CyberQP

CUSTOMER REFERENCE GUIDE

Comprehensive CMMC Shared Responsibility Matrix for Audit Preparation

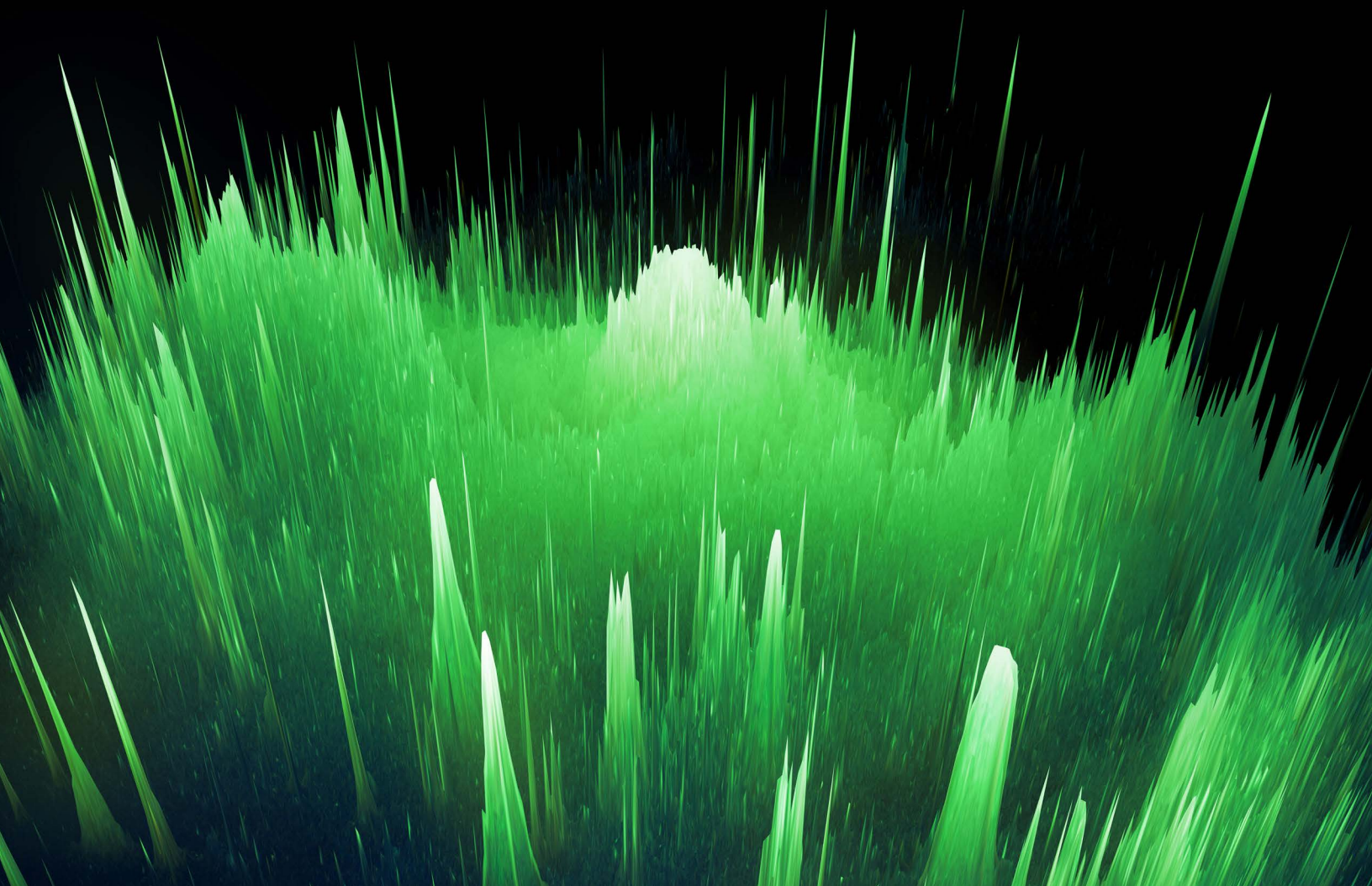

Table of Contents

CyberQP

Access Control

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.1.1[a]	3.1.1	AC.L1-3.1.1	Partial	CyberQP enforces RBAC; Customer manages IAM and provisioning.
3.1.1[b]	3.1.1	AC.L1-3.1.1	Partial	
3.1.1[c]	3.1.1	AC.L1-3.1.1	Partial	
3.1.1[d]	3.1.1	AC.L1-3.1.1	Partial	
3.1.1[e]	3.1.1	AC.L1-3.1.1	Partial	
3.1.1[f]	3.1.1	AC.L1-3.1.1	Partial	
3.1.2[a]	3.1.2	AC.L1-3.1.2	Partial	Privileged access inside CyberQP; Customer defines privilege policy.
3.1.2[b]	3.1.2	AC.L1-3.1.2	Partial	
3.1.3[a]	3.1.3	AC.L2-3.1.3	N/A	CyberQP controls access to its platform which does store CUI; Customer manages CUI access.
3.1.3[b]	3.1.3	AC.L2-3.1.3	N/A	
3.1.3[c]	3.1.3	AC.L2-3.1.3	N/A	
3.1.3[d]	3.1.3	AC.L2-3.1.3	N/A	
3.1.3[e]	3.1.3	AC.L2-3.1.3	N/A	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.1.4[a]	3.1.4	AC.L2-3.1.4	Partial	CyberQP platform enforces RBAC; Customer defines RBAC and configures enforcement in CyberQP tool.
3.1.4[b]	3.1.4	AC.L2-3.1.4	Partial	
3.1.4[c]	3.1.4	AC.L2-3.1.4	Partial	
3.1.5[a]	3.1.5	AC.L2-3.1.5	Partial	CyberQP authorizes platform access; Customer authorizes access to enterprise systems.
3.1.5[b]	3.1.5	AC.L2-3.1.5	Partial	
3.1.5[c]	3.1.5	AC.L2-3.1.5	Partial	
3.1.5[d]	3.1.5	AC.L2-3.1.5	Partial	
3.1.6[a]	3.1.6	AC.L2-3.1.6	Partial	CyberQP platform enforces least privilege; Customer defines and configures enforcement in CyberQP tool.
3.1.6[b]	3.1.6	AC.L2-3.1.6	Partial	
3.1.7[a]	3.1.7	AC.L2-3.1.7	Partial	CyberQP manages privileged access policies; Customer manages enterprise privileged accounts.
3.1.7[b]	3.1.7	AC.L2-3.1.7	Partial	
3.1.7[c]	3.1.7	AC.L2-3.1.7	Partial	
3.1.7[d]	3.1.7	AC.L2-3.1.7	Partial	
3.1.8[a]	3.1.8	AC.L2-3.1.8	Partial	CyberQP enforces login failure handling and lockouts through customer defined configura-tions; Customer defined all lockout periods and access configurations.
3.1.8[b]	3.1.8	AC.L2-3.1.8	Partial	
3.1.9[a]	3.1.9	AC.L2-3.1.9	N/A	Customer configures all CUI related notices
3.1.9[b]	3.1.9	AC.L2-3.1.9	N/A	
3.1.10[a]	3.1.10	AC.L2-3.1.10	Partial	CyberQP enforces session lock on it's platform, Customer defines session lock out times and configurations.
3.1.10[b]	3.1.10	AC.L2-3.1.10	Partial	
3.1.10[c]	3.1.10	AC.L2-3.1.10	Partial	

