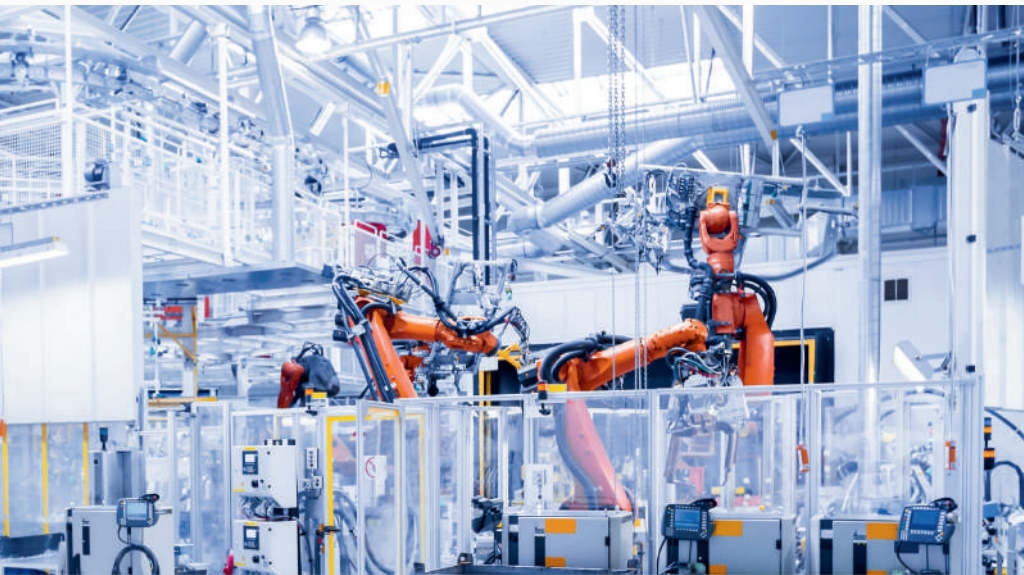


# MANUFACTURER'S GUIDE

to the **14 Domains** of  
**CMMC**  
and how to achieve them



# WELCOME

## CMMC Doesn't Have to Be Complicated

**Most manufacturers approach CMMC the same way they approach a new piece of equipment:** they squint at it, try to understand the manual, and wonder how many things they can ignore without breaking anything.

If that sounds familiar, you're in the right place.

This book exists for one reason: to make CMMC make sense. Not in a dry, academic way. Not in a "here's 400 pages of policy" way. But in a clear, practical, "I actually understand what to do next" way.

**Because here's the truth no one says out loud:**

- You don't need to become a cybersecurity expert.
- You just need to understand the rules of the game well enough to win.

## CMMC isn't about perfection. It's about predictability.

It's about protecting your operations, proving you can be trusted with sensitive data, and unlocking contracts that require a higher bar of security. Manufacturers who get this right don't just avoid headaches; they strengthen their business, reduce downtime, and become the vendor primes want to work with.

Inside this book, you'll find the 14 pillars of CMMC explained in plain English, with real examples pulled straight from the shop floor, not a classroom. You'll learn what auditors look for, what evidence actually matters, and why certain controls make or break your score. You'll also see how everyday decisions like passwords, updates, network layout, and vendor access connect directly to compliance without overwhelming your team.

By the end, you will understand the entire framework in a way that feels manageable. And more importantly, you'll know what steps to take next, whether you're just starting your compliance journey or refining a mature program.

This is the guide I wish every manufacturer had before they tried to decode CMMC on their own. The goal isn't to scare you. The goal is to give you confidence, clarity, and momentum.

So, take a breath. Turn the page.

You're about to learn a system that will make your business stronger, safer, and better prepared for the opportunities ahead.

## Let's get started.

# FOUNDATIONS

## Why Does CMMC Exist?

When the Department of Defense launched the **Cybersecurity Maturity Model Certification (CMMC)**, it was reacting to an uncomfortable truth: the weakest link in national security was no longer the prime contractors with huge budgets, but the small and mid-sized manufacturers feeding parts, code, and materials into the supply chain.

These companies handle sensitive designs, production data, and CUI every day, yet often operate with limited staff, aging systems, and razor-thin margins. This makes them prime targets for attackers. CMMC was designed to close that gap and bring the entire defense ecosystem up to a secure, consistent baseline.

**One compromised job shop could leak Controlled Unclassified Information (CUI) from an aircraft design.**

It consolidates two decades of fragmented rules (FAR 52.204-21, DFARS 252.204-7012, and NIST SP 800-171) into one framework that proves an organization is protecting data at a measurable level of maturity.

CMMC 2.0 focuses on three levels. Level 2 maps directly to NIST 800-171's 110 controls and represents the certification target for nearly all small-to-mid manufacturers. So, that's where this guide will focus.

### How CMMC Fits In

Adds maturity, verification, and an audit mechanism.

CMMC 2.0

Specifies the 110 controls protecting CUI across 14 domains.

NIST 800-171

Extends requirements to DoD contracts and introduces NIST 800-171.

DFARS 252.204-7012

Establishes 17 baseline security practices for all federal suppliers.

FAR 52.204-21

**CMMC turns good-faith promises into verified performance.**

# FOUNDATIONS

## Why CMMC 2.0 Level 2 Actually Matters to Manufacturers

**CMMC Level 2 isn't just another regulatory box to check; it directly affects whether a manufacturer can keep (or win) DoD contracts.** Level 2 is the standard for protecting Controlled Unclassified Information (CUI), which includes drawings, schematics, tolerances, production workflows, supplier data, and even certain emails. If your shop touches that information at any point, then Level 2 is the minimum bar you must meet.

For manufacturers, that bar is high for a reason. The DoD depends on small and mid-sized shops across the supply chain, and adversaries know those shops are often the easiest entry point. Level 2 puts structure and discipline around your cybersecurity program so your business isn't the weak link in a \$900B defense ecosystem.

It also matters financially. As more primes and large contractors tighten their own cybersecurity expectations, non-compliant manufacturers risk being cut from preferred vendor lists, even before CMMC becomes fully mandatory. Insurers are already using these same NIST 800-171 controls when pricing cyber policies, which means Level 2 compliance can lower premiums, reduce exclusions, and prevent denied claims.

Most importantly, Level 2 isn't about doing "extra IT work." It's about stabilizing your environment, reducing downtime, preventing IP theft, and giving your team the operational confidence to take on bigger contracts. Compliance protects your ability to compete.

- In short: if you work in the DoD supply chain, Level 2 is the key to staying in that supply chain. It protects revenue, opens doors, strengthens your security posture, and keeps your business viable in a tightening defense market.

**CMMC certification isn't a cost center—it's a catalyst for growth in any DIB organization.**

## Compliance as a Competitive Advantage

For years, manufacturers viewed compliance as a burden. As something you deal with only because the government says you have to. But in today's defense ecosystem, CMMC Level 2 has become one of the clearest differentiators in the market. When you can prove that your environment is secure, controlled, and aligned with NIST 800-171, you instantly move into a smaller, more trusted category of suppliers.

Primes increasingly prefer working with partners who won't introduce risk into their programs. Many have already started requiring proof of compliance before sending out drawings, quoting work, or awarding new business. Being CMMC-ready doesn't just keep you eligible, it elevates you above competitors who are still scrambling to catch up.

# FOUNDATIONS

## Compliance as a Competitive Advantage

Compliance also strengthens your negotiating position. A secure environment means fewer disruptions, stronger data controls, and lower insurance costs, all of which translate into more predictable performance for your customers. It tells them you're not just another machine shop; you're a mature, stable, reliable part of their production chain.

And when contract officers can choose between two similar vendors, the one with a verified, audited cybersecurity posture almost always wins. Simply put: CMMC is no longer just a checkbox. It's a credibility signal. A trust signal. And in many cases, it's the deciding factor that determines who gets the work.

**CMMC is not "new rules" – it's accountability for rules already on the books.**

## The Scoring System (–203 to 110)

**Every control in NIST 800-171 is assigned a point value — 1, 3, or 5 points — based on how critical it is to protecting CUI.**

Instead of starting at zero and working upward, the DoD flips the model: you begin at -203, the total number of points you lose if none of the required security practices are in place.

From there, you earn back points for every control you've fully implemented. Some practices, like enforcing MFA or restricting admin privileges, carry heavier weight because they close high-risk attack paths. Others, such as creating policies or maintaining logs, are assigned lower values but still contribute to your overall posture.

A perfect score is 110, which means you've implemented all 110 NIST 800-171 practices with no gaps or exceptions. Most manufacturers won't start anywhere near that, and that's expected because the scoring system is designed to show progress over time, not perfection on day one.

Once you calculate your score, you must report it to the Supplier Performance Risk System (SPRS), where primes and the DoD can see your current cybersecurity standing. This makes accuracy essential: your SPRS score directly influences contract eligibility, risk assessments, and how seriously customers view your commitment to protecting sensitive information.

Range	Interpretation
110	Full implementation
88 – 109	Substantial compliance
70 – 87	Partial – remediation
<70	May lose eligibility

Scores expire every three years or sooner if your environment changes. Continuous improvement keeps contracts safe.

# FOUNDATIONS

## Foreword from our CISO

Hi there! I'm Dave Owens, CISM, and I lead the security and compliance efforts here at Micro Solutions.

If you're reading this, you're probably trying to make sense of CMMC, and I want you to know something up front: you're not alone in this process.

I've worked with countless manufacturers who started in the exact same place you are now...**unsure where to begin, concerned about the workload, or questioning whether the effort is really worth it.**

What I've seen time and time again is that once the fog lifts, companies realize CMMC isn't just government red tape. When you approach it intentionally, it becomes a framework that strengthens your operation, protects your people, and gives leadership the confidence that systems are running the way they should. More importantly, it positions you for the opportunities ahead. Many manufacturers don't realize how much business is gated behind basic security expectations until they start meeting them consistently.

My role in this guide is simple: give you clarity, remove the guesswork, and show you what actually matters. No fear tactics, no jargon for the sake of jargon, just straightforward explanations and real-world steps that fit a manufacturing environment.

I hope this resource gives you the confidence and direction you need as you move forward with your compliance journey.

And when you're ready for a partner who can help implement the work behind these pages, my team and I are only a phone call away.

— Dave Owens, CISM



**START  
HERE**



[www.micro-solutions.net](http://www.micro-solutions.net)

607-415-3151



**Dave Owens, CISM**



Certified Information Security Manager

# FOUNDATIONS

SourceYour Compliance Capability

**Manufacturers achieve compliance via three routes:**

## In-House Program

You build an internal IT & security department, hire or train compliance staff, and manage controls directly.

**Pros:** maximum control, direct knowledge retention.

**Cons:** high staffing cost, difficulty recruiting cyber talent, slower maturity.

## Managed Service Provider (MSP/MSSP)



A partner like Micro Solutions provides the technology stack (MFA, SIEM, EDR, backups) and governance assistance.

**Pros:** predictable monthly cost, continuous monitoring, access to experts.

**Cons:** requires trust and well-defined SLAs.

## Consultant / C3PAO Engagement

Used mainly for audits or short-term remediation.

