**CUSTOMER RESPONSIBILITY MATRIX**

NIST SP 800-171 Rev 2 Control Mapping • Metal Finishing Calculator v3.0.0

|  |  |
| --- | --- |
| **Version:** | 1.0 | January 30, 2026 | Psyrcuit LLC |
| **Audience:** | Compliance Officers, CMMC Assessors, IT Security Teams |

# 1. Introduction

This document maps NIST SP 800-171 Rev 2 security controls to responsibility assignments for Metal Finishing Calculator (MFC). Due to MFC's 100% offline architecture, the majority of controls are either the customer's responsibility (implemented at the workstation/environment level) or not applicable (no network functionality exists).

## How to Read This Matrix

|  |  |
| --- | --- |
| **Customer** | Control is implemented by customer's IT environment, policies, or procedures |
| **Vendor** | Control has vendor involvement (documentation, updates, secure defaults) |
| **N/A** | Control does not apply due to offline architecture (no network/auth) |

# 2. Executive Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Family** | **Customer** | **Vendor** | **N/A** | **Total** |
| 3.1 Access Control | **22** | 0 | 0 | 22 |
| 3.2 Awareness & Training | **3** | 0 | 0 | 3 |
| 3.3 Audit & Accountability | **9** | 0 | 0 | 9 |
| 3.4 Configuration Management | **8** | **1** | 0 | 9 |
| 3.5 Identification & Authentication | 0 | 0 | **11** | 11 |
| 3.6 Incident Response | **3** | 0 | 0 | 3 |
| 3.7 Maintenance | **5** | **1** | 0 | 6 |
| 3.8 Media Protection | **9** | 0 | 0 | 9 |
| 3.9 Personnel Security | **2** | 0 | 0 | 2 |
| 3.10 Physical Protection | **6** | 0 | 0 | 6 |
| 3.11 Risk Assessment | **2** | **1** | 0 | 3 |
| 3.12 Security Assessment | **3** | **1** | 0 | 4 |
| 3.13 System & Comm Protection | 0 | 0 | **16** | 16 |
| 3.14 System & Info Integrity | **5** | **2** | 0 | 7 |
| **TOTALS** | **77** | **6** | **27** | **110** |

|  |
| --- |
| **KEY TAKEAWAYS**  • 27 controls (25%) are N/A due to offline architecture - no network or authentication  • 77 controls (70%) are customer responsibility - workstation and environment level  • 6 controls (5%) have vendor involvement - documentation, updates, secure defaults  **CMMC assessors will find minimal vendor-side controls to evaluate. Assessment focuses on customer's environment.** |

# 3. Detailed Control Mapping by Family

## 3.1 Access Control (22 Controls)

*All access control requirements are implemented at the workstation and operating system level. MFC has no user accounts or authentication system.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.1.1 | Limit system access to authorized users | **Customer** | Windows login |
| 3.1.2 | Limit system access to authorized transactions/functions | **Customer** | OS permissions |
| 3.1.3 | Control flow of CUI per authorizations | **Customer** | Network/file policies |
| 3.1.4 | Separate duties to reduce malicious activity | **Customer** | Org policy |
| 3.1.5 | Employ principle of least privilege | **Customer** | OS user rights |
| 3.1.6 | Use non-privileged accounts for non-security functions | **Customer** | Standard user |
| 3.1.7 | Prevent non-privileged users from executing privileged functions | **Customer** | UAC/OS controls |
| 3.1.8 | Limit unsuccessful logon attempts | **Customer** | Windows policy |
| 3.1.9 | Provide privacy and security notices | **Customer** | Logon banner |
| 3.1.10 | Use session lock with pattern-hiding displays | **Customer** | Screensaver/lock |
| 3.1.11 | Terminate session after defined period | **Customer** | Inactivity timeout |
| 3.1.12 | Monitor and control remote access | **Customer** | VPN/RDP policy |
| 3.1.13 | Employ cryptographic mechanisms for remote access | **Customer** | VPN encryption |
| 3.1.14 | Route remote access via managed access control points | **Customer** | Network arch. |
| 3.1.15 | Authorize remote execution of privileged commands | **Customer** | Admin policy |
| 3.1.16 | Authorize wireless access prior to connection | **Customer** | WiFi policy |
| 3.1.17 | Protect wireless access using authentication and encryption | **Customer** | WPA2/3 |
| 3.1.18 | Control connection of mobile devices | **Customer** | MDM policy |
| 3.1.19 | Encrypt CUI on mobile devices | **Customer** | Device encrypt |
| 3.1.20 | Verify and control connections to external systems | **Customer** | Firewall rules |
| 3.1.21 | Limit use of portable storage devices | **Customer** | USB policy |
| 3.1.22 | Control CUI posted to publicly accessible systems | **Customer** | Publishing policy |

