



Compliance Island Shared Responsibility Matrix

For NIST SP 800-171 Rev. 2

Note:

To meet all compliance requirements, the OSC must adhere to the system-specific policies and procedures provided with the Compliance Island solution. The OSC is the system owner and uses the MSP, CI, and MS as providers which help it meet its compliance requirements. Full details are included in the Compliance Island documentation.

Term	Definition
OSC	Organization Seeking Certification
MSP	Managed Service Provider
CI	Compliance Island solution
MS	Microsoft Azure / Microsoft 365 Cloud
DoDAM	DoD Assessment Methodology

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
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).	X		X	X	OSC must authorize users.	5	1
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.			X	X		5	1
3.1 Access Control	3.1.3 Control the flow of CUI in accordance with approved authorizations.			X	X		1	1
3.1 Access Control	3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.			X	X		1	2
3.1 Access Control	3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.			X	X		3	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMC Level
3.1 Access Control	3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.			X	X		1	2
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.			X	X		1	2
3.1 Access Control	3.1.8 Limit unsuccessful logon attempts.			X	X		1	2
3.1 Access Control	3.1.9 Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.			X	X		1	2
3.1 Access Control	3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.			X	X		1	2
3.1 Access Control	3.1.11 Terminate (automatically) user sessions after a defined condition.			X	X		1	2
3.1 Access Control	3.1.12 Monitor and control remote access sessions.			X	X		5	1
3.1 Access Control	3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.			X	X		5	2
3.1 Access Control	3.1.14 Route remote access via managed access control points.			X	X		1	1
3.1 Access Control	3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.			X	X		1	2
3.1 Access Control	3.1.16 Authorize wireless access prior to allowing such connections.			N/A			5	2
3.1 Access Control	3.1.17 Protect wireless access using authentication and encryption.			N/A			5	2
3.1 Access Control	3.1.18 Control connection of mobile devices.			X	X		5	2
3.1 Access Control	3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.			X	X		3	2
3.1 Access Control	3.1.20 Verify and control/limit connections to and use of external information systems.			X	X		1	1
3.1 Access Control	3.1.21 Limit use of portable storage devices on external systems.			X			1	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.1 Access Control	3.1.22 Control information posted or processed on publicly accessible information systems.			X	X		1	1
3.2 Awareness and Training	3.2.1 Ensure that managers, system administrators and users of organizational 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 those systems.	X				OSC may acquire suitable training from any valid source	5	1
3.2 Awareness and Training	3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	X				OSC may acquire suitable training from any valid source	5	1
3.2 Awareness and Training	3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	X				OSC may acquire suitable training from any valid source	1	2
3.3 Audit and Accountability	3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.			X	X		5	1
3.3 Audit and Accountability	3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.			X	X		3	1
3.3 Audit and Accountability	3.3.3 Review and update logged events.		X				1	2
3.3 Audit and Accountability	3.3.4 Alert in the event of an audit logging process failure.			X	X		1	2
3.3 Audit and Accountability	3.3.5 Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.		X	X	X		5	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.3 Audit and Accountability	3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.			X	X		1	2
3.3 Audit and Accountability	3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.				X		1	1
3.3 Audit and Accountability	3.3.8 Protect audit information and audit logging tools from unauthorized access, modification and deletion.				X		1	2
3.3 Audit and Accountability	3.3.9 Limit management of audit logging functionality to a subset of privileged users.			X			1	2
3.4 Configuration Management	3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.			X			5	1
3.4 Configuration Management	3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.			X			5	1
3.4 Configuration Management	3.4.3 Track, review, approve or disapprove and log changes to organizational systems.	X	X	X			1	1
3.4 Configuration Management	3.4.4 Analyze the security impact of changes prior to implementation.	X	X	X			1	1
3.4 Configuration Management	3.4.5 Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.			X			5	2
3.4 Configuration Management	3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.			X			5	1
3.4 Configuration Management	3.4.7 Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.			X	X		5	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.4 Configuration Management	3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.			X			5	2
3.4 Configuration Management	3.4.9 Control and monitor user-installed software.			X	X		1	1
3.5 Identification and Authentication	3.5.1 Identify information system users, processes acting on behalf of users or devices.	X	X	X	X	OSC must identify users and Terminal Devices.	5	1
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.			X	X		5	1
3.5 Identification and Authentication	3.5.3 Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.			X	X		5	2
3.5 Identification and Authentication	3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.				X		1	2
3.5 Identification and Authentication	3.5.5 Prevent the reuse of identifiers for a defined period.			X	X		1	2
3.5 Identification and Authentication	3.5.6 Disable identifiers after a defined period of inactivity.			X	X		1	2
3.5 Identification and Authentication	3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.			X	X		1	1
3.5 Identification and Authentication	3.5.8 Prohibit password reuse for a specified number of generations.			X	X		1	1
3.5 Identification and Authentication	3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.			X	X		1	1
3.5 Identification and Authentication	3.5.10 Store and transmit only cryptographically-protected passwords.				X		5	1

