CM.L2-3.4.8

Configuration Management

Application Execution Policy

"Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software."

Objectives

[a]

A policy specifying whether whitelisting or blacklisting is to be implemented is specified.

[b]

The software allowed to execute under whitelisting or denied use under blacklisting is specified.

[c]

Whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.

Key Discussion Points

Choose One, Document It:
Pick blacklisting or whitelisting, document the policy, and implement it — choosing nothing is not acceptable.

Whitelist Is Stronger:
Whitelist (deny-all, permitbyexception) is far more secure — attackers can always write new malware not yet on a deny list.

Define the List:
Whether whitelist or blacklist, the specific software must be enumerated — a vague policy without a named list does not satisfy [b].

Verify Integrity:
The guide recommends verifying whitelisted software via cryptographic checksums, digital signatures, or hash functions — not just filename.

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing least functionality; system security plan; configuration management plan; list of software programs authorized or not authorized to execute; security configuration checklists; review and update records for authorized/unauthorized software lists; system audit logs.

INTERVIEW

Personnel with responsibilities for identifying software authorized or not authorized to execute; personnel with information security responsibilities; system or network administrators.

TEST

Organizational process for identifying, reviewing, and updating authorized or unauthorized programs; process for implementing blacklisting or whitelisting; mechanisms supporting or implementing blacklisting or whitelisting.

CM.L2-3.4.8

CONFIGURATION MANAGEMENT — Application Execution Policy

Plain English

What this control is really saying:

Pick a lane: blacklist (allow everything except what's blocked) or whitelist (block everything except what's approved). Then document your policy, build your list, and technically enforce it. The guide is clear — whitelisting is the stronger choice and the direction most assessors will look for.

How it is used:

- Organization policy specifies whitelisting — only digitally signed, approved executables may run; AppLocker enforces this on all CUI workstations.
- The approved software list is maintained as a controlled document and reviewed quarterly — additions go through change control before AppLocker is updated.
- Any executable not on the whitelist is blocked automatically and generates an alert — the IT admin reviews all blocked attempts weekly.
- Integrity verification uses digital signatures — only publisher-signed software is added to the whitelist; unsigned executables require additional review.

Real World Example

The Scenario

Acme Defense relies on Windows Defender as its only software control. Users have local admin rights and can install any software they choose. Three users have installed personal file sync tools that connect to consumer cloud storage.

What the assessor finds

No application execution policy exists. No whitelist or blacklist beyond AV signatures has been implemented. Consumer cloud sync tools on three workstations are actively syncing files from the CUI network to personal accounts. No policy decision or list was ever documented.

SPRS Score Impact

3.4.8 carries a point value of 5. Uncontrolled program execution is how most malware, ransomware, and data exfiltration tools get a foothold — a whitelist is one of the most effective single controls a small DIB company can implement.

What Good Looks Like

Policy documented (whitelist or blacklist), approved/denied software list maintained and version-controlled, technical enforcement in place (AppLocker, GPO, or MDM), list reviewed quarterly, integrity verification for whitelisted software.

Common Gaps

What assessors actually find in the field:

✗ No policy defined

The organization has neither a whitelist nor a blacklist — no decision has been made and no list exists.

✗ Antivirus treated as blacklist

AV is present but the organization hasn't formally designated it as the blacklist mechanism or documented it as such.

✗ List exists but not enforced

An approved software list is documented but nothing technically prevents users from running unlisted software.

✗ List not maintained

A whitelist was configured a year ago but new software approvals are not being added — users are blocked from needed tools.

✗ No integrity verification

Whitelisting is implemented by executable name only — no hash or signature verification prevents renamed malware from running.