Exostar’s Managed Microsoft 365 for CMMC

CMMC v 2.0 L2/NIST SP 800-171r2 Compliance Support Matrix

Version 1.0

The purpose of this document is to describe how Exostar’s Managed Microsoft 365 for CMMC solution reduces the effort of a Subscriber to support the compliance requirements within CMMC v 2.0 L2 / NIST SP 800-171, Protecting Controlled Unclassified Information (CUI) in Non-federal Information Systems and Organizations, Revision 2. Specific Subscriber scenarios may necessitate additional compensating controls to meet regulations. Some requirements are outside of the responsibility/scope of Exostar’s software and systems.

Definitions

Subscriber

An organization that purchases this solution and stores content within Exostar’s systems.

Full Compliance Status

Exostar’s systems comply with the CMMC v 2.0 L2/NIST 800-171r2 regulations when content is stored within the system

Shared Compliance Status

For the Subscriber to be fully compliant with the CMMC v 2.0 L2/NIST 800-171r2 regulations, the Subscriber must comply with its independent obligations regarding the controls beyond Exostar’s processes or technology. This Subscriber compliance obligation is true for any product a subscriber will purchase.

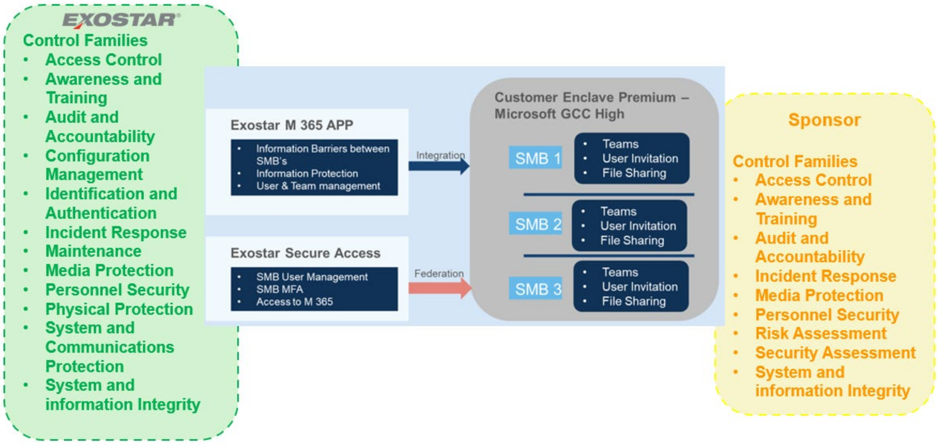
References

252.204-7021 Cybersecurity Maturity Model Certification

Requirements

Supplier Security Requirements Compliance Matrix

Solution



NIST SP 800-171 Rev 2 Section	Family	Req. ID	Requirement Text	Compliance Status	Rationale for Full Compliance
3.1	Access Control	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Full	Users are authorized for application access by their own organization in the Identity and Access Management (IAM) platform' portal.
3.1	Access Control	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Full	Users are authorized for specific content access by the data owner within the application using Exostar's embedded application.
3.1	Access Control	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Full	Sponsor organization determines the internal and external users that have rights to the Teams created and users invited via the Exostar embedded application.
3.1	Access Control	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Full	There is separation of duties between application administrators and data owners in both IAM and Exostar's Managed Microsoft 365 for CMMC.
3.1	Access Control	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Full	The IAM platform and Exostar's Managed Microsoft 365 for CMMC employ the principle of least privilege. Users must be explicitly granted access to each privileged accounts and security functions.
3.1	Access Control	3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	Full	See 3.1.5
3.1	Access Control	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Full	See 3.1.5
3.1	Access Control	3.1.8	Limit unsuccessful logon attempts.	Full	Users are locked out of the login process after five unsuccessful attempts in a set time-period.
3.1	Access Control	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Full	Privacy and security notices are configurable within the application to applicable CUI/CDI rules.
3.1	Access Control	3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Full	The IAM platform has a session time-out of 30 minutes. Exostar's Managed Microsoft for CMMC has an 8-hour session time-out. The session timeout will log a person out and take them to a general screen thus hiding the data
3.1	Access Control	3.1.11	Terminate (automatically) a user session after a defined condition.	Full	See 3.1.10. Deployed based on specific definition of the conditions.
3.1	Access Control	3.1.12	Monitor and control remote access sessions.	Full	All access is remote, as a cloud system, and is monitored and controlled.
3.1	Access Control	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Full	Exostar uses TLS to protect remote access sessions
3.1	Access Control	3.1.14	Route remote access via managed access control points.	Full	Exostar restricts solution user access to managed secure access points exposed to the Internet. Microsoft Azure routes access to the management portal through managed public access points. Remote access to the solution's platform (hosts) is restricted to managed bastions that can only be accessed through a company managed VPN system.