## 3.2 Awareness and Training (3 Controls)

*All training requirements are organizational responsibilities. MFC includes an in-app tutorial for application operation only.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.2.1 | Ensure personnel are aware of security risks | **Customer** | Security training |
| 3.2.2 | Ensure personnel are trained to carry out duties | **Customer** | Role-based training |
| 3.2.3 | Provide security awareness training on recognizing threats | **Customer** | Insider threat |

## 3.3 Audit and Accountability (9 Controls)

*MFC does not generate audit logs. All auditing is performed at the operating system level using Windows Event Logs and file system auditing.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.3.1 | Create and retain audit logs | **Customer** | Windows logs |
| 3.3.2 | Ensure actions can be traced to individual users | **Customer** | File ownership |
| 3.3.3 | Review and update logged events | **Customer** | Audit policy |
| 3.3.4 | Alert on audit logging process failures | **Customer** | SIEM/monitoring |
| 3.3.5 | Correlate audit review, analysis, and reporting | **Customer** | Log aggregation |
| 3.3.6 | Provide audit reduction and report generation | **Customer** | SIEM tools |
| 3.3.7 | Provide system capability for comparing audit records | **Customer** | Time sync (NTP) |
| 3.3.8 | Protect audit information from unauthorized access | **Customer** | Log permissions |
| 3.3.9 | Limit management of audit logging to subset of users | **Customer** | Admin access |

## 3.4 Configuration Management (9 Controls)

*Vendor provides Configuration & Hardening Guide (Document 5). Customer implements configuration management for their environment.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.4.1 | Establish and maintain baseline configurations | **Customer** | System baseline |
| 3.4.2 | Establish and enforce security configuration settings | **Vendor** | Hardening guide |
| 3.4.3 | Track, review, approve changes to systems | **Customer** | Change mgmt |
| 3.4.4 | Analyze security impact of changes | **Customer** | Change review |
| 3.4.5 | Define and enforce physical/logical access restrictions | **Customer** | Access policy |
| 3.4.6 | Employ principle of least functionality | **Customer** | Disable services |
| 3.4.7 | Restrict, disable, or prevent nonessential programs | **Customer** | App allowlisting |
| 3.4.8 | Apply deny-by-exception policy for unauthorized software | **Customer** | Software policy |
| 3.4.9 | Control and monitor user-installed software | **Customer** | Install rights |

## 3.5 Identification and Authentication (11 Controls)

*MFC has NO user authentication system. All controls in this family are N/A for the application. Authentication occurs at the Windows/domain level.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.5.1 | Identify system users, processes, or devices | **N/A** | No app auth |
| 3.5.2 | Authenticate users, processes, or devices | **N/A** | No app auth |
| 3.5.3 | Use multifactor authentication for local access | **N/A** | No app auth |
| 3.5.4 | Employ replay-resistant authentication | **N/A** | No app auth |
| 3.5.5 | Prevent reuse of identifiers | **N/A** | No app auth |
| 3.5.6 | Disable identifiers after period of inactivity | **N/A** | No app auth |
| 3.5.7 | Enforce minimum password complexity | **N/A** | No app auth |
| 3.5.8 | Prohibit password reuse | **N/A** | No app auth |
| 3.5.9 | Allow temporary passwords for system login | **N/A** | No app auth |
| 3.5.10 | Store and transmit cryptographically protected passwords | **N/A** | No app auth |
| 3.5.11 | Obscure feedback of authentication information | **N/A** | No app auth |

## 3.6 Incident Response (3 Controls)

*Incident response is an organizational responsibility. Vendor provides Incident Response Support Policy (Document 8).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.6.1 | Establish incident handling capability | **Customer** | IR program |
| 3.6.2 | Track, document, and report incidents | **Customer** | Incident tracking |
| 3.6.3 | Test incident response capability | **Customer** | IR testing |

## 3.7 Maintenance (6 Controls)

*Vendor provides software updates. System maintenance is customer's responsibility.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.7.1 | Perform maintenance on organizational systems | **Customer** | System maint. |
| 3.7.2 | Provide controls on maintenance tools | **Customer** | Tool controls |
| 3.7.3 | Ensure equipment removed for maintenance is sanitized | **Customer** | Media sanitation |
| 3.7.4 | Check media containing diagnostics for malicious code | **Customer** | AV scanning |
| 3.7.5 | Require MFA for establishing remote maintenance | **Customer** | Remote access |
| 3.7.6 | Supervise maintenance activities | **Vendor** | Update process |

## 3.8 Media Protection (9 Controls)

*All media protection is customer's responsibility. MFC data files follow customer's media handling policies.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.8.1 | Protect media containing CUI | **Customer** | Media handling |
| 3.8.2 | Limit access to CUI on media | **Customer** | Access control |
| 3.8.3 | Sanitize media prior to disposal | **Customer** | Sanitization |
| 3.8.4 | Mark media with CUI markings | **Customer** | Labeling |
| 3.8.5 | Control access to media containing CUI | **Customer** | Physical security |
| 3.8.6 | Implement cryptographic mechanisms for CUI during transport | **Customer** | Encrypted transport |
| 3.8.7 | Control use of removable media | **Customer** | USB policy |
| 3.8.8 | Prohibit use of portable storage when no owner | **Customer** | Found media |
| 3.8.9 | Protect backup CUI at storage locations | **Customer** | Backup security |

