Securing Acumatica for ITAR, CMMC & FedRAMP Compliance

How Defense Contractors and Aerospace Firms Can Deploy ERP Without Creating Compliance Risk

Executive Summary: ERP Is Now a Compliance Decision

Defense contractors, aerospace manufacturers, and government suppliers are facing three converging pressures:

- **ITAR (International Traffic in Arms Regulations)**
- **CMMC 2.0 cybersecurity requirements**
- **FedRAMP-aligned cloud expectations**

Modernizing your ERP system is no longer just an operational upgrade.

It is a compliance exposure decision.

The wrong ERP deployment can:

- Trigger export violations
- Cause CMMC audit failure
- Expose Controlled Unclassified Information (CUI)
- Disqualify government contracts
- Reduce enterprise valuation during M&A
- The right deployment embeds compliance directly into your daily operations.

Can Acumatica Meet ITAR and CMMC Requirements?

This is the wrong question:

"Is Acumatica ITAR compliant?"

The right question is:

"Can Acumatica be deployed and governed in a way that meets ITAR, CMMC, and FedRAMP requirements?"

Answer: Yes—but only with the right architecture, configuration, and governance.

Compliance is not built into software by default.

Compliance = Infrastructure + ERP Configuration + Security Policy + Ongoing Oversight

What Makes an ERP System ITAR and CMMC Compliant?

To meet ITAR and CMMC requirements, your ERP system must support:

- Controlled access to sensitive data (U.S. persons only)
- Strong identity and authentication controls (MFA, SSO)
- Full audit logging and traceability
- Secure handling of Controlled Unclassified Information (CUI)
- Data residency and infrastructure compliance
- Process-level enforcement (not just IT policies)

If these controls are not enforced inside the ERP, your compliance posture is weak—regardless of your hosting provider.

ERP Deployment Options for FedRAMP-Aligned Environments

Acumatica can be deployed in:

- Microsoft Azure Government
- AWS GovCloud
- Other compliant cloud environments
- Properly secured on-premise infrastructure

However, here's where companies get it wrong:

- **FedRAMP-certified infrastructure does NOT make your ERP compliant.**

It only provides a foundation.

- **Compliance depends on how your ERP is configured, secured, and managed.**

Key ERP Security Risks for Defense Contractors

Most compliance failures don't come from infrastructure.

They come from ERP-level misconfiguration.

Common Risk Areas:

- Overly broad user access permissions
- Lack of role-based security enforcement
- No audit trail or log retention
- Weak authentication controls
- Shared environments exposing unnecessary data

If user access is not tightly governed inside the ERP, audit failure is a matter of time—not possibility.

ITAR Compliance Inside the ERP: Where Risk Actually Lives

Many organizations misunderstand ITAR risk.

It's not just about shipping exports.

ITAR risk lives inside your ERP system, including:

- Bills of Material (BOMs)
- Engineering change control
- Technical documentation

- Inventory and part classification
- User access to regulated data

ERP-Level ITAR Controls Must Include:

- Regulated item classification
- Commodity jurisdiction tracking
- Engineering change logging
- Denied party screening
- Data location restrictions
- Encryption of sensitive data
- Record retention policies
- This is especially critical for:
- Aerospace manufacturers
- Aviation MRO organizations
- Defense subcontractors
- Hybrid commercial/defense companies

CMMC 2.0 Requirements and ERP System Design

CMMC Level 2 and Level 3 focus heavily on:

- Access control
- Identification and authentication
- System integrity
- Auditability
- Data protection

ERP Must Support:

- Role-based access control (RBAC)
- Azure AD or identity provider integration
- Multi-factor authentication (MFA)
- Single sign-on (SSO)
- End-to-end encryption
- Continuous monitoring

If your ERP does not enforce these controls, your CMMC readiness is compromised.

Where Most Companies Miscalculate ERP Compliance

Across the industry, we see the same assumptions:

- "We're in the cloud, so we're compliant."
- "Our hosting provider handles security."
- "We passed a self-assessment, so we're covered."
- "ITAR only applies to shipping."

This is operational blindness.

Compliance is not a checkbox—it is a system of controls embedded in your ERP.

How to Architect a Compliant Acumatica Deployment

A compliant ERP deployment requires a **governance-first approach**:

1. Architecture Review

- Validate cloud environment (GovCloud, Azure Gov)
- Confirm data residency requirements

- Define segmentation strategy

2. Role & Access Modeling

- Restrict access to U.S. persons where required
- Implement role-based permissions
- Map users to controlled access groups

3. Compliance Workflow Integration

- Embed denied party screening
- Track engineering changes
- Maintain audit-ready documentation

4. Policy Integration

- Store ITAR/export compliance plans
- Track training and certifications
- Define incident response workflows

5. Ongoing Monitoring

- Continuous audit log review
- Access control validation
- Security assessments and updates

Common ERP Failures That Break CMMC Compliance

These are the most frequent causes of audit failure:

1. Admin rights granted too broadly
2. MFA not enforced across all users
3. Logs not retained or reviewed

4. No documented system baseline
5. Shared environments exposing data
6. No formal access review process

These are not technical failures—they are governance failures.

Executive Risk: Why This Matters to CFOs and CEOs

This is not just an IT issue.

It directly impacts:

- **Contract eligibility**
- **Enterprise valuation**
- **Audit defensibility**
- **Cyber insurance exposure**
- **Regulatory liability**

Your ERP system becomes the **compliance backbone of the business**.

If it is misconfigured, the entire organization is exposed.

Executive Checklist: Questions You Should Be Asking

Before or during ERP modernization:

- Where is our ERP physically hosted?
- Can foreign persons access controlled data?
- Is our system aligned with NIST 800-171?
- Are regulated items classified within our ERP?
- Do we track engineering changes tied to compliance?

- Can we pass a CMMC audit today?
- Can we respond to a DDTC inquiry with confidence?

If these answers are unclear, your ERP strategy needs adjustment.

FAQ: Acumatica, ITAR, and CMMC Compliance

Is Acumatica ITAR compliant?

Acumatica can support ITAR compliance, but only when deployed with proper access controls, data governance, and security architecture.

Can Acumatica meet CMMC Level 2 requirements?

Yes, when configured with strong identity management, audit logging, encryption, and role-based access controls aligned with NIST 800-171.

Does FedRAMP certification make an ERP compliant?

No. FedRAMP-certified infrastructure provides a foundation, but ERP compliance depends on configuration, governance, and operational controls.

What is the biggest ERP compliance risk?

Uncontrolled user access and lack of auditability inside the ERP system.

Final Thought: Flexibility Without Governance Creates Risk

Acumatica is flexible enough to support regulated industries.

But without disciplined implementation:

Flexibility becomes exposure.

Call to Action

Build Your ERP the Right Way—From Day One

If you're evaluating ERP in a regulated environment, the most important decision isn't the software.

It's how it's deployed and governed.

Here's what happens next:

- A senior ERP compliance specialist reviews your situation
- We determine if your requirements align with our expertise
- If it makes sense, we schedule a focused 30-minute conversation
- No generic demos. No pressure. No obligation.