Exostar's ForumPass Defense

NIST SP 800-171 Compliance Support Matrix

Version 4.0

The purpose of this document is to describe how Exostar's ForumPass Defense solution reduces the effort of a Subscriber to support the compliance requirements within NIST SP 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, Revision 1, December 2016. ForumPass Defense is the combined cloud hosted solution of Exostar's Managed Access Gateway (MAG), security enhanced SharePoint 2013 & Digital Rights Management (DRM) technology. 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 an Exostar ForumPass Defense License and stores content within Exostar's systems.

Full Compliance Status

Exostar's systems comply with the NIST 800-171 regulations when content is stored within the system or protected by Digital Rights Management.

Shared Compliance Status

For the Subscriber to be fully compliant with the NIST 800-171 regulations they have independent obligations the controls above Exostar's processes or technology.

References

252.204-7008 Compliance with Safeguarding Covered Defense Information, 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

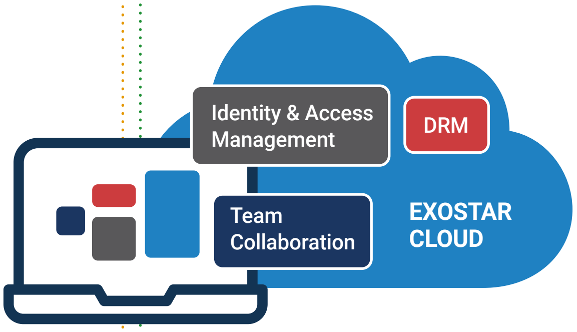
Supplier Security Requirements Compliance Matrix

Solution

SUBSCRIBER

Documents not supported by DRM

Control Families
- Access Control
- Awareness and Training
- Audit and Accountability
- Incident Response
- Media Protection
- Personnel Security
- Risk Assessment
- Security Assessment
- System and information Integrity



EXOSTAR

Documents stored in ForumPass and/or supported by DRM

Control Families
- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical Protection
- Personnel Security
- System and Communications Protection
- System and information Integrity

NIST SP 800-171 Section	Family	Req. ID	Requirement Text	Compliance Status	Rationale for Full Compliance
3.1	Access Control	3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Full	Users are authorized for application access by their own organization in the MAG portal.
3.1	Access Control	3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Shared	Users are authorized for specific content access by the data owner within the ForumPass application using Access Control Lists (ACL).
3.1	Access Control	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Full	ForumPass employs ACLs and DRM protection to authorize access to CUI/CDI within and outside of the ForumPass environment.
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 MAG and ForumPass.
3.1	Access Control	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Full	MAG and ForumPass 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 audit the execution of such functions.	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 four unsuccessful attempts.
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	MAG has a session time-out of 30 minutes. ForumPass has an 8-hour session time-out. We do not currently have a pattern-hiding display. 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 utilizes: -SSL/HTTPS in Transit • AES 256 for connection (FIPs compliant) • RSA for key exchange (FIPs compliant) • HMAC for message authentication (FIPs compliant)
3.1	Access Control	3.1.14	Route remote access via managed access control points.	Full	Remote access is via the Managed Access Gateway (MAG) cloud systems.

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.	Full	Internal Exostar employee wireless LAN is authenticated and encrypted. Access to ForumPass is behind MAG authentication and through HTTPS connection.
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.	Full	ForumPass DRM Protection ensures CUI/CDI is encrypted on mobile devices.
3.1	Access Control	3.1.20	Verify and control/limit connections to and use of external information systems.	Full	ForumPass 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	DRM protects documents regardless of the document location. Exostar employees do not have access to Subscriber data, and it is never stored on external information systems. Subscriber is responsible for content that is not protected by DRM stored on external information systems.
3.1	Access Control	3.1.22	Control information posted or processed on publicly accessible information systems.	Full	DRM compatible content is protected regardless of its location.
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	Security notices are configurable to be displayed within the application. Exostar provides training to Administrators. Subscriber is responsible for training it's 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 working with MAG and ForumPass. Subscriber is responsible for training it's organizational users. Subscriber is responsible for training it's 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 it's 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	ForumPass and MAG have full audit capability.
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	See 3.3.2. Two-factor authentication ensures nonrepudiation.

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 monitors audit logs. If an alert occurs in the event of an audit process failure.
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 we use Splunk 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 own.
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 a baseline security configurations for Exostar systems. Subscriber is responsible for their own.
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 own.
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 their own.
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. Subscriber is responsible for their own restriction above and beyond Exostar.
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.
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

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 does this within the scope of ForumPass.
3.4	Configuration Management	3.4.9	Control and monitor user-installed software.	Full	Exostar does this within the scope of ForumPass.
3.5	Identification and Authentication	3.5.1	Identify information system users, processes acting on behalf of users, or devices.	Full	Exostar does this within the scope of ForumPass.
3.5	Identification and Authentication	3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information 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 in FP-Defense at the document level, regardless of the document location.
3.5	Identification and Authentication	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Full	FP-DRM Users and Exostar administrators use 2FA authentication.
3.5	Identification and Authentication	3.5.5	Prevent reuse of identifiers for a defined period.	Full	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	Servers and infrastructure does this.
3.5	Identification and Authentication	3.5.8	Prohibit password reuse for a specified number of generations.	Full	See 3.5.5
3.5	Identification and Authentication	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	Full	Servers and infrastructure does this.
3.5	Identification and Authentication	3.5.10	Store and transmit only encrypted representation of passwords.	Full	Servers and infrastructure does this.
3.5	Identification and Authentication	3.5.11	Obscure feedback of authentication information.	Full	Servers and infrastructure does this. This is handled by MAG today
3.6	Incident Response	3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	Full	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.

