

Writing the Technical Truth: How to Document Your Controls in the SSP

Presented by:



Ozzie Saeed, Founder/CEO



What We'll Cover (and What You'll Leave With)

1



**Why SSP
implementation
statements
matter**

2



**Practice-level
vs AO-level
statements**

3



**Mapping
tooling and
services to
specific 800-
171 controls**

4



**Avoiding “checkbox
language” and other
common writing
mistakes**

5



**Methods:
ODP/ODV +
Who/What/
When/Where/
How**

6



**Covering
Technology /
Facilities /
Personnel in
real examples**

7



**Optional Hands-
on work:
You'll draft at
least two AO level
statements and
one practice-level
summary you can
reuse**

SSP: Your Operating Manual, Not a Homework Assignment

CMMC assessors don't just want "Implemented" – they want how.

Your SSP is:

- The playbook for assessment week
- The reference for engineers and vCISO staff

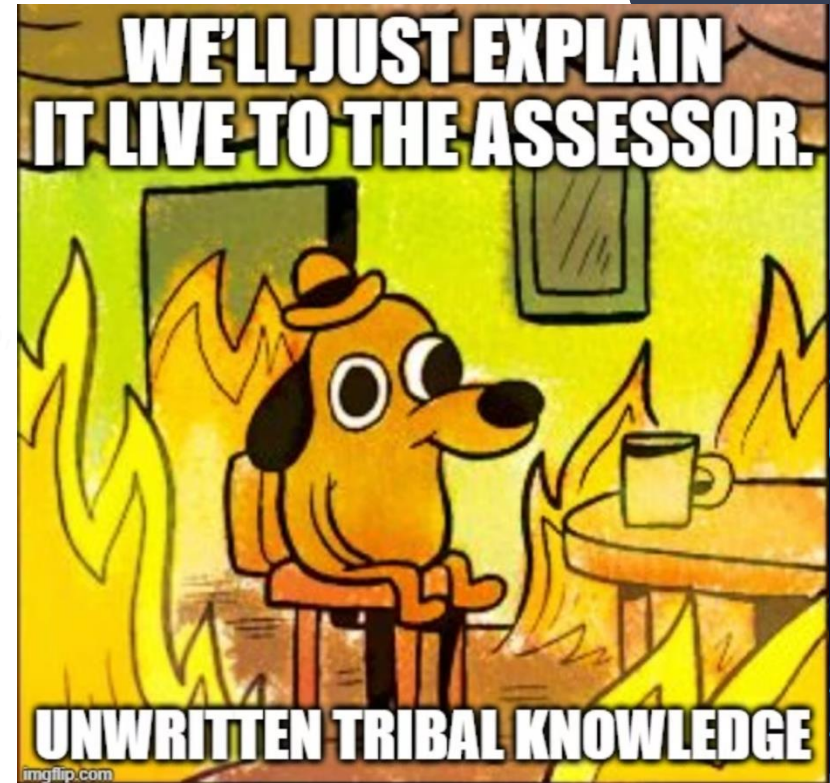
For MSPs, SSP content should align with:

- Services you sell (IDP, Vuln Management, MDR, EDR, backup, M365, etc.)
- Tools you actually operate
- SLAs and responsibilities you've promised clients

