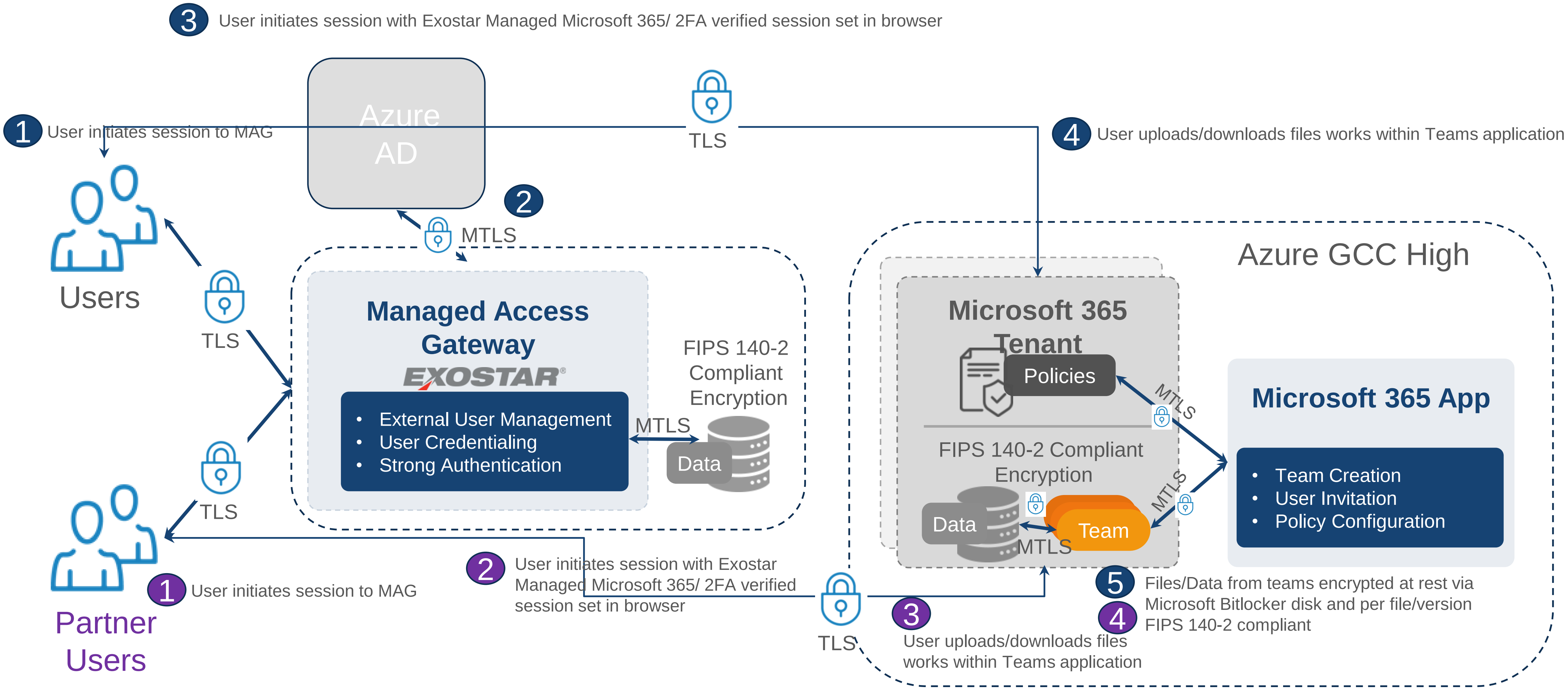
Is there a strong DMZ?

Is there proper monitoring?

Is there centralized user management?

Is data protected?

System Diagram



3 User initiates session with Exostar Managed Microsoft 365/ 2FA verified session set in browser

1 User initiates session to MAG

Azure AD

2

MTLS

TLS

4 User uploads/downloads files works within Teams application

Users

TLS

Managed Access Gateway

EXOSTAR

- External User Management
- User Credentialing
- Strong Authentication

FIPS 140-2 Compliant Encryption

MTLS

Data

TLS

Partner Users

1 User initiates session to MAG

2 User initiates session with Exostar Managed Microsoft 365/ 2FA verified session set in browser

TLS

Azure GCC High

Microsoft 365 Tenant

Policies

FIPS 140-2 Compliant Encryption

Data

Team

MTLS

MTLS

MTLS

Microsoft 365 App

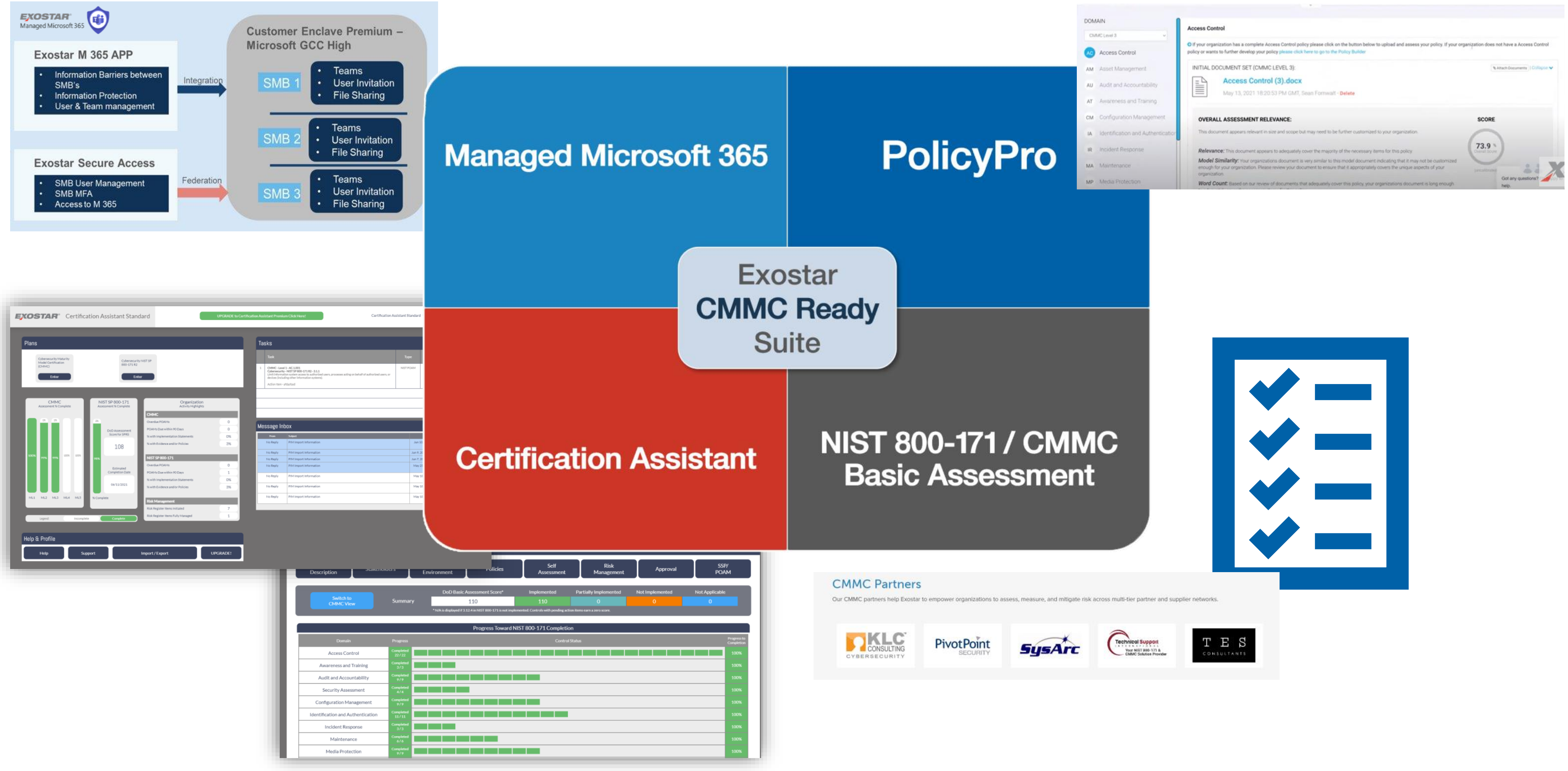
- Team Creation
- User Invitation
- Policy Configuration