3.1	Access Control	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	Full	We only allow remote execution of privilege commands under certain conditions and by certain people and this is documented.
3.1	Access Control	3.1.16	Authorize wireless access prior to allowing such connections.	Shared	Internal Exostar employee wireless LAN is authenticated and encrypted. Subscriber is responsible for control of their wireless connections.
3.1	Access Control	3.1.17	Protect wireless access using authentication and encryption.	Shared	Internal Exostar employee wireless LAN is authenticated and encrypted. Subscriber is responsible for control of their wireless access.
3.1	Access Control	3.1.18	Control connection of mobile devices.	Shared	Exostar manages all mobile devices using an MDM solution. Subscriber is responsible for control of their mobile devices.
3.1	Access Control	3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	Shared	Exostar employees do not have access to Subscriber data, and it is never stored on external information systems. Subscriber is responsible for content on their user's mobile devices.
3.1	Access Control	3.1.20	Verify and control/limit connections to and use of external information systems.	Full	Exostar's Managed Microsoft 365 is an external information system and Exostar verifies and controls user access.
3.1	Access Control	3.1.21	Limit use of organizational portable storage devices on external information systems.	Shared	Exostar employees do not have access to Subscriber data, and it is never stored on external information systems. Subscriber is responsible for information stored on external information systems.
3.1	Access Control	3.1.22	Control CUI posted or processed on publicly accessible systems.	Shared	Exostar employees do not have access to subscriber data. Subscriber is responsible for information posted or processed on publicly accessible systems.
3.2	Awareness and Training	3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	Shared	Exostar provides regular security policy, standards, and practices training to Exostar personnel. Subscriber is responsible for training its organizational users.
3.2	Awareness and Training	3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security- related duties and responsibilities.	Shared	Exostar provides training to all personnel and makes available user guides and other information on myExostar. Subscriber is responsible for training its organizational users.
3.2	Awareness and Training	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Shared	Exostar provides security awareness training for staff, including mandatory annual training, and regular security newsletters. Subscriber is responsible for training its organizational users.
3.3	Audit and Accountability	3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Full	Exostar's Managed Microsoft 365 for CMMC and IAM sends event logs, to a central security event monitoring system (SIEM)for analysis, alerting, and forensic capabilities. Event logs are retained for over one year for audit and forensic purposes.
3.3	Audit and Accountability	3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Full	All users have unique account IDs; group accounts are not issued or permitted. User authentication events, security related events, and key user actions are logged.

3.3	Audit and Accountability	3.3.3	Review and update audited events.	Full	Audit logs are available on-demand to designated administrators. Content audits are available to Subscriber administrators.
3.3	Audit and Accountability	3.3.4	Alert in the event of an audit process failure.	Full	Exostar security event monitoring and audit logging systems generate alerts if logging processes fail or logs. The security operations team monitor alerts and logs 24x7.
3.3	Audit and Accountability	3.3.5	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	Full	In the case of audit review/analysis Exostar uses a SIEM to integrate and correlate.
3.3	Audit and Accountability	3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	Full	Audit logs are available on-demand to designated administrators.
3.3	Audit and Accountability	3.3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Full	Current NTP is synced to NIST time source.
3.3	Audit and Accountability	3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Full	Only designated authorized users have access to the audit tools.
3.3	Audit and Accountability	3.3.9	Limit management of audit functionality to a subset of privileged users.	Full	See 3.3.8
3.4	Configuration Management	3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Shared	Exostar maintains a baseline inventory for Exostar systems. Subscriber is responsible for their inventory.
3.4	Configuration Management	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Shared	Exostar maintains baseline security configurations for Exostar systems and services. Subscriber is responsible for their baseline security configurations.
3.4	Configuration Management	3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	Shared	Exostar tracks changes to Exostar information systems. Subscriber is responsible for their inventory.
3.4	Configuration Management	3.4.4	Analyze the security impact of changes prior to implementation.	Shared	Exostar tracks security of its systems. Subscriber is responsible for this on their systems.
3.4	Configuration Management	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Full	Exostar complies with Security standards for access to physical and logical access to our information systems. Exostar utilizes Microsoft Azure Commercial, Government, and GCC High environments to restrict physical access to systems.
3.4	Configuration Management	3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	Full	Exostar designs systems using only the essential functions and removes unnecessary software components from systems.
3.4	Configuration Management	3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Full	Exostar designs systems using only the essential functions. Endpoint control software, network port and protocol restrictions, and host intrusion prevention / detection software to control the use of unauthorized software and services.