**Pros:** point-in-time validation.

**Cons:** lacks day-to-day operational coverage; compliance can drift.

**Most SMB manufacturers succeed with a hybrid: internal champions supported by a full-service MSP to handle the technical heavy lifting and evidence collection.**



# FOUNDATIONS

**Now that we've laid out the reasoning behind CMMC and the real-world impact it can have on your organization, you're ready for the practical part.**

This is where the ideas become tangible and start connecting directly to your daily operations.

From here on, we'll move through each pillar one by one and break down what it actually means for a manufacturer: what you need to understand, what you need to put in place, and what auditors expect to see when they evaluate your environment.

Think of the next sections as your guided tour. We'll translate the technical language into everyday terms, show you how the controls fit into real workflows, and highlight the places where companies succeed... or get tripped up, during assessments.

Along the way, you'll see how small actions create meaningful improvements and how each pillar supports the next. The goal is not to turn you into a compliance expert. It's to give you the clarity and confidence to make informed decisions and build a program that works reliably in the real world.

So without further ado, let's jump into the first pillar and start turning these concepts into action.

## **CMMC Doesn't Have to Be Complicated**

If you can run a shop, you can understand CMMC.



**Let's Dive in.**



# ACCESS CONTROL

## Executive Summary

**Access Control defines who can see what, and it is the core of confidentiality.** In a manufacturing environment, it separates production data from payroll, design files from email, and protects sensitive CUI from unnecessary exposure. Done well, it ensures every employee and every system has only the access they need, nothing more. Done poorly, it gives attackers room to roam freely. Access Control is the gatekeeper of your entire security program, limiting blast radius, preventing insider misuse, and keeping critical data exactly where it belongs.

## Regulatory Background

Access Control aligns directly with NIST SP 800-171 controls 3.1.1 through 3.1.22, the core requirements that dictate who is allowed to access what information and under what conditions. These controls mandate that organizations:

- Limit access strictly to authorized users, processes, and devices.
- Enforce least privilege, ensuring individuals only have the permissions necessary to perform their job.
- Manage remote and wireless connections so external access points cannot become attack vectors.
- Define and monitor account types, including admin accounts, shared accounts, and service accounts.
- Control session activity, including automatic logouts and secure session handling.
- Prevent unauthorized data transfer, including portable media restrictions.

### Auditors will request:

**Written access-control policy.**  
**List of active accounts vs. employees.**  
**Proof of MFA.**  
**Records Of Quarterly Reviews**

## Business Impact

**Improper access is the No. 1 cause of insider incidents.**

A machinist who accidentally opens engineering drawings or an engineer who stores prototypes in an unprotected share both create instant breach exposure.

These mistakes aren't malicious... they're the result of unclear boundaries. Strong access control enforces true "need-to-know" separation across teams and systems, reducing risk without slowing down the work that keeps the factory moving.

**Recommended Technology Stack: Azure AD + Conditional Access + on-prem Group Policy+ Intune device management.**

# ACCESS CONTROL

Responsible Role	Description	Evidence
IT Manager	Map CUI Location – identify servers, M365 sites, CAD storage.	Data-flow diagram
Security Lead	Define Roles – engineering, finance, operations.	RBAC matrix
Sys Admin	Apply MFA Everywhere.	Screenshots, logs
Manager	Quarterly Review Access. Remove dormant accounts.	Review sign-off
HR +IT	Automate Off-boarding. Disable on termination.	Ticket history

**A complete trail earns full points for controls 3.1.1 – 3.1.22.**

(Missing documentation drops 5 points per unmet practice.)

## Integration with Other Frameworks

**Access Control aligns cleanly with other major frameworks.**

ISO 27001 Clause 9 and NIST CSF PR.AC map directly to these same requirements, so the evidence you generate for CMMC like access reviews, permission reports, MFA enforcement, and audit trails, also satisfies these broader standards.

## Procurement Decision

**If you manage fewer than 250 accounts, in-house administration may be feasible.**

Beyond that, the volume of permissions, on/offboarding, and access review become too complex to manage manually. At that scale, automating identity control through an MSP with access-management expertise is the secure, efficient, and cost-effective choice.

## Case Example

**A precision machine shop implemented MFA on email but overlooked its ERP software.**

An attacker phished a single user, logged in through the unprotected ERP portal, and quietly downloaded engineering drawings. After Micro Solutions integrated SSO, enforced MFA everywhere, and added conditional access policies, the attack path was closed. Breach risk dropped to near zero, and the company's audit score improved by 15 points.

Micro Solutions is a proud partner of



# AWARENESS & TRAINING

## Executive Summary

**Technology can't fix carelessness...** and it can't outpace human behavior. Awareness & Training is what turns employees from potential risks into active sentinels. When people understand how attacks work and what to look for, they become an extension of your security program rather than a vulnerability to manage.

Strong training builds instincts, reduces mistakes, and creates a culture where **everyone** plays a role in protecting CUI and keeping operations running smoothly.

## Regulatory Background

From a regulatory standpoint, Awareness & Training is not optional. It's baked directly into the rules for handling CUI. NIST SP 800-171 controls 3.2.1 through 3.2.3 require you to educate users on security risks, their individual responsibilities, and how to recognize and report incidents. In other words, it's not enough to deploy good tools; you must also prove that the people using them have been trained to spot threats and follow proper procedures.

## Business Impact

A well-trained workforce often detects attacks before the tools ever flag them. That human layer of defense is becoming so critical that insurance underwriters and prime contractors increasingly require documented proof of cybersecurity training. Without it, coverage can be limited, premiums can rise, and subcontract approval can stall. This makes training not just a security best practice, but a business requirement.

## Audit Expectations

Auditors expect proof: training materials, attendance logs, and phishing-test results. They're looking for evidence of a consistent, documented annual cycle, not a one-time session. Strong records earn all three points in this domain and clearly demonstrate that your team's security readiness is tracked, measured, and enforced.



# AWARENESS & TRAINING

Description	Tool / Evidence
Launch annual training program with monthly micro-modules.	FULL IMPLEMENTATION
Conduct quarterly phishing simulations.	SUBSTANTIAL COMPLIANCE
Post visual reminders near terminals and timeclocks.	PARTIAL – REMEDIATION
Require policy acknowledgment on hire and annually.	HIGH RISK – MAY LOSE ELIGIBILITY
Report results to management for accountability.	KPI DASHBOARD

**A complete trail earns full points for controls 3.1.1 – 3.1.22.**

(Missing documentation drops 5 points per unmet practice).

## Procurement Decision

If you manage fewer than 250 accounts, in-house administration can work. Beyond that point, partnering with an MSP that specializes in identity management is strongly recommended to keep access secure, consistent, and scalable.

(Our team can help here!)

**[www.micro-solutions.net/contact-us/](http://www.micro-solutions.net/contact-us/)**

## Case Example

**It started how many incidents do: with a single click on a malicious PDF...**

It wasn't a full-blown disaster, but it was enough to slow production, rattle the team, and earn a not-so-friendly nudge from their cyber insurance provider. In other words, a bright neon sign that their "human firewall" wasn't exactly fireproof.

So the manufacturer rolled out Micro Solutions' cybersecurity awareness and phishing-resilience program... and things changed fast. Quick, easy training sessions helped people understand why good habits matter, not just what buttons not to press.

Then came the simulated phishing tests, turning those lessons into muscle memory.

Six months later, their click rate plummeted from 22% to just 3%. That big drop in human-factor risk helped lower their insurance premiums by more than 10%, and even better, gave leadership real peace of mind knowing their team had become a dependable part of their security posture.

Micro Solutions is a proud partner of

**KnowBe4**

SCAN ME



# AUDIT & ACCOUNTABILITY

## Executive Summary

If Access Control defines who may enter, Audit & Accountability records who actually did enter—and what they did once they were inside.

Think of it as the digital equivalent of a facility's security camera system: always on, always observing, and essential for understanding the full picture of system activity.

In a CMMC environment, this pillar ensures that every meaningful action (logins, file access, permission changes, administrative tasks, failed authentication attempts, remote sessions) is captured, stored, and reviewable. These records become the backbone of incident investigations, compliance validation, and insurance claims. More importantly, they help manufacturers spot suspicious behavior early, before it becomes a costly breach.

## Regulatory Background

CMMC's Audit & Accountability requirements are grounded in the federal standards manufacturers must follow to handle Controlled Unclassified Information (CUI).

**NIST SP 800-171 controls 3.3.1 through 3.3.9 establish the foundation:** organizations must **generate audit logs**, **protect** those logs from tampering, **retain** them for defined periods, and regularly **review** them for signs of inappropriate or suspicious activity. These standards ensure that every meaningful event in your environment can be traced, verified, and acted upon. This provides both regulatory assurance and operational security.

## Business Impact

Strong Audit & Accountability practices have a direct impact on your bottom line. Good logs let you quickly trace what happened during an incident, why it happened, and how to prevent it from happening again. They also give assessors clear proof that your controls are actually working. Just as important, audit evidence protects you when the stakes are highest. If you can't produce logs, you can't prove that CUI stayed contained. What could have been a small issue can suddenly become a reportable breach, trigger disclosures, jeopardize contracts, or even complicate an insurance claim. Put simply: without logs, you have no way to defend your decisions or your business when it matters most.

# AUDIT & ACCOUNTABILITY

## Implementation Blueprint

RESPONSIBLE ROLE	DESCRIPTION	EVIDENCE
MSP	Centralize Logs in a SIEM.	SYSTEM DASHBOARDS
SECURITY LEAD	Define Events to collect – login success/fail, privilege changes, file access.	CONFIG FILES
SOC	Automate Alerts for anomalies.	ALERT TICKETS
IT	Protect Logs from modification.	ACCESS POLICY
IT	Retain 90 days online / 1 year archived.	RETENTION POLICY

### Full implementation earns up to nine points

(Missing retention policy or proof of review often costs 5 points per control).

## Audit Expectations

Auditors will review your SIEM dashboard, sample log entries, and proof of regular log reviews ("who checked the logs and when"). They may even simulate an incident and ask you to produce the exact records, timestamps, and alerts tied to that event.

## Procurement Decision

A SIEM is only effective with true 24x7 monitoring. Unless you operate a dedicated security operations center, it's best to partner with an MSSP to handle real-time alerting and analysis.

## Case Example

### A tooling company learned this the hard way.

One Monday morning, several CNC controllers were offline and engineering files wouldn't open, which are signs of a breach. But when the team went looking for answers, they discovered the firewall only kept 24 hours of logs. The entire weekend breach window had been overwritten.

With no evidence to trace, they spent three days pulling machines offline, checking systems by hand, and trying to reconstruct the incident. This halted production and delayed orders.

After switching to Micro Solutions' managed SIEM, logs were retained for a full year and automatically correlated across systems. Their next audit was night-and-day: clear visibility, faster response, and an audit score that jumped from -27 to +98.

