PREVEIL

WEBINAR

SSP Teardown: Would Yours Hold Up?

Today’s session and speakers

What we’ll cover

01 What an assessment-ready SSP includes

02 Three mistakes that weaken control narratives

03 Anatomy of a well-prepared control

04 Bad vs. good: three controls, side by side

05 Q&A



Christina Reynolds

Managing Director, BDO



Robert Teague

Manager CMMC Services, Redspin

What an assessment-ready SSP includes

Recommended structure for a NIST SP 800-171 / CMMC Level 2 System Security Plan

01

Context, obligations & policy

Environment/Scope description, types of CUI, legal obligations

02

Architecture & data flows

System design, interconnections, and CUI data flow diagrams

03

Assets, services & users

Components, protection assets, inventories, and user roles

04

Governance & maintenance

Approval, review, and update process; yearly review

05

TODAY

Controls & objectives

A narrative and evidence reference for every objective

What assessors check first

Scope statement

Up front: employees, endpoints, and how CUI enters and moves

Version control

Version, date, and revision history that match today's environment

CAGE codes

Every CAGE code in the assessment scope

Accountable signature

Signed by the IT or security lead who owns the systems

Three mistakes that weaken control narratives

Explain how each objective is met across the entire assessment boundary

01

Not enough detail

- Name the tools, configurations, and procedures
- Identify the responsible roles
- State frequencies or triggering events

Fix: Make the narrative verifiable

02

Missing assessment objectives

- Break each control into its objectives
- Use the CMMC Level 2 Assessment Guide
- Check NIST SP 800-171A for clarification

Fix: Write to each objective

03

Leaving out affected assets

- Cover every in-scope asset, system, and service
- Include cloud, external connections, and shared services
- Explain customer and provider responsibilities

Fix: Trace the control across the boundary

Every objective. Every affected asset. Clear implementation details.

Anatomy of a well-prepared control

Example: AC.L1-3.1.2 | Transaction & Function Control

1 AC.L1-3.1.2

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

2 Assessment objectives, from the CMMC Assessment Guide Level 2 v2.13

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[b] system access is limited to the defined types of transactions and functions for authorized users.

3 Implementation status

☐ MET	☐ NOT MET	☐ Not Applicable

4 Inheritance status

☐ Inherited	☐ Shared	☐ Customer

5 Implementation statement

Answer 3.1.2[a] and 3.1.2[b] separately, then list references an assessor can pull

Why it works

1 Requirement in view

Control ID and requirement text, verbatim

2 Objectives listed

Every objective the assessor will test

3 One clear status

Implemented, partial, planned, or not applicable

4 Inheritance status

Who meets it: the provider, both, or you. Back inherited and shared with the provider's CRM.

5 Statement per objective

Answer [a] and [b] separately, then cite references

Three controls, three versions of each narrative

Too generic

Nothing to test

Restates the requirement and assessment objectives, so there is nothing for an assessor to test against evidence.

Too expansive

Too much to defend

The answer gets buried, the statement contradicts itself or its references, and every extra detail becomes a commitment to prove or a gap reported on itself.

Good

Specific and verifiable

Answers each objective on its own, with named tools, defined boundaries or timelines, and references an assessor can pull.

Controls covered

RA.L2-3.11.3 Vulnerability Remediation

SC.L1-3.13.1 Boundary Protection

CM.L2-3.4.8 Application Execution Policy

A useful narrative connects each objective to people, technology, actions, and evidence.

Training examples only: names, tools, and values are illustrative and must match actual practice.

Too generic: nothing for the assessor to test

RA.L2-3.11.3 | Vulnerability Remediation

Requirement: Remediate vulnerabilities in accordance with risk assessments.

Bad: as written in the SSP

Full statement · 93 words

[a] The organization identifies vulnerabilities[1] in organizational systems and applications through vulnerability scanning[2] and other methods as appropriate[4].

[b] The organization remediates vulnerabilities in accordance with risk assessments.[1] Vulnerabilities discovered through scanning are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation of specific vulnerabilities.[3] Vulnerabilities are remediated in a timely manner[2,4] consistent with organizational policy and industry best practices[4].

References: Organizational security policies and procedures[5] · Risk assessment

What's wrong

1. **Restates the objectives**
   Says it's done, never how, with what, or by when
2. **No tools, thresholds, or timelines**
   No scanner, severity ratings, or windows
3. **Copied NIST discussion text**
   Lifted from NIST SP 800-171 Rev. 2
4. **Undefined qualifiers**
   Can't be met or failed; never defined
5. **Vague references**
   No document or section to pull

Too expansive: every detail becomes a commitment

RA.L2-3.11.3 | Vulnerability Remediation

Requirement: Remediate vulnerabilities in accordance with risk assessments.