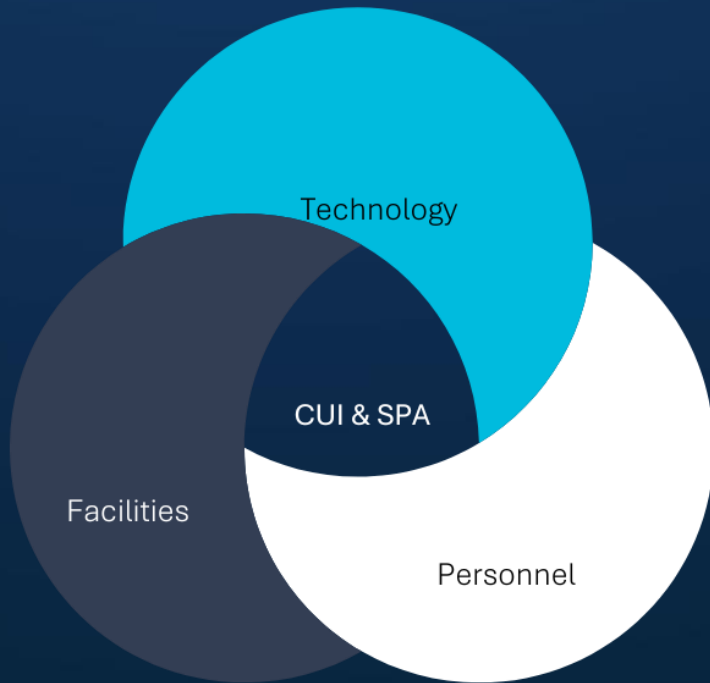
SSP as dust collector



SSP as daily playbook



What Are You Actually Writing About?



Technology

- CUI assets: e.g., M365 GCC tenant, Windows 11, line-of-business apps
- SPAs: EDR, SIEM, MDM, Entra ID, Windows Server AD, firewalls, backup, RMM

Facilities

Offices with CUI access, data closets, co-lo cages, SOC rooms

Personnel

General users, admins, SOC team, MSP engineers, subcontracted NOC

For each AO, ask: Which tech, which facility, which people are in scope?

Where the Real Writing Happens

Practice-Level vs AO-Level Statements

Practice-level statements:

- Short, narrative summary of how you meet the whole requirement
- Use AO letters in front of sentences: [a], [b], [c]...

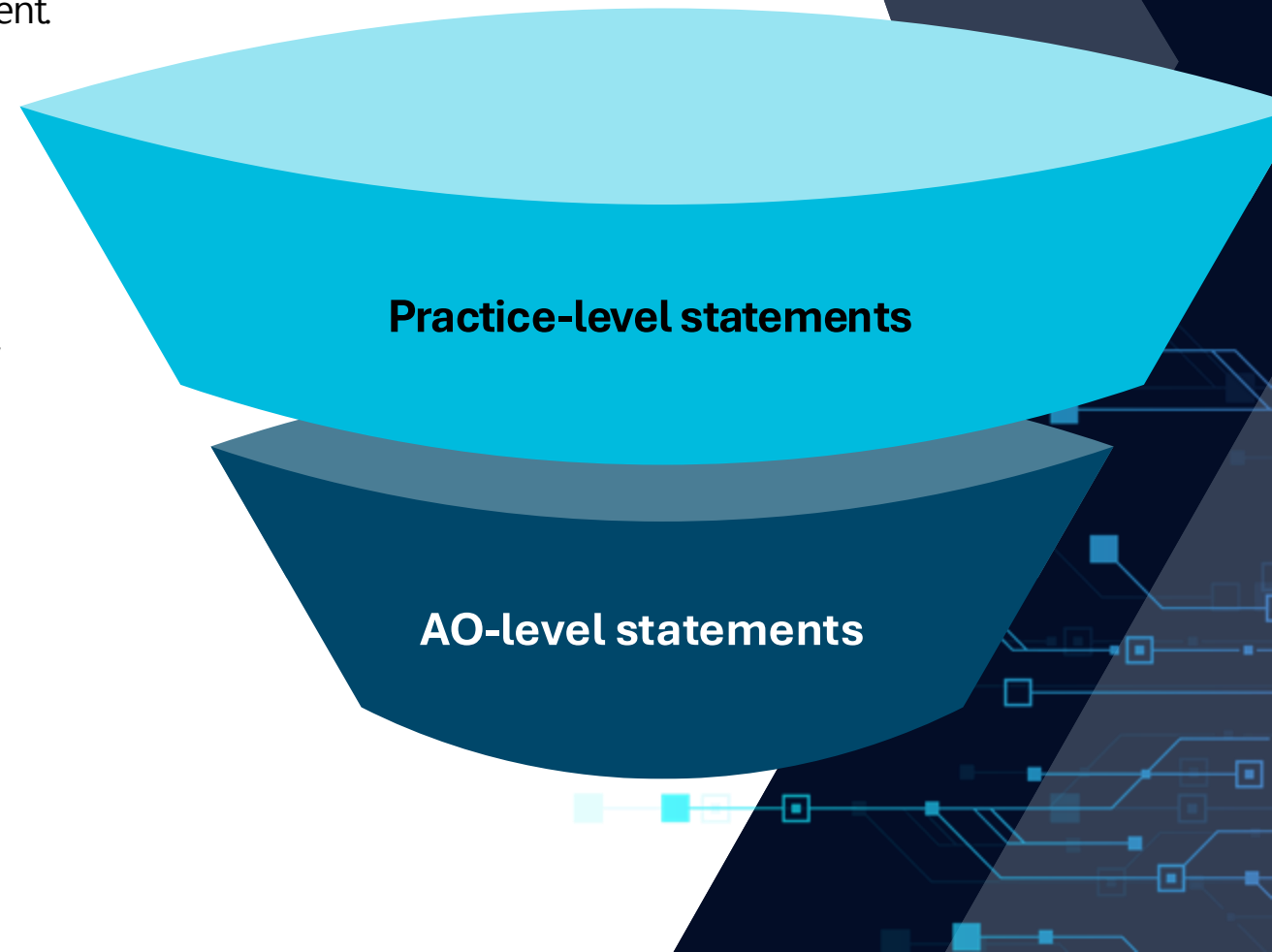
AO-level statements:

Highly recommended primary place for detail

- Each AO = clear chunk answering Who/What/When/Where/How
- SLAs and responsibilities you've promised clients

Model:

- **Practice:** "story of the control"
- **AOs:** "receipts for each piece of that story"



Stop Paraphrasing, Start Describing

Stop Storytelling vs "Checkbox Language, Start Describing



Bad "checkbox" examples

- "The organization enforces password policies as required"
- "The organization enforces password policies as required"
- "Users receive security training."



Improved patterns

- Specific tools (Entra, Intune, Veeam, etc.)
- ODPs/ODVs (how many attempts, length, special character, duration, how many days, what frequency)
- Scope (Platforms and System Components: endpoints vs SaaS vs servers vs admin accounts)
- Evidence you actually have



Does your statement...

- Describe behavior and mechanism?
- Avoid generic phrases like "as appropriate," "as needed," "regularly"?
- Make it obvious what screenshot/log/procedure would prove it?



Restating
the
requirement in
my own words.



Explaining
what our
tools and people
actually do.

ODP + ODV = Less Rework, More Clarity

ODPs & ODVs: Making Writing Scalable

ODP (Parameter) – what you measure or set:

Password length, log retention, review frequency, lockout threshold

ODV (Variable) – your actual chosen value:

14 characters, 365 days, quarterly, 10 attempts, etc

Put ODVs in policy and standards → Reference them in SSP → Enforce in tools

Example: "Account lockout after [ODV] failed attempts within [ODV] minutes, defined in Access Control Policy §4.2.9 and enforced via Entra ID/AD GPO."



"Managing expectations: the art of making 'meh' feel 'great!'"

Control	ODP	ODV	Where enforced
Password length	Minimum characters	14 characters	Entra ID/AD GPO
Log retention	Days retained	365 days	SIEM
Access review	Review frequency	Quarterly	Identity management
Account lockout	Failed attempts	10 attempts	Entra ID/AD

Use This Skeleton for Every AO Statement as Applicable

Who / What / When / Where / How Template



Who – role/department

- Security Engineer
- Helpdesk Tier 2”
- HR Manager”
- SOC Lead



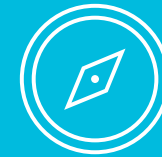
What – specific action

- Reviews Intune compliance reports
- approves access requests



When – frequency or trigger

- Quarterly
- Upon hire
- Prior to granting admin access



Where – system/service/ location

- M365 GCC tenant
- SOC cage
- ConnectWise ticket queue CMMC



How – toolkit + method

- Using Intune baseline CUI Endpoints-Baseline and a monthly checklist

Example: "[Who] performs [What] on [Where] [When] using [How]. Evidence: [artifact list]."

