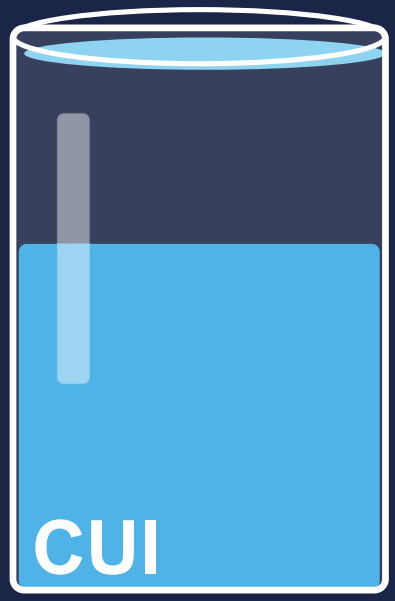
CMMC LEVEL 2 • ARCHITECTURE DECISION CONSIDERATIONS

Keep the Water in the Cup



Cloud, On-prem, Or Hybrid: Building the Right Containment Architecture for CUI.

Koren Wise, CMMC Lead Assessor and Instructor
CEO, Wise Technical Innovations • Authorized C3PAO

WTI.US – HOME OF "SPRS FRIDAY"

WISE TECHNICAL INNOVATIONS

Grounded in: 32 CFR Part 170 (§170.19 Scoping) • CMMC Scoping Guide Level 2 v2.13 • NIST SP 800-171 R2

The cup is the protective boundary that protects the data in all scenarios where your organization is accountable.

The name of the game is preventing unauthorized access to CUI. NIST SP 800-171 is fundamentally about preserving the confidentiality of CUI - everything else is mechanics.

1	**Where water enters**	How CUI is received, created, imported, or generated.
2	**Where it sits**	Systems, shares, databases, devices, paper, backups, logs.
3	**Where it flows**	People, tools, machines, subcontractors, cloud services.
4	**Where it must not go**	Personal email, unmanaged devices, broad enterprise IT.

Confidentiality

Whether the cup sits in a plant, an office, a home, or a hyperscale cloud is not the first question. The first question is whether the flow is understood and unauthorized access is prevented.

Source basis: NIST SP 800-171 R2 and 32 CFR Part 170 center on protecting the confidentiality of CUI.

ANATOMY OF THE CUP — §170.19(c)(1), TABLE 3

Five Asset Categories Decide What the Assessor Examines

CUI Assets	CAN Process, store, or transmit CUI. Can potentially hold the water.	*Assessed against all 110 requirements*
Security Protection Assets	Provide security functions to the scope: SIEM, firewall, MSP/SOC. Fortify the cup.	*Assessed for relevant capabilities*
Contractor Risk Managed Assets	Could hold water, but policy and practice keep them dry. Understand the attestation here – it's real. You are promising they don't get wet!	*SSP review; checked only if questions arise*
Specialized Assets	OT, IIoT, GFE, test equipment — CAN and often DO touch CUI, can't be fully secured.	*Inventory + SSP; risk-based management*
Out-of-Scope Assets	CANNOT touch CUI. Separated. KVM-only VDI endpoints qualify.	*Be ready to justify the separation*

Source basis: 32 CFR §170.19(c)(1) Table 3; CMMC Scoping Guide Level 2 v2.13.

WISE TECHNICAL INNOVATIONS

DECISION DISCIPLINE

One Template for Every Architecture Choice

Run cloud, on-prem, and hybrid through the same six questions. Nothing is good or bad: an architecture option either supports the DoW work or it doesn't.

1 CUI activity

What exact work creates, receives, uses, prints, stores, or sends CUI?

2 Asset category

Which asset category does it fit: CUI, SPA, CRMA, Specialized, or Out-of-Scope?

3 Containment

What stops the water: isolation, VDI, data boundary, DLP, physical control?

4 Operational fit

Can the business still produce, make, test, inspect, deliver, or consult? Does the architecture support the CUI flow needs.

5 Evidence story

Do the SSP, diagrams, inventory, and CRM tell one consistent story?

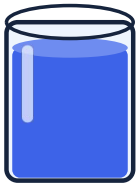
6 Residual risk

What is accepted, transferred, inherited, or engineered out?