3.4	Configuration Management	3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Full	Exostar maintains a deny-all, permit-by-exception policy to allow the use of authorized software.
3.4	Configuration Management	3.4.9	Control and monitor user-installed software.	Shared	Exostar uses endpoint protection / monitoring software to control and monitor software installation. Subscriber is responsible for these controls on their systems
3.5	Identification and Authentication	3.5.1	Identify system users, processes acting on behalf of users, and devices.	Full	Exostar Products utilize unique, user specific account identifiers and restrict access to Products to authenticated user accounts.
3.5	Identification and Authentication	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Shared	Exostar employees and contractors are screened prior to allowing access to organization information systems. Subscriber utilizes Exostar Identities to access content.
3.5	Identification and Authentication	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Full	Exostar is enforcing 2FA to access Exostar's Managed Microsoft 365 for CMMC.
3.5	Identification and Authentication	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Full	Exostar uses multiple replay-resistant authentication mechanisms to control network access for privileged and non-privileged accounts
3.5	Identification and Authentication	3.5.5	Prevent reuse of identifiers for a defined period.	Full	Exostar's Managed Microsoft 365 for CMMC prevents reuse of account identifiers. User passwords and token passwords expire and cannot be reused within a specified time.
3.5	Identification and Authentication	3.5.6	Disable identifiers after a defined period of inactivity.	Full	**Entire Account** • Permanently deactivated after 760 days of inactivity (or 180 days of inactivity if the account holder has not yet logged in and accepted Ts and Cs) • App-level subscription – configurable per app, but the default settings are: **User** • Access suspended after 180 days of not accessing the app • Access deleted after having been suspended for 185 days
3.5	Identification and Authentication	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Full	Exostar's IAM platform enforces password complexity and password reuse controls
3.5	Identification and Authentication	3.5.8	Prohibit password reuse for a specified number of generations.	Full	Exostar prohibits reuse of passwords for 10 generations
3.5	Identification and Authentication	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	Full	Exostar's IAM platform supports the use of one-time, temporary passwords that must be changed upon first login.
3.5	Identification and Authentication	3.5.10	Store and transmit only cryptographically-protected passwords	Full	Exostar's IAM platform encrypts passwords at rest and in transit.
3.5	Identification and Authentication	3.5.11	Obscure feedback of authentication information.	Full	Exostar's IAM platform obscures sensitive authentication data fields and failure feedback.
3.6	Incident Response	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Shared	Exostar has controls to detect and address incidents. Exostar's Incident response team and associated processes are patterned after Nation Institute of Standards and Technology (NIST) 800- 61 and US CERT. Subscriber is responsible for its own incident handling processes.

3.6	Incident Response	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Shared	Exostar has mechanisms in place through its incident response process to track, document, and report incidents to the appropriate individuals in the appropriate timeframes. Subscriber is responsible for its own process.
3.6	Incident Response	3.6.3	Test the organizational incident response capability.	Shared	Exostar has a tested incident response plan. Executive and legal incident response team training is in place. Subscriber is responsible for their own incident response plan.
3.7	Maintenance	3.7.1	Perform maintenance on organizational systems.	Full	Exostar performs ongoing maintenance on its systems.
3.7	Maintenance	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Full	System maintenance is conducted by only authorized Exostar engineers using vetted, authorized software and techniques
3.7	Maintenance	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Full	Exostar and Microsoft Azure Government and GCC High following NIST 800-88 sanitization guidelines when disposing data
3.7	Maintenance	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Full	Any new media is checked for viruses before the media is used in an information system
3.7	Maintenance	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Full	Exostar requires two-factor authentication to access the application and associated systems in all situations local access and non-local access.
3.7	Maintenance	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	Full	Exostar and Microsoft Azure Government and GCC High Environments enforce this control.
3.8	Media Protection	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Full	Exostar's Managed Microsoft 365 for CMMC encrypts and securely stores all system data including any CUI Subscriber may choose to store in the solution. Physically controlled media cannot leave the data center unless disposed of using NIST 800-88 Sanitization and DoD guidelines or properly secured.
3.8	Media Protection	3.8.2	Limit access to CUI on system media to authorized users.	Full	Exostar's Managed Microsoft 365 for CMMC securely stores CUI and provides access to it only to those authorized by the subscriber. Exostar engineers do not have access to customer data.
3.8	Media Protection	3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	Full	Exostar and Microsoft Azure Government and GCC High data sanitation procedure is aligned with US DOD standards.
3.8	Media Protection	3.8.4	Mark media with necessary CUI markings and distribution limitations	Shared	Marking of CUI data is done by the subscriber or the organization that originated the CUI data. Exostar's Managed Microsoft 365 for CMMC limits who has access to the data, though it is the Subscriber's responsibility to manage / grant / revoke user access to CUI data.
3.8	Media Protection	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Shared	Exostar's Managed Microsoft 365 for CMMC control access to and accountability for media when the data is transported outside the solution. The subscriber is responsible for the data on their own systems.
3.8	Media Protection	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Shared	Exostar's Managed Microsoft 365 for CMMC encrypt data at rest and while in transit to and from the hosted solution. The subscriber would be responsible for data encryption and protection on their own systems.