3 User uploads/downloads files works within Teams application

5 4 Files/Data from teams encrypted at rest via Microsoft Bitlocker disk and per file/version FIPS 140-2 compliant

Start the Journey

EXOSTAR®
We build trust.



EXOSTAR Managed Microsoft 365

Exostar M 365 APP

- Information Barriers between SMB's
- Information Protection
- User & Team management

Exostar Secure Access

- SMB User Management
- SMB MFA
- Access to M 365

Customer Enclave Premium – Microsoft GCC High

- Teams
- User Invitation
- File Sharing

- Teams
- User Invitation
- File Sharing

- Teams
- User Invitation
- File Sharing

DOMAIN

CMMC Level 3

AC	Access Control
AM	Asset Management
AU	Audit and Accountability
AT	Awareness and Training
CM	Configuration Management
IA	Identification and Authenticatio
IR	Incident Response
MA	Maintenance
MP	Media Protection

Access Control

If your organization has a complete Access Control policy please click on the button below to upload and assess your policy. If your organization does not have a Access Control policy or wants to further develop your policy please click here to go to the Policy Builder

INITIAL DOCUMENT SET (CMMC LEVEL 3):

Access Control (3).docx

May 13, 2021 18:20:53 PM GMT, Sean Fornwalt - Delete

OVERALL ASSESSMENT RELEVANCE:

This document appears relevant in size and scope but may need to be further customized to your organization.

Relevance: This document appears to adequately cover the majority of the necessary items for this policy

Model Similarity: Your organizations document is very similar to this model document indicating that it may not be customized enough for your organization. Please review your document to ensure that it appropriately covers the unique aspects of your organization.

Word Count: Based on our review of documents that adequately cover this policy, your organizations document is long enough

SCORE

73.9 %

Got any questions? [illegible] help.

EXOSTAR Certification Assistant Standard

UPGRADE to Certification Assistant Premium Click Here!
Certification Assistant Standard

Plans

Cybersecurity Maturity Model Certification (CMMC) — Enter

Cybersecurity NIST SP 800-171 R2 — Enter

CMMC Assessment % Complete

NIST SP 800-171 Assessment % Complete

DoD Assessment Score for SPRS: 108

Estimated Completion Date: 06/11/2021

Organization Activity Highlights

CMMC	
Overdue POAMs	0
POAMs Due within 90 Days	0
% with Implementation Statements	0%
% with Evidence and/or Policies	3%
NIST SP 800-171	
Overdue POAMs	0
POAMs Due within 90 Days	1
% with Implementation Statements	0%
% with Evidence and/or Policies	3%
Risk Management	
Risk Register Items Initiated	7
Risk Register Items Fully Managed	1

Tasks

	Task	Type
1	CMMC - Level 1 - AC.1.001 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Action Item - afdasfasd	NIST POAM

Message Inbox

From	Subject	
No Reply	PIM Import Information	Jun 10
No Reply	PIM Import Information	Jun 9, 20
No Reply	PIM Import Information	Jun 7, 20
No Reply	PIM Import Information	May 25
No Reply	PIM Import Information	May 18
No Reply	PIM Import Information	May 18
No Reply	PIM Import Information	May 18

Help & Profile

Summary	DoD Basic Assessment Score*	Implemented	Partially Implemented	Not Implemented	Not Applicable
	110	110	0	0	0

* N/A is displayed if 3.12.4 in NIST 800-171 is not implemented. Controls with pending action items earn a zero score.