Bad: as written in the SSP

Excerpts · 683 words (good version: 104)

Overview The Company is fully committed to protecting the Controlled Unclassified Information (CUI) entrusted to us[7] … Vulnerability management is the responsibility of John Martinez, IT Manager[6] …

[a] … The four Ubuntu 22.04 servers … are scanned manually when time permits[3]. … A full authenticated scan is performed every Sunday at 02:00 ET, the IT Manager reviews the SIEM dashboard every morning[2] …

[b] Critical vulnerabilities … are remediated within 72 hours of discovery; High within 30 days; Medium within 45 days[1] … Medium vulnerabilities on servers are remediated within 60 days[1] to allow for maintenance windows. (see Table I[1] in Vulnerability Management Procedure) … the IT Manager emails the CEO requesting an exception and adds the vulnerability to the POA&M[4]. For example, the shop-floor CNC programming workstation (SHOP-CNC-04, Windows 7 Embedded, 10.246.46.40) remains vulnerable to CVE-2019-0708[5] (BlueKeep) …

References (15 listed) … Patch Management SOP (DRAFT) … CEO exception approval emails · IT Manager's patch tracking spreadsheet[8] …

What's wrong

1. **Contradicts its own procedure**
   Assessor tests the strictest claim
2. **Commitments that need evidence**
   Proof for every sampled period
3. **Reports its own gaps**
   Every admission is a finding
4. **Weak exception path**
   An email, not a risk acceptance
5. **OPSEC exposure**
   Host, OS, IP, and CVE: a target list
6. **Goes stale fast**
   Use roles; cite the system of record
7. **Scope creep and filler**
   Answers neither [a] nor [b]
8. **References invite requests**
   Drafts and emails become requests

Good: name the tool, the timeline, and the proof

RA.L2-3.11.3 | Vulnerability Remediation

Requirement: Remediate vulnerabilities in accordance with risk assessments.

Good: specific, objective by objective

Full statement · 104 words

1 [a] Vulnerabilities are identified

CrowdStrike Falcon EDR/XDR is used for threat detection and response and **Microsoft Defender Vulnerability Management** for endpoint vulnerability discovery/remediation. The network is monitored and data correlated using **CrowdStrike Next-Gen SIEM**.

2 [b] Remediated in accordance with risk assessments

Vulnerabilities are remediated according to a schedule defined in our **Vulnerability Management procedure**, based on their **severity as identified by CrowdStrike**. Vulnerabilities rated as Critical or High are remediated **within 30 days** of discovery, vulnerabilities rated as Medium are remediated **within 60 days**, and vulnerabilities rated as Low are remediated **within 90 days**. (see **Table I** in Vulnerability Management Procedure)

References: Vulnerability Management Procedure, Table I · CrowdStrike Next-Gen SIEM – Vulnerability scan results

Why it works

1 [a] Named tools

vs. "vulnerability scanning and other methods as appropriate"

2 [b] Severity-based timelines

30 / 60 / 90 days vs. "remediated in a timely manner"

3 [b] Tied to a procedure table

Table I vs. "organizational policy and industry best practices"

Too generic: the boundary is never actually defined

SC.L1-3.13.1 | Boundary Protection

Requirement: Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Bad: as written in the SSP

Full statement · 183 words

[a] The organization has defined the external boundary of the information system.[1]

[b] The organization has defined key internal boundaries within the information system[1] as appropriate[4].

[c] The organization monitors communications at the external system boundary using boundary protection devices[2].

[d] The organization monitors communications at key internal boundaries as appropriate[4].

[e] The organization controls communications at the external system boundary through managed interfaces[2], which include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encryption tunnels[3].

[f] The organization controls communications at key internal boundaries in accordance with organizational policy[4].

[g] The organization protects communications at the external system boundary using industry-standard security mechanisms[2].

[h] The organization protects communications at key internal boundaries as appropriate[4].