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.5 Identification and Authentication	3.5.11 Obscure feedback of authentication information.				X		1	1
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.	X	X				5	1
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.	X	X	X	X		5	2
3.6 Incident Response	3.6.3 Test the organizational incident response capability.	X	X				1	2
3.7 Maintenance	3.7.1 Perform maintenance on organizational systems.		X	X	X		3	1
3.7 Maintenance	3.7.2 Provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.		X	X	X		5	1
3.7 Maintenance	3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.				X		1	2
3.7 Maintenance	3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.				X		3	2
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.		X	X	X		5	1
3.7 Maintenance	3.7.6 Supervise the maintenance activities of personnel without required access authorization.	X	X	X	X		1	1
3.8 Media Protection	3.8.1 Protect (e.g., physically control and securely store) system media containing Federal Contract Information, both paper and digital.				X		3	1
3.8 Media Protection	3.8.2 Limit access to CUI on system media to authorized users.				X		3	1

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.8 Media Protection	3.8.3 Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.				X		5	1
3.8 Media Protection	3.8.4 Mark media with necessary CUI markings and distribution limitations.			X			1	2
3.8 Media Protection	3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.				X		1	2
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.			X	X		1	2
3.8 Media Protection	3.8.7 Control the use of removable media on system components.			X	X		5	1
3.8 Media Protection	3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.			X	X		3	2
3.8 Media Protection	3.8.9 Protect the confidentiality of backup CUI at storage locations.			X	X		1	1
3.9 Personnel Security	3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	X	X	X	X		3	1
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.	X	X	X	X		5	1
3.10 Physical Protection	3.10.1 Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.				X		5	1
3.10 Physical Protection	3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.				X		5	1

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.10 Physical Protection	3.10.3 Escort visitors and monitor visitor activity.				X		1	1
3.10 Physical Protection	3.10.4 Maintain audit logs of physical access.				X		1	1
3.10 Physical Protection	3.10.5 Control and manage physical access devices.				X		1	1
3.10 Physical Protection	3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	X	X	X	X		1	2
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.	X	X	X	X		3	1
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.			X	X		5	1
3.11 Risk Assessment	3.11.3 Remediate vulnerabilities in accordance with risk assessments.	X	X	X	X		1	1
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.	X	X	X	X		5	1
3.12 Security Assessment	3.12.2 Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	X	X	X	X		3	1
3.12 Security Assessment	3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	X	X	X			5	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.12 Security Assessment	3.12.4 Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.	X	X	X	X	Mandatory	-203	1
3.13 System and Communications Protection	3.13.1 Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	X	X	X	X		5	1
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.			X	X		5	2
3.13 System and Communications Protection	3.13.3 Separate user functionality from system management functionality.			X	X		1	2
3.13 System and Communications Protection	3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.				X		1	2
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.			X	X		5	1
3.13 System and Communications Protection	3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).			X	X		5	2
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 (e.g., split tunneling).			X			1	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
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.			X	X		3	2
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.			X	X		1	2
3.13 System and Communications Protection	3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.				X		1	2
3.13 System and Communications Protection	3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.			X	X		5	2
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.			X	X		1	1
3.13 System and Communications Protection	3.13.13 Control and monitor the use of mobile code.			X			1	2
3.13 System and Communications Protection	3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.			X	X		1	2
3.13 System and Communications Protection	3.13.15 Protect the authenticity of communications sessions.				X		5	2
3.13 System and Communications Protection	3.13.16 Protect the confidentiality of CUI at rest.			X	X		1	2

Compliance Island Shared Responsibility Matrix for NIST SP 800-171 Rev. 2

Category	Name	OSC	MsP	CI	MS	Notes	DoDAM Points	CMMC Level
3.14 System and Information Integrity	3.14.1 Identify, report and correct information and information system flaws in a timely manner.	X	X	X	X		5	1
3.14 System and Information Integrity	3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.			X	X		5	1
3.14 System and Information Integrity	3.14.3 Monitor system security alerts and advisories and take action in response.		X				5	1
3.14 System and Information Integrity	3.14.4 Update malicious code protection mechanisms when new releases are available.			X	X		5	1
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.			X			3	1
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.		X	X	X		5	1
3.14 System and Information Integrity	3.14.7 Identify unauthorized use of organizational systems.	X	X	X			3	1

DoD Assessment Methodology Score (SPRS Score)

110