ACCESS CONTROL

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.1.11[a]	3.1.11	AC.L2-3.1.11	Partial	CyberQP controls remote privileged access into itself, Customer can define and enforces conditions in the tool.
3.1.11[b]	3.1.11	AC.L2-3.1.11	Partial	
3.1.12[a]	3.1.12	AC.L2-3.1.12	Partial	CyberQP monitors internal account activity; Customer monitors remote access to their infrastructure.
3.1.12[b]	3.1.12	AC.L2-3.1.12	Partial	
3.1.12[c]	3.1.12	AC.L2-3.1.12	Partial	
3.1.12[d]	3.1.12	AC.L2-3.1.12	Partial	
3.1.13[a]	3.1.13	AC.L2-3.1.13	N/A	CyberQP uses the Customer encryption settings to enforce remote session security; Session encryption is defined by the Customer
3.1.13[b]	3.1.13	AC.L2-3.1.13	N/A	
3.1.14[a]	3.1.14	AC.L2-3.1.14	N/A	Customer determines which remote access points are authorized
3.1.14[b]	3.1.14	AC.L2-3.1.14	N/A	
3.1.15[a]	3.1.15	AC.L2-3.1.15	N/A	Customer defines and configures remote execution commands.
3.1.15[b]	3.1.15	AC.L2-3.1.15	N/A	
3.1.15[c]	3.1.15	AC.L2-3.1.15	N/A	
3.1.15[d]	3.1.15	AC.L2-3.1.15	N/A	
3.1.16[a]	3.1.16	AC.L2-3.1.16	N/A	Customer enforces authorized wireless and mobile access.
3.1.16[b]	3.1.16	AC.L2-3.1.16	N/A	
3.1.17[a]	3.1.17	AC.L2-3.1.17	N/A	Customer enforces authorized wireless and mobile access.
3.1.17[b]	3.1.17	AC.L2-3.1.17	N/A	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.1.18[a]	3.1.18	AC.L2-3.1.18	N/A	Customer enforces authorized wireless and mobile access.
3.1.18[b]	3.1.18	AC.L2-3.1.18	N/A	
3.1.18[c]	3.1.18	AC.L2-3.1.18	N/A	
3.1.19[a]	3.1.19	AC.L2-3.1.19	N/A	Customer enforces authorized wireless and mobile access.
3.1.19[b]	3.1.19	AC.L2-3.1.19	N/A	
3.1.20[a]	3.1.20	AC.L1-3.1.20	Partial	CyberQP can enforce external system access if customer uses it as an IdP;Customer controls access to external systems.
3.1.20[b]	3.1.20	AC.L1-3.1.20	Partial	
3.1.20[c]	3.1.20	AC.L1-3.1.20	Partial	
3.1.20[d]	3.1.20	AC.L1-3.1.20	Partial	
3.1.20[e]	3.1.20	AC.L1-3.1.20	Partial	
3.1.20[f]	3.1.20	AC.L1-3.1.20	Partial	
3.1.21[a]	3.1.21	AC.L2-3.1.21	N/A	Customer enforces portable storage use
3.1.21[b]	3.1.21	AC.L2-3.1.21	N/A	
3.1.21[c]	3.1.21	AC.L2-3.1.21	N/A	
3.1.22[a]	3.1.22	AC.L1-3.1.22	N/A	Customer controls information flow and exposure
3.1.22[b]	3.1.22	AC.L1-3.1.22	N/A	
3.1.22[c]	3.1.22	AC.L1-3.1.22	N/A	
3.1.22[d]	3.1.22	AC.L1-3.1.22	N/A	
3.1.22[e]	3.1.22	AC.L1-3.1.22	N/A	

CyberQP

Awareness & Training

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.2.1[a]	3.2.1	AT.L2-3.2.1	N/A	Customer is responsible for formal security training in their organization
3.2.1[b]	3.2.1	AT.L2-3.2.1	N/A	
