CYBER READINESS REPORT

# Bayside Precision Parts (fictional sample)

CMMC Level 2 readiness, Q4 2026 · NIST SP 800-171 Rev 2 (CMMC Level 1 and 2)

Generated Oct 20, 2026 · Assessment started Oct 1, 2026

PolicyScore

## SUMMARY

READINESS
**90%**
Optimizing
Based on all 110 questions

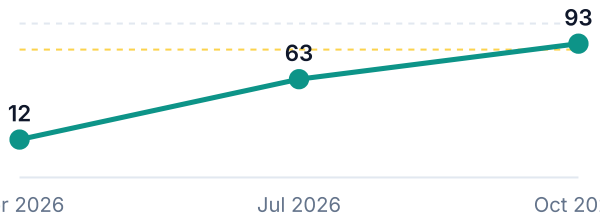
QUESTIONS ANSWERED
**110** / 110
15 gaps (No or Partial)

SPRS SCORE (SELF-ASSESSED)
**93** / 110
All requirements answered

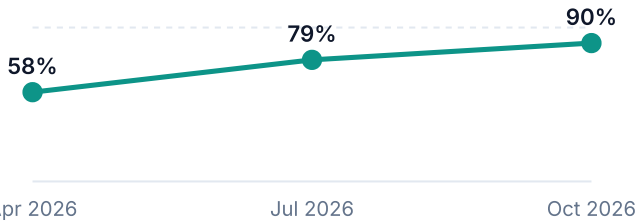
CMMC Level 1: **Met** · CMMC Level 2: **Not met** · Conditional Level 2: **Eligible**

## PROGRESS OVER TIME

SPRS SCORE




READINESS




Since Apr 2026: readiness 58% → 90%, SPRS 12 → 93, gaps 41 → 15.

Each point is one assessment. Hollow points were not fully answered; their scores are provisional. The dashed amber line is the 88-point minimum for Conditional Level 2.

## MUST DO NOW: PRIORITIZED ACTIONS

### Fix this week (1)

| ACTION | EFFORT | COST | QUESTION |
|---|---|---|---|
| Keep at least one backup copy that ransomware cannot reach (offline or immutable) partly in place | Days | Moderate ($1,000 to $10,000 a year) | 3.8.9 |

### Plan for later (14)

| ACTION | EFFORT | COST | QUESTION |
|---|---|---|---|
| Run a tabletop exercise of your incident response plan | Days | Usually no added cost | 3.6.3 |
| Encrypt laptops, phones and stored sensitive data partly in place | Days | Usually no added cost | 3.13.11 |
| Audit Failure Alerting | — | — | 3.3.4 |
| Log Reduction and Reporting | — | — | 3.3.6 |
| Media Marking | — | — | 3.8.4 |
| Mobile Code Control | — | — | 3.13.13 |
| Security Impact Analysis | — | — | 3.4.4 |
| Session Termination | — | — | 3.1.11 |
| Insider Threat Awareness partly in place | — | — | 3.2.3 |
| Log Review and Update partly in place | — | — | 3.3.3 |
| Media Accountability partly in place | — | — | 3.8.5 |
| Portable Storage Limits partly in place | — | — | 3.1.21 |
| Replay-Resistant Authentication partly in place | — | — | 3.5.4 |
| Session Lock partly in place | — | — | 3.1.10 |

Ranked by how commonly each gap is linked to ransomware, email compromise and payment fraud at smaller companies. Effort and cost are rough estimates for a company of 20 to 250 people and depend on your systems and providers.

## REMEDIATION PLAN

15 open tasks, 3 done. Tasks are tracked by Bayside Precision Parts (fictional sample) in PolicyScore.