Progress Toward NIST 800-171 Completion

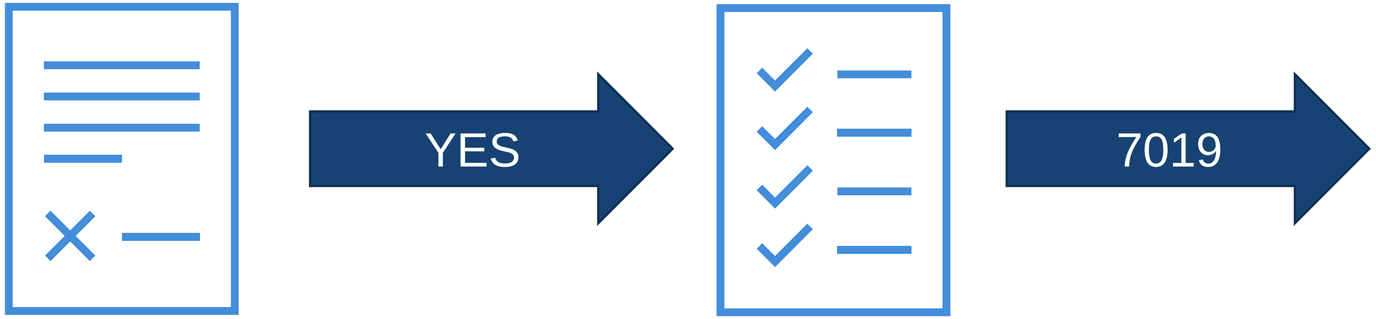
Domain	Progress	Progress to Completion
Access Control	Completed 22 / 22	100%
Awareness and Training	Completed 3 / 3	100%
Audit and Accountability	Completed 9 / 9	100%
Security Assessment	Completed 4 / 4	100%
Configuration Management	Completed 9 / 9	100%
Identification and Authentication	Completed 11 / 11	100%
Incident Response	Completed 3 / 3	100%
Maintenance	Completed 6 / 6	100%
Media Protection	Completed 9 / 9	100%

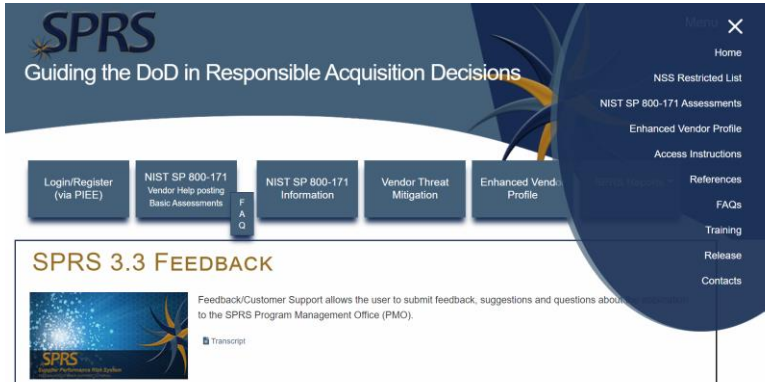
CMMC Partners

Our CMMC partners help Exostar to empower organizations to assess, manage, and mitigate risk across multi-tier partner and supplier networks.

KLC CONSULTING CYBERSECURITY
PivotPoint SECURITY
SysArc
Technical Support International — Your NIST 800-171 & CMMC Solution Provider
T E S CONSULTANTS

Leverage Existing Materials





Guiding the DoD in Responsible Acquisition Decisions

SPRS 3.3 Feedback

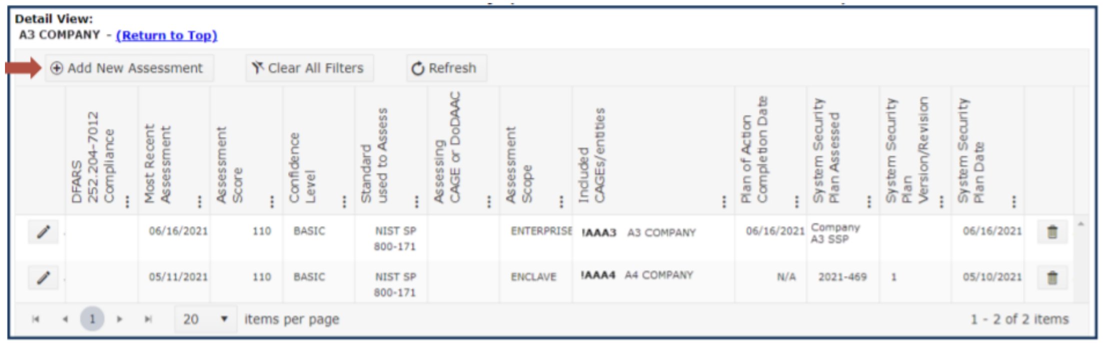
Feedback/Customer Support allows the user to submit feedback, suggestions and questions about [illegible] to the SPRS Program Management Office (PMO).

Check your contracts

DFARS Clauses

- **252.204-7012**
- **252.204-7019**
- **252.204-7020**

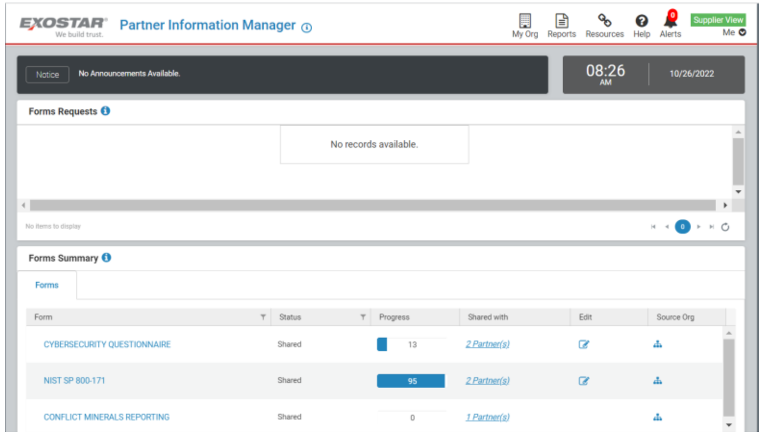
NIST 800-171 Compliance



Detail View:
A3 COMPANY - (Return to Top)

	DFARS 252.204-7012 Compliance	Most Recent Assessment	Assessment Score	Confidence Level	Standard used to Assess	Assessing CAGE or DoDAAC	Assessment Scope	Included CAGEs/entities	Plan of Action Completion Date	System Security Plan Assessed	System Security Plan Version/Revision	System Security Plan Date	
✎		06/16/2021	110	BASIC	NIST SP 800-171		ENTERPRISE	!AAA3 A3 COMPANY	06/16/2021	Company A3 SSP		06/16/2021	🗑
✎		05/11/2021	110	BASIC	NIST SP 800-171		ENCLAVE	!AAA4 A4 COMPANY	N/A	2021-469	1	05/10/2021	🗑

1 | 20 items per page | 1 - 2 of 2 items



Partner Information Manager

Notice: No Announcements Available.

08:26 AM 10/26/2022

Forms Requests

No records available.

