Securing Acumatica for ITAR, CMMC & FedRAMP

Industry: Defense Contractors
Primary Persona: CEO, CFO, VP of Operations
Sales Stage: Discovery / Pre-Demo

Executive Overview

Defense, aerospace, and government contractors face three converging pressures:

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

Modernizing ERP is no longer just an operational upgrade.
It is a compliance exposure decision.

The wrong deployment model can:

- Create export violations
- Trigger CMMC audit failures
- Expose Controlled Unclassified Information (CUI)
- Reduce acquisition valuation
- Disqualify government contracts

The right deployment model embeds compliance into daily operations.

The Strategic Question

It's not:

> *"Is Acumatica ITAR compliant?"*

It's:

> *"Can our Acumatica deployment be architected, governed, and monitored in a way that supports ITAR, CMMC, and FedRAMP requirements?"*

That distinction matters.

> *Compliance is achieved through **deployment architecture, configuration discipline, and governance controls**, not by default software settings*

1. Deployment Environment Matters

Acumatica can be deployed in:

- Microsoft Azure for Government
- AWS GovCloud
- Other compliant environments
- Properly secured on-prem infrastructure

The cloud provider's certification (FedRAMP High, etc.) is foundational — but it does NOT make the ERP automatically compliant.

Compliance = Infrastructure + Configuration + Policy + Oversight

2. Access Control is the Core Risk Area

CMMC Level 2 and 3 emphasize:

- Access control
- Identification & authentication
- Auditability
- System integrity
- Azure AD integration
- Role-based security

- MFA
- SSO
- End-to-end encryption

Acumatica Compliance

For executives, the takeaway:

If user access isn't governed at the ERP layer, you have audit risk.

3. ITAR-Specific ERP Controls

The ITAR section identifies several ERP-level requirements

Acumatica Compliance

- Assembly-level management of regulated items
- Tracking commodity jurisdiction
- Engineering change control
- Denied party screening
- Data location restrictions
- End-to-end encryption
- License usage monitoring
- Record retention

This is critical for:

- Aerospace manufacturers
- Aviation MRO firms
- Defense subcontractors
- Hybrid commercial/defense manufacturers

ITAR risk is not just export shipping.
It lives in BOMs, technical documents, change control, and user access.