## 3.9 Personnel Security (2 Controls)

*Personnel security is entirely customer's organizational responsibility.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.9.1 | Screen individuals prior to authorizing access | **Customer** | Background checks |
| 3.9.2 | Ensure CUI is protected during personnel actions | **Customer** | Termination proc. |

## 3.10 Physical Protection (6 Controls)

*Physical protection is entirely customer's facility responsibility.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.10.1 | Limit physical access to authorized individuals | **Customer** | Facility access |
| 3.10.2 | Protect and monitor physical facility | **Customer** | Physical security |
| 3.10.3 | Escort visitors and monitor visitor activity | **Customer** | Visitor policy |
| 3.10.4 | Maintain audit logs of physical access | **Customer** | Access logs |
| 3.10.5 | Control physical access devices | **Customer** | Keys/badges |
| 3.10.6 | Enforce safeguarding measures for CUI at alternate sites | **Customer** | Remote work |

## 3.11 Risk Assessment (3 Controls)

*Vendor performs risk assessment of software. Customer assesses their overall environment.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.11.1 | Periodically assess risk to operations and assets | **Customer** | Risk assessment |
| 3.11.2 | Scan for vulnerabilities periodically | **Vendor** | Software vuln scan |
| 3.11.3 | Remediate vulnerabilities per risk assessments | **Customer** | Patch management |

## 3.12 Security Assessment (4 Controls)

*Vendor provides security documentation. Customer performs ongoing assessment of their environment.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.12.1 | Periodically assess security controls | **Customer** | Control assessment |
| 3.12.2 | Develop and implement plans of action | **Customer** | POA&M |
| 3.12.3 | Monitor security controls on ongoing basis | **Customer** | Continuous monitoring |
| 3.12.4 | Develop and update system security plans | **Vendor** | This documentation |

## 3.13 System and Communications Protection (16 Controls)

*MFC has NO network functionality. All 16 controls in this family are N/A for the application itself. Network protection is implemented at customer's infrastructure level.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.13.1 | Monitor communications at external boundaries | **N/A** | No network |
| 3.13.2 | Employ architectural designs to protect CUI | **N/A** | No network |
| 3.13.3 | Separate user functionality from management | **N/A** | No network |
| 3.13.4 | Prevent unauthorized transfer via shared resources | **N/A** | No network |
| 3.13.5 | Implement subnetworks for publicly accessible components | **N/A** | No network |
| 3.13.6 | Deny network traffic by default | **N/A** | No network |
| 3.13.7 | Prevent remote devices from simultaneous connections | **N/A** | No network |
| 3.13.8 | Implement cryptographic mechanisms for CUI transmission | **N/A** | No transmission |
| 3.13.9 | Terminate network connections after period of inactivity | **N/A** | No network |
| 3.13.10 | Establish cryptographic keys per applicable policies | **N/A** | No network |
| 3.13.11 | Employ FIPS-validated cryptography | **N/A** | No network |
| 3.13.12 | Prohibit remote activation of collaborative devices | **N/A** | No network |
| 3.13.13 | Control and monitor use of mobile code | **N/A** | No network |
| 3.13.14 | Control and monitor use of VoIP | **N/A** | No network |
| 3.13.15 | Protect authenticity of communications sessions | **N/A** | No network |
| 3.13.16 | Protect confidentiality of CUI at rest | **N/A** | Customer encrypt |

## 3.14 System and Information Integrity (7 Controls)

*Vendor provides software updates and flaw remediation. Customer maintains system integrity through AV and patching.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Requirement** | **Resp.** | **Notes** |
| 3.14.1 | Identify, report, and correct system flaws | **Vendor** | Software updates |
| 3.14.2 | Provide protection from malicious code | **Customer** | AV/EDR |
| 3.14.3 | Monitor security alerts and advisories | **Customer** | Threat intel |
| 3.14.4 | Update malicious code protection mechanisms | **Customer** | AV updates |
| 3.14.5 | Perform periodic and real-time scans | **Customer** | AV scanning |
| 3.14.6 | Monitor system for attacks and indicators | **Customer** | SIEM/EDR |
| 3.14.7 | Identify unauthorized use of systems | **Vendor** | License system |

# 4. Summary Statement

|  |
| --- |
| Metal Finishing Calculator's offline architecture significantly simplifies CMMC compliance:  • 27 controls (25%) are completely N/A *— no network or authentication to assess*  • 77 controls (70%) are customer responsibility *— standard workstation/environment controls*  • 6 controls (5%) have vendor involvement *— documentation, updates, secure defaults*  **The application introduces minimal additional compliance burden. It inherits and operates within the customer's existing security boundary.** |

For compliance inquiries: security@psyrcuit.com • Psyrcuit LLC • Tucson, Arizona