CMMC, CUI, FCA Compliance

To answer Isabel Wells (CIO) or an auditor, you must move beyond generic IT questions. You need questions that test **Governance**, **Scope**, and **Evidence**.
If you cannot answer these 4 questions about your documents (Word, Excel, PDF, Emails), you are likely non-compliant with CMMC and at risk of a False Claims Act violation.

Question 1: The "Inventory" Question (Scope)

"Can we definitively state where CUI *does not* exist in our unstructured file shares?"

- **The Trap:** Most companies can point to where data *should* be (e.g., "The Secure Engineering Drive"). Almost no one can prove it isn't sitting in "Mary's Desktop Folder" or "The Marketing Share Drive."
- **Why it Matters:** CMMC requires you to define a "boundary." If CUI is found outside that boundary (feral data), your entire "Scope" is false, making your certification void and your contract attestations fraudulent.
- **The Unstructured Risk:** A single PDF exported from SAP and emailed to a vendor breaks the boundary if not tracked.

Question 2: The "Access vs. Authorization" Question (Control)

"Is access to these documents controlled by *file attributes* (tags) or just by *folder location*?"

- **The Trap:** "We put all sensitive files in the HR Folder, and only HR has access."
- **The Failure Mode:** If an employee moves a sensitive file *out* of that folder to a public drive to work on it, the protection vanishes.
- **The Compliance Standard: NIST 3.1.3** requires you to control the flow of CUI. If the security doesn't travel *with* the document (e.g., via metadata labeling or encryption), you have lost control the moment the file moves.

Question 3: The "Evidence" Question (Audit)

"If a specific engineering drawing was leaked today, could we produce a log showing every individual who opened, printed, or emailed that specific file in the last 12 months?"

- **The Trap:** "We have logs of who logged into the *server*."
- **The Failure Mode:** Knowing who logged into the server is not enough. You must know who **touched the data**.
- **The Compliance Standard: NIST 3.3.1 (Audit & Accountability)** mandates that you trace actions to specific users. Without granular "file-level" auditing, you cannot prove to the DOJ that you were monitoring your data.

Question 4: The "Lifecycle" Question (Sanitization)
"When we delete a project folder containing CUI, is the data actually destroyed, or does it sit in a 'Recycle Bin' or backup tape for 7 years?"

- **The Trap:** "We hit delete."
- **The Failure Mode:** Unstructured data in backups is a massive liability. If you are hoarding CUI from 5 years ago that you no longer need, you are paying to protect liability.
- **The Compliance Standard: NIST 3.8.3 (Media Protection)** requires you to sanitize media containing CUI before disposal or reuse. "Deleting" isn't sanitizing.

Summary Slide for the CIO

The Question	The Compliance Risk	The Operational Fix
1. Where isn't it?	**False Scope:** If you miss one file, your "Secure Boundary" is a lie.	**Auto-Discovery:** Tools that scan *everything* to find the leaks.
2. Does security travel?	**Loss of Control:** Moving a file shouldn't break the security.	**Tagging:** Embed the "CUI" label into the file's DNA (Metadata).
3. Who opened it?	**No Evidence:** You can't defend against a lawsuit without a file log.	**Audit Trails:** Immutable logs for every click, print, and share.
4. Is it truly gone?	**Data Hoarding:** Protecting useless data costs money and adds risk.	**Retention Policy:** Automated "Defensible Deletion" based on contract end dates.

To uncover the real risk and drive urgency with Isabel Wells (CIO) and her leadership team, you need to move beyond technical questions ("Do you have a firewall?") and ask **Governance & Liability** questions.

Here are the critical questions to ask, categorized by the specific "Pain Point" they expose.

The "Golden" Question (The Opener)

"If the DOJ issued a subpoena tomorrow regarding a specific contract at Abaco Systems, could we produce the full 'Chain of Custody' for every CUI file associated with that project within 4 hours, or would it trigger a manual scramble?"

- *Why ask this:* It tests their "Evidence Readiness." A manual scramble = Audit Failure.

Category 1: The M&A "Inherited Risk" Questions

Targeting the acquisition strategy (Superior Tube lesson).

1. **"When Ametek acquires a new defense supplier, how do we currently scan their unstructured data (file shares, emails, desktops) for 'Toxic CUI' *before* we connect them to the corporate network?"**
   - *The Trap:* If they say "We don't," they are admitting they import liability blindly.
2. **"Do we have a standardized 'Day 1' data governance playbook for new acquisitions, or does every new business unit keep using their legacy systems for the first 12-24 months?"**
   - *The Trap:* Legacy systems are where compliance failures hide.

Category 2: The "False Affirmation" Questions

Targeting the Raytheon/Aerojet risk (Lying to get paid).

3. **"For high-volume divisions like Rotron, is the linkage between the Invoice (in SAP) and the Compliance Certification (in the security plan) automated? Or does the system allow us to send an invoice even if the underlying security controls are failing?"**
   - *The Trap:* If the system allows billing while non-compliant, they are actively committing False Claims violations.
4. **"How does the Senior Official who signs the annual CMMC affirmation verify the data? Do they rely on a verbal 'we are good' from IT, or do they have a dashboard showing real-time control validation?"**
   - *The Trap:* Verbal confirmation creates personal liability for the executive.

Category 3: The "Scope & Data" Questions

Targeting the "Feral Data" problem (CUI on desktops).

5. **"We know that 80% of CUI lives outside of SAP—in PDFs, emails, and CAD drawings. How are we currently ensuring that an engineer at Ametek SCP doesn't email a drawing to a supplier without encryption?"**
   - *The Trap:* This exposes the "User Behavior" gap that EIM solves.
6. **"How do we currently distinguish between 'Commercial Data' and 'Government Data' in our shared storage? Is it tagged automatically, or do we rely on employees to organize it correctly?"**
   - *The Trap:* Relying on employees is "Gross Negligence" in the eyes of the DOJ.

Category 4: The Audit Trail Questions

Targeting the Treble Damages defense.

7. **"Can we prove exactly *who* accessed a specific engineering drawing 18 months ago? Not just who had *permission* to see it, but who actually opened it?"**
   - *The Trap:* Permission $\neq$ Access Log. CMMC requires the log.
8. **"If a whistleblower claimed today that we ignored a security gap at Ametek PDS, what 'Immutable Evidence' do we have to prove we acted on it?"**
   - *The Trap:* Without an EIM audit trail, it is just their word against the whistleblower's.

Summary Checklist for the Workshop

If you get to the workshop, these are the 3 questions to write on the whiteboard:

1. **Where does the data live?** (Inventory)
2. **Who controls the data?** (Access)
3. **How do we prove it?** (Audit)