Micro Solutions is a proud partner of



Microsoft  
Sentinel

SCAN ME



# CONFIGURATION MANAGEMENT

## Executive Summary

**Configuration Management keeps systems predictable and trustworthy.**

It's the discipline of knowing exactly how every workstation, server, switch, and PLC is built and ensuring no one can quietly change those configurations without approval from the proper parties.

When every device follows a known, documented baseline, you eliminate guesswork, avoid "mystery settings," and drastically reduce the risk of unauthorized changes introducing vulnerabilities.

Paired with **configuration checklists, hardening guides, and change-control records**, this discipline gives you full visibility into how each system is supposed to behave. In a manufacturing environment where uptime matters, this level of control keeps operations stable, secure, and consistent day after day.

## Regulatory Background

Under the hood, Configuration Management is anchored by NIST SP 800-171 controls 3.4.1 through 3.4.8, which require organizations to establish secure configuration baselines, apply standardized settings across all systems, document every meaningful change, and correct anything that drifts from the approved state. These controls also expect you to track who made a change, when it happened, why it was approved, and how it was validated afterward.

The purpose is simple: prevent silent misconfigurations from creeping into your environment. These small, unnoticed changes are often the root cause of avoidable vulnerabilities, unexpected downtime, or failed audits. Effective Configuration Management stops that drift before it becomes a problem and keeps your environment operating the same way every day—predictable, secure, and audit-ready.

## Business Impact

Uncontrolled change is chaos. A technician installs "temporary" software to test a sensor, and suddenly that workstation stops receiving Windows updates, quietly turning into the breach point that halts production. One small tweak becomes a hidden weakness, and no one realizes it until operators are standing idle on the shop floor.

Small, undocumented changes like this create inconsistencies, vulnerabilities, and hours of unnecessary troubleshooting. Configuration Management prevents these surprises by ensuring every device follows a known-good baseline, every change is intentional and documented, and nothing in your environment drifts in ways that put operations, security, or audit readiness at risk.





# CONFIGURATION MANAGEMENT

## Implementation Blueprint

Responsible Role	Description	Evidence
IT Manager	Define authorized configurations for each device type (OS version, antivirus, firewall settings).	Baseline Docs
Sys Admin	Use imaging or Intune profiles so all new devices deploy identically.	RBAC matrix
Change Board	Require a ticket for every configuration change; log approval and rollback plan.	Change Log
Sec Analyst	Run Vulnerability Scans weekly; Compare to baseline	Scan Reports
Ops Lead	Patch management policy—critical within 15 days, all within 30.	Patch Summary

## Audit Expectations

- A configuration baseline document
- Change-control records
- Patch-management evidence
- Proof that deviations are corrected

**Full evidence across 3.4.1–3.4.8 adds up to 8 points.**

No baselines = automatic 5-point deduction per control.

## Case Example

**A plastics manufacturer operated 50 “identical” CNC stations—except none of them were actually identical.**

Over the years, technicians had made small tweaks during troubleshooting, so every machine behaved a little differently. Updates were unpredictable, maintenance took longer than it should, and auditors couldn’t confirm which systems met the baseline.

Micro Solutions stepped in to rebuild the environment using standardized configuration templates. Every CNC station was brought back to a known-good baseline, updates became consistent, and troubleshooting time dropped dramatically. Maintenance windows shrank by 40 percent, and the company’s CMMC audit readiness jumped from 65 to 101 points thanks to clean documentation and full configuration control.

Micro Solutions - How We Standardize Your Environment

SCAN ME



# IDENTIFICATION & AUTHENTICATION

## Executive Summary


**Identity is the new perimeter. In today's environment, attackers don't break in — they log in.**

Every user, device, and service must prove exactly who they are before they're trusted with access to systems or data. Identification & Authentication establishes that proof. It enforces strong identities, verifies every login attempt, and ensures credentials can't be reused, shared, or exploited.

Done well, it closes off the front door of your environment and forces every request, human or machine, to authenticate before it's allowed to operate.

## Regulatory Background

From a regulatory standpoint, Identification & Authentication is tightly defined. NIST 800-171 controls 3.5.1 through 3.5.11 require organizations to issue unique user IDs, enforce MFA, apply strong password policies, and properly protect authentication secrets like tokens and keys. These requirements ensure every identity can be traced, verified, and trusted, which forms the backbone of secure access throughout the environment.



Require FIDO2 or certificate-based MFA for all privileged accounts. It eliminates passwords and blocks credential theft outright.

## Business Impact

A single compromised credential costs manufacturers an average of \$180K in downtime (often from just one reused password or unchecked login). Strong identity controls are the cheapest insurance you'll ever buy. By enforcing MFA, unique IDs, and protected authentication secrets, you stop attackers before they ever reach your systems and avoid the costly cascade of outages, recovery work, and operational disruption that follows a bad login.



[www.micro-solutions.net](http://www.micro-solutions.net)

607-415-3151



CALL US  
NOW

# IDENTIFICATION & AUTHENTICATION

1

## Unique User Accounts

Ban shared credentials; each person gets their own ID.

2

## MFA Everywhere

VPN, email, firewall, ERP —all enforced with a second factor.

3

## Password Hygiene

12-character minimum; no reuse; password vaults for admins.

4

## Device Trust

Use Intune or certificate-based auth so only known devices connect.

5

## Lifecycle Automation

Accounts auto-created and disabled via HR system integration.

## Required Evidence:

Screenshots of MFA policies, terminated-user log showing deactivation, and Azure AD security reports.

## Audit Expectations

**Auditors will expect to see clear evidence that every identity is unique, verified, and protected.**

They'll review MFA enforcement reports, password-policy settings, conditional-access rules, and logs showing successful and failed authentication attempts.

They may also sample user accounts to confirm there are no shared credentials and verify that disabled or offboarded accounts are fully removed.

Consistent documentation (MFA logs, identity inventories, and password-policy records) is the key to earning full points in this domain.

## Procurement Decision

If you have more than 50–75 users or rely on multiple cloud applications, managing identities manually becomes risky and time-consuming.

At that scale, adopting a unified identity platform, such as Entra ID with SSO and MFA, and partnering with an MSP experienced in identity governance is the most cost-effective and secure option.

Smaller environments may manage on their own, but once credentials span multiple systems, centralized authentication and automated controls are essential to preventing credential misuse and login-based attacks.

## Case Example

**A contract fabricator thought they were secure because MFA was enabled on email, but several legacy apps still used simple, or even shared, passwords.**

An attacker phished one supervisor and reused the stolen password to access a connected system without triggering alerts.

Micro Solutions centralized identities with Entra ID, enforced MFA everywhere, and eliminated shared logins. Unauthorized attempts were blocked automatically, stale accounts were cleaned up, and leadership finally had visibility into who had access to what. Their I&A score jumped from 58 to 104 in the next audit.

Micro Solutions - How We Standardize Your Environment

We deploy MFA & conditional access in Azure AD, enforce SSO for apps, and provide password-policy reporting for audit evidence.

# INCIDENT RESPONSE

## Executive Summary

**Incident Response (IR) is the fire drill for cyber events. It turns panic into procedure.**

In a manufacturing environment where downtime can be costly, a practiced IR plan is what keeps a bad day from becoming a full-scale operational disaster.

Instead of scrambling when something goes wrong, Incidence response planning gives your team a predefined playbook: who to call, what to contain, what evidence to preserve, and how to get systems back online safely.

## Regulatory Background

From a regulatory standpoint, Incident Response is tightly prescribed. NIST 800-171 controls 3.6.1 through 3.6.3 require organizations to maintain a documented IR plan, provide a clear mechanism for reporting incidents, and show evidence that the plan is actually tested. Auditors want to see that you don't just have a plan, but that you can execute it, measure its effectiveness, and improve it over time. We achieve this improvement through practice exercises referred to as "Table Top Exercise".

## Business Impact

A well-practiced Incident Response plan can mean the difference between a brief interruption and days of costly downtime. Manufacturers lose an average of \$22K per hour during a cyber-related outage, and most of that loss comes from slow decision-making, unclear roles, and missing evidence. A strong IR program shortens recovery time, preserves critical forensic data, guides communication with customers and insurers, and prevents small incidents from escalating into full production stoppages. In short, IR protects both your operations and your balance sheet.

## Table Top Notes

**Run tabletop exercises twice per year and record attendance.**

Auditors will ask for a copy of your IR plan, test schedule, and tickets showing real or simulated events.

(See appendix for a table top exercise playbook)

 [www.micro-solutions.net](http://www.micro-solutions.net)

607-415-3151



  
CALL US  
NOW

# INCIDENT RESPONSE

1	<b>Preparation</b>	Draft IR Plan; define roles and contact tree.	<b>Approved Plan</b>
2	<b>Detection</b>	Enable 24x7 alerting from EDR and SIEM.	<b>Alerts</b>
3	<b>Containment</b>	Isolate infected devices, block malicious IPs.	<b>Ticket Trail</b>
4	<b>Eradication</b>	Clean systems and reset credentials.	<b>Remediation Report</b>
5	<b>Recovery</b>	Restore Validated Backups.	<b>Post-incident Report</b>
6	<b>Lessons Learned</b>	Update IR plan & Train Staff.	<b>Revision Log</b>

## Required Evidence:

A fully documented and tested IR cycle earns all points for controls 3.6.1–3.6.3.

## Audit Expectations

Auditors will look for a documented Incident Response Plan, clear evidence of an incident-reporting process, and proof that the plan has been tested.

C3PAO's may ask for tabletop exercise records, communication logs, or sample incident tickets to confirm your team can execute the plan effectively. Full points are awarded when organizations show a complete, repeatable IR cycle... not just a written document.

## Procurement Decision

If your team lacks 24x7 monitoring or doesn't have staff with forensic, SIEM, or containment experience, partnering with an MSP or MSSP is the most reliable and cost-effective option.

Smaller organizations may manage IR internally, but once you handle CUI or operate OT environments, outside support ensures incidents are detected quickly, escalated properly, and documented in a way that satisfies auditors and insurers.

## Case Example

**One of the world's largest aluminum producers, Norsk Hydro, was hit by the LockerGoga ransomware strain in 2019.**

The attack began with a compromised employee credential on a single workstation, then spread across Active Directory and into production systems. Entire plants had to switch to manual operations.

Hydro's team credited their well-practiced Incident Response Plan for preventing permanent damage:

- They immediately isolated networks and shut down infected systems.
- Communication flowed quickly to executives, operations, and the public.
- Their IR team preserved forensic evidence for law enforcement and insurers.
- They continued production manually while systems were rebuilt.

Despite the scope of the attack, Hydro maintained transparency and regained full operations with minimal long-term impact. Cyber insurers later cited the company's mature IR process as a key reason the event did not destroy the business.

See Appendix for a sample Incident Response Plan!

# MAINTENANCE

## Executive Summary

**Maintenance controls govern how systems are serviced, who is allowed to touch them, and what happens before, during, and after any work is performed.**

In many environments, the biggest risks don't come from bad actors. They come from well meaning vendors, technicians, or contractors who introduce changes without oversights or proper change management processes.