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.

3.12	Security Assessment	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Sha red	Exostar has an assessment/audit program that provides visibility and governance into how well controls are being applied. Subscriber is responsible assessing their controls regarding granting access to the system data.
3.12	Security Assessment	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Full	Exostar's assessment/audit program identifies control weaknesses and works with the system owners to remediate them in a prioritized approach.
3.12	Security Assessment	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Full	Exostar's assessment/audit program assessment control weaknesses on an ongoing basis.
3.12	Security Assessment	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Full	Exostar has a system security plan that outlines the system and operating environment, security requirement implementation, and how it connects with other systems/operating environments.
3.13	System and Communications Protection	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Full	Microsoft controls, protects, and monitors the Azure Government and GCC High management and data communications networks while Exostar monitors, controls, and protects the private virtual networks within the company's environments.
3.13	System and Communications Protection	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Full	Microsoft has implemented processes to promote and maintain effective security controls within the Azure Government and GCC High environments. Exostar has implemented processes and controls to provide secure information systems.
3.13	System and Communications Protection	3.13.3	Separate user functionality from system management functionality.	Full	Exostar has implemented effective separation of duties controls to separate system engineering and administration functions from general user access within systems. Information management is handled by a dedicated Technical Operations resource.
3.13	System and Communications Protection	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Full	Exostar uses both ACLs and Firewall rules to prevent unauthorized and unintended information transfer via shared system resources.
3.13	System and Communications Protection	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Full	Exostar has implemented a multi-tier architecture of VLANs and firewalls to separate external from internal networks.
3.13	System and Communications Protection	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Full	Exostar employs a least privilege model for access and communications allowing only what is absolutely needed to communicate.
3.13	System and Communications Protection	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	Full	For Exostar employees all traffic is routed through the VPN for remote devices and has prohibited split tunnelling for remote devices used to administer the system platform
3.13	System and Communications Protection	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Full	Communications are encrypted with TLS per guidance from NIST SP800-52r2.

3.13	System and Communications Protection	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Full	See 3.1.10
3.13	System and Communications Protection	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Full	Cryptographic keys for Exostar's solution are maintained and managed in hardware security module systems and Azure Government Key Vaults.
3.13	System and Communications Protection	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Full	The cryptographic keys used in the solution are created using FIPS 140-2 validated encryption ciphers / systems.
3.13	System and Communications Protection	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Full	N/A collaborative computing devices are prohibited.
3.13	System and Communications Protection	3.13.13	Control and monitor the use of mobile code.	Full	N/A Mobile code is not deployed
3.13	System and Communications Protection	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies	Full	N/A VOIP is not used
3.13	System and Communications Protection	3.13.15	Protect the authenticity of communications sessions	Full	Data in transit is encrypted and all sessions are authenticated
3.13	System and Communications Protection	3.13.16	Protect the confidentiality of CUI at rest.	Full	Exostar configured the solution to encrypt data at rest with FIPS 140-2 certified ciphers.
3.14	System and Information Integrity	3.14.1	Identify, report, and correct system flaws in a timely manner.	Full	Exostar deploys both internal and external synthetic monitoring to detect and alert the Technical Operational team to remediate any issues.
3.14	System and Information Integrity	3.14.2	Provide protection from malicious code at designated locations within organizational systems.	Full	Anti-virus scans all content when checked-in or checked-out of Exostar's Managed Microsoft 365 for CMMC.
3.14	System and Information Integrity	3.14.3	Monitor system security alerts and advisories and take action in response.	Full	Exostar monitors the solution and responds to security alerts and advisories according to established procedures and policies. .
3.14	System and Information Integrity	3.14.4	Update malicious code protection mechanisms when new releases are available.	Full	Exostar downloads virus signature updates automatically.
3.14	System and Information Integrity	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Full	Exostar performs vulnerability scans regularly, malicious code scans continuously, and scans files uploaded to the solution in real time.
3.14	System and Information Integrity	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Full	Exostar monitors the solution for indicators of an attack or system compromise and responds to security alerts and advisories according to established procedures and policies. .
3.14	System and Information Integrity	3.14.7	Identify unauthorized use of organizational systems.	Full	Exostar identifies unauthorized use of information system and responds promptly per established policies and procedures.