



CYBERQP PRODUCT MAPPING:

CMMC v2.0, NIST SP 800-53 Rev. 5 & CIS Controls v8

This guide outlines how CyberQP products map to CMMC v2.0, NIST SP 800-53 Rev. 5 and CIS Controls v8 to help secure you and your customers.



Table of Contents

3 CMMC v2.0 CyberQP Product Mapping

4 What is CMMC v2.0?

5 CMMC v2.0 Control Families

6 Access Control (AC)

7 Audit and Accountability (AU)

7 Identification and Authentication (IA)

8 System and Communications Protection (SC)

9 NIST SP 800-53 Rev. 5 CyberQP Product Mapping

10 What is NIST SP 800-53 Rev. 5?

10 NIST Security and Privacy Control Families

12 Access Control (AC)

13 Audit and Accountability (AU)

14 Identification and Authentication (IA)

15 CIS Controls v8

16 What is CIS Controls V8?

17 Implementation Groups

18 Secure Configuration of Enterprise Assets and Software

18 Account Management

19 Access Control Management

19 Audit Log Management

20 Service Provider Management

CMMC v2.0 CyberQP Product Mapping

This section outlines how CyberQP products map to CMMC v2.0 to help secure you and your customers.



What is CMMC v2.0?

CMMC stands for Cybersecurity Maturity Model Certification. It is a unified standard for implementing cybersecurity measures and protecting sensitive information within the defense industrial base (DIB) of the United States. The CMMC framework was developed by the Department of Defense (DoD) to address growing concerns about cybersecurity threats and to enhance the protection of controlled unclassified information (CUI) that is handled by defense contractors and subcontractors.

CMMC is designed to assess and certify the cybersecurity maturity of organizations operating within the DIB. It provides a set of requirements and practices that organizations must meet to demonstrate their cybersecurity readiness and ability to safeguard sensitive information. CMMC v2.0 is an updated framework with three control levels, as opposed to the five maturity levels in CMMC v1.0. The CMMC framework consists of three maturity levels, each with increasing requirements and capabilities. The levels range from “Foundational” (Level 1) to “Expert” (Level 3).

The CMMC v2.0 framework incorporates a wide range of cybersecurity controls and best practices from existing standards and references, such as NIST SP 800-171, NIST SP 800-53, ISO 27001, and others. Organizations in the DIB must achieve the appropriate CMMC level to be eligible for certain DoD contracts and to demonstrate their commitment to protecting sensitive information.

It's important to note that the CMMC framework is still being implemented and enforced by the DoD. Organizations working with or seeking contracts from the DoD should familiarize themselves with the specific requirements of CMMC and work towards achieving the appropriate level of certification.

CMMC v2.0 Control Families

The CMMC v2.0 framework consists of controls organized into 14 distinct control families. These controls provide a framework for organizations to follow to enhance their security posture and mitigate cyber threats. They cover a wide range of security areas, including controls related to access control, incident response, system and information integrity, risk management, and more.

ID	Family	ID	Family
AC	Access Control	PE	Physical Protection
AT	Awareness and Training	PS	Personnel Security
AU	Audit and Accountability	RA	Risk Assessment
CM	Configuration Management	SC	System and Communications Protection
IA	Identification and Authentication	SI	System and Information Integrity
IR	Incident Response	CA	Security Assessment
MA	Maintenance	MP	Media Protection

CyberQP products help achieve CMMC certification in the highlighted controls below:

ID	Family	ID	Family
AC	Access Control	PE	Physical Protection
AT	Awareness and Training	PS	Personnel Security
AU	Audit and Accountability	RA	Risk Assessment
CM	Configuration Management	SC	System and Communications Protection
IA	Identification and Authentication	SI	System and Information Integrity
IR	Incident Response	CA	Security Assessment
MA	Maintenance	MP	Media Protection

Access Control (AC)

CMMC Control Definition

Use processes and tools to establish who has access to systems, control internal system access, and limit data access to authorized users and processes.