With mature maintenance practices in place, firmware updates, vendor support sessions, OT servicing, and remote troubleshooting all follow a controlled, auditable workflow. These controls protect CUI during servicing, prevent configuration drift, detect unauthorized or unsafe maintenance activity, and ensure systems return to operation in a known-secure state. In high-stakes manufacturing environments, MA is what keeps "routine maintenance" from turning into an unexpected outage (or a silent compromise).

## Regulatory Background

**NIST 800-171 controls 3.7.1 through 3.7.6 define the requirements for secure maintenance.**

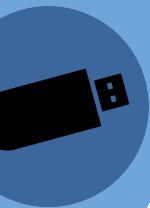
These include authorizing all maintenance actions, validating the identities of anyone performing the work, restricting remote maintenance, and documenting every service session from start to finish. The standard also requires monitoring maintenance tools and ensuring no unauthorized software, devices, or vendor equipment ever touches systems that handle CUI. These rules exist to prevent servicing activities, often overlooked, from becoming a direct path to compromise.

## Business Impact

Maintenance activities introduce some of the highest operational and security risks in a manufacturing environment. A single unauthorized firmware update can shut down a production line; an unvetted vendor laptop can introduce malware; and an overlooked remote session can expose CUI without anyone realizing it. Poorly controlled maintenance is a leading cause of unexpected downtime, equipment misconfiguration, and audit failures.

Strong maintenance controls eliminate these blind spots. By authorizing every service action, validating technician identity, logging all remote access, and verifying systems before they go back into production, you dramatically reduce the chance of sabotage, mistakes, or misconfigurations.

The result is lower downtime, fewer emergency service calls, stronger audit posture, and predictable operations. This is the case even when multiple vendors or OT systems are involved. In short, MA protects both your uptime and the integrity of the systems that keep your factory running.



# MAINTENANCE

1	Authorization	Draft IR Plan; define roles and contact tree.
2	Secure Remote Access	Enable 24x7 alerting from EDR and SIEM.
3	Containment	Isolate infected devices, block malicious IPs.
4	Eradication	Clean systems and reset credentials.
5	Recovery	Restore Validated Backups.

**Required Evidence:** A complete, traceable maintenance workflow earns full points for controls 3.7.1–3.7.6.

## Audit Expectations

**Auditors will look for clear evidence that all maintenance, whether it is internal or vendor-performed, is authorized, logged, and monitored.**

They'll review maintenance records, remote-access logs, technician identities, and proof that systems were validated before returning to production. Expect them to sample vendor sessions, request screenshots or SIEM entries, and verify that no unapproved tools or devices ever touched systems that handle CUI.

Full credit is earned when maintenance activities follow a repeatable, documented workflow with complete traceability.

## Procurement Decision

If your environment relies on multiple vendors, complex OT systems, or frequent remote servicing, managing maintenance controls internally becomes difficult and error-prone.

In these cases, partnering with an MSP that provides controlled remote access, session recording, vendor management, and maintenance documentation is the most secure path.

Smaller organizations with limited vendor activity may handle maintenance in-house, but once CUI systems or production equipment are involved, outsourced support ensures consistent enforcement, clean audit trails, and significantly reduced downtime risk.

607-415-3151



www.micro-solutions.net



Require vendors to use your remote-access tool so every maintenance session is logged and auditable.





# MEDIA PROTECTION

## Executive Summary

**Data isn't just digital. Flash drives, external hard drives, laptops, printed drawings, backup tapes, and even PLC configuration files often contain CUI, and all of them can physically leave the building.**

Media Protection controls ensure that sensitive data can't "walk out the door," get misplaced in a toolbox, or end up in a recycling bin.

MP establishes strict rules for how removable media is labeled, stored, encrypted, transported, and ultimately destroyed. It governs who is allowed to handle CUI-bearing media, how it must be tracked, and what protections must be in place when it moves between systems, facilities, or vendors.

In manufacturing environments where physical workflows intersect with digital systems, strong media controls prevent accidental exposure, insider risk, and unauthorized data duplication.

Done well, Media Protection creates a closed-loop system that keeps CUI contained—no matter where it lives or how it moves.

## Regulatory Background

NIST 800-171 controls 3.8.1 through 3.8.9 define how organizations must handle CUI-bearing media. These requirements cover media access restrictions, proper marking and labeling, secure storage, controlled transport, encryption for digital media, and approved sanitization or destruction methods. Together, they ensure that any device or physical item containing CUI is protected throughout its entire lifecycle all the way from creation to disposal.

## Business Impact

Media losses are some of the most costly and preventable security failures. A single misplaced flash drive, unencrypted laptop, or discarded printout can trigger a reportable CUI breach, regardless of how strong your digital security tools are. For manufacturers, this can mean contract disruption, mandatory disclosures, insurance complications, and regulatory scrutiny.

Strong media protection eliminates these silent risks. By controlling who can handle removable media, enforcing encryption, tracking where CUI-bearing items go, and ensuring proper disposal, you prevent data from slipping beyond your security perimeter. The result is fewer accidental exposures, reduced insider risk, and a dramatically lower chance of facing the fines, downtime, or reputational damage that follow a physical data loss. Media Protection keeps CUI contained in the real world; not just the digital one.



# MEDIA PROTECTION

1	Media Access	Limit Portable media use to authorized staff; disable USB ports by policy	GPO Settings
2	Encryption	Require BitLocker or hardware-encrypted drives	Drive inventory
3	Labeling	Mark CUI Media "CUI- Confidential Do Not Copy"	Photos
4	Storage	Lock in cabinets or safes with access logs	Log Sheets
5	Transport	Use secure courier or encrypted transfer	Shipping Records
6	Disposal	Shred or degauss; document serial numbers	Disposal Certificate

Full points are awarded when media is consistently controlled from creation to disposal, with documentation that matches real-world handling.

## Audit Expectations

**Auditors expect complete traceability for any media that contains CUI.**

They'll review access restrictions, labeling practices, encryption settings, and storage locations for removable media, backup drives, printed documents, and portable devices.

Full points are awarded when media is consistently controlled from creation to disposal, with documentation that matches real-world handling.

## Internal Training & Changes

**Combine technical USB-blocking with policy training.**

Micro Solutions enforces media restrictions through endpoint management and manages encrypted backup rotation for disaster recovery and compliance.

## Case Example

### U.S. Department of Defense – Lost USB Drive Exposing Sensitive Data (2017)\*\*

In 2017, a U.S. military contractor found an unmarked USB flash drive in a public parking lot near an Air Force base. When plugged in, it contained highly sensitive drone surveillance footage and mission logs. The data traced back to a contractor employee who had copied CUI onto personal media to "work from home."

#### The incident triggered:

- A full security investigation
- Mandatory breach reporting
- Contract reviews
- Revocation of classified system access
- Updated media-handling procedures across the contractor's division

**This case is now used in federal training materials as a textbook example of how improper media control, not hacking, can expose critical information.**

Micro Solutions - How We Standardize Your Environment

We deploy MFA & conditional access in Azure AD, enforce SSO for apps, and provide password-policy reporting for audit evidence.

# PERSONNEL SECURITY

## Executive Summary

**Technology can only secure so much. The rest comes down to the people who access, manage, and support your systems.**

Personnel Security ensures that individuals with access to CUI and critical infrastructure are trustworthy, properly vetted, and removed promptly when they no longer need that access. It establishes the human guardrails around your environment: background screening, role-based access, onboarding and offboarding controls, and continuous monitoring for behavior that may pose risk.

In manufacturing environments where turnover, contractors, and shift-based work are common, weak personnel controls can create invisible gaps (lingering accounts, excessive privileges, or unvetted individuals touching sensitive systems). Strong PS practices close these gaps before they become security incidents.

By ensuring the right people have the right access at the right time, Personnel Security reduces insider risk, strengthens audit posture, and protects the integrity of both IT and OT systems across the plant floor.

## Regulatory Background

NIST 800-171 controls 3.9.1 and 3.9.2 define the core requirements for Personnel Security. These include verifying individuals before granting them access to CUI and ensuring access is immediately revoked when employment ends or roles change. The standard also requires organizations to maintain clear onboarding and offboarding processes, document personnel screening requirements, and monitor for changes that may impact a user's trustworthiness.

These controls ensure that only authorized, vetted individuals can access sensitive information throughout their employment lifecycle.

## Business Impact

**Typical risk scenarios in a plant environment:**

- A disgruntled employee who is about to be let go quietly copies design files or customer lists.
- A contractor with "temporary" access remains in your Active Directory long after their engagement ends.
- A machine operator leaves the company, but their shared login remains on the shop-floor PC.

These aren't theoretical; auditors see them constantly. And more importantly: primes and insurers care. A strong personnel security program signals that you take insider risk seriously.

**For CMMC Level 2, this isn't optional HR "nice-to-have" – it's part of your security architecture. One poorly managed termination or unchecked contractor can undo millions of dollars of controls.**

# PERSONNEL SECURITY

1	HR	Define positions that require background checks (any CUI access).	Job Descriptions, policy
2	HR + Legal	Select Screening Criteria.	Background Check
3	Hr + IT	Tie account creation to HR onboarding; no account without HR-approved record.	Onboard Checklist
4	Hr + IT + MAnager	Build offboarding checklist that includes account disablement, badge return, and exit interview.	Completed Checklists
5	Compliance	Use secure courier or encrypted transfer.	Shipping Records

**Important:** Personnel security isn't just pre-employment checks. It's a lifecycle: vet → onboard → manage → offboard.

## Audit Expectaions

**Auditors will typically ask for:**

- A formal Personnel Security Policy describing background checks, access authorization, and offboarding.
- Sample background check records (sanitized).
- Completed onboarding/offboarding checklists including IT access.
- Evidence that terminated employees' accounts are promptly disabled.

**They are looking for consistency:** do you do the same thing every time, or only when someone remembers?

## Procurement Decision

### In-House vs MSP Help

- **HR Process Design** – Almost always internal; this is about company culture and legal risk.
- **Account Lifecycle Automation** – Often easier with an MSP, who can integrate identity management with HR systems and ticketing tools.

**Micro Solutions' typical model:**

HR owns the policy; we make sure access control, MFA, and account lifecycle technically match that policy and are provable to an auditor.

### Integration & Scoring

If 3.9.1 or 3.9.2 are missing, you can lose 3–5 points each.

More importantly, findings here often cascade into other domains (Access Control, Identification & Authentication) because "account not disabled" shows up multiple times.

# PHYSICAL PROTECTION

## Executive Summary

**Physical Protection is everything that stands between your systems and the outside world:** doors, badges, cameras, visitor logs, locked cabinets, and controlled access points.

If CUI is stored or handled anywhere in your facility, even on a single workstation, physical safeguards become just as important as firewalls or antivirus software.

A stolen laptop, an unlocked networking closet, or an unescorted visitor on the shop floor can compromise data just as quickly as a cyberattack.

Effective physical security ensures only authorized people can reach sensitive areas, prevents tampering, deters insider threats, and creates a clear record of who enters high-risk zones. In practice, this means badge access for restricted rooms, cameras that actually retain footage, locked server racks, and a real visitor check-in process, not a clipboard that gets ignored.