The correct option is the one that supports the contract work and produces a defensible scoping story.

KNOW WHERE THE WATER FLOWS BEFORE YOU PICK YOUR CUP

Three DIB Archetypes, Three Common Flow Patterns

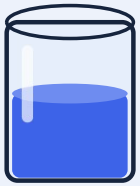


The Manufacturer

machine shop • aerospace parts • electronics

CUI must reach the shop floor: drawings become toolpaths, setup sheets, inspection data. CNC, 3D printing, and CMM gear can't run normal security agents. Workers pick parts and use kits with drawings to assemble.

CUI touches machines

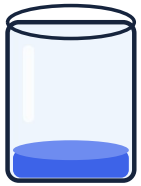


Professional Services

engineering • logistics • program support

CUI lives in documents, models, and email - created and exchanged daily from laptops. No physical process consumes it; highly portable to a cloud enclave.

CUI lives in documents



Read-Only Reference

e.g., QA verifying specs of parts sold

A few people must LOOK at CUI - a spec, a drawing - to do their job. They never author, manipulate, or create derivatives of it. View-only patterns keep almost everything out of scope.

CUI is only looked at

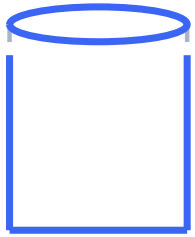
Source basis: Specialized Assets (OT, IIoT, GFE, test equipment) per Scoping Guide L2; VDI/KVM condition for out-of-scope endpoints.

WISE TECHNICAL INNOVATIONS

UNDERSTAND INHERITANCE

Sometimes You Buy the Cup; Sometimes You Build It

The same requirements apply in all four. What changes is how much of the cup already exists when you arrive.

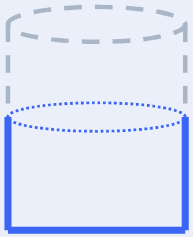


SaaS

Most of the cup is included

The platform, the patching, and the physical security arrive already built. You still own identity, sharing, and what gets poured in.

MOST INHERITED

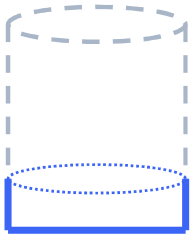


PaaS

A cup kit

The platform is hardened for you. The shape of the cup, meaning configuration, code, and data paths, is still yours to form and prove.

PARTLY INHERITED

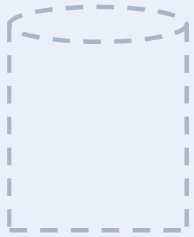


IaaS

Glass and a kiln

The provider secures the foundation. You form the cup yourself: OS, network, identity, monitoring, and all of the evidence.

LITTLE INHERITED



On-Prem

You blow the glass

Nothing arrives built. Every control is yours to implement, operate, and prove. Total control, and the total burden of evidence.