CMMC AC CONTROL MAPPING TO CYBERQP:

NIST Control #	CMMC Control Title:	CyberQP Solution:	CMMC Control Level
3.1.1	Authorized Access Control	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	1
3.1.2	Transaction & Function Control	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	1
3.1.4	Separation of Duties	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	2
3.1.5	Least Privilege	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	2
3.1.6	Non-Privileged Account Use	CyberQP QGuard Just-in-Time Account Creation	2
3.1.7	Privileged Functions	CyberQP QGuard Just-in-Time Account Creation	2
3.1.12	Control Remote Access	CyberQP QGuard Just-in-Time Account Creation	2
3.1.15	Privileged Remote Access	CyberQP QGuard Just-in-Time Account Creation	2

Audit and Accountability (AU)

CMMC Control Definition

Use processes and tools in place to track users that have access to Controlled Unclassified Information (CUI) and perform secure audits of those logs to ensure accountability.

CMMC AU CONTROL MAPPING TO CYBERQP: _____

NIST Control #	CMMC Control Title:	CyberQP Solution:	CMMC Control Level
3.1.1	System Auditing	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation	2

Identification and Authentication (IA)

CMMC Control Definition

Use processes and tools to ensure the proper roles within the organization have the correct level of access and can be authenticated for reporting and accountability purposes.

CMMC IA CONTROL MAPPING TO CYBERQP: _____

NIST Control #	CMMC Control Title:	CyberQP Solution:	CMMC Control Level
3.5.2	Authentication	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	1
3.5.3	Multifactor Authentication	CyberQP QGuard Just-in-Time Account Creation	2
3.5.6	Identifier Handling	CyberQP QGuard Just-in-Time Account Creation	2
3.5.7	Password Complexity	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	2

System and Communications Protection (SC)

CMMC Control Definition

Use processes and tools to define the security requirements of each system and communication channel used to provide evidence that there is control of communications at system boundaries.

CMMC SC CONTROL MAPPING TO CYBERQP: _____

NIST Control #	CMMC Control Title:	CyberQP Solution:	CMMC Control Level
3.1.3	Role Separation	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	2



NIST SP 800-53 Rev. 5 CyberQP Product Mapping

This section outlines how CyberQP products map to NIST SP 800-53 Rev. 5. to help secure you and your customers.



What is NIST SP 800-53 Rev. 5?

This update to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 5 addresses the Defense Science Board's (DSB) recommendations by adopting a proactive, systematic approach to developing and providing comprehensive safeguarding measures for a wide range of computing platforms. The safeguarding measures encompass security and privacy controls designed to protect critical operations, organizational assets, and individuals' privacy. The primary objectives are to enhance the penetration resistance of information systems, minimize damage from cyberattacks, ensure cyber resilience and survivability, and uphold privacy protections.

NIST Security and Privacy Control Families

The NIST SP 800-53 Rev. 5 framework consists of 1,189 controls organized into 20 distinct control families. These controls provide a framework for organizations to follow to enhance their security posture and mitigate cyber threats. They cover a wide range of security areas, including asset management, vulnerability management, secure configuration, access control, and incident response.

ID	Family	ID	Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

CYBERQP PRODUCT MAPPING

CyberQP products help achieve NIST Safeguards in the highlighted controls below:

ID	Family	ID	Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Access Control (AC)

NIST Control Definition

The Access Control (AC) family encompasses controls like identification and authentication, authorization, and non-repudiation. These measures ensure that only authorized users can access sensitive information and that their actions are verifiable and traceable.