Physical protection isn't just about blocking intruders. It creates accountability, prevents accidental exposure, and establishes a controlled environment where CUI can safely exist. In short: if someone can walk up and touch the device that holds your data, cybersecurity alone won't save you.

## Regulatory Background

Physical Protection maps directly to NIST SP 800-171 controls 3.10.1 – 3.10.6, which define how organizations must restrict physical access to systems, equipment, and environments that handle CUI.

**These controls require manufacturers to:**

- 3.10.1 – Limit physical access to systems, equipment, and environments.
- 3.10.2 – Protect and monitor physical facilities.
- 3.10.3 – Escort and monitor visitors.
- 3.10.4 – Maintain audit logs of physical access.
- 3.10.5 – Control physical access devices (keys, cards, codes).

Under CMMC 2.0, these same requirements appear in the Physical Protection (PE) domain at Level 2, which is the required level for any business processing Controlled Unclassified Information. The DoD's goal is to ensure that CUI is protected not only from remote attacks, but also from theft, tampering, or unauthorized viewing inside the facility.

Auditors will look for documented policies, consistent physical controls, and clear evidence that access is restricted, monitored, and recorded. If a facility allows uncontrolled foot traffic, shared workspaces with unlocked devices, or unlogged visitors, it will not meet the regulatory standard, regardless of how strong the cybersecurity is on paper.

All of those can result in CUI exposure without any computer being hacked. And if there's a breach investigation, physical protections are scrutinized.

# PHYSICAL PROTECTION

## Business Impact

### Consider a few real-world scenarios:

- A server closet in a production area that's left unlocked "for convenience."
- A maintenance vendor wandering unescorted through offices where CUI printouts sit on desks.
- Facility keys that never get reissued, even after an employee departure or a theft.

**None of these involve a hacker breaking into your network**, yet each can expose CUI just as easily as a phishing email or ransomware attack. Physical weak points are often the simplest paths for data to walk out the door.

And when a breach investigation happens, physical protections are examined right alongside firewalls, logs, and policies. Investigators look at who had access, whether doors were locked, whether visitors were supervised, and whether sensitive areas were properly controlled. If those basics aren't in place, even the strongest cybersecurity tools can't compensate.

### Try Verkada (Our Security choice) for Free

Join tens of thousands of organizations worldwide and experience the benefits of Verkada's hybrid cloud system firsthand, at no cost to you.

In just 10 minutes, our devices are online and fully operational. Best of all? Verkada offers unlimited user seats so you can share the benefits of our modern solution with anyone in your organization.

Get started with a free trial by scanning the QR code or visiting [verkada.com/try](https://verkada.com/try)

#### Your 30-day free trial includes

- Brand-new Verkada device
- 24/7 support via phone, chat, or email
- Full access to Command software
- Pre-paid return shipping label



# PHYSICAL PROTECTION

## Video Security

A Wide Range of Options  
to Meet Any Need

[Watch Demo](#)

See how Verkada provides the most scalable, actionable, and easy-to-use video security solution on the market.





# PHYSICAL PROTECTION

## A Modern and Secure Unlock Experience

Keep your existing readers and cards, or upgrade to modern credentials. Either way, Verkada helps increase security and provides a seamless unlock experience.

- Mobile NFC in Apple Wallet
- Customizable Bluetooth via the Verkada Pass app
- Encrypted keycards and fobs
- License plate unlock
- PIN codes



# PHYSICAL PROTECTION

1	Facility Access	Use badges or keys with documented issuance; restrict CUI areas.	Badge-issuance Records
2	Visitor Mangement	Require sign-in, ID check, escort, and visible badges.	Visitor logs
3	Server & Network Rooms	Locked doors, limited keys, monitored cameras.	Access Logs & Cam Footage
4	Workstations	Auto-lock screens; physically secure devices; cable locks where needed.	GPO Config Photos
5	Physical Tokens	Maintain logs for keys, access cards, and codes; revoke when staff depart.	Key card inventory

Augmenting this with Verkada cloud video and access-control platforms gives real-time, searchable evidence for audits.

## Audit Expectaions

**Auditors will want to verify that your physical protections actually work in practice;not just on paper.**

**Expect them to:**

- Walk the facility to observe how people move through production areas, offices, and restricted zones.
- Inspect server rooms, wiring closets, and storage areas to confirm they are locked, monitored, and limited to authorized personnel.
- Review visitor logs, badge reports, and access-control records to ensure you can account for who entered sensitive areas and when.
- Evaluate camera coverage, retention periods, and monitoring practices to confirm you're able to detect and respond to physical security events.
- Check for unsecured workstations, unlocked cabinets, or CUI left in plain sight, especially in mixed-use spaces or shared work areas.

If an auditor can walk straight into a server room, find a networking closet unlocked, or observe unescorted visitors moving freely through the building, you should expect findings. Physical protection is one of the fastest domains to fail. This is not because the requirements are complicated, but because gaps are easy to see with your own eyes.

**Full points are awarded when media is consistently controlled from creation to disposal, with documentation that matches real-world handling.**

## Case Example

In a well-known FBI case involving U.S. Steel, attackers were able to break in after exploiting weak physical and access controls at a smaller contractor's facility. That foothold let them move deeper into connected systems and steal valuable production data. A single supplier with poor physical security created risk for the entire chain, which turned a small gap into a major breach.

# RISK ASSESSMENT

## Executive Summary

Risk Assessment is the steering wheel of your security program. It forces you to map out the terrain: **What could go wrong? How likely is it? How bad would it be? And what should we fix first?**

Instead of reacting to whatever pops up next, risk assessment gives you a structured way to prioritize.

It identifies which weaknesses pose real threats to your contracts, operations, and reputation, and which ones are low-impact distractions.

Without a formal risk assessment, you're flying blind. You end up buying tools, adding controls, and deploying software without knowing whether any of it meaningfully reduces risk. Many manufacturers overspend in some areas, neglect others, and still end up vulnerable because the work wasn't guided by a clear understanding of their true exposure.

Risk assessment provides direction. It connects your business objectives with your security decisions, ensuring every dollar and every hour is spent on the controls that actually protect CUI, prevent downtime, and keep you eligible for DoD work. In short: it's not just paperwork. It's the difference between guessing and managing your risk with intent.

## Regulatory Background

Risk Assessment maps to NIST SP 800-171 controls 3.11.1 – 3.11.3 and forms a mandatory part of CMMC Level 2. These controls require organizations to regularly assess risks to CUI, document potential threats and vulnerabilities, and update security measures based on those findings.

**The DoD expects manufacturers to maintain a living risk register, track mitigation efforts, and use assessment results to guide security priorities.**

Without documented, repeatable risk assessments, organizations cannot meet NIST 800-171 or achieve a passing CMMC Level 2 audit.

## Business Impact

Effective risk assessment helps manufacturers focus effort where it counts. By identifying which threats could disrupt production, expose CUI, or jeopardize contracts, you can prioritize fixes that deliver real protection.

It also improves decision-making: leadership gains clarity on what needs action now versus what can wait. Insurers and primes see documented risk assessments as signs of maturity, often leading to better underwriting and stronger customer confidence.

In short, risk assessment reduces surprises, lowers overall business risk, and keeps your compliance strategy aligned with real operational needs.

Looking for a free baseline assessment?

SCAN ME



# RISK ASSESSMENT

## Procurement Decision

- Internal teams may run the day-to-day monitoring.
- An external partner is extremely useful for initial baseline, documentation, and ongoing “audit readiness.”

**Micro Solutions commonly serves as “CMMC program manager” for manufacturers:** we maintain the SSP/POA&M, coordinate assessments, and coach clients through interactions with C3PAOs and primes.

## Implementation Blueprint

### 1. Define Scope

- Include all systems that store, process, or transmit CUI.
- Map dependencies: ERP, MES, CAD systems, file servers, cloud platforms.

### 2. Identify Threats & Vulnerabilities

- Threats: ransomware, insider misuse, misconfigurations, physical theft, supplier compromise.
- Vulnerabilities: unpatched systems, weak passwords, shared accounts, unsupported OS, single points of failure.

### 3. Assess Likelihood & Impact

- Likelihood: Rare, Unlikely, Possible, Likely, Almost Certain.
- Impact: Low, Moderate, High, Critical.
- Score: e.g., 1–5 for each, multiply for a composite risk score.

### 4. Prioritize & Plan Mitigation

- Anything “High” or “Critical” gets a specific mitigation action with a due date  
-> added into the POA&M.

### 5. Document & Review

- Produce a Risk Register.
- Present top risks to management.
- Review at least annually and after significant incidents.

CMMC expects a structured risk assessment at least annually, plus after significant changes (e.g., major system upgrades or mergers).



### QUICK TIPS

Weight risks by control inheritance. A single weak control—like access reviews or logging—can cascade across multiple domains. Fixing one inherited control often eliminates several high-impact risks at once and yields the biggest SPRS score gains with the least effort.

# SECURITY ASSESSMENT

## Executive Summary

**Security Assessment is the oversight mechanism that ensures your entire security program actually works.**

While the other pillars establish controls, CA verifies they are implemented correctly, functioning as intended, and improving over time. It transforms cybersecurity from a set-and-forget checklist into a measurable, ongoing discipline.

This pillar requires organizations to perform scheduled reviews, vulnerability scans, internal audits, and control evaluations against NIST 800-171. It also includes identifying gaps, documenting findings, and maintaining a POA&M so weaknesses are tracked and remediated with clear ownership.

For manufacturers, this is crucial because environments change quickly. New equipment is added, software evolves, vendor access shifts, and production systems are updated. Without routine assessment, gaps emerge quietly until an auditor or attacker exposes them. A strong CA program gives leadership visibility into what is working, what is not, and what needs to be fixed. It keeps your compliance efforts accountable and ensures your security posture continues to mature in a predictable, controlled way.

## Regulatory Background

NIST 800-171 controls 3.12.1 through 3.12.4 set the requirements for Security Assessment. These controls mandate regular evaluation of implemented safeguards, documented POA&M tracking, scheduled risk reviews, and defined monitoring activities.

Together, they ensure organizations are not simply putting controls in place but are actively verifying their effectiveness and addressing weaknesses on a routine basis. Continuous assessment is a core expectation of CMMC and a key indicator of a mature and reliable security program.

### How Micro Solutions Fits In

Micro Solutions commonly serves as "CMMC program manager" for manufacturers:

We maintain the SSP/POA&M, coordinate assessments, and coach clients through interactions with C3PAOs and primes.

# SECURITY ASSESSMENT

## Business Impact

**Security Assessment gives you a clear picture of what is actually happening inside your environment, not what you assume is happening.**

In most organizations, controls work well on day one but begin to drift as people, processes, and systems change. New machines are added, old ones are repurposed, permissions pile up, and vendors connect systems without always updating documentation. Over time, these small changes compound into meaningful risk.

CA interrupts that drift. It reveals when a firewall rule has been quietly overwritten, when a dormant account still has access to production data, or when a system has not received updates in months. These findings shape real business decisions: which equipment to refresh, where to allocate budget, which vendors to trust, and how to prioritize remediation so production stays reliable.