| REQUIREMENT | OWNER | DUE | STATUS |
|---|---|---|---|
| `3.1.10` Session Lock | Dana Lee (IT Manager) | Nov 15, 2026 | In progress |
| `3.1.11` Session Termination | Dana Lee (IT Manager) | Nov 15, 2026 | To do |
| `3.1.21` Portable Storage Limits | Dana Lee (IT Manager) | Dec 1, 2026 | To do |
| `3.3.1` Audit Log Creation | Sam Patel (MSP) | Sep 15, 2026 | Done |
| `3.3.3` Log Review and Update | Dana Lee (IT Manager) | Oct 15, 2026 (overdue) | To do |
| `3.3.4` Audit Failure Alerting | Sam Patel (MSP) | Nov 30, 2026 | In progress |
| `3.3.6` Log Reduction and Reporting | Sam Patel (MSP) | Dec 15, 2026 | To do |
| `3.2.3` Insider Threat Awareness | Alex Kim (HR) | Nov 20, 2026 | In progress |
| `3.4.4` Security Impact Analysis | Dana Lee (IT Manager) | Jan 31, 2027 | To do |
| `3.5.3` Multi-Factor Authentication | Sam Patel (MSP) | Aug 31, 2026 | Done |
| `3.5.4` Replay-Resistant Authentication | Sam Patel (MSP) | Jan 31, 2027 | To do |
| `3.6.3` Incident Response Testing | Dana Lee (IT Manager) | Dec 31, 2026 | To do |
| `3.8.4` Media Marking | Jordan Rivera (Operations) | Dec 15, 2026 | To do |
| `3.8.5` Media Accountability | Jordan Rivera (Operations) | Dec 15, 2026 | To do |
| `3.8.9` Backup Media Protection | Sam Patel (MSP) | Oct 31, 2026 | To do |
| `3.12.4` System Security Plan | Dana Lee (IT Manager) | Jul 31, 2026 | Done |
| `3.13.11` FIPS-Validated Cryptography | Sam Patel (MSP) | Jan 15, 2027 | In progress |
| `3.13.13` Mobile Code Control | Sam Patel (MSP) | Feb 28, 2027 | To do |

## RESULTS BY DOMAIN

| DOMAIN | ANSWERED | GAPS | SCORE |
|---|---|---|---|
| AC Access Control | 22 / 22 | 3 | 91% |
| AU Audit & Accountability | 9 / 9 | 3 | 72% |
| AT Awareness & Training | 3 / 3 | 1 | 83% |
| CM Configuration Management | 9 / 9 | 1 | 89% |
| IA Identification & Authentication | 11 / 11 | 1 | 95% |
| IR Incident Response | 3 / 3 | 1 | 67% |
| MA Maintenance | 6 / 6 | 0 | 100% |
| MP Media Protection | 9 / 9 | 3 | 78% |
| PS Personnel Security | 2 / 2 | 0 | 100% |
| PE Physical Protection | 6 / 6 | 0 | 100% |
| RA Risk Assessment | 3 / 3 | 0 | 100% |
| CA Security Assessment | 4 / 4 | 0 | 100% |
| SC System & Communications Protection | 16 / 16 | 2 | 90% |
| SI System & Information Integrity | 7 / 7 | 0 | 100% |

## ANSWERS

### AC · Access Control

| | | | |
|---|---|---|---|
| 3.1.1 | Authorized Access Control | 1 evidence | In place |
| 3.1.2 | Transaction and Function Access | 1 evidence | In place |
| 3.1.20 | External System Connections | | In place |
| 3.1.22 | Public-Facing System Controls | | In place |
| 3.1.3 | Controlled Information Flow | | In place |
| 3.1.4 | Separation of Duties | | In place |
| 3.1.5 | Least Privilege | 1 evidence | In place |
| 3.1.6 | Non-Privileged Account Use | 1 evidence | In place |
| 3.1.7 | Privilege Function Restriction | 1 evidence | In place |
| 3.1.8 | Unsuccessful Login Attempts | 1 evidence | In place |
| 3.1.9 | Privacy and Security Notices | | In place |
| 3.1.10 | Session Lock | | Partially in place |
| 3.1.11 | Session Termination | | Not in place |
| 3.1.12 | Remote Access Monitoring | | In place |
| 3.1.13 | Remote Access Encryption | | In place |
| 3.1.14 | Managed Remote Access Points | | In place |
| 3.1.15 | Remote Privileged Commands | | In place |
| 3.1.16 | Wireless Access Authorization | | In place |
| 3.1.17 | Wireless Access Protection | | In place |
| 3.1.18 | Mobile Device Control | | In place |
| 3.1.19 | Encryption of CUI on Mobile Devices | | In place |
| 3.1.21 | Portable Storage Limits | | Partially in place |

### AU · Audit & Accountability

| | | | |
|---|---|---|---|
| 3.3.1 | Audit Log Creation | 1 evidence | In place |
| 3.3.2 | User Action Traceability | 1 evidence | In place |
| 3.3.3 | Log Review and Update | | Partially in place |
| 3.3.4 | Audit Failure Alerting | | Not in place |
| 3.3.5 | Log Analysis and Correlation | 1 evidence | In place |
| 3.3.6 | Log Reduction and Reporting | | Not in place |
| 3.3.7 | Time Synchronization | | In place |
| 3.3.8 | Audit Log Protection | 1 evidence | In place |
| 3.3.9 | Log Management Access Control | | In place |

### AT · Awareness & Training

| | | | |
|---|---|---|---|
| 3.2.1 | Security Awareness | 1 evidence | In place |
| 3.2.2 | Role-Based Security Training | 1 evidence | In place |
| 3.2.3 | Insider Threat Awareness | | Partially in place |