No items to display

Forms Summary

Form	Status	Progress	Shared with	Edit	Source Org
CYBERSECURITY QUESTIONNAIRE	Shared	13	2 Partner(s)	✎	
NIST SP 800-171	Shared	95	2 Partner(s)	✎	
CONFLICT MINERALS REPORTING	Shared	0	1 Partner(s)		

DFARS 7019 requires a self-assessment and accurate reporting of your Supplier Performance Risk System (SPRS) score

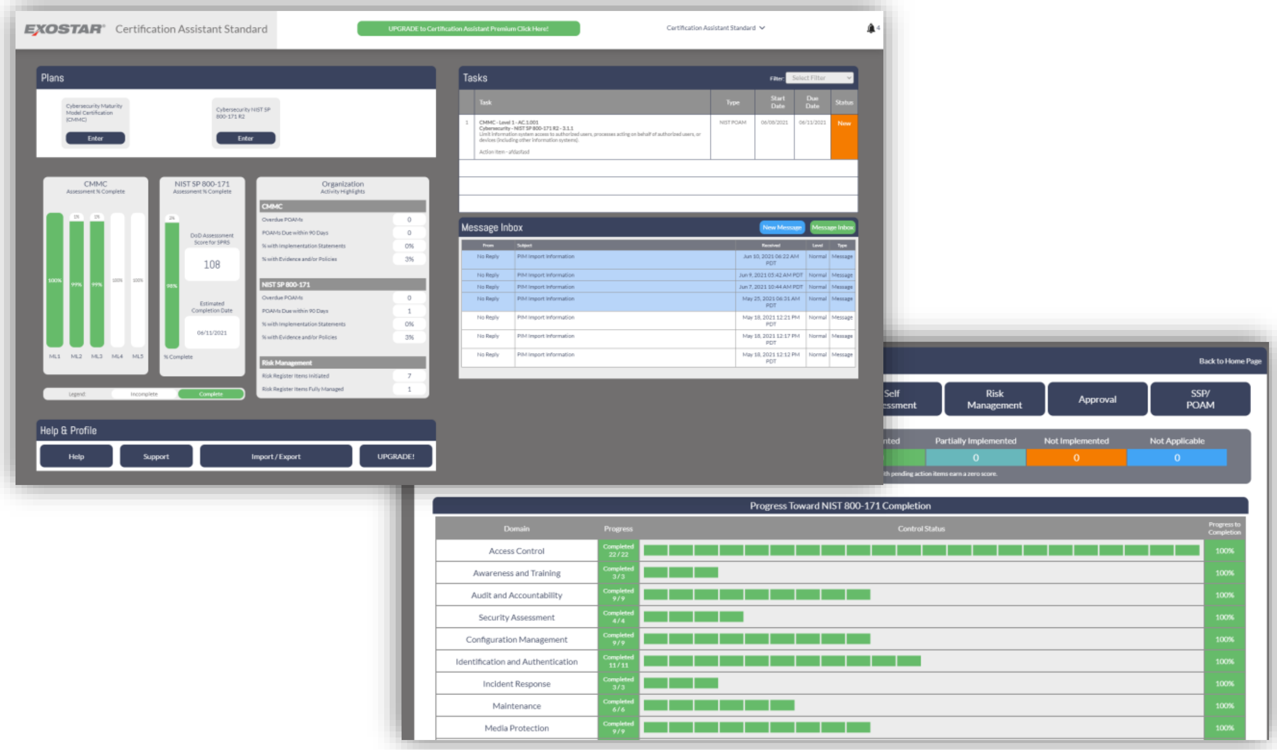
Initial Assessment

EXOSTAR® We build trust.

Benefits

- Easy to use
- Provides repository for all system policies, procedures and supporting material
- Tracks and reports progress on CMMC Compliance
- Opens POAMS and allows you to see progress on closure
- Output is the DAMM Score for SPRS reporting, a System Security Plan (SSP) and Report of any open POAMS and your plan to close them

EXOSTAR® Certification Assistant Standard



DoD Assessment Score for SPRS: 108

Estimated Completion Date: 06/11/2021

Organization
Activity Highlights

CMMC	
Overdue POAMs	0
POAMs Due within 90 Days	0
% with Implementation Statements	0%
% with Evidence and/or Policies	3%
NIST SP 800-171	
Overdue POAMs	0
POAMs Due within 90 Days	1
% with Implementation Statements	0%
% with Evidence and/or Policies	3%
Risk Management	
Risk Register Items Initiated	7
Risk Register Items Fully Managed	1

	Task	Type	Start Date	Due Date	Status
1	CMMC - Level 1 - AC.1.001 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Action Item - afdasfasd	NIST POAM	06/08/2021	06/11/2021	New

From	Subject	Received	Level	Type
No Reply	PIM Import Information	Jun 10, 2021 06:22 AM PDT	Normal	Message
No Reply	PIM Import Information	Jun 9, 2021 05:42 AM PDT	Normal	Message
No Reply	PIM Import Information	Jun 7, 2021 10:44 AM PDT	Normal	Message
No Reply	PIM Import Information	May 25, 2021 06:31 AM PDT	Normal	Message
No Reply	PIM Import Information	May 18, 2021 12:21 PM PDT	Normal	Message
No Reply	PIM Import Information	May 18, 2021 12:17 PM PDT	Normal	Message
No Reply	PIM Import Information	May 18, 2021 12:12 PM PDT	Normal	Message