3.6	Incident Response	3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Full	Exostar has mechanisms in place through its incident response process to track, document, and report incidents to the appropriate individuals in the appropriate timeframes.
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, based on additional systems above ForumPass.
3.7	Maintenance	3.7.1	Perform maintenance on organizational information systems.	Full	Exostar Technical Operations operate a patch management process, implementing patches at least once a quarter.
3.7	Maintenance	3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Full	System maintenance is conducted by only authorized Tech Ops engineers.
3.7	Maintenance	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Full	Exostar follows NIST 800-88 sanitization guidelines when disposing of data.
3.7	Maintenance	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	Full	Any new media (such as USB/CD) 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 escorts all visitors accessing Exostar cage space.
3.8	Media Protection	3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Full	DRM Protection controls and protects managed documents. Physically controlled media cannot leave the data center unless disposed of using NIST 800-88 Sanitization guidelines
3.8	Media Protection	3.8.2	Limit access to CUI on information system media to authorized users.	Full	DRM Protection controls and protects managed documents regardless of the media.
3.8	Media Protection	3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Full	Exostar 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	Full	Any document checked into FP-DRM will contain metadata marking for US DOD CDI documents.
3.8	Media Protection	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Full	FP-DRM will be used for all CDI data, and it will be encrypted at all times inside and outside of the system.
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.	Full	DRM Protection ensures compatible CUI/CDI is encrypted on all transportable digital media devices.

3.8	Media Protection	3.8.7	Control the use of removable media on information system components.	Full	Exostar does not allow any unauthorized removable media into the data center cage space.
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 into the data center cage space.
3.8	Media Protection	3.8.9	Protect the confidentiality of backup CUI at storage locations.	Full	Exostar maintains direct control of all backups in Exostar's backup facility. Furthermore, Subscriber content 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 CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Full	DRM Protection removes user access to documents immediately when user is removed from the permission group. Access to documents are removed regardless of document location.
3.10	Physical Protection	3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Full	Exostar limits physical access to authorized personnel who are Exostar employees (and US Persons)
3.10	Physical Protection	3.10.2	Protect and monitor the physical facility and support infrastructure for those information systems	Full	Exostar cage includes biometric access and cage locks and includes safety features including an enclosed cage with roof around cabinets. 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 escorts all visitors accessing Exostar's cage space.
3.10	Physical Protection	3.10.4	Maintain audit logs of physical access.	Full	Exostar audits physical access logs to data center.
3.10	Physical Protection	3.10.5	Control and manage physical access devices.	Full	Exostar facilities and data centers are secured.
3.10	Physical Protection	3.10.6	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	Full	Exostar employee remote access is via encrypted 2FA VPN. Use of FP-DRM ensures CUI/CDI content is safeguarded with 2FA and encryption regardless of location.
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 information 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 the information system and applications periodically and when new vulnerabilities affecting the system are identified.	Shared	Exostar has an active vulnerability management program. This program identifies vulnerabilities in infrastructure, applications, and databases. Subscriber is responsible for scanning internal applications.
3.11	Risk Assessment	3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	Shared	Exostar’s vulnerability management program identifies vulnerabilities and works with the system owners to remediate them in a prioritized approach. Subscriber is responsible for remediation of their own systems.

3.12	Security Assessment	3.12.1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	Shared	Exostar has an assessment/audit program that provides visibility and governance into how well controls are being applied. Subscriber is responsible for their own assessment.
3.12	Security Assessment	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	Shared	Exostar's assessment/audit program identifies control weaknesses and works with the system owners to remediate them in a prioritized approach. Subscriber is responsible for remediation of their own systems.
3.12	Security Assessment	3.12.3	Monitor information system 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.	Shared	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. Subscriber is responsible for the system security plan for shared controls.
3.13	System and Communications Protection	3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Shared	Exostar monitors and protects the Exostar infrastructure. The Subscriber is responsible for their own.
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 information systems.	Full	Exostar monitors and protects the Exostar infrastructure.
3.13	System and Communications Protection	3.13.3	Separate user functionality from information system management functionality.	Full	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 implements 3 tier architecture 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 the information system and communicating via some other connection to resources in external networks.	Shared	For Exostar employees all traffic is routed through the VPN for remote devices. Subscribers are responsible for their own.
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	Data is encrypted in transit. Data is encrypted at rest. DRM data is encrypted regardless of its location.

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 the information system	Full	Relevant cryptography for FP is managed within the HSM.
3.13	System and Communications Protection	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Full	Thales HSM is FIPs-validated
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	Data is encrypted in transit. Data is encrypted at rest. FP-DRM data is encrypted regardless of its location.
3.14	System and Information Integrity	3.14.1	Identify, report, and correct information and information 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 appropriate locations within organizational information systems.	Shared	Anti-virus scans all content when checked-in or checked-out of the FP-DRM system. Subscriber is responsible for implementing their own protections.
3.14	System and Information Integrity	3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	Full	In case of security alerts those are sent to a standard distribution that tech ops manages.
3.14	System and Information Integrity	3.14.4	Update malicious code protection mechanisms when new releases are available.	Shared	Exostar downloads virus signature updates automatically. Subscriber is responsible for updating their own systems.
3.14	System and Information Integrity	3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Full	Exostar scans regularly.
3.14	System and Information Integrity	3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Full	Exostar monitors constantly.
3.14	System and Information Integrity	3.14.7	Identify unauthorized use of the information system.	Full	Exostar identifies unauthorized use of information system.