3.2.1[c]	3.2.1	AT.L2-3.2.1	N/A	
3.2.1[d]	3.2.1	AT.L2-3.2.1	N/A	
3.2.2[a]	3.2.2	AT.L2-3.2.2	N/A	Customer is responsible for formal security training in their organization
3.2.2[b]	3.2.2	AT.L2-3.2.2	N/A	
3.2.2[c]	3.2.2	AT.L2-3.2.2	N/A	
3.3.2[a]	3.3.2	AU.L2-3.3.2	Partial	CyberQP generates audit logs for authentications, privileged actions, and system activity; customer integrates logs into log aggregator.
3.3.2[b]	3.3.2	AU.L2-3.3.2	Partial	
3.2.3[a]	3.2.3	AT.L2-3.2.3	N/A	Customer is responsible for formal security training in their organization
3.2.3[b]	3.2.3	AT.L2-3.2.3	N/A	

CyberQP

Audit & Accountability

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.3.1[a]	3.3.1	AU.L2-3.3.1	Partial	CyberQP generates audit logs for authentications, privileged actions, and system activity; customer integrates logs into log aggregator.
3.3.1[b]	3.3.1	AU.L2-3.3.1	Partial	
3.3.1[c]	3.3.1	AU.L2-3.3.1	Partial	
3.3.1[d]	3.3.1	AU.L2-3.3.1	Partial	
3.3.1[e]	3.3.1	AU.L2-3.3.1	Partial	
3.3.1[f]	3.3.1	AU.L2-3.3.1	Partial	
3.3.2[a]	3.3.2	AU.L2-3.3.2	Partial	CyberQP generates audit logs for authentications, privileged actions, and system activity; customer integrates logs into log aggregator.
3.3.2[b]	3.3.2	AU.L2-3.3.2	Partial	
3.3.3[a]	3.3.3	AU.L2-3.3.3	N/A	Customer is responsible for formal security training in their organization
3.3.3[b]	3.3.3	AU.L2-3.3.3	N/A	
3.3.3[c]	3.3.3	AU.L2-3.3.3	N/A	
3.3.4[a]	3.3.4	AU.L2-3.3.4	Partial	CyberQP tools will alert on logging events; Customer performs alert reviews.
3.3.4[b]	3.3.4	AU.L2-3.3.4	Partial	
3.3.4[c]	3.3.4	AU.L2-3.3.4	Partial	
3.3.5[a]	3.3.5	AU.L2-3.3.5	N/A	Customer would perform log analysis in their aggregator
3.3.5[b]	3.3.5	AU.L2-3.3.5	N/A	
3.3.6[a]	3.3.6	AU.L2-3.3.6	Partial	CyberQP provides report generation; customer performs deeper analysis in their log aggregator.
3.3.6[b]	3.3.6	AU.L2-3.3.6	Partial	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.3.7[a]	3.3.7	AU.L2-3.3.7	N/A	CyberQP tools support NTP configurations; Customer configures NTP services.
3.3.7[b]	3.3.7	AU.L2-3.3.7	N/A	
3.3.7[c]	3.3.7	AU.L2-3.3.7	N/A	
3.3.8[a]	3.3.8	AU.L2-3.3.8	Partial	CyberQP tools timestamp their internal logs and activities; Customer ensures logs are reviewed and actions validated
3.3.8[b]	3.3.8	AU.L2-3.3.8	Partial	
3.3.8[c]	3.3.8	AU.L2-3.3.8	Partial	
3.3.8[d]	3.3.8	AU.L2-3.3.8	Partial	
3.3.8[e]	3.3.8	AU.L2-3.3.8	Partial	
3.3.8[f]	3.3.8	AU.L2-3.3.8	Partial	
3.3.9[a]	3.3.9	AU.L2-3.3.9	Partial	CyberQP tool supports RBAC and SOD; Customer configures who will have access to the logs.
3.3.9[b]	3.3.9	AU.L2-3.3.9	Partial	