For manufacturing leaders, the value is simple. Regular assessments reduce uncertainty. They replace guesswork with evidence, help forecast impacts before they reach the plant floor, and prevent auditors or attackers from discovering weaknesses first. The result is fewer surprises, clearer priorities, and a security program that improves with each cycle rather than slowly falling behind.

## Integration & Scoring

**Security assessment is the central nervous system of CMMC:**

- It pulls in findings from Access Control, Risk, Incident Response, etc.
- It drives your SPRS score and contract eligibility.

Engaging a skilled MSP or adding a vCISO style consultant here can often raise a manufacturer's score by 20–40 points over 12–18 months simply by organizing and maintaining evidence properly.

(Micro Solutions can often do this in a fraction of that timeline).

## Case Example

**A shop owner thought they were “about 80% compliant.” Before we did a formal security assessment:**

- Only ~50 controls were fully implemented and provable.
- ~30 were partially implemented.
- The rest were not addressed.

Their realistic SPRS score was +9, not the estimated +80. Over the next year, through a structured POA&M, we helped them reach +83—unlocking eligibility for several new DoD programs.

# SECURITY ASSESSMENT

## Audit Expectations

**Auditors will typically ask for:**

- A formal Security Assessment Policy that outlines how and when assessments are performed.
- Recent internal assessment reports that show what was tested and what was found.
- A current POA&M with clear ownership, timelines, and remediation progress.
- Vulnerability scan results and evidence that findings were reviewed and acted on.
- Documentation of monitoring activities, such as log reviews or control checks.

**They are looking for consistency:** do you assess your controls on a defined schedule, record the results, and follow through on remediation every time, or only when someone remembers?

## Procurement Decision

**Organizations with limited security staff often struggle to run assessments, manage POA&M items, and conduct regular vulnerability scans on their own.**

If you lack in-house expertise or do not have someone who can dedicate time to reviewing controls and tracking remediation, partnering with an MSP or security firm is the more reliable option. External support provides structured assessments, independent verification, and documentation that holds up during audits.

Smaller environments may manage internally, but once you handle CUI or operate mixed IT and OT systems, outside assistance ensures your assessments are accurate, your findings are prioritized, and nothing critical is overlooked.

## Implementation Blueprint

### 1. Baseline Self-Assessment

- Map yourself against all 110 NIST 800-171 controls.
- Mark each as Implemented, Partially Implemented, Not Implemented.

### 2. Build and Maintain the SSP

- For each control: describe how it is implemented, who owns it, and what evidence exists.
- Keep this current; treat it like a living system blueprint.

### 3. Create a POA&M

- For every gap, add an entry: control ID, issue, mitigation action, owner, target date, risk level.

### 4. Ongoing Security Assessments

- Quarterly mini-assessments on high-risk controls.
- Annual full reassessment to update SSP and POA&M.

### 5. Management Oversight

- Present progress and updated scores to the executive team.
- Use this to justify budget decisions.



# SYSTEM & COMMUNICATIONS PROTECTION

## Executive Summary

**System and Information Integrity protects your environment from the threats that slip through the cracks.** While firewalls and access controls defend the perimeter, SI focuses on what happens inside your network: detecting suspicious behavior, blocking known threats, correcting corrupted files, and ensuring systems stay healthy and trustworthy.

System and Information Integrity protects your environment from the threats that slip through the cracks. While firewalls and access controls defend the perimeter, SI focuses on what happens inside your network: detecting suspicious behavior, blocking known threats, correcting corrupted files, and ensuring systems stay healthy and trustworthy.

This pillar brings together a collection of safeguards that work continuously in the background. It covers antivirus and endpoint protection, automated patching, malicious code detection, network monitoring, and alerts that notify your team when something looks wrong. In a manufacturing setting, where outdated devices, legacy software, and OT systems often coexist with modern IT, these controls make the difference between a minor anomaly and a full production outage.

Strong SI practices ensure that issues are identified early, addressed quickly, and prevented from spreading across the environment. The result is a more stable operation, fewer surprises during audits, and greater confidence that the data guiding your business decisions is accurate and uncompromised.

## Regulatory Background

NIST 800-171 controls 3.12.1 through 3.12.4 set the requirements for Security Assessment. These controls mandate regular evaluation of implemented safeguards, documented POA&M tracking, scheduled risk reviews, and defined monitoring activities.

Together, they ensure organizations are not simply putting controls in place but are actively verifying their effectiveness and addressing weaknesses on a routine basis. Continuous assessment is a core expectation of CMMC and a key indicator of a mature and reliable security program.

**If your environment still looks like “everything on one big LAN,” expect findings and scoring penalties.**

# SYSTEM & COMMUNICATIONS PROTECTION

## Business Impact

System and Communications Integrity protects the accuracy and reliability of the data that drives your business. When patches fail, malware slips through, or files change unexpectedly, the impact reaches far beyond IT. Production schedules drift, engineering files become untrustworthy, and operators lose confidence in the systems they rely on every day.

Strong SC controls stop these issues before they reach the plant floor. Timely updates reduce vulnerability windows. Malicious code detection prevents downtime caused by infected workstations or compromised HMIs. Integrity monitoring ensures that CNC programs, PLC configurations, and engineering drawings remain unaltered and reliable.

For manufacturers, the result is fewer re-runs, less scrap, more predictable production, and stronger confidence that the information feeding your processes is correct. SC does more than secure your systems. It protects product quality, operational stability, and the trust your customers place in your output.

**Micro Solutions frequently redesigns manufacturer networks to meet these requirements.**



## Audit Expectations

**Auditors will typically ask for:**

- A documented System and Communications Protection Policy that describes how flaws are identified, patched, and monitored.
- Evidence of timely patching, such as update logs or vulnerability scan reports.
- Samples of endpoint protection alerts and how they were reviewed.
- Records showing malicious code was detected, quarantined, and resolved.
- Logs from monitoring tools that track abnormal activity or unauthorized changes.
- Documentation proving systems with CUI receive updates and integrity checks on a defined schedule.

**They are looking for proof that issues are caught early and handled consistently.**

If patches are delayed, alerts are ignored, or integrity checks are not performed, they will treat SC controls as partially or not implemented.

## Procurement Decision

Most organizations can manage basic patching and antivirus tools on their own, but SC becomes difficult to handle internally once you support mixed IT and OT environments or operate on a fast production schedule. Keeping up with software updates, reviewing alerts, responding to endpoint detections, and monitoring for abnormal behavior requires time and expertise that many teams do not have.

If you lack a dedicated security analyst or struggle to patch systems consistently, partnering with an MSP is the safer choice. An outside provider can manage patch deployment, monitor threat alerts, and ensure integrity checks run on CUI systems without disrupting production. Smaller environments may stay in-house, but once you introduce legacy OT equipment, shared workstations, or dozens of endpoints, external support helps maintain stability and reduces the chance of downtime caused by missed updates or overlooked threats.

# SYSTEM & COMMUNICATIONS PROTECTION

## Implementation Blueprint

### 1. Network Segmentation

- Split corporate, engineering, and production networks into separate VLANs.
- Control traffic between them using firewalls and access rules.

### 2. Secure Remote Access

- Require VPN with MFA for all remote connections.
- Prohibit direct inbound RDP or vendor-specific tunnels without oversight.
- Use jump servers or secure remote-access gateways for OT vendors.

### 3. Encrypt Communications

- Enforce TLS for web interfaces and email.
- Use S/MIME or other encryption for email with CUI.
- Disable legacy, unencrypted protocols where possible.

### 4. Boundary Monitoring

- Deploy IDS/IPS on the perimeter and critical internal chokepoints.
- Log and alert on weird traffic (e.g., big data transfers, unusual ports).

### 5. Protect Management Traffic

- Separate network management interfaces from user networks.
- Limit access to firewall and switch management to admin VLANs.

Integrity failures rarely explode. They erode. And erosion is expensive.

## Case Example

**A machining company believed they were in good shape.**

Updates ran “**most of the time**,” the antivirus dashboard was mostly green, and no one had complained recently. Everything seemed fine.

**Until production slowed down.**

CNC programs began loading a little slower. Then a little more. Operators blamed the network. Supervisors shrugged it off. Three days later, lines were behind schedule.

**When IT finally dug in, they found the problem in minutes:** a piece of malware quietly tampering with temporary files and consuming CPU cycles. No ransomware, no alerts screaming for attention. Just a slow integrity leak.

The real shock was how long it had been there.

**Twenty-seven days.**

All the warning signs had already fired:

- One unresolved EDR alert
- Five failed patches
- A PLC configuration file that changed unexpectedly

Each one was dismissed. Together, they formed the incident.

The IT TEam deployed SC controls and uncovered 30+ unresolved alerts, seventeen missed patches, and several altered engineering files. The impact added up to nearly 100 lost labor hours.

Once automated patching and real alert monitoring were in place, downtime incidents dropped 74 percent in the next quarter.

# SYSTEM & INFORMATION INTEGRITY

## Executive Summary

**System and Information Integrity ensures your environment can detect, correct, and prevent the kinds of issues that undermine trust in your systems.**

SI focuses on identifying flaws, applying updates, blocking malicious code, monitoring for abnormal activity, and protecting the accuracy of the data your business relies on. It is the early warning system of your security program.

For manufacturers, this matters because most incidents begin quietly. A failed update, a suspicious process, a corrupted file, or a strange login attempt often appears long before a full breach or production outage. Without SI controls in place, these early indicators are easy to miss. With SI in place, they become visible signals your team can investigate before they spread.

Strong integrity controls keep systems healthy, data reliable, and operations stable. They ensure vulnerabilities are patched on time, malware is contained quickly, and unexpected changes are detected before they affect quality or production. SI protects the environment from slow degradation and silent failures that cost more than any single high-profile attack.

## Regulatory Background

NIST 800-171 controls 3.14.1 through 3.14.7 define the requirements for System and Information Integrity. These controls require organizations to identify and correct system flaws in a timely manner, deploy security updates, detect and respond to malicious code, monitor systems for abnormal or suspicious activity, and protect the integrity of critical files and configurations. They also require organizations to receive and act on security advisories so new vulnerabilities are addressed quickly. Together, these practices ensure systems remain stable, trustworthy, and capable of resisting both known and emerging threats.

## Business Impact

System and Information Integrity protects the quality of the data and the reliability of the systems your business depends on. When flaws go unpatched or suspicious activity goes unnoticed, small issues grow into slowdowns, corrupted files, rework, and equipment that behaves unpredictably. **(See Domain 13!)**

Strong SI practices stop these problems early. Timely patching closes vulnerabilities, malicious code detection prevents spread, and integrity monitoring alerts your team when files or configurations change in ways that affect quality or safety. For manufacturers, this means less downtime, fewer rejected parts, and greater confidence in the systems that support production.

