AC.L2-3.1.3

Access Control

Control CUI Flow

"Control the flow of CUI in accordance with approved authorizations."

Objectives

[a]
Information flow control policies are defined.

[b]
Methods and enforcement mechanisms for controlling the flow of CUI are defined.

[c]
Designated sources and destinations for CUI within the system and between interconnected systems are identified.

[d]
Authorizations for controlling the flow of CUI are defined.

[e]
Approved authorizations for controlling the flow of CUI are enforced.

Key Discussion Points

Flow vs. Access:
3.1.3 controls WHERE CUI travels — not just who can see it. A user authorized to access CUI may not be authorized to email it to an external address.

Map It First:
[c] requires identifying designated sources and destinations — without a data flow diagram, you cannot define authorizations or demonstrate enforcement.

Technical Enforcement:
[e] requires that approved authorizations are enforced — DLP, firewall rules, and proxy settings are the mechanisms. Policy alone does not satisfy [e].

Encrypt in Transit:
CUI traversing public networks must be encrypted — the flow authorization for internet-bound CUI requires encryption as a condition of the authorization.

Assessment Methods

EXAMINE

Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings; list of information flow authorizations; system baseline configuration; system audit logs and records.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developers.

TEST

Mechanisms implementing information flow enforcement policy.

AC.L2-3.1.3

ACCESS CONTROL — Control CUI Flow

Plain English

What this control is really saying:

3.1.3 is about WHERE CUI can travel, not just who can see it. Every path CUI can take — email, USB, cloud sync, firewall boundary — must be mapped, authorized, and technically enforced. If an engineer can forward a CUI drawing to personal Gmail, this control is not met regardless of what any policy document says.

How it is used:

- A data flow diagram in the SSP maps every path CUI travels — internal file shares, encrypted email to the prime, VPN for remote access — and identifies each authorized source and destination.
- DLP software scans outbound email and blocks CUI content from being transmitted to unauthorized external addresses.
- The perimeter firewall enforces allow/deny rules based on the flow authorizations documented in the SSP — only approved traffic between approved endpoints is permitted.
- CUI transmitted over the internet is encrypted — engineers use a designated secure file-sharing portal, not personal cloud storage or personal email.

Real World Example

The Scenario

Acme Defense receives CUI engineering drawings from its prime contractor via encrypted email. Files are saved to a shared network drive. Engineers frequently work from home and need access to the drawings. No data flow analysis has been performed.

What the assessor finds

Three engineers are emailing CUI drawings to their personal Gmail accounts to work from home. One engineer's personal laptop syncs the company file share to Dropbox. No DLP tool exists. No data flow diagram has been created. The SSP has no boundary definition or authorized flow listing.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Data flow diagram in SSP identifying all authorized CUI sources and destinations, DLP configured on email and endpoints, VPN required for remote access to CUI, personal cloud storage blocked, all internet-bound CUI transmission encrypted.

Common Gaps

What assessors actually find in the field:

✗ No data flow diagram

CUI flow paths have never been mapped — the organization does not know where CUI travels and cannot define authorizations for what it has not identified.

✗ Personal email in use

Engineers routinely forward CUI drawings to personal Gmail or Yahoo accounts to work from home — no DLP controls exist to detect or block this.

✗ No DLP enforcement

A policy prohibiting unauthorized CUI transmission exists on paper but nothing technically prevents it — policy without enforcement does not satisfy [e].

✗ Undefined boundary

The system boundary is not defined in the SSP — without a defined boundary, CUI flow cannot be controlled at the edges.

✗ Unapproved cloud storage

CUI files sync to personal Dropbox or Google Drive through endpoint cloud clients — no authorization was established for these flow paths.