CyberQP

Configuration Management

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.4.1[a]	3.4.1	CM.L2-3.4.1	N/A	CyberQP maintains baseline configurations for its SaaS platform; Customer maintains baselines for their systems.
3.4.1[b]	3.4.1	CM.L2-3.4.1	N/A	
3.4.1[c]	3.4.1	CM.L2-3.4.1	N/A	
3.4.1[d]	3.4.1	CM.L2-3.4.1	N/A	
3.4.1[e]	3.4.1	CM.L2-3.4.1	N/A	
3.4.1[f]	3.4.1	CM.L2-3.4.1	N/A	
3.4.2[a]	3.4.2	CM.L2-3.4.2	Partial	CyberQP tools will assist with policy validation on integrated systems; Customer is responsible for documenting system configurations.
3.4.2[b]	3.4.2	CM.L2-3.4.2	Partial	
3.4.3[a]	3.4.3	CM.L2-3.4.3	Partial	CyberQP log will track access related changes; customer controls all access changes and decisions
3.4.3[b]	3.4.3	CM.L2-3.4.3	Partial	
3.4.3[c]	3.4.3	CM.L2-3.4.3	Partial	
3.4.3[d]	3.4.3	CM.L2-3.4.3	Partial	
3.4.4	3.4.4	CM.L2-3.4.4	N/A	Customer enforces configuration change control on their infrastructure.
3.4.5[a]	3.4.5	CM.L2-3.4.5	N/A	CyberQP tool helps enforce access control; Customer manages all logical and physical change control processes and alerts
3.4.5[b]	3.4.5	CM.L2-3.4.5	N/A	
3.4.5[c]	3.4.5	CM.L2-3.4.5	N/A	
3.4.5[d]	3.4.5	CM.L2-3.4.5	N/A	
3.4.5[e]	3.4.5	CM.L2-3.4.5	N/A	
3.4.5[f]	3.4.5	CM.L2-3.4.5	N/A	
3.4.5[g]	3.4.5	CM.L2-3.4.5	N/A	
3.4.5[h]	3.4.5	CM.L2-3.4.5	N/A	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.4.6[a]	3.4.6	CM.L2-3.4.6	N/A	CyberQP tool helps enforce access control; Customer manages all logical and physical change control processes and alerts
3.4.6[b]	3.4.6	CM.L2-3.4.6	N/A	
3.4.7[a]	3.4.7	CM.L2-3.4.7	N/A	Customer is responsible for system integrity verification for their endpoints and servers.
3.4.7[b]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[c]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[d]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[e]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[f]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[g]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[h]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[i]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[j]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[k]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[l]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[m]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[n]	3.4.7	CM.L2-3.4.7	N/A	
3.4.7[o]	3.4.7	CM.L2-3.4.7	N/A	
3.4.8[a]	3.4.8	CM.L2-3.4.8	N/A	CyberQP tools support enforcement of allow/ blocking of access; Customer defines all allow/ blocking policies
3.4.8[b]	3.4.8	CM.L2-3.4.8	N/A	
3.4.8[c]	3.4.8	CM.L2-3.4.8	N/A	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.4.9[a]	3.4.9	CM.L2-3.4.9	Partial	CyberQP tools can enforce application installation policies; Customer applies software installation policies on their systems.
3.4.9[b]	3.4.9	CM.L2-3.4.9	Partial	
3.4.9[c]	3.4.9	CM.L2-3.4.9	Partial	