NIST AC CONTROL MAPPING TO CYBERQP:

NIST Control #	NIST Control Title:	CyberQP Solution:
AC-1	Policy and Procedures	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
AC-2	Account Management	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation CyberQP QGuard Just-in-Time Account Creation
AC-2(1)	Automated System Account Management	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation CyberQP QGuard Just-in-Time Account Creation
AC-2(3)	Disable Accounts	CyberQP QGuard Just-in-Time Account Creation
AC-5	Separation of Duties	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
AC-6	Least Privilege	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
AC-6(1)	Authorize Access to Security Functions	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
AC-6(2)	Non-Privileged Access for Nonsecurity Functions	CyberQP QGuard Just-in-Time Account Creation
AC-6(5)	Privileged Accounts	CyberQP QGuard Just-in-Time Account Creation
AC-6(7)	Review of User Privileges	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management

Audit and Accountability (AU)

NIST Control Definition

The Audit and Accountability (AU) control family ensures that events are properly logged, audited, and securely maintained. It mandates centralized logging, regular log rotation, and access controls to prevent unauthorized modifications.

NIST AU CONTROL MAPPING TO CYBERQP:

NIST Control #	NIST Control Title:	CyberQP Solution:
AU-2	Event Logging	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation
AU-3	Content of Audit Records	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation
AU-3(1)	Additional Audit Information	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation
AU-7	Audit Record Reduction and Report Generation	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation
AU-9(4)	Access by Subset of Privileged Users	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
AU-11	Audit Record Retention	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation
AU-12	Audit Record Generation	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation

Identification and Authentication (IA)

NIST Control Definition

The Identification and Authentication (IA) control family safeguards user and device identities through measures such as multifactor authentication, device identification, and fingerprinting. These controls ensure only authorized users access sensitive information and verify device integrity, enhancing overall security.

NIST IA CONTROL MAPPING TO CYBERQP:

NIST Control #	NIST Control Title:	CyberQP Solution:
IA-2(1)	Multi-factor Authentication (Organizational Users)	CyberQP QGuard Just-in-Time Account Creation
IA-4	Identifier Management	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
IA-5	Authenticator Management	CyberQP QGuard Privileged Identity Management CyberQP Password Manager CyberQP QGuard Just-in-Time Account Creation
IA-5(1)	Password-based Authentication	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management

CIS Controls v8

This section outlines how CyberQP products map to CIS Controls v8 to help secure you and your customers.



What is CIS Controls v8?

The Center for Internet Security maintains a list of 18 cybersecurity controls organizations can implement to protect their systems and data. These controls provide a framework for organizations to follow to enhance their security posture and mitigate cyber threats. They cover a wide range of security areas, including asset management, vulnerability management, secure configuration, access control, and incident response.

The CIS Controls are designed to be practical and actionable, offering specific steps and guidance for organizations to implement each control effectively. They are regularly updated to align with the evolving threat landscape and industry best practices. By adopting and implementing CIS Controls, organizations can establish a strong foundation for their cybersecurity defenses, improve their resilience to attacks, and reduce the risk of data breaches and other security incidents.

Implementation Groups

CIS maps controls to implementation groups, which are categories that help organizations prioritize the implementation of the CIS Controls. There are three implementation groups: IG1, IG2, and IG3.

Implementation Group 1 (IG1)

IG1 controls are foundational and should be implemented by all organizations. They include fundamental security measures with a high impact on security posture. These controls are relatively easier to implement.

Implementation Group 2 (IG2)

IG2 controls build upon IG1 and provide additional security measures to enhance security posture. They involve more advanced practices and technologies like privileged access management and security monitoring. Implementing IG2 controls strengthens an organization's security defenses against a wider range of threats.

Implementation Group 3 (IG3)

IG3 controls are advanced and require more resources and expertise to implement. They address emerging threats and provide additional security measures to mitigate advanced attacks. These controls involve sophisticated technologies like threat intelligence and advanced security analytics. Implementing IG3 controls helps organizations increase their resilience against sophisticated cyber attacks.

CYBERQP PRODUCT MAPPING

Implementation Groups

CIS maps controls to implementation groups, which are categories that help organizations prioritize the implementation of the CIS Controls. There are three implementation groups: IG1, IG2, and IG3.