References: ~~Network Security Policy~~ · System Security Plan[5]

What's wrong

1. **Never defines the boundary**
   [a] and [b] can't be assessed; [c]–[h] depend on them
2. **No devices named**
   Which firewall? Which monitoring tool?
3. **Copied NIST discussion text**
   Every component type, none from this environment
4. **Internal boundaries left open**
   Leaves the internal objectives undefined
5. **Circular reference**
   Cites the document it's written in

Too expansive: the SSP writes its own findings

SC.L1-3.13.1 | Boundary Protection

Requirement: Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Bad: as written in the SSP

Excerpts · 843 words (good version: 220)

[a] … outside of the following address ranges: 10.238.0.0/16 … The Company's Microsoft 365 GCC High tenant, CrowdStrike Falcon console, LogicMonitor SaaS platform, and vendor-hosted ERP are also considered inside the boundary[1] …

[b] … the edges of the address ranges that serve each network site, as well as the boundary between every VLAN[2]. … the PA-3220 management interface (10.238.99.1, HTTPS admin portal on tcp/4443)[5] … inter-VLAN routing among VLANs 10, 20, and 30 is performed on the core Cisco Catalyst 9300 switch stack rather than through a firewall[2].

[c] … polls the PA-3220 via SNMPv3 every 60 seconds for interface utilization, session counts, CPU, memory, and HA status[4]. …

[d] … their logs are stored locally on each device with a 7-day rollover and are not currently forwarded to the SIEM[3].

[e] … The security policy contains 214 rules[6] … Rule 37 permits inbound RDP (tcp/3389) from 203.0.113.50[5] (Mastercam vendor support) to FS01 – temporary, added 2023[3] …

References (17 listed) … Network Diagram (Visio, v14 – 2022) … Fortinet – Firewall rules (legacy)[7] …

What's wrong

1. **Inconsistent boundary**
   Two definitions of the same boundary
2. **Creates its own finding**
   [f] and [h] fail its own definition
3. **Reports its own gaps**
   Every admission is a finding
4. **Overexplains the monitoring**
   Reads as device health, not traffic
5. **OPSEC exposure**
   Adds up to a reconnaissance package
6. **Goes stale fast**
   Out of date by assessment day
7. **Stale references**
   Docs don't match the environment

Good: define the boundaries, then name each device

SC.L1-3.13.1 | Boundary Protection

Requirement: Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Good: specific, objective by objective

Full statement · 220 words

1. **[a] External boundary:** all hosts and internet traffic outside of the **corporate network.** Fully outlined in the **ports and protocols appendix and network diagram.**

2. **[b] Key internal boundaries:** the **edges of the address ranges that serve each network site**.

	External boundary	Key internal boundaries
Monitor	**[c]** LogicMonitor	**[d]** LogicMonitor
Control	**[e]** Palo Alto firewall	**[f]** Cisco Firepower 1120 (ASA mode)
Protect	**[g]** Palo Alto firewall	**[h]** Cisco Firepower 1120 (ASA mode)

References: Corporate IT Policy §2.3 · Access Management Policy §3 · Configuration Management Policy §2.6 · Continuous Monitoring Policy §3.1 · Network Diagram · Palo Alto firewall rules · Cisco Firepower 1120 (ASA mode) ACLs

Why it works

1. **[a][b] Boundaries stated**
   vs. "has defined the external boundary"

2. **[c]–[h] A device per objective**
   vs. "boundary protection devices"

3. **[d][f][h] Internal side covered**
   vs. "as appropriate"

Too generic: it never picks an approach

CM.L2-3.4.8 | Application Execution Policy

Requirement: 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.

Bad: as written in the SSP

Full statement · 136 words

[a] The organization has established a policy that specifies whether whitelisting or blacklisting[1] is implemented on organizational systems.

[b] The organization specifies the software[2] that is allowed to execute or denied use, as applicable[1].

[c] The organization employs a deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or a deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.[1,2] The organization considers verifying the integrity[3] of authorized software using cryptographic checksums, digital signatures, or hash functions. Software restrictions are reviewed and updated periodically[4].

References: Configuration Management Policy · Authorized software list

What's wrong

1. **Never picks one**
   [a] requires one approach; "whether … or" fails it
2. **No mechanism**
   No AppLocker, no GPO, no list location
3. **Guidance verbs, not commitments**
   NIST discussion language; "considers" commits to nothing
4. **No cadence or owner**
   No frequency and no responsible role

Too expansive: every exemption shows where to look

CM.L2-3.4.8 | Application Execution Policy

Requirement: 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.