CyberQP

Identification & Authentication

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.5.1[a]	3.5.1	IA.L1-3.5.1	Partial	CyberQP provides account identification; Customer enforces RBAC and SoD configurations in enterprise systems.
3.5.1[b]	3.5.1	IA.L1-3.5.1	Partial	
3.5.1[c]	3.5.1	IA.L1-3.5.1	Partial	
3.5.2[a]	3.5.2	IA.L1-3.5.2	Partial	CyberQP enforces authentication measures set by the customer; Customer implements authentication requirements for internal systems and endpoints.
3.5.2[b]	3.5.2	IA.L1-3.5.2	Partial	
3.5.2[c]	3.5.2	IA.L1-3.5.2	Partial	
3.5.3[a]	3.5.3	IA.L2-3.5.3	Partial	CyberQP enforces authentication measures set by the customer; Customer implements authentication requirements for internal systems and endpoints.
3.5.3[b]	3.5.3	IA.L2-3.5.3	Partial	
3.5.3[c]	3.5.3	IA.L2-3.5.3	Partial	
3.5.3[d]	3.5.3	IA.L2-3.5.3	Partial	
3.5.4	3.5.4	IA.L2-3.5.4	Partial	CyberQP enforces replay resistant MFA as defined by the customer; Customer enforces replay resistant authentication enterprise-wide.
3.5.5[a]	3.5.5	IA.L2-3.5.5	Partial	CyberQP tool enforces the access policies and configurations; Customer configuration and policies set the rules for identifier reuse.
3.5.5[b]	3.5.5	IA.L2-3.5.5	Partial	
3.5.6[a]	3.5.6	IA.L2-3.5.6	Partial	CyberQP tool enforces the access policies and configurations; Customer configuration and policies set the rules for account timeouts.
3.5.6[b]	3.5.6	IA.L2-3.5.6	Partial	
3.5.7[a]	3.5.7	IA.L2-3.5.7	Partial	CyberQP tool enforces the access policies and configurations; Customer configuration and policies set the rules for password complexity.
3.5.7[b]	3.5.7	IA.L2-3.5.7	Partial	
3.5.7[c]	3.5.7	IA.L2-3.5.7	Partial	
3.5.7[d]	3.5.7	IA.L2-3.5.7	Partial	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.5.8[a]	3.5.8	IA.L2-3.5.8	Partial	CyberQP tool enforces the access policies and configurations; Customer configuration and policies set the rules for password reuse.
3.5.8[b]	3.5.8	IA.L2-3.5.8	Partial	
3.5.9	3.5.9	IA.L2-3.5.9	Partial	CyberQP tool enforces the access policies and configurations; Customer configuration and policies set the rules for temporary password use and reset.
3.5.10[a]	3.5.10	IA.L2-3.5.10	Partial	CyberQP has full encryption for all passwords stored or in transmission; Customer enforces password encryption on their enterprise systems
3.5.10[b]	3.5.10	IA.L2-3.5.10	Partial	
3.5.11	3.5.11	IA.L2-3.5.11	Partial	CyberQP enforces session integrity and authentication obfuscation on its tool.; Customer enforces password obfuscation on their enterprise systems

CyberQP

Incident Response

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.6.1[1]	3.6.1	IR.L2-3.6.1	N/A	CyberQP provides logs and identity/privileged activity data used during incident response; customer executes IR program and integrates logs into their aggregator
3.6.1[b]	3.6.1	IR.L2-3.6.1	N/A	
3.6.1[c]	3.6.1	IR.L2-3.6.1	N/A	
3.6.1[d]	3.6.1	IR.L2-3.6.1	N/A	
3.6.1[e]	3.6.1	IR.L2-3.6.1	N/A	
3.6.1[f]	3.6.1	IR.L2-3.6.1	N/A	
3.6.1[g]	3.6.1	IR.L2-3.6.1	N/A	
3.6.2[a]	3.6.2	IR.L2-3.6.2	N/A	CyberQP provides logs and identity/privileged activity data used during incident response; customer executes IR program and integrates logs into their aggregator
3.6.2[b]	3.6.2	IR.L2-3.6.2	N/A	
3.6.2[c]	3.6.2	IR.L2-3.6.2	N/A	
3.6.2[d]	3.6.2	IR.L2-3.6.2	N/A	
3.6.2[e]	3.6.2	IR.L2-3.6.2	N/A	
3.6.2[f]	3.6.2	IR.L2-3.6.2	N/A	
3.6.3	3.6.3	IR.L2-3.6.3	N/A	Customer reports incidents, tests IT capabilities, manages escalation, and handles communications.