NOTHING INHERITED

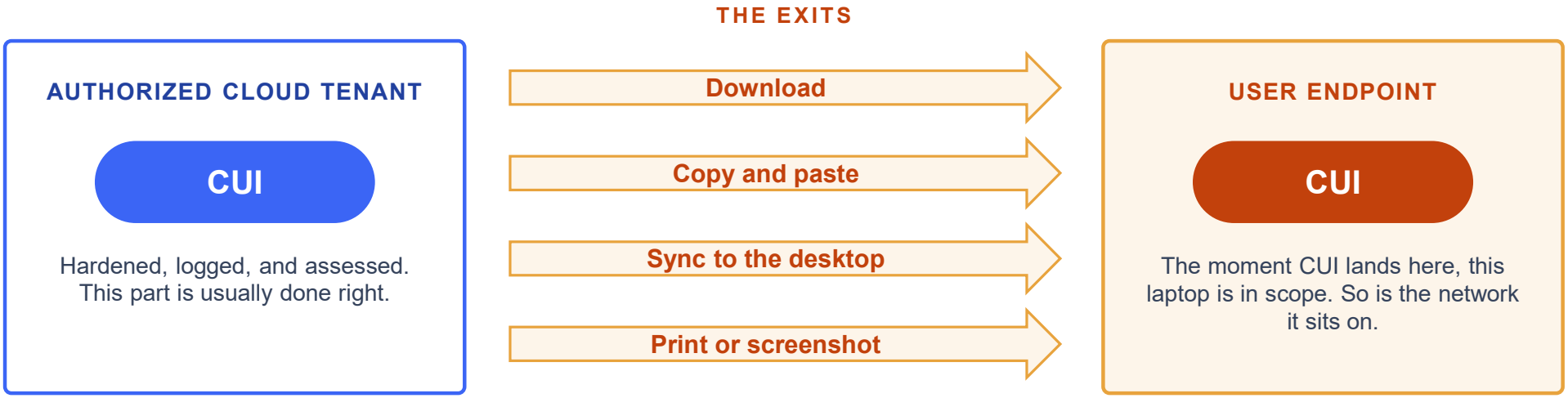
Solid = the provider built it

Dashed = you build it

ARCHITECTURE PATTERN 1 OF 4

Cloud Enclave: You do not Have an Enclave if the Data Can Leave

Plenty of companies believe they built a cloud enclave. The tenant is usually fine. The exits are what put the endpoint back in scope.



If a user CAN move the data out, the endpoint is in scope. That is a hybrid, not an enclave.

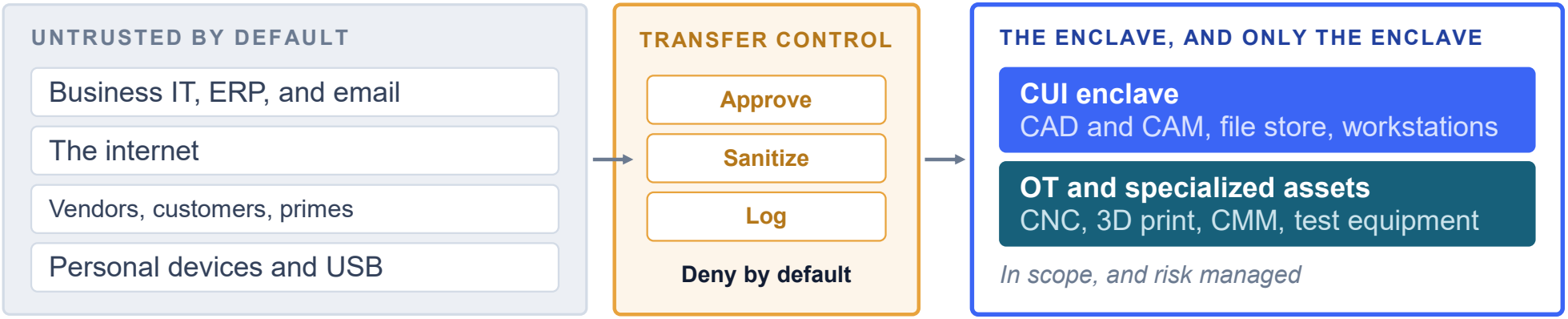
Close the exits
Block download, copy and paste, sync, and print. Then produce the evidence that they are blocked.

Or widen the scope
Leave them open and assess the endpoints too. There is no third option.

ARCHITECTURE PATTERN 2 OF 4

On-prem Enclave: Everything Outside the Line is Untrusted

You draw the boundary yourself, and you draw it around the machines. Nothing crosses it except on purpose.



WHY YOU WOULD CHOOSE THIS

A boundary you can walk

You drew the line, so you can point at it. An assessor can follow it end to end without taking anyone's word for it.

CUI reaches the machines

Toolpaths, build files, and scan data get to the shop floor using controlled and protected mechanisms.

Nothing to inherit or chase

No provider matrix to reconcile, no authorization to monitor, and no sunset date that somebody else controls.

The trade: inheritance is near zero. Every control inside that line is yours to implement, operate, and prove.

Source basis: Specialized Assets, meaning OT, IIoT, GFE, and test equipment, are in scope but risk managed per the Scoping Guide for Level 2.

ARCHITECTURE PATTERN 3 OF 4

On-prem Enterprise: The Whole Company is the Boundary

No enclave, no carve-out, everything in scope. On purpose that is cheaper than separating.