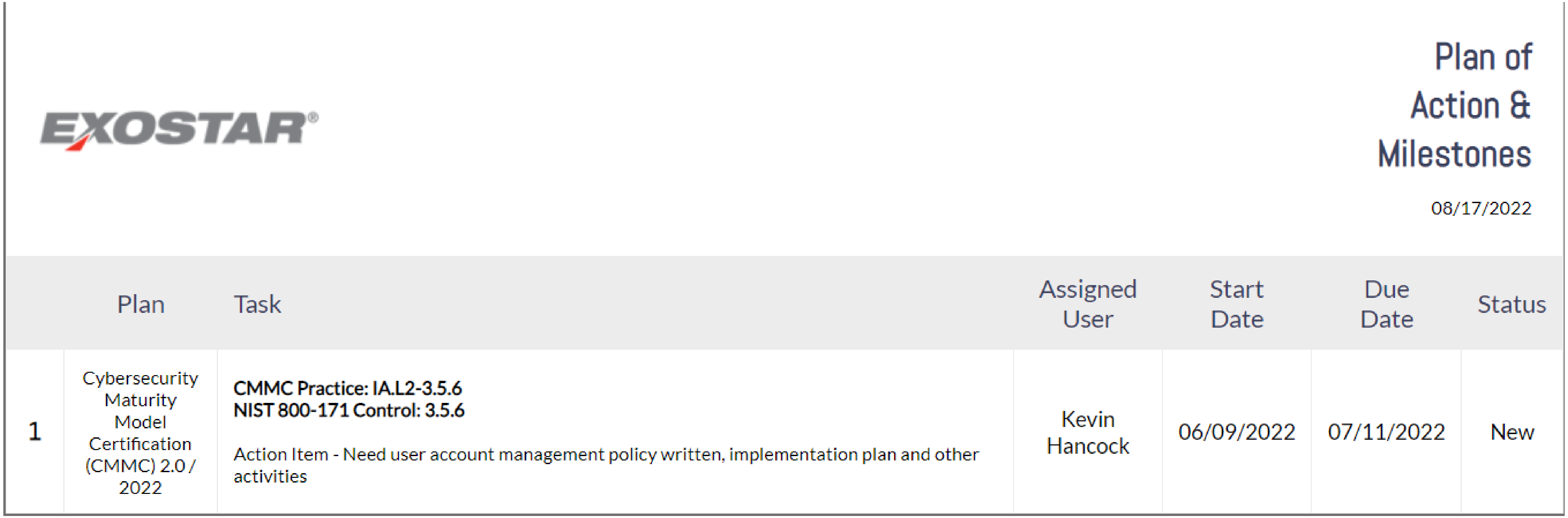
…nted	Partially Implemented	Not Implemented	Not Applicable
	0	0	0

…th pending action items earn a zero score.

Progress Toward NIST 800-171 Completion

Domain	Progress	Control Status	Progress to Completion
Access Control	Completed 22 / 22		100%
Awareness and Training	Completed 3 / 3		100%
Audit and Accountability	Completed 9 / 9		100%
Security Assessment	Completed 4 / 4		100%
Configuration Management	Completed 9 / 9		100%
Identification and Authentication	Completed 11 / 11		100%
Incident Response	Completed 3 / 3		100%
Maintenance	Completed 6 / 6		100%
Media Protection	Completed 9 / 9		100%

Plan of Action and Milestones (POAM)



Plan of Action & Milestones

08/17/2022

	Plan	Task	Assigned User	Start Date	Due Date	Status
1	Cybersecurity Maturity Model Certification (CMMC) 2.0 / 2022	**CMMC Practice: IA.L2-3.5.6** **NIST 800-171 Control: 3.5.6** Action Item - Need user account management policy written, implementation plan and other activities	Kevin Hancock	06/09/2022	07/11/2022	New

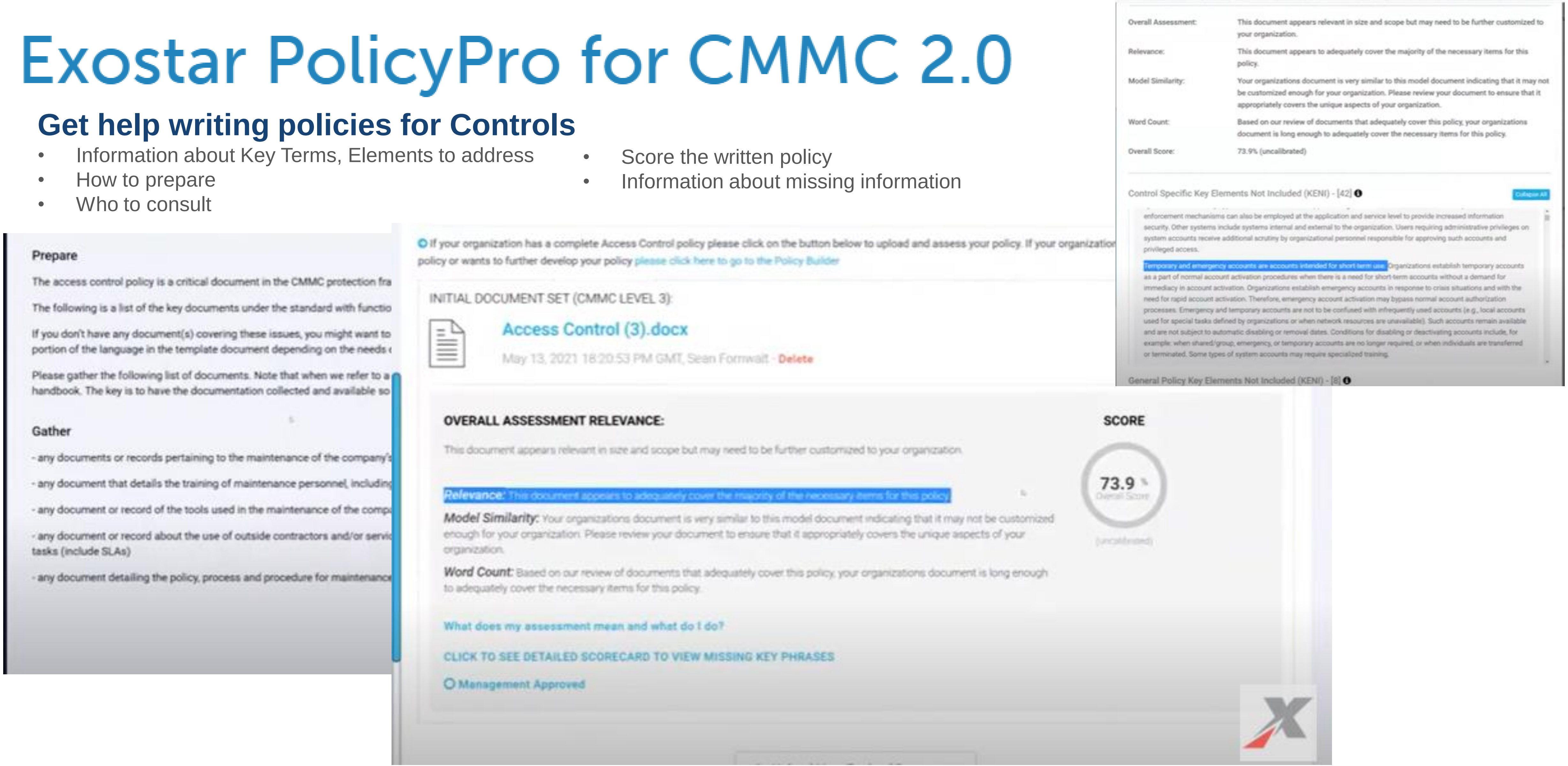
Progress against your POAMS

Exostar PolicyPro for CMMC 2.0

Get help writing policies for Controls

- Information about Key Terms, Elements to address
- How to prepare
- Who to consult

