Post-assessment review:

What an assessor looks for

The first assessment tested whether you built it. Anything that brings someone back tests whether you have been living in it — and that evidence either accumulated as you went or it did not. Work the checklist before you affirm. The reference behind it explains any line that needs it.

THE CHECKLIST

Your SSP, as dated claims

- [ ] List every implementation statement that names a frequency — weekly, monthly, quarterly, annually, continuously.
- [ ] For each, count the records that frequency should have produced since your assessment. Can you produce them?
- [ ] Flag any statement where the real cadence no longer matches the written one, and decide which is wrong.
- [ ] Flag any statement nobody could test. “Appropriate controls are in place” is not a claim.
- [ ] Confirm the SSP has been edited since the assessment.

Scope

- [ ] Run discovery, compare it to the asset inventory, and investigate every asset that is new, missing or unexpected.
- [ ] List every system that has touched CUI since the assessment, and confirm each was in the assessed scope.
- [ ] Identify anything that brought CUI into a new form — printing you did not do before means physical CUI is in scope.

- [ ] Ask whether the system boundary itself has moved. If it has, that is reassessment territory.
- [ ] Run every change from the past year through the three-question check.
- [ ] Write the one-page scope confirmation memo.

People

- [ ] Pick a recent hire: training completed before CUI access, with dates that prove the order.
- [ ] Pick a recent departure: access removed inside the window your SSP commits to.
- [ ] Check contractor and service accounts specifically — they linger longest and nobody owns them.
- [ ] Confirm annual training was completed, not just assigned.
- [ ] Name who performs each recurring task in the SSP, and when.

What you inherit

- [ ] List every External and Cloud Service Provider in scope.
- [ ] Re-check each one's current status and certifications — confirm nothing lapsed.
- [ ] Compare each current Customer Responsibility Matrix to the version you relied on.
- [ ] Confirm your side of each shared responsibility is done, and that you hold the evidence.

Before you affirm

- [ ] Pull fresh evidence dated inside the review period — not last year's screenshots.
- [ ] Fix anything no longer met. Affirming over a known gap is the scenario the enforcement cases describe.
- [ ] Record who reviewed what, and when. That record is evidence next year.
- [ ] Confirm the person signing has seen the evidence, not a summary of it.

REFERENCE

Why the cadence is yours to choose

Nobody hands you the number. Many requirements say “periodically” without defining it: you decide what it means, write it in the SSP, and are measured against what you wrote from then on. Choose from your risk and your actual capacity, not from what sounds rigorous to an assessor. A small organization nobody has ever tried to attack does not have to write like a prime — but it does have to do what it wrote.

The three-question check for any change

1	**Does it move the boundary?**
2	**Does it add systems, tools or configurations that were never assessed?**
3	**Does it change where CUI lives or how it is protected?**

Any yes means a scope review before you affirm the old scope as though nothing had happened. Build the check into change control so the question surfaces when a project is approved, not at affirmation time. Write down the reasoning either way — a documented “we considered this and concluded it was not significant” is worth far more later than silence.

The scope confirmation memo

One page a year: here is the boundary we were assessed on, here are this year's changes, here is why none of them were significant. It is the document you will want if anyone later asks why you affirmed.

Where the gap usually opens

The drift patterns that show up most often between one assessment and the next. If a row describes your organization, that statement is the one to re-test first.

THE SSP SAYS	WHAT HAPPENS OVER A YEAR
Audit logs reviewed weekly	Reviews stop when the analyst leaves; no record for months
FIPS-validated encryption for CUI at rest	A new file share or backup target uses a non-validated setting
All endpoints run EDR, patched within 30 days	A batch of replacement laptops misses enrollment
Annual security awareness training	New hires start work before completing it
Accounts disabled within 24 hours of separation	Contractor and service accounts linger
Incident response plan tested annually	The last tabletop was the one done for the assessment
CUI shared only through the approved enclave	Staff email CUI from personal accounts

Maintained, or assembled

Two organizations can hold the same documents and leave completely different impressions. The difference is the shape of the evidence, not its volume.

READS AS MAINTAINED	READS AS ASSEMBLED
Records spread evenly across the year	Records clustered around dates that look like an audit
Evidence dated inside the review period	Last year's screenshots, re-submitted
Decisions written down when they were made	Decisions reconstructed afterward from memory
Exceptions documented as choices, with a rationale	Gaps that are simply silent
An SSP with an edit history	An SSP untouched since the assessment
Someone who can say who does this and when	A search for the person who might know

Making it sustainable

Test a slice of the requirements each quarter rather than all of them in the month before you affirm. Two of the 110 already expect periodic and ongoing assessment, so this is work you owe anyway — spreading it out is simply the cheaper way to do it.