ONE BOUNDARY: THE ENTERPRISE

Everything below is in scope

- All users
- All endpoints
- All servers and apps
- All OT and specialized assets

WHAT SUCCESS LOOKS LIKE

Every asset is on one list

A single current inventory. Each asset has a category, an owner, and a reason it is there.

One baseline, few exceptions

The same hardened build on every workstation and server. Deviations are documented, approved, and rare.

Identity covers everyone

MFA and conditional access on every account. No shared logins, and no standing local admin you cannot explain.

Logging with no blind spots

Every in scope asset ships logs to one place, with retention you can show and alerts somebody actually reads.

No unmanaged corners

No personal device holding CUI, no shadow SaaS, no forgotten lab subnet. On the network means managed.

Evidence applies to enterprise

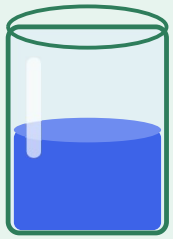
Diagrams, the SSP, and the POA&M are reflective of enterprise environment.

Success here is not a smaller scope. It is a scope you can prove, end to end, on any day of the year.

Source basis: asset categories and Specialized Asset treatment per the CMMC Scoping Guide for Level 2.

ARCHITECTURE PATTERN 4 OF 4

Hybrid: Two Cups, One Controlled Spout



Plant-floor cup

CNC • 3D print • CMM • build files
Limited local CUI - because the part needs it.

← →

CONTROLLED SPOUT
approved transfer • malware scan • logging • release gate

Cloud cup

collaboration • evidence • customer exchange
Authoritative source of truth, fully audited.

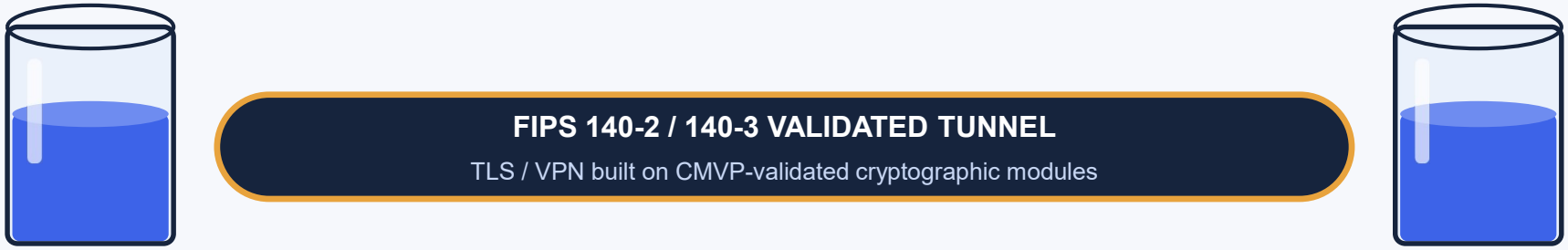
Does CUI have to touch the machine or printer?
If yes - design floor containment first.

Can the cloud be authoritative?
If yes - keep endpoints and OT as thin as possible.

Where is transfer decided?
Document the gate, the approver, and the evidence.

BETWEEN CUPS, WATER MUST NOT LEAK

The Tunnel is a Control: FIPS-Validated Encryption



Water in motion is still water — encrypt it, or it has already leaked.

What the rule requires

SP 800-171: protect CUI in transit (3.13.8) and employ FIPS-validated cryptography for CUI confidentiality (3.13.11). “Encrypted” is not enough — the module must be validated.

The one POA&M nuance

Under 32 CFR §170.21, CUI Encryption (SC.L2-3.13.11) may sit on a POA&M only if encryption IS employed but not yet FIPS-validated - and the POA&M closes within 180 days.

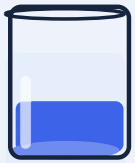
Where tunnels run

Cloud cup ⇄ plant cup. Enclave ⇄ home cup. Enclave ⇄ customer and supplier exchange. Enclave ⇄ CSP APIs. Every pipe between cups is in scope and on the diagram.

Source basis: NIST SP 800-171 R2, 3.13.8 & 3.13.11; 32 CFR §170.21 POA&M conditions; CMVP module validation.