CyberQP

Maintenance

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.7.1	3.7.1	MA.L2-3.7.1	N/A	Customer manages system maintenance activities on internal systems.
3.7.2[a]	3.7.2	MA.L2-3.7.2	N/A	Customer ensures remote maintenance tools are authorized and secure.
3.7.2[b]	3.7.2	MA.L2-3.7.2	N/A	
3.7.2[c]	3.7.2	MA.L2-3.7.2	N/A	
3.7.2[d]	3.7.2	MA.L2-3.7.2	N/A	
3.7.3	3.7.3	MA.L2-3.7.3	N/A	Customer controls equipment removal and CUI sanitization.
3.7.4	3.7.4	MA.L2-3.7.4	N/A	Customer sanitizes or secures information system components prior to maintenance.
3.7.5[a]	3.7.5	MA.L2-3.7.5	Partial	CyberQP tools help enforce access controls from external networks; Customer configures and sets policies for access.
3.7.5[b]	3.7.5	MA.L2-3.7.5	Partial	
3.7.6	3.7.6	MA.L2-3.7.6	N/A	Customer inspects equipment after maintenance to ensure no tampering occurred.

CyberQP

Media Protection

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.8.1[a]	3.8.1	MP.L2-3.8.1	N/A	Media protection is customer-owned.; CyberQP does not have access to any CUI.
3.8.1[b]	3.8.1	MP.L2-3.8.1	N/A	
3.8.1[c]	3.8.1	MP.L2-3.8.1	N/A	
3.8.1[d]	3.8.1	MP.L2-3.8.1	N/A	
3.8.2	3.8.2	MP.L2-3.8.2	N/A	Media access is controlled by the customer.
3.8.3[a]	3.8.3	MP.L1-3.8.3	N/A	CyberQP does not manage physical media labeling.
3.8.3[b]	3.8.3	MP.L1-3.8.3	N/A	
3.8.4[a]	3.8.4	MP.L2-3.8.4	N/A	Customers handle their own media sanitization.
3.8.4[b]	3.8.4	MP.L2-3.8.4	N/A	
3.8.5[a]	3.8.5	MP.L2-3.8.5	N/A	Customer determines media marking requirements.
3.8.5[b]	3.8.5	MP.L2-3.8.5	N/A	
3.8.6	3.8.6	MP.L2-3.8.6	N/A	Customer is responsible for controlling media transport within and outside facilities.
3.8.7	3.8.7	MP.L2-3.8.7	N/A	Customer ensures use of secured media storage.
3.8.8	3.8.8	MP.L2-3.8.8	N/A	Customer implements access restrictions to media.
3.8.9	3.8.9	MP.L2-3.8.9	N/A	Customer defines media protection roles and controls.

CyberQP

Personnel Security

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.9.1	3.9.1	PS.L2-3.9.1	N/A	Customer performs personnel screening and suitability determinations.
3.9.2[a]	3.9.2	PS.L2-3.9.2	N/A	Customer ensures personnel adhere to security policies and agreements.
3.9.2[b]	3.9.2	PS.L2-3.9.2	N/A	
3.9.2[c]	3.9.2	PS.L2-3.9.2	N/A	

CyberQP

Physical Protection

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.10.1[a]	3.10.1	PE.L1-3.10.1	N/A	Customer controls physical facility access.
3.10.1[b]	3.10.1	PE.L1-3.10.1	N/A	
3.10.1[c]	3.10.1	PE.L1-3.10.1	N/A	
3.10.1[d]	3.10.1	PE.L1-3.10.1	N/A	
3.10.2[a]	3.10.2	PE.L2-3.10.2	N/A	Customer controls physical access to systems, wiring closets, and hardware.
3.10.2[b]	3.10.2	PE.L2-3.10.2	N/A	
3.10.2[c]	3.10.2	PE.L2-3.10.2	N/A	
3.10.2[d]	3.10.2	PE.L2-3.10.2	N/A	
3.10.4	3.10.4	PE.L1-3.10.4	N/A	Customer maintains monitoring of physical access to sensitive areas.
3.10.5[a]	3.10.5	PE.L1-3.10.5	N/A	Customer enforces access control for physical entry.
3.10.5[b]	3.10.5	PE.L1-3.10.5	N/A	
3.10.5[c]	3.10.5	PE.L1-3.10.5	N/A	
3.10.6[a]	3.10.6	PE.L2-3.10.6	N/A	Environmental and emergency controls (HVAC, fire, UPS) are customer managed; CyberQP environments are managed by our CSP.
3.10.6[b]	3.10.6	PE.L2-3.10.6	N/A	