Bad: as written in the SSP

Excerpts · 496 words (good version: 92)

[a] The Company's Configuration Management Policy (CMP-002, Rev. 4, …) specifies that a deny-all, permit-by-exception (whitelisting) policy is implemented on all Company endpoints[1]. Before 2024, the Company used a blacklisting approach through Symantec Endpoint Protection Application and Device Control[5] … Blacklisting is still used on the four Ubuntu engineering servers[1] … and the six MacBook Pros used by the marketing team are not currently covered by application control[1] …

[b] … Appendix C lists 143 approved applications … the most recent export of the GPO (August 2025) reflects 128[3]. … Script rules are configured in Audit Only mode[2] … Nine users currently hold local administrator rights[2] for software licensing reasons.

[c] … except those in the "Exempt-AppLocker" OU, which currently contains 14 workstations (shop-floor kiosks, the CNC programming workstation, the CEO's laptop, and IT staff machines)[2]. … emergency requests may be approved verbally by the IT Manager and documented afterward[5]. Because Microsoft does not consider AppLocker a defensible security feature[4], the Company plans to migrate to App Control for Business (formerly WDAC) in 2027.

What's wrong

1. **Contradicts its own scope**
   Also raises whether the Macs are in CUI scope
2. **Reveals bypasses**
   Each exemption is a question to answer
3. **Two sources of truth**
   143 approved vs. 128 enforced
4. **Undermines its own control**
   Invites the assessor to discount it
5. **Filler and process holes**
   Tool history adds nothing; verbal approvals weaken change control

Good: pick one approach and name what enforces it

CM.L2-3.4.8 | Application Execution Policy

Requirement: 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.

Good: specific, objective by objective

Full statement · 92 words

1 [a] Policy specifies whitelisting

The **Configuration Management Policy** specifies that a **deny-all, permit-by-exception (whitelisting)** policy is implemented to allow the execution of authorized software.

2 [b] Allowed software is specified

The software allowed to execute under whitelisting is specified within the **Microsoft Active Directory group policy object** that enforces the whitelisting policy.

3 [c] Whitelisting is implemented

Software whitelisting is configured using **Microsoft AppLocker**, which is enforced using a **group policy object** within Microsoft Active Directory.

References: Configuration Management Policy, Table 4 · Microsoft Active Directory – "ALL–AppLocker" group policy object

Why it works

1 [a] Picks one approach

vs. "whether whitelisting or blacklisting"

2 [b] Says where the list lives

vs. "allowed to execute or denied use, as applicable"

3 [c] Names the enforcement

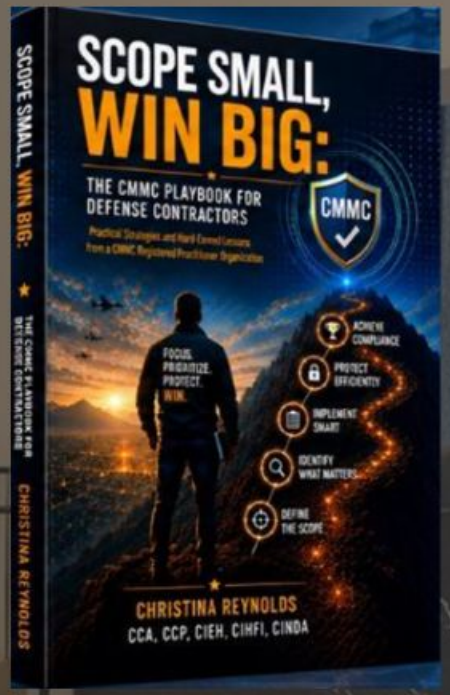
AppLocker via GPO vs. restating the requirement



THANK YOU

Continue the Conversation

Christina Reynolds
Managing Director | BDO USA



Scan to Buy on Amazon

Buy the book:
Scope Small, Win Big

a.co/d/0ayDPQKp

About BDO USA

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: **www.bdo.com**.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2026 BDO USA, P.C. All rights reserved.

Redspin®
A Division of Clearwater

THE FIRST AUTHORIZED CMMC C3PAO

CMMC Expertise, at Every Step

Protecting the Defense Industrial Base is our mission.

Get started at redspin.com

info@redspin.com

HOW REDSPIN HELPS

CMMC Level 2 Assessments
Certification assessments from an authorized C3PAO

Readiness & Consulting
Find out exactly what it takes to become CMMC ready and certified

Managed Services & Cloud
Managed security and compliance

CCP & CCA Training
Courses for Certified CMMC Professionals and Assessors

PREVEIL

Q&A

Questions?

Type your question in the Q&A panel.

preveil.com