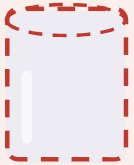
THE CUP TRAVELS

There Must be a Cup, Even in Alternate Workspaces – Small Cups are Welcome!



A home office is a small cup

If CUI is viewed or stored at home, the home is part of the flow the Scoping Guide treats remote work like any other location. So build a real cup there:



Some places can't hold a cup

Airports, hotels, coffee shops, personal email, consumer file-sharing: no boundary can be formed there. The answer is not a better lid - it is: don't pour.

The test never changes either a cup exists where the water goes, or the water must not go there. Important reminders:

- Managed endpoint only - no family PCs
- FIPS-validated VPN tunnel into the enclave
- No local copies, no home printing unless secured
- Screen privacy and paper discipline
- Stream pixels, not water: KVM-only VDI
- The water never lands on the device
- Endpoint can stay Out-of-Scope by rule, when architected properly
- No offline CUI for travel - plan the work

Source basis: Scoping Guide L2: remote/home locations with CUI are in scope; KVM-only VDI endpoints may be Out-of-Scope.

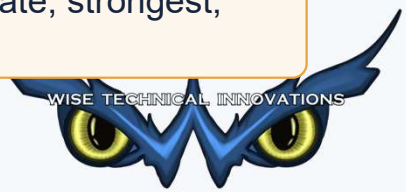
NOT PLATFORM MORALITY

Decision Points: Consider DoW Work when Choosing Cup

Mostly documents, reviews, evidence?	→ **CLOUD ENCLAVE**	*collaboration + auditability + inheritance*
CUI drives production, test, or inspection gear?	→ **ON-PREM FIRST**	*equipment containment before elegance*
Both lives - shop floor and collaboration?	→ **HYBRID**	*two cups, one controlled, encrypted spout*
Endpoint only ever sees pixels (KVM)?	→ **OUT-OF-SCOPE CANDIDATE**	*prove no local CUI - then it's not in the cup*

Wrong question: "Which architecture passes CMMC?" and easiest to sustain/explain?"

Right question: "Which cup is appropriate, strongest,



EVIDENCE STORY

What the Assessor Needs to Hear

A good architecture decision sounds boring, consistent, and provable.

1	**Boundary**	“Here is where CUI is allowed to exist - and nowhere else.”
2	**Asset treatment**	“Here is why each asset is CUI, SPA, CRMA, Specialized, or Out-of-Scope.”
3	**Inheritance**	“Here is what we implement - and what we inherit, exactly as the provider CRM says.”
4	**Operations**	“Here is how people and machines do real work without breaking the cup.”

Evidence package: SSP • asset inventory • network & data-flow diagrams (tunnels included) • CRM/CIS • policies & procedures • logs & transfer records

Source basis: Level 2 scoping requires SSP asset treatment, inventory, and network diagrams; CSP/ESP CRMs documented.

COMMON SPILLS

Five Ways Good Companies Leak

“We bought GCC High, so we're compliant”	The cup you bought still needs your lid: identity, sharing, endpoints, and a CRM story in the SSP. Inheritance is never abdication.
Enclave synced to unmanaged laptops	One consumer sync client quietly pours water onto every device it touches.
Forgotten paths	Print trays, screenshots, home devices, personal email - all part of the flow, all in the cup or all leaks.
Scoping the whole enterprise	A cup the size of the company is expensive, fragile, and impossible to narrate.
Wishing away Specialized Assets	CNC, 3D printers, CMMs must be inventoried and risk-managed in the SSP - invisible is not out-of-scope.

CLOSE

Build the Right Cup

CLOUD

best when CUI is documents, collaboration, evidence, remote work - and you want to buy most of the cup.

ON-PREM

best when CUI must touch production, test, or inspection equipment - and you must create the contained environment yourself.

HYBRID

best when both are true - two cups joined by a controlled, FIPS-validated spout.

The best CMMC architecture lets you do the DoW work without spillage, the strongest tunnels, and the clearest evidence story.

Key sources: 32 CFR Part 170 • CMMC Scoping Guide L2 v2.13 • NIST SP 800-171 R2 • NIST SP 800-160 V1/V2 (engineering guidance; V2R1 IBR'd for definitions) • provider compliance documentation