**SI strengthens security, stabilizes operations, and protects the trust your customers place in every job you deliver.**



[www.micro-solutions.net](http://www.micro-solutions.net)

607-415-3151



CALL US  
NOW



# SYSTEM & INFORMATION INTEGRITY

## Audit Expectations

**Auditors will typically ask for:**

- A documented System and Information Integrity Policy that explains how flaws are identified, patched, and monitored.
- Evidence of timely patch deployment, such as update histories or vulnerability scan results.
- Samples of malicious code alerts and how they were handled.
- Logs that show monitoring for unusual activity or unauthorized changes.
- Proof that systems containing CUI receive updates and integrity checks on a defined schedule.

**They want to see that issues are found quickly and addressed the same way every time, not only when someone notices a problem.**

## Procurement Decision

Organizations can usually manage basic patching and antivirus tools internally, but SI becomes challenging once you support mixed IT and OT systems or operate on tight production schedules. Missed updates, unreviewed alerts, or unnoticed configuration changes can create risks that internal teams may not have the time or expertise to catch.

If your environment includes legacy equipment, shared workstations, or dozens of endpoints, partnering with an MSP is the more dependable option. External support ensures patches are applied consistently, alerts are monitored in real time, and integrity checks are performed without disrupting production. Smaller organizations may stay in-house, but once CUI systems are involved, dedicated monitoring and timely remediation become essential for stability and compliance.

### Quick Self-Assessment: Are Your Integrity Controls Working?

**Ask yourself these three questions:**

1. Can we prove when every system was last patched, and were any updates missed?
2. If you are guessing, SI controls are not fully implemented.
3. Do we review endpoint alerts every day, or only when something breaks?
4. Infrequent review is one of the biggest sources of silent compromise.
5. Would we know immediately if a CNC program, PLC configuration, or engineering file changed unexpectedly?
6. If the answer is no, integrity monitoring is incomplete.

**If any of these questions create hesitation, your SI maturity is likely below CMMC expectations and may not prevent early-stage incidents.**



**QUICK  
TIPS**

**Set patching deadlines based on risk, not convenience. High-severity updates should install within hours, not on the next monthly cycle. This prevents attackers from exploiting known flaws before you have a chance to react.**

# CONCLUSIONS

**Learning the 14 pillars is only half the journey. The harder part is turning each concept into something your team can actually run day after day.**

It is one thing to understand Access Control or Incident Response. It is something very different to build a routine, collect evidence, and make sure those controls hold up in an audit without slowing down production.

The easiest way to think about CMMC is to treat it like a manufacturing process plan. You start by understanding the materials, mapping the flow, choosing the right tools, and creating a repeatable process that produces consistent quality. Compliance follows the same pattern: know what is in scope, decide how you will protect it, and build a workflow that creates the evidence you need.

Micro Solutions will soon release a full CMMC Implementation Guide, along with additional free resources to help DIB manufacturers put this into practice with less friction. What follows is a preview of that larger playbook, designed to give you clear direction without overwhelming your team.

Everything begins with understanding your scope. Before you fix gaps, you must know where CUI enters your business, where it goes, and which systems, applications, and workstations it touches on the way to the shop floor. Most organizations discover their true CUI footprint is wider than expected simply because no one has ever mapped it.

Once you trace the flow, you can outline the boundary of your CMMC environment. This is where you decide what is in scope, what is out, and which systems sit on the edge. Being deliberate here prevents you from securing equipment that never touches CUI in the first place, and it keeps your compliance effort focused on what matters.

## **Two simple rules help anchor this step:**

1. A system is in scope if it stores, processes, or transmits CUI.
2. A system can be excluded only if you can clearly prove it never interacts with CUI in any way.

With the boundary defined, you capture it inside your System Security Plan (SSP). This becomes the master blueprint. Auditors study it first because it explains the logic behind your decisions and the structure of your environment.

From here, you move into the gap assessment, which compares your current practices to the 110 controls of NIST 800-171. The goal is not to pass or fail. The goal is to understand your starting point. Some controls will already be solid, some will need refinement, and some will need to be built from the ground up.

During this phase, evidence matters. A control only counts if you can prove it exists through screenshots, logs, training records, or policy excerpts. Many teams underestimate this step. They know they are doing the work, but without documentation, the auditor has nothing to verify.

**Once you understand your baseline, you can begin turning your findings into a real plan and moving your organization toward audit readiness.**

# CONCLUSIONS

**With your gaps identified, the next step is turning everything you've learned into a functioning security program.**

This begins with refining your System Security Plan. The SSP is not a formality. It is the document that explains how your security controls actually work in daily operations. Auditors read it first because it tells them whether you understand your own environment and why you made certain decisions.

A good SSP describes your systems, boundaries, and how each requirement is implemented. It should feel like a guided walkthrough, not a technical maze. Each control needs a short explanation, the responsible owner, and the location of supporting evidence. When written clearly, the SSP becomes the backbone of your entire program. After building the SSP, you shift to your POA&M. This is the plan that converts findings into action. Each gap becomes a task with an owner, a timeline, and a clear description of what needs to be corrected. A well-managed POA&M keeps your compliance work steady and prevents anything from slipping through the cracks. Many organizations say this step brings the most clarity because it turns a long list of weaknesses into a structured project plan.

Then comes implementation. This is where controls turn into routine behavior. Some items are technical, like enabling MFA, tightening firewall rules, or deploying EDR. Others are administrative, such as creating policies, defining onboarding steps, or documenting access reviews. And some are simply operational: reviewing logs, locking restricted areas, or recording maintenance activities. Over time, these small actions build the muscle memory auditors expect to see.

Different companies take different paths here. Some do everything internally. Others rely heavily on an MSP. Most choose a hybrid model, where internal staff manage culture and day-to-day decisions while the MSP handles monitoring, patching, backups, alerts, evidence collection, and ongoing tuning. This blended approach usually provides the best long-term balance for manufacturers.

As implementation continues, evidence becomes your quality control system. Controls only matter if you can prove they exist. Screenshots, logs, tickets, sign-in sheets, and training acknowledgments all serve as validation. The key is consistency. Collect evidence as you go, not all at once during an audit rush. Store it in a simple structure that mirrors the 14 CMMC domains so you can retrieve anything within seconds.

## **Two reminders help teams stay organized:**

1. Evidence must be backed up somewhere secure and versioned.
2. Each file name should clearly tie back to a control so nothing is ambiguous.

By the time you complete these phases, your environment is taking shape. Controls are working, habits are forming, and you have the documentation to prove it.

**The final step is becoming audit-ready, maintaining compliance, and turning everything you've built into a predictable rhythm.**

# CONCLUSIONS

**Once your controls are implemented and your evidence is organized, the final step is preparing for the audit itself.**

Audit readiness is less about technical skill and more about consistency. A good way to test your maturity is to run a mock audit internally. Pick a handful of controls, pull the SSP, gather the evidence, and answer questions as if a C3PAO were sitting across the table. This simple exercise exposes gaps long before an auditor arrives.

Your SPRS score should be recalculated at this stage as well. As controls improve and evidence builds, your score will rise. Submitting an accurate score is important, especially if prime contractors ask for updates or validation. A stable score supported by clear documentation signals to partners that your environment is under control.

Team preparation also matters. Everyone who interacts with CUI or in-scope systems should know what role they play during an audit. Some will answer technical questions. Others will escort the auditor through the facility. Others will provide screenshots or policy references. When individuals know exactly what to expect, the entire process runs smoother and feels less stressful.

Once your internal review looks strong, you can finalize your documentation, confirm that the SSP and POA&M match the evidence you've collected, and either submit your self-assessment or schedule with a C3PAO. Most manufacturers are ready for a self-assessment in four to six months. Full audit readiness may take six to twelve months depending on scope, staffing, and the condition of your systems at the start.

The last phase is ongoing operations. Compliance is not something you "finish." It becomes a rhythm built into the way you work. Monthly vulnerability scans, quarterly control reviews, routine updates to the SSP and POA&M, and an annual management review keep your program aligned with the reality of your environment. Manufacturing changes constantly. Your documentation must change with it.

When done well, the benefits go far beyond passing an audit. Mature programs reduce downtime, improve insurance eligibility, increase customer trust, and open the door to contracts that were previously out of reach. The work pays off both operationally and financially.

Micro Solutions will continue supporting DIB manufacturers through this process. In the coming months, we will release a full CMMC Implementation Guide, a library of templates, evidence checklists, policy starter kits, and additional free assets that make the compliance journey achievable for organizations of all sizes. This book gives you the foundation. The next wave of resources will help you turn that foundation into a durable, reliable program.

**Your compliance journey does not end here. It begins here.  
Let Micro Solutions walk the rest of the path with you.**



607-415-3151







# Managed vCISO

Retain an executive-facing resource who acts as an extension of your staff – managing your security strategy, budget, and cyber risk programs.

► *Help your business make security decisions, understand security threats, and optimize security processes. Become cyber resilient.*

## Strategic Cyber Advisory

- Swiftly performs initial risk & infosec program review to identify quick wins while building long-term roadmaps for lasting resilience.

## Risk Intelligence

- Expertly synthesizes the risk landscape with a business approach to provide boards and executive teams with clarity on cyber decisions.

## Governance

- Drives accountability throughout your organization by building consensus to ensure teams are working together to move cyber initiatives forward.

## Performance Management

- Verifies internal technical teams and vendors, such as MSP/MSSP, are providing services as required and meeting SLA commitments.

## Audit Support

- Provides guidance for audits, including security executive representation, advisory, auditor interface, and supervisory function for evidence gathering.

**Access proven  
top-tier cyber  
leadership.**

**Our vCISO team  
is battle tested;  
having run cyber  
programs with  
clear success.**



607-415-3151



**CALL US  
NOW**



# Managed vCISO

## Services and Deliverables

- ▶ Defined, regular touchpoints and value-packed deliverables are the cornerstone of how your vCISO ensures the success of your cyber program.
- ▶ In addition to the items below, your vCISO will also provide ad-hoc security memos, security guidance for business teams, and security operations advisory.

### vCISO Packages

#### Entry

#### Shared

#### Managed

- ▶ Cyber Risk SaaS App License
- ▶ InfoSec Program Management
- ▶ Develop Incident Response Policy
- ▶ Advise on Business Continuity Plan
- ▶ Annual Risk Assessment and Roadmap

- ▶ Baseline Policies

- ▶ Annual Policy-to-Controls Alignment

- ▶ Compliance/Regulatory Advisory
- ▶ Managed Risk Register

- ▶ Auditor Interface

- ▶ Onboarding Fee

- ▶ Compliance Support Model

- ▶ Program Management Cadence

- ▶ Strategic Audit and Analysis Report

- ▶ Cyber State-of-the-Union / Board Report



Applicable

None

Monthly

Monthly



Applicable

Shared

Bi-weekly

Monthly

Addl. Cost



Waived

Managed

Weekly

Monthly

Annual



[www.micro-solutions.net](http://www.micro-solutions.net)

607-415-3151



CALL US  
NOW

# APPENDIXES

## Appendix: Sample Incident Response Plan (IRP)

### How to Use This Resource

This sample Incident Response Plan is provided as a basic starting point for manufacturers beginning their CMMC journey. It outlines the minimum structure and core activities expected in a compliant IR program. Every organization should customize this plan to their own environment, systems, roles, and business processes.

