CyberQP

# CMMC Access Control Checklist

## As threat actors continue to target privileged accounts to obtain initial access and launch major data breaches, regulators and lawmakers are taking notice.

As help desks continue to prepare for the implementation and enforcement of the Cybersecurity Maturity Model Certification (CMMC) framework, here are steps they can take to align with the best practices to secure your admin accounts and end user identities, and the Access Controls you can align to with CyberQP.

## Relevant CMMC Access Control

**AC.L1-3.1.4** Limit Information System Access to the Types of Transactions and Functions That Authorized Users Are Permitted to Execute

**AC.L2-3.1.5** Limit the Use of Privileged Accounts to Perform Authorized Functions

**AC.L2-3.1.7** Prevent Non-Privileged Users from Executing Privileged Functions and Capture the Execution of Such Functions in Audit Logs

**AC.L2-3.1.6** Employ the Principle of Least Privilege, Including for Specific Security Functions and Privileged Accounts

**AC.L3-3.1.8** Limit Information System Access to Authorized Users, Processes Acting on Behalf of Authorized Users, or Devices (Including Other Information Systems)

## Questions to Ask

- ✔ Are you removing admin access from your end users?
- ✔ Are you implementing Just-in-Time administrator access to ensure that technicians are only taking actions they're authorized to?
- ✔ Are you implementing the Principle of Least Privilege across your help desk and your customer base?
- ✔ Do you have visibility into the users, processes, and devices that have privileged access across your environment?