### CM · Configuration Management

| | | | |
|---|---|---|---|
| 3.4.1 | Baseline Configuration | 1 evidence | In place |
| 3.4.2 | Security Configuration Enforcement | 1 evidence | In place |
| 3.4.3 | Change Management | | In place |
| 3.4.4 | Security Impact Analysis | | Not in place |
| 3.4.5 | Access Restrictions for Change | | In place |
| 3.4.6 | Least Functionality | 1 evidence | In place |
| 3.4.7 | Nonessential Functionality Restriction | 1 evidence | In place |
| 3.4.8 | Application Deny-by-Exception | | In place |
| 3.4.9 | User-Installed Software Control | | In place |

### IA · Identification & Authentication

| | | | |
|---|---|---|---|
| 3.5.1 | User and Device Identification | 1 evidence | In place |
| 3.5.2 | User Authentication | 1 evidence | In place |
| 3.5.3 | Multi-Factor Authentication | 1 evidence | In place |
| 3.5.4 | Replay-Resistant Authentication | | Partially in place |
| 3.5.5 | Non-Organizational User Authentication | | In place |
| 3.5.6 | Authenticator Management | | In place |
| 3.5.7 | Password Complexity | 1 evidence | In place |
| 3.5.8 | Password Reuse Prevention | 1 evidence | In place |
| 3.5.9 | Temporary Passwords | | In place |
| 3.5.10 | Cryptographic Password Protection | | In place |
| 3.5.11 | Obscured Authentication Feedback | | In place |

### IR · Incident Response

| | | | |
|---|---|---|---|
| 3.6.1 | Incident Handling Capability | 1 evidence | In place |
| 3.6.2 | Incident Tracking and Reporting | 1 evidence | In place |
| 3.6.3 | Incident Response Testing | | Not in place |

### MA · Maintenance

| | | | |
|---|---|---|---|
| 3.7.1 | System Maintenance | | In place |
| 3.7.2 | Maintenance Tool Controls | | In place |
| 3.7.3 | Equipment Sanitization | 1 evidence | In place |
| 3.7.4 | Media Check During Maintenance | | In place |
| 3.7.5 | Remote Maintenance MFA | | In place |
| 3.7.6 | Maintenance Supervision | | In place |

### MP · Media Protection

| | | | |
|---|---|---|---|
| 3.8.3 | Media Sanitization | 1 evidence | In place |
| 3.8.1 | Media Protection | | In place |
| 3.8.2 | Media Access Control | | In place |
| 3.8.4 | Media Marking | | Not in place |
| 3.8.5 | Media Accountability | | Partially in place |
| 3.8.6 | Portable Storage Encryption | 1 evidence | In place |
| 3.8.7 | Removable Media Use Control | | In place |
| 3.8.8 | Identifiable Portable Storage | | In place |
| 3.8.9 | Backup Media Protection | | Partially in place |

### PS · Personnel Security

| | | | |
|---|---|---|---|
| 3.9.1 | Personnel Screening | 1 evidence | In place |
| 3.9.2 | Personnel Termination/Transfer | 1 evidence | In place |

### PE · Physical Protection

| | | | |
|---|---|---|---|
| 3.10.1 | Physical Access Limitation | 1 evidence | In place |
| 3.10.3 | Visitor Escort | 1 evidence | In place |
| 3.10.4 | Physical Access Logs | 1 evidence | In place |
| 3.10.5 | Physical Access Device Management | 1 evidence | In place |
| 3.10.2 | Physical Facility Monitoring | 1 evidence | In place |
| 3.10.6 | Alternate Work Site Controls | | In place |

### RA · Risk Assessment

| | | | |
|---|---|---|---|
| 3.11.1 | Risk Assessment | 1 evidence | In place |
| 3.11.2 | Vulnerability Scanning | 1 evidence | In place |
| 3.11.3 | Vulnerability Remediation | 1 evidence | In place |

### CA · Security Assessment

| | | | |
|---|---|---|---|
| 3.12.1 | Security Control Assessment | 1 evidence | In place |
| 3.12.2 | Plan of Action | 1 evidence | In place |
| 3.12.3 | Continuous Monitoring | 1 evidence | In place |
| 3.12.4 | System Security Plan | 1 evidence | In place |