- Score the written policy
- Information about missing information



Prepare

The access control policy is a critical document in the CMMC protection fra

The following is a list of the key documents under the standard with functio

If you don't have any document(s) covering these issues, you might want to portion of the language in the template document depending on the needs c

Please gather the following list of documents. Note that when we refer to a handbook. The key is to have the documentation collected and available so

Gather

- any documents or records pertaining to the maintenance of the company's

- any document that details the training of maintenance personnel, including

- any document or record of the tools used in the maintenance of the compa

- any document or record about the use of outside contractors and/or servic tasks (include SLAs)

- any document detailing the policy, process and procedure for maintenance

○ If your organization has a complete Access Control policy please click on the button below to upload and assess your policy. If your organization policy or wants to further develop your policy please click here to go to the Policy Builder

INITIAL DOCUMENT SET (CMMC LEVEL 3):

Access Control (3).docx

May 13, 2021 18:20:53 PM GMT, Sean Formwalt - Delete

OVERALL ASSESSMENT RELEVANCE:

This document appears relevant in size and scope but may need to be further customized to your organization.

Relevance: This document appears to adequately cover the majority of the necessary items for this policy

Model Similarity: Your organizations document is very similar to this model document indicating that it may not be customized enough for your organization. Please review your document to ensure that it appropriately covers the unique aspects of your organization.

Word Count: Based on our review of documents that adequately cover this policy, your organizations document is long enough to adequately cover the necessary items for this policy.

What does my assessment mean and what do I do?

CLICK TO SEE DETAILED SCORECARD TO VIEW MISSING KEY PHRASES

○ Management Approved

SCORE

73.9 %
Overall Score
(uncalibrated)

Overall Assessment:	This document appears relevant in size and scope but may need to be further customized to your organization.
Relevance:	This document appears to adequately cover the majority of the necessary items for this policy.
Model Similarity:	Your organizations document is very similar to this model document indicating that it may not be customized enough for your organization. Please review your document to ensure that it appropriately covers the unique aspects of your organization.
Word Count:	Based on our review of documents that adequately cover this policy, your organizations document is long enough to adequately cover the necessary items for this policy.
Overall Score:	73.9% (uncalibrated)

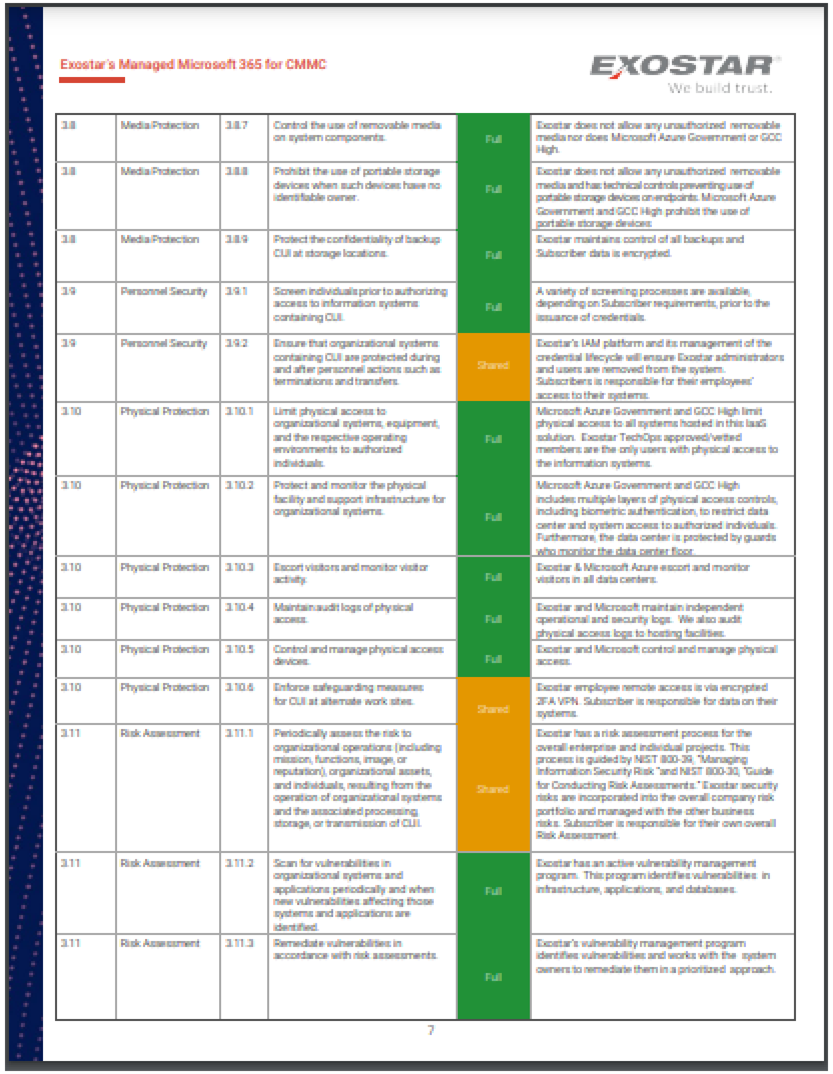
Control Specific Key Elements Not Included (KENI) - [42] 🛈

enforcement mechanisms can also be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access.

Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without a demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: when shared/group, emergency, or temporary accounts are no longer required, or when individuals are transferred or terminated. Some types of system accounts may require specialized training.