CyberQP

Risk Assessment

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.11.1[a]	3.11.1	RA.L2-3.11.1	N/A	Customer performs formal risk assessments.
3.11.1[b]	3.11.1	RA.L2-3.11.1	N/A	
3.11.2[a]	3.11.2	RA.L2-3.11.2	N/A	Customer controls physical access to systems, wiring closets, and hardware.
3.11.2[b]	3.11.2	RA.L2-3.11.2	N/A	
3.11.2[c]	3.11.2	RA.L2-3.11.2	N/A	
3.11.2[d]	3.11.2	RA.L2-3.11.2	N/A	
3.11.2[e]	3.11.2	RA.L2-3.11.2	N/A	
3.11.3[a]	3.11.3	RA.L2-3.11.3	Partial	CyberQP manages and remediates any vulnerabilities on their tool; Customer manages vulnerabilities on their enterprise assets.
3.11.3[b]	3.11.3	RA.L2-3.11.3	Partial	

CyberQP

Security Assessment

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.12.1[a]	3.12.1	CA.L2-3.12.1	N/A	Customer maintains the system security plan (SSP) and describes how CyberQP is used.
3.12.1[b]	3.12.1	CA.L2-3.12.1	N/A	
3.12.2[a]	3.12.2	CA.L2-3.12.2	Partial	
3.12.2[b]	3.12.2	CA.L2-3.12.2	Partial	
3.12.2[c]	3.12.2	CA.L2-3.12.2	Partial	
3.12.3	3.12.3	CA.L2-3.12.3	N/A	
3.12.3	3.12.3	CA.L2-3.12.3	N/A	Customer must continuously monitor and assess security controls across their enterprise. Security plans are developed by the customer.
3.12.4[a]	3.12.4	CA.L2-3.12.4	N/A	Customer must continuously monitor and assess security controls across their enterprise. Security plans are developed by the customer.
3.12.4[b]	3.12.4	CA.L2-3.12.4	N/A	
3.12.4[c]	3.12.4	CA.L2-3.12.4	N/A	
3.12.4[d]	3.12.4	CA.L2-3.12.4	N/A	
3.12.4[e]	3.12.4	CA.L2-3.12.4	N/A	
3.12.4[f]	3.12.4	CA.L2-3.12.4	N/A	
3.12.4[g]	3.12.4	CA.L2-3.12.4	N/A	
3.12.4.[h]	3.12.4	CA.L2-3.12.4	N/A	

CyberQP

System & Communications Assessment

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.13.1[a]	3.13.1	SC.L1-3.13.1	N/A	Customer controls all information encryption. CyberQP does not touch any CUI in it's systems.
3.13.1[b]	3.13.1	SC.L1-3.13.1	N/A	
3.13.1[c]	3.13.1	SC.L1-3.13.1	N/A	
3.13.1[d]	3.13.1	SC.L1-3.13.1	N/A	
3.13.1[e]	3.13.1	SC.L1-3.13.1	N/A	
3.13.1[f]	3.13.1	SC.L1-3.13.1	N/A	
3.13.1[g]	3.13.1	SC.L1-3.13.1	N/A	
3.13.1[h]	3.13.1	SC.L1-3.13.1	N/A	
3.13.2[a]	3.13.2	SC.L2-3.13.2	N/A	Customer holds all diagrams and configurations for its systems.
3.13.2[b]	3.13.2	SC.L2-3.13.2	N/A	
3.13.2[c]	3.13.2	SC.L2-3.13.2	N/A	
3.13.2[d]	3.13.2	SC.L2-3.13.2	N/A	
3.13.2[e]	3.13.2	SC.L2-3.13.2	N/A	
3.13.2[f]	3.13.2	SC.L2-3.13.2	N/A	
3.13.3[a]	3.13.3	SC.L2-3.13.3	N/A	Customer controls configurations for user and system management. CyberQP enforces those configurations
3.13.3[b]	3.13.3	SC.L2-3.13.3	N/A	
3.13.3[c]	3.13.3	SC.L2-3.13.3	N/A	
3.13.2[d]	3.13.2	SC.L2-3.13.2	N/A	
3.13.2[e]	3.13.2	SC.L2-3.13.2	N/A	
3.13.2[f]	3.13.2	SC.L2-3.13.2	N/A	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.13.4	3.13.4	SC.L2-3.13.4	N/A	Customer controls all of their information's shares and access.
3.13.5[a]	3.13.5	SC.L1-3.13.5	N/A	Customer manages and configures all network segmentations
3.13.5[b]	3.13.5	SC.L1-3.13.5	N/A	
3.13.6[a]	3.13.6	SC.L2-3.13.6	N/A	Customer manages all network traffic and configurations for their organization.
3.13.6[b]	3.13.6	SC.L2-3.13.6	N/A	
3.13.7	3.13.7	SC.L2-3.13.7	N/A	Customer manages all network traffic and configurations for their organization.
3.13.8[a]	3.13.8	SC.L2-3.13.8	N/A	Customer controls all information encryption. CyberQP does not touch any CUI in it's systems.
3.13.8[b]	3.13.8	SC.L2-3.13.8	N/A	
3.13.8[c]	3.13.8	SC.L2-3.13.8	N/A	
3.13.9[a]	3.13.9	SC.L2-3.13.9	N/A	Customer configures all session timeouts; CyberQP tools can enforce the configurations.
3.13.9[b]	3.13.9	SC.L2-3.13.9	N/A	
3.13.9[c]	3.13.9	SC.L2-3.13.9	N/A	
3.13.10[a]	3.13.10	SC.L2-3.13.10	Partial	CyberQP leverages a hardware security module (HSM) to generate, store, and manage cryptographic keys; Customer manages all keys for their organization.
3.13.10[b]	3.13.10	SC.L2-3.13.10	Partial	
3.13.11	3.13.11	SC.L2-3.13.11	N/A	Customer controls all information encryption. CyberQP does not touch any CUI in it's systems.
3.13.11	3.13.11	SC.L2-3.13.11	N/A	Customer controls all information encryption. CyberQP does not touch any CUI in it's systems.
3.13.9[b]	3.13.9	SC.L2-3.13.9	N/A	
3.13.9[c]	3.13.9	SC.L2-3.13.9	N/A	