### SC · System & Communications Protection

| | | | |
|---|---|---|---|
| 3.13.1 | Boundary Protection | 1 evidence | In place |
| 3.13.5 | Public-Facing System Segmentation | 1 evidence | In place |
| 3.13.2 | Security Engineering Principles | | In place |
| 3.13.3 | Separation of User and Admin Functionality | | In place |
| 3.13.4 | Shared Resource Information Control | | In place |
| 3.13.6 | Network Communication Deny-by-Default | 1 evidence | In place |
| 3.13.7 | Split Tunneling Prevention | | In place |
| 3.13.8 | Transmission Encryption | | In place |
| 3.13.9 | Network Connection Termination | | In place |
| 3.13.10 | Cryptographic Key Management | | In place |
| 3.13.11 | FIPS-Validated Cryptography | 1 evidence | Partially in place |
| 3.13.12 | Collaborative Device Control | | In place |
| 3.13.13 | Mobile Code Control | | Not in place |
| 3.13.14 | VoIP Controls | | Not applicable |
| 3.13.15 | Communication Session Authenticity | | In place |
| 3.13.16 | Data at Rest Protection | 1 evidence | In place |

### SI · System & Information Integrity

| | | | |
|---|---|---|---|
| 3.14.1 | Flaw Remediation | | In place |
| 3.14.2 | Malicious Code Protection | 1 evidence | In place |
| 3.14.4 | Malware Protection Updates | 1 evidence | In place |
| 3.14.5 | System Scanning | 1 evidence | In place |
| 3.14.3 | Security Alert Monitoring | | In place |
| 3.14.6 | Attack Detection | | In place |
| 3.14.7 | Unauthorized System Use Detection | | In place |

## EVIDENCE INDEX

Documents are held in the organization's PolicyScore evidence vault and are available on request.

| DOCUMENT | TYPE | SUPPORTS | ADDED |
|---|---|---|---|
| System Security Plan v2.1<br>SSP-v2.1.pdf | System Security Plan | 3.12.4, 3.12.1, 3.12.2, 3.12.3 | Jul 28, 2026 |
| Access Control Policy<br>access-control-policy.pdf | Policy | 3.1.1, 3.1.2, 3.1.5, 3.1.6, 3.1.7 | May 4, 2026 |
| MFA enrollment report<br>entra-mfa-registration.png | Screenshot | 3.5.3, 3.5.1, 3.5.2 | Aug 30, 2026 |
| Account lockout settings<br>gpo-account-lockout.png | Configuration export | 3.1.8, 3.5.7, 3.5.8 | May 12, 2026 |
| Security awareness training completions<br>training-completions-2026.csv | Training record | 3.2.1, 3.2.2 | Sep 2, 2026 |
| Incident Response Plan<br>incident-response-plan.pdf | Plan (IR, BCP, DR) | 3.6.1, 3.6.2 | Jun 10, 2026 |
| SIEM log sources and retention<br>siem-sources.png | Configuration export | 3.3.1, 3.3.2, 3.3.5, 3.3.8 | Sep 14, 2026 |
| Configuration baseline (hardened images)<br>baseline-images.xlsx | Configuration export | 3.4.1, 3.4.2, 3.4.6, 3.4.7 | Jun 22, 2026 |
| Vulnerability scan summary, September<br>vuln-scan-2026-09.pdf | Report or scan result | 3.11.2, 3.11.3 | Sep 30, 2026 |
| Risk assessment 2026<br>risk-assessment-2026.pdf | Report or scan result | 3.11.1 | Apr 18, 2026 |
| Firewall rule review<br>firewall-review-q3.pdf | Report or scan result | 3.13.1, 3.13.5, 3.13.6 | Aug 8, 2026 |
| Badge access and visitor log procedure<br>physical-access-procedure.pdf | Procedure | 3.10.1, 3.10.2, 3.10.3, 3.10.4, 3.10.5 | May 20, 2026 |
| Media sanitization certificates<br>sanitization-certs.pdf | Other | 3.7.3, 3.8.3 | Jul 1, 2026 |
| Endpoint protection console<br>edr-console.png | Screenshot | 3.14.2, 3.14.4, 3.14.5 | Aug 15, 2026 |
| Personnel screening and offboarding checklist<br>offboarding-checklist.pdf<br>Review overdue since Oct 1, 2026 | Procedure | 3.9.1, 3.9.2 | Apr 30, 2026 |

| DOCUMENT | TYPE | SUPPORTS | ADDED |
| --- | --- | --- | --- |
| BitLocker compliance report<br>bitlocker-report.png | Screenshot | `3.13.11, 3.13.16, 3.8.6` | Sep 21, 2026 |

This is a self-assessment completed by Bayside Precision Parts (fictional sample) using PolicyScore. Answers have not been independently verified. The report is informational: it is not an insurance application, does not guarantee coverage, terms or premiums, and PolicyScore is not an insurance producer. The SPRS score and CMMC status shown are self-assessed estimates and are not a CMMC certification.

ⓘ PolicyScore is a self-assessment and preparation tool only. It is not an audit, a certification, an attestation, or legal advice. CMMC Level 2 certification requires an assessment by an authorized C3PAO (Level 2 self-assessments are submitted in SPRS by an affirming official).