General Policy Key Elements Not Included (KENI) - [8] 🛈

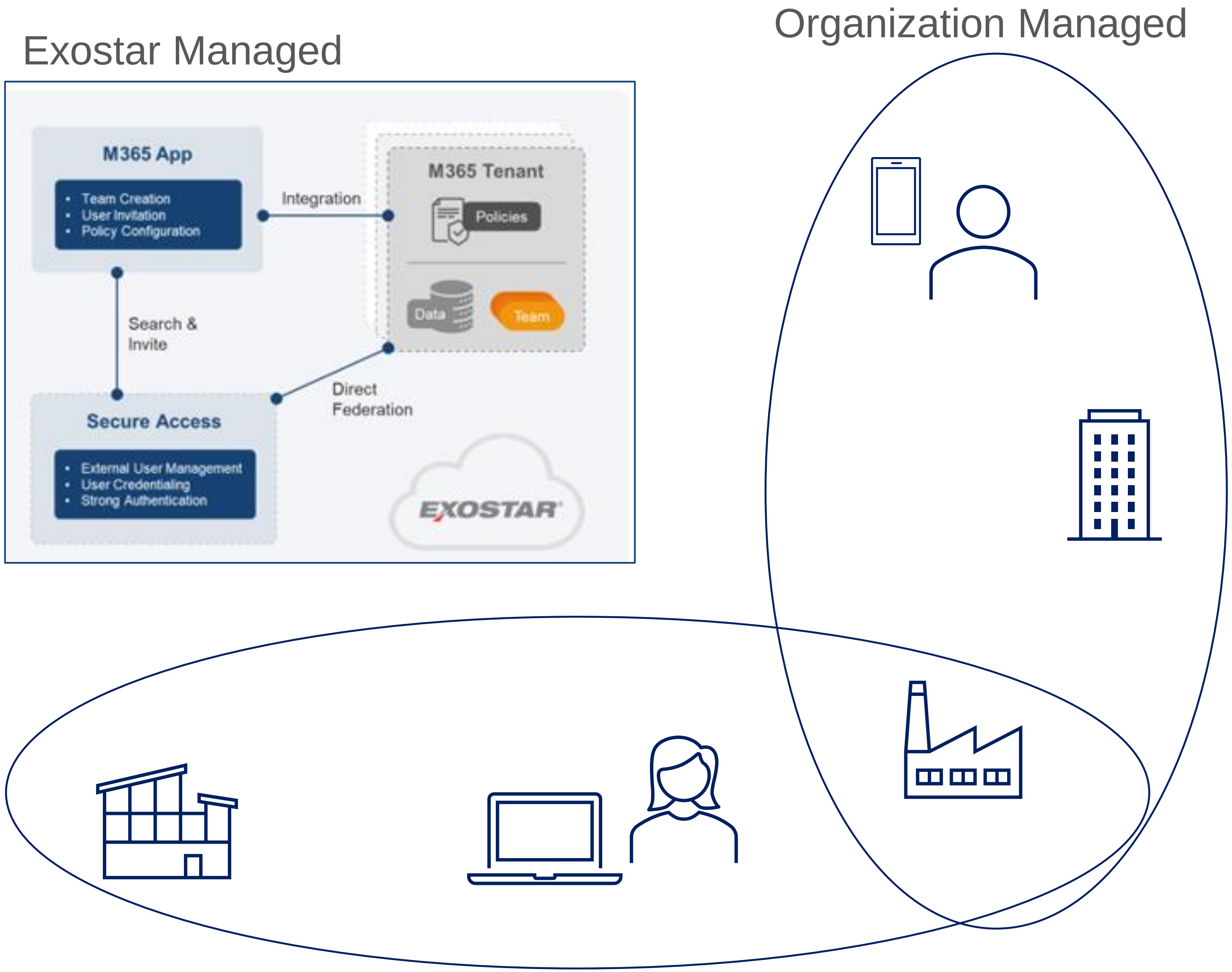
Shared Responsibility – What it means



Exostar's Managed Microsoft 365 for CMMC

3.8	Media Protection	3.8.7	Control the use of removable media on system components.	Full	Exostar does not allow any unauthorized removable media nor does Microsoft Azure Government or GCC High.
3.8	Media Protection	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Full	Exostar does not allow any unauthorized removable media and has technical controls preventing use of portable storage devices on endpoints. Microsoft Azure Government and GCC High prohibit the use of portable storage devices.
3.8	Media Protection	3.8.9	Protect the confidentiality of backup CUI at storage locations.	Full	Exostar maintains control of all backups and Subscriber data is encrypted.
3.9	Personnel Security	3.9.1	Screen individuals prior to authorizing access to information systems containing CUI.	Full	A variety of screening processes are available, depending on Subscriber requirements, prior to the issuance of credentials.
3.9	Personnel Security	3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Shared	Exostar's IAM platform and its management of the credential lifecycle will ensure Exostar administrators and users are removed from the system. Subscribers is responsible for their employees' access to their systems.
3.10	Physical Protection	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Full	Microsoft Azure Government and GCC High limit physical access to all systems hosted in this IaaS solution. Exostar TechOps approved/vetted members are the only users with physical access to the information systems.
3.10	Physical Protection	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	Full	Microsoft Azure Government and GCC High includes multiple layers of physical access controls, including biometric authentication, to restrict data center and system access to authorized individuals. Furthermore, the data center is protected by guards who monitor the data center floor.
3.10	Physical Protection	3.10.3	Escort visitors and monitor visitor activity.	Full	Exostar & Microsoft Azure escort and monitor visitors in all data centers.
3.10	Physical Protection	3.10.4	Maintain audit logs of physical access.	Full	Exostar and Microsoft maintain independent operational and security logs. We also audit physical access logs to hosting facilities.
3.10	Physical Protection	3.10.5	Control and manage physical access devices.	Full	Exostar and Microsoft control and manage physical access.
3.10	Physical Protection	3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	Shared	Exostar employee remote access is via encrypted 2FA VPN. Subscriber is responsible for data on their systems.
3.11	Risk Assessment	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Shared	Exostar has a risk assessment process for the overall enterprise and individual projects. This process is guided by NIST 800-39, "Managing Information Security Risk "and NIST 800-30, "Guide for Conducting Risk Assessments." Exostar security risks are incorporated into the overall company risk portfolio and managed with the other business risks. Subscriber is responsible for their own overall Risk Assessment.
3.11	Risk Assessment	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Full	Exostar has an active vulnerability management program. This program identifies vulnerabilities in infrastructure, applications, and databases.
3.11	Risk Assessment	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	Full	Exostar's vulnerability management program identifies vulnerabilities and works with the system owners to remediate them in a prioritized approach.