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.13.12[a]	3.13.12	SC.L2-3.13.12	N/A	Customer manages device level access controls configurations.
3.13.12[b]	3.13.12	SC.L2-3.13.12	N/A	
3.13.12[c]	3.13.12	SC.L2-3.13.12	N/A	
3.13.13[a]	3.13.13	SC.L2-3.13.13	N/A	Customer controls the use of mobile code in their organization.
3.13.13[b]	3.13.13	SC.L2-3.13.13	N/A	
3.13.14[a]	3.13.14	SC.L2-3.13.14	N/A	Customer controls all VOIP configurations in their organization.
3.13.14[b]	3.13.14	SC.L2-3.13.14	N/A	
3.13.15	3.13.15	SC.L2-3.13.15	N/A	Customer manages all network traffic and configurations for their organization.
3.13.16	3.13.16	SC.L2-3.13.16	N/A	Customer controls all information encryption. CyberQP does not touch any CUI in it's systems.

CyberQP

System & Information Integrity

AO Label	NIST800-171 Requirement	CMMC Practice	CyberQP Responsibility	Notes
3.14.1[a]	3.14.1	SI.L1-3.14.1	N/A	Customer identifies and manages all systems, flaws and remediations on their assets; CyberQP has a process which covers this for their platform.
3.14.1[b]	3.14.1	SI.L1-3.14.1	N/A	
3.14.1[c]	3.14.1	SI.L1-3.14.1	N/A	
3.14.1[d]	3.14.1	SI.L1-3.14.1	N/A	
3.14.1[e]	3.14.1	SI.L1-3.14.1	N/A	
3.14.1[f]	3.14.1	SI.L1-3.14.1	N/A	
3.14.2[a]	3.14.2	SI.L1-3.14.2	N/A	Customer handles alerts around malicious code for its assets.
3.14.2[b]	3.14.2	SI.L1-3.14.2	N/A	
3.14.3[a]	3.14.3	SI.L2-3.14.3	Partial	Customer deploys updates, patches, and AV signatures on their systems; CyberQP handles its own platform updates.
3.14.3[b]	3.14.3	SI.L2-3.14.3	Partial	
3.14.3[c]	3.14.3	SI.L2-3.14.3	Partial	
3.14.4	3.14.4	SI.L1-3.14.4	N/A	Customer handles alerts and updates around malicious code protection for its assets.
3.14.5[a]	3.14.5	SI.L1-3.14.5	N/A	Customer configures protections to prevent unauthorized use of systems and external file downloads
3.14.5[b]	3.14.5	SI.L1-3.14.5	N/A	
3.14.5[c]	3.14.5	SI.L1-3.14.5	N/A	
3.14.6[a]	3.14.6	SI.L2-3.14.6	Partial	CyberQP logs events around account use/ access; Customer monitors enterprise logs for threat indicators.
3.14.6[b]	3.14.6	SI.L2-3.14.6	Partial	
3.14.6[c]	3.14.6	SI.L2-3.14.6	Partial	
3.14.7[a]	3.14.7	SI.L2-3.14.7	Partial	CyberQP logs events around account use/ access; Customer monitors enterprise logs for threat indicators.
3.14.7[b]	3.14.7	SI.L2-3.14.7	Partial	