Inventory and Control of Enterprise Assets	1	Inventory and Control of Software Assets	2	Data Protection	3	Secure Configuration of Enterprise Assets and Software	4
Account Management	5	Access Control Management	6	Continuous Vulnerability Management	7	Audit Log Management	8
Email and Web Browser Protections	9	Malware Defenses	10	Data Recovery	11	Network Infrastructure Management	12
Network Monitoring and Defense	13	Security Awareness and Skills Training	14	Service Provider Management	15	Application Software Security	16
		Incident Response Management	17	Penetration Testing	18		

CyberQP products help achieve CIS Safeguards in the green controls below:

Inventory and Control of Enterprise Assets	1	Inventory and Control of Software Assets	2	Data Protection	3	Secure Configuration of Enterprise Assets and Software	4
Account Management	5	Access Control Management	6	Continuous Vulnerability Management	7	Audit Log Management	8
Email and Web Browser Protections	9	Malware Defenses	10	Data Recovery	11	Network Infrastructure Management	12
Network Monitoring and Defense	13	Security Awareness and Skills Training	14	Service Provider Management	15	Application Software Security	16
		Incident Response Management	17	Penetration Testing	18		

4. Secure Configuration of Enterprise Assets and Software

CIS Control Definition

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

CIS CONTROL 4 MAPPING TO CYBERQP:

CIS Control #	CIS Control Title:	CyberQP Solution:	CIS Implementation Group
4.7	Manage Default Accounts on Enterprise Assets and Software	CyberQP QGuard Privileged Identity Management CyberQP Password Manager	IG1, IG2, IG3

5. Account Management

CIS Control Definition

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

CIS CONTROL 5 MAPPING TO CYBERQP:

CIS Control #	CIS Control Title:	CyberQP Solution:	CIS Implementation Group
5.1	Establish and Maintain an Inventory of Accounts	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation	IG1, IG2, IG3
5.2	Use Unique Passwords	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	IG1, IG2, IG3
5.3	Disable Dormant Accounts	CyberQP QGuard Just-in-Time Account Creation	IG1, IG2, IG3
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	CyberQP QGuard Just-in-Time Account Creation	IG1, IG2, IG3
5.5	Establish and Maintain an Inventory of Service Accounts	CyberQP QGuard Privileged Identity Management	IG2, IG3
5.6	Centralize Account Management	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation	IG2, IG3

6. Access Control Management

CIS Control Definition

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

CIS CONTROL 6 MAPPING TO CYBERQP:

CIS Control #	CIS Control Title:	CyberQP Solution:	CIS Implementation Group
6.1	Establish an Access Granting Process	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	IG1, IG2, IG3
6.2	Establish an Access Revoking Process	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	IG1, IG2, IG3
6.5	Require MFA for Administrative Access	CyberQP QGuard Just-in-Time Account Creation	IG1, IG2, IG3
6.8	Define and Maintain Role-Based Access Control	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	IG3

8. Audit Log Management

CIS Control Definition

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

CIS CONTROL 8 MAPPING TO CYBERQP:

CIS Control #	CIS Control Title:	CyberQP Solution:	CIS Implementation Group
8.2	Collect Audit Logs	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation	IG1, IG2, IG3
8.5	Collect Detailed Audit Logs	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation	IG2, IG3
8.10	Retain Audit Logs	CyberQP QGuard Privileged Identity Management CyberQP QDesk Helpdesk Automation	IG2, IG3

15. Service Provider Management

CIS Control Definition

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise’s critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

CIS CONTROL 15 MAPPING TO CYBERQP: _____

CIS Control #	CIS Control Title:	CyberQP Solution:	CIS Implementation Group
15.7	Securely Decommission Service Providers	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management	IG3

CyberQP redefines help desk security through privileged access management, help desk verification, and privilege elevation. Backed by SOC 2 Type 2 certification, we empower IT professionals to eliminate security risks, enforce compliance, and enhance operational efficiency. Our mission is simple: "Empowering Access, Redefining Privilege" for help desks across the globe.

Learn more at cyberqp.com/tours/