7

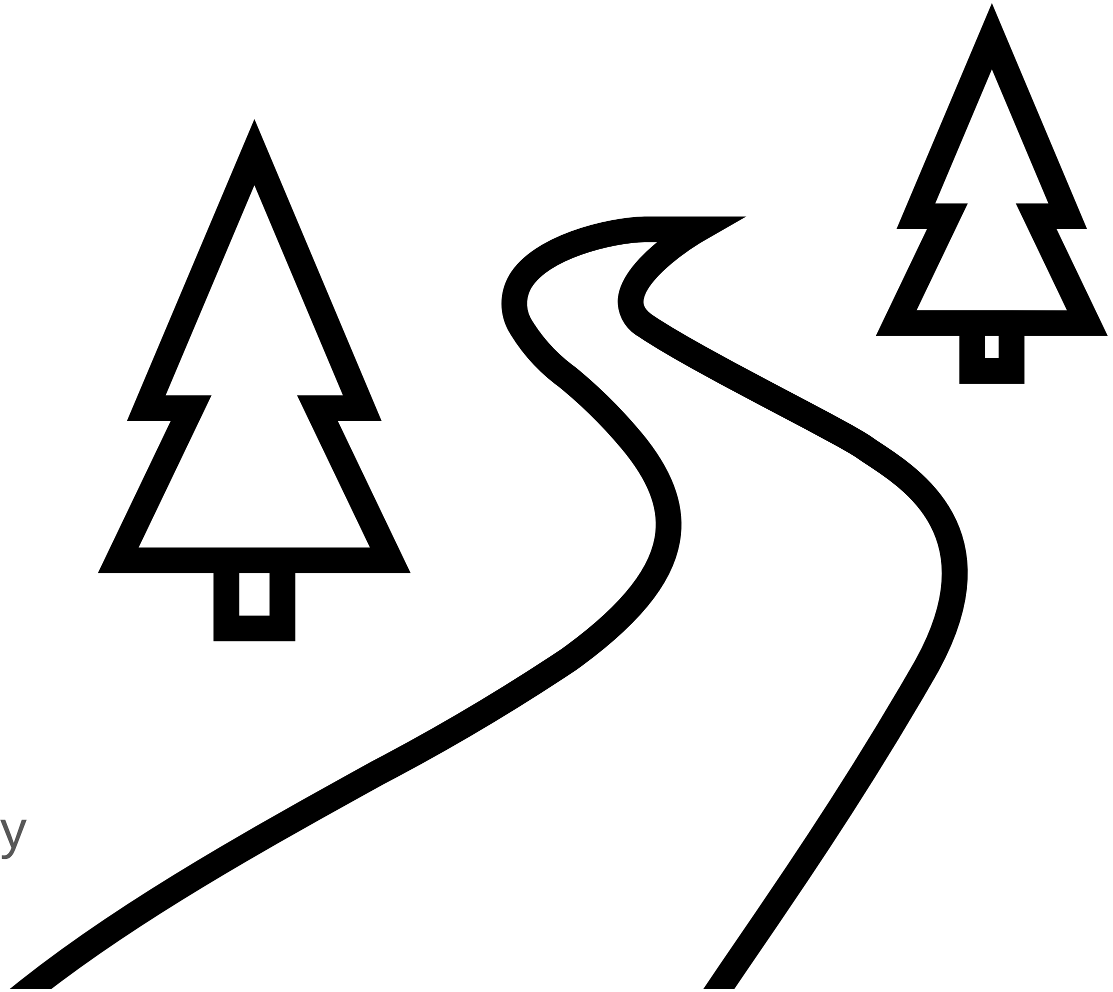


Ready for Assessment

- Close your POAMS or have solid plans in place to complete
- Consolidate Assessment Material
  - Policies
  - Procedures
  - Logs, Roles/Permissions, Groups etc.
- Engage with a CMMC Third-Party Assessment Organization (C3PAO)
- Complete Assessment

Recap

1. Choose your destination (CMMC Level)
2. Identify the system, individuals and existing resources
3. Perform an initial assessment and identify gaps
4. Start the Journey
    a) Tools to help
    b) Cloud Services
    c) Partners
5. Consolidate policies, procedures, control systems, logs, etc.
6. Perform self assessment or engage with 3rd party to do readiness assessment
7. Engage C3PAO for assessment



Exit Poll

See link in YouTube description

Q&A

CMMC Questions

1. Timeline for CMMC Implementation
   - Is the 10/1/2024 date changing to May 2023?
   - Will CMMC 2.0 be implemented immediately in May 2023 and appear in contracts immediately or will there be a phase-in period?
   - Where do we find official documentation regarding the May 2023 date
   - When will the industry audits begin?

2. How do I determine which CMMC 2.0 Level (1, 2, or 3) I will need?
   - What are the requirements for a very small business, 2 employees, no current Govt contracts?
   - I am a small business utilizing 2 computers. One is used only for email and web searching using a VPN and the other is internal information saving and is not at all online or any network. I would certainly like to know what else is needed to become compliant

3. What is the difference between NIST and CMMC?
4. Microsoft Questions
   - How does CMMC 2.0 apply to a company leveraging primarily Microsoft Web Products?
   - How many (and which ones) of the controls does Office 365 satisfy?

5. Is there an Individual Certification that prepares someone on CMMC for their organization?

Useful sources of information

- Learn more about CUI at https://www.dodcui.mil/
- CMMC Accreditation Body website https://cyberab.org/
- DoD Procurement reference website https://dodprocurementtoolbox.com/
- DoD CMMC Acquisition website https://www.acq.osd.mil/cmmc/index.html

Summary of the SPRS process with links to authoritative PIEE and SPRS materials hosted by DoD
https://www.exostar.com/blog/nist-800-171-basic-assessment-reporting-easy-as-1-2-3/

- Exostar Partner Listing https://www.exostar.com/partners/ (note – select CMMC)

Free Trial Information:

- Exostar Certification Assistant https://www.exostar.com/product/certification-assistant/
- Exostar PolicyPro https://www.exostar.com/product/policypro/

Exostar Solution Specific

EXOSTAR®
We build trust.

1. Are there other Exostar offerings that will help compliance and what are their costs? I need a total overall expense required for CMMC compliance to present to get approval for purchasing."
2. What is the difference between Managed Microsoft for CMMC and Microsoft 365 E5 ?
3. What is the cost of Exostar's managed Microsoft program?
4. What is the cost of Exostar's Policy Pro?

Contact

cmmc-team@Exostar.com

EXOSTAR®
We build trust.

Exit Poll Reminder

See link in YouTube description

Thank you for joining us.

cmmc-team@exostar.com

EXOSTAR®

We build trust.