#### Disclaimer:

This IRP is an example template, not a complete or legally sufficient plan. Your final IRP should be tailored to your technology stack, operational requirements, and contract obligations under DFARS, NIST 800-171, and CMMC. Micro Solutions can help you build a fully aligned, auditable version based on your environment.

### Sample Incident Response Plan

#### 1. Purpose

This Incident Response Plan defines how the organization detects, reports, analyzes, contains, eradicates, and recovers from cybersecurity incidents. Its purpose is to minimize operational disruption, protect CUI, preserve evidence for audits and insurance, and ensure timely communication with leadership, partners, and regulators.

#### 2. Scope

##### This plan applies to:

- All employees, contractors, and vendors
- All systems handling business data or CUI
- All production, OT, and IT assets (workstations, servers, CNC controllers, PLCs, cloud systems, etc.)

#### 3. Incident Definitions

##### An "incident" includes any of the following:

- Suspicious logins or credential misuse
- Malware, ransomware, or EDR alerts
- Unauthorized access to CUI
- Unexplained outages or system instability
- Loss or theft of devices
- Misconfigurations that expose sensitive data
- Alerts from SIEM, EDR, firewall, MDR/MSSP tools
- Any employee may report an incident through the designated IR channel.

# APPENDIXES

## Appendix: Sample Incident Response Plan (IRP)

### 4. Roles & Responsibilities

Incident Response Lead (IRL)

- Coordinates the entire response
- Authorizes containment and recovery actions
- Communicates status to leadership

IT / Security Team

- Investigates alerts
- Preserves forensic evidence
- Executes containment and remediation tasks

Operations Manager

- Manages impact on production
- Approves or schedules downtime windows

Communications Lead

- Handles all messaging
- Coordinates external notifications

Executive Sponsor

- Oversees legal, financial, and insurance obligations
- Approves major decisions (shutdowns, disclosures, etc.)

### 5. Incident Response Phases

#### Phase 1 — Preparation

- Maintain updated IR plan and contact lists
- Conduct annual tabletop exercises
- Ensure SIEM, EDR, and logging are active and monitored
- Validate backup integrity (3-2-1 strategy)

#### Phase 2 — Identification

Goal: Determine whether the event is an actual incident.

**Actions:**

- Review alerts from SIEM/EDR/firewall
- Validate suspicious authentication attempts
- Check for unauthorized changes or OT anomalies
- Assign severity (Low / Medium / High / Critical)
- Notify IR Lead

#### Phase 3 — Containment

Goal: Limit impact and prevent spread.

**Short-term actions:**

- Isolate affected endpoints
- Disable compromised accounts
- Block malicious IPs/domains
- Capture volatile evidence

Long-term actions:

- Apply patches
- Reset compromised credentials
- Strengthen firewall and conditional access rules

# APPENDIXES

## Appendix: Sample Incident Response Plan (IRP)

### Phase 4 — Eradication

Goal: Remove the root cause.

#### Actions:

- Remove malware/persistence mechanisms
- Delete rogue or unused accounts
- Patch exploited vulnerabilities
- Validate no lateral movement remains

### Phase 5 — Recovery

Goal: Restore systems safely.

#### Actions:

- Restore from backups if required
- Reconnect validated systems to the network
- Monitor SIEM/EDR for recurrence
- Coordinate with Operations before resuming production

### Phase 6 — Lessons Learned

Goal: Improve defenses and close gaps.

#### Within 72 hours of closing the incident:

- Document a full timeline
- Update IR procedures and access controls
- Add new SIEM detections
- Review findings with leadership

### 6. Evidence Collection Requirements

Preserve the following for audits, insurance, and legal purposes:

- SIEM and firewall logs (30 days minimum; 1 year recommended)
- EDR alerts, file hashes, and timelines
- Screenshots and packet captures
- User activity surrounding the event
- List of affected systems and accounts

Store evidence in a secured, access-controlled repository.

### 7. Communication Requirements

#### Internal

- IT/Security Team — Immediately
- Operations Manager — Within 30 minutes
- Executive Sponsor — Within 1 hour

#### External (If Required)

- Cyber insurer
- Customers or partners
- Regulatory bodies (DFARS, CMMC, state breach laws)
- Law enforcement (only with Executive approval)

No employee may communicate externally without authorization.

# APPENDIXES

## Appendix: Sample Incident Response Plan (IRP)

### 8. Severity Levels

- **Critical:** Production halted; CUI exposure; ransomware active
- **High:** Confirmed unauthorized access; malware detected
- **Medium:** Suspicious activity requiring investigation
- **Low:** Benign or false-positive activity

Severity dictates escalation and documentation depth.

### 9. Contact List (Example)

**IR Lead:** John Smith – (555) 123-4567

**Security Analyst:** Sarah Johnson – (555) 987-6543

**Operations Manager:** Bill Martinez – (555) 321-7890

**Executive Sponsor:** CEO – (555) 111-2222

**Cyber Insurance Hotline:** 1-800-###-####

**MSSP / SIEM Provider:** Micro Solutions SOC – (555) 444-8888

### 10. IR Plan Review

- Updated annually or after significant incidents
- Stored in digital and printed format
- Distributed to IR team and relevant leaders

### Closing Statement: How to Use Your Incident Response Plan

An Incident Response Plan is only valuable if it's practiced, updated, and understood by the people who need it most. Treat this plan as a living document—review it annually, test it through tabletop exercises, and refine it whenever your tools, staff, or environment change.

During a real incident, no one should be guessing about their role or searching for the next step. A well-maintained IR plan turns chaos into coordination, protects production, preserves evidence for audits and insurance, and gives leadership the confidence that your team can respond quickly and effectively. The goal isn't just to recover—it's to recover smarter every time.

# APPENDIXES

## Appendix: Table Top Exercise Playbook

### How to Use This Tabletop Guide

This playbook is designed to help your team practice your Incident Response Plan before an actual security event occurs. A tabletop exercise is a guided, low-pressure simulation where your staff walks through a realistic cyber incident step-by-step. The goal isn't to "win"—it's to reveal blind spots, strengthen communication, and confirm that everyone understands their role.

#### This guide provides:

- A clear structure for running an effective tabletop
- Roles and responsibilities during the exercise
- A realistic scenario tailored for manufacturing environments
- Injects (new information) that force decision-making
- Questions to evaluate your readiness
- A debrief template you can use to improve your IR plan

#### Disclaimer:

This is a baseline tabletop playbook. Every organization should adapt the scenario, severity, and response steps to match their own systems, staffing, and operational dependencies. Micro Solutions can facilitate advanced, multi-scenario tabletops with live log reviews, OT/IT crossovers, and attacker simulation.

### Tabletop Exercise Overview

#### Purpose

To evaluate the organization's ability to detect, assess, contain, respond to, and recover from a cybersecurity incident while following the documented Incident Response Plan.

#### Duration

60–90 minutes

#### Participants

- Incident Response Lead
- IT / Security Team
- Operations Manager
- Communications Lead
- HR / Legal (optional)
- Executive Sponsor

#### Materials Needed

- Printed or digital IR Plan
- Network diagrams
- SIEM/EDR alert examples
- Contact lists
- This playbook



# APPENDIXES

## Appendix: Table Top Exercise Playbook

### Roles During the Tabletop

#### Facilitator

Guides the exercise, presents injects, and keeps time.

#### Scribe

Captures decisions, questions, timing, gaps, and needed improvements.

#### Players

Respond as they would during a real incident, following their assigned IR roles.

#### **Scenario:** Suspicious Lateral Movement in Manufacturing Network

A workstation on the production floor shows signs of abnormal authentication attempts. OT machines dependent on this workstation for file dispatch begin to lag. A malware alert appears shortly after.

#### **This scenario evaluates:**

- Detection
- Escalation
- Communication
- Containment
- Evidence handling
- Decision-making under time pressure





# APPENDIXES

## Appendix: Table Top Exercise Playbook

### Inject Timeline (Facilitator Script)

#### Inject 1 — 9:00 AM

**EDR Alert:** "Suspicious Credential Use — Multiple Failed Logins from CNC-WS-14."

Operators report slow file transfers to CNC machines.

#### Discussion Questions:

- Who receives the alert?
- What initial checks are performed?
- Do you escalate yet? If so, how?

#### Inject 2 — 9:10 AM

**SIEM Log:** Successful login from the same workstation using an admin account not typically used on the production floor.

#### Discussion Questions:

- Is this now an incident?
- Who gets notified (IR Lead, Operations Manager)?
- Do you isolate the workstation? What's the impact?

#### Inject 3 — 9:20 AM

Production complains one CNC is frozen mid-job. Supervisor asks whether to stop the line.

#### Discussion Questions:

- Who authorizes production stoppage?
- How do you communicate with Operations?
- What alternatives exist to avoid full shutdown?

#### Inject 4 — 9:30 AM

**New Evidence:** Malware hash detected matching a known lateral movement tool.

#### Discussion Questions:

- What containment actions occur now?
- Do you disable accounts? Which ones?
- How do you preserve forensic data?

# APPENDIXES

## Appendix: Table Top Exercise Playbook

### Inject 5 — 9:45 AM

Cyber insurance requires notification within one hour of suspected breach.

#### Discussion Questions:

- Who makes the call?
- What info must be included?
- Who controls external communication?

### Inject 6 — 10:00 AM

IT identifies a shared credential used on multiple CNC workstations.

#### Discussion Questions:

- Does this impact eradication?
- What long-term corrective action comes from this?
- How is the credential rotated and validated across devices?

### Technical Decision Points

#### During the simulation, the team must address:

- Network isolation strategy
- Account lockdown processes
- Evidence preservation requirements
- Backup validation if recovery is needed
- Communication channels during downtime
- OT/IT handoff and safety considerations

### Success Criteria

#### Your team should be able to:

- Identify the incident quickly
- Escalate following the IR plan
- Communicate internally and externally with clarity
- Isolate affected systems with minimal disruption
- Preserve evidence (logs, captures, timestamps)
- Restore operations from a known-good state
- Document everything for audits and insurers
- Provide leadership a timeline and summary

# APPENDIXES

## Appendix: Table Top Exercise Playbook

### Debrief & Lessons Learned Template

After completing the tabletop, spend 20–30 minutes debriefing.

#### 1. What Went Well?

- 

#### 2. What Delayed or Confused Response?

- 

#### 3. Evidence Gaps Identified

- 

#### 4. Communication Gaps Identified

- 

#### 5. Technical Gaps (Tools, Access, Logging)

- 

#### 6. Policy or Documentation Gaps

- 

#### 7. Improvements to Implement (Next 30 Days)

- 

#### 8. Improvements to Test in Next Tabletop

- 

### Closing Note

Tabletop exercises only work when they're repeated. Run this scenario annually at a minimum—and ideally incorporate variations such as insider misuse, OT malware, or vendor-related compromise. Each session strengthens your IR readiness, tightens your audit posture, and ensures your team can respond with confidence when a real incident occurs.