Your Stack, Your Controls: Make the Connection Explicit

Mapping Tooling & Services to 800-171 Controls

Most MSPs already have:

- Entra ID / AD, Intune/RMM, EDR, SIEM, backup, M365, ticketing, CRM/PSA.

Map each tool/service to specific 800-171 controls

- Entra ID → AC/IA/AU controls (auth, lockout, MFA, SSO).
- Intune/RMM → CM/SC (hardening, patching, config baselines).
- EDR → SI/SC (malware detection, isolation).
- Backup service → CP (data backup & restoration).
- Ticketing/CRM → CA/RA/IR (risk, change, incidents, approvals).

Use this mapping to:

- Decide what goes into AO statements.
- Ensure every tool/service in your stack shows up somewhere in the SSP (if it's in scope).

Tool or Service Provided	Example 800-171 requirements	Where referenced in SSP
Directory and privilege management tools	AC.L2-3.1.2, AC.L2-3.1.6, CA.L2-3.12.3	Administrative Privileges (Weekly)
Identity management & audit reporting tools	AC.L2-3.1.1, AC.L2-3.1.2, CA.L2-3.12.3	Authorized User Reviews (Weekly & Monthly)
Endpoint protection / EDR platform	AC.L2-3.1.1, AC.L2-3.1.2, CA.L2-3.12.3	Malware Detection (Weekly)
Application control / whitelisting solution	CM.L2-3.4.6, CM.L2-3.4.7, CA.L2-3.12.3	Application Monitoring (Monthly)
Endpoint configuration or policy management	CM.L2-3.4.7, CA.L2-3.12.3	Browser Policy Enforcement (Weekly)
Vulnerability management scanner / risk dashboard	RA.L2-3.11.2, SI.L2-3.14.5, CA.L2-3.12.3	Vulnerability Monitoring (Monthly & After Maintenance)

Practice-Level Example – AC.L2-3.1.8 (Limit Unsuccessful Logon Attempts)

Technical Practice-Level Example (Endpoints + SaaS)

[a] [Company] defines account lockout thresholds in Access Control Policy §4.2.9: user accounts lock after 10 failed logon attempts within 15 minutes, with a lockout duration of 30 minutes; counters reset after 15 minutes.

[b] These thresholds are enforced for Windows endpoints via domain GPO CUI_DefaultDomainPolicy and for cloud/SaaS applications (M365 GCC, Salesforce, Jira) federated to Entra ID using Entra Password Protection and Conditional Access policies. Repeated lockouts generate alerts in the SIEM for investigation by the SOC in accordance with the Incident Response Plan.



Note where tools/services map: Entra ID, AD, SIEM, M365.

AO-Level Example – IA.L2-3.5.7 [Password Complexity]

AO-Level Technical Example – Multi-Platform

Windows & Entra-backed SaaS:

- **Who:** Infrastructure Engineers maintain identity and password baselines.
- **What/How:**
 - Password complexity ODP/ODVs defined in Identification & Authentication Policy (min 14 chars, 3 of 4 character types, lockout thresholds, etc.).
- Enforced via:
 - Entra ID Password Protection for SSO-integrated SaaS (M365 GCC, ServiceNow, etc.).
- **When:** Baselines reviewed annually and upon Microsoft security baseline updates.
- **Where:** Group Policy Management Console & Entra ID portal (Security > Authentication methods).

Mac/Linux endpoints not in AD:

- **How:** Baseline configuration scripts apply pam_pwquality.so settings (e.g., minlen, ucredit, lcredit, dcredit, difok) during provisioning.
- **How:** Baseline configuration scripts apply pam_pwquality.so settings (e.g., minlen, ucredit, lcredit, dcredit, difok) during provisioning.

Key teaching point:

- Different implementation per platform? → Say so explicitly.
- Shared solution? → Document once, list all platforms it covers.

AO-Level Example – CA.L2-3.12.4 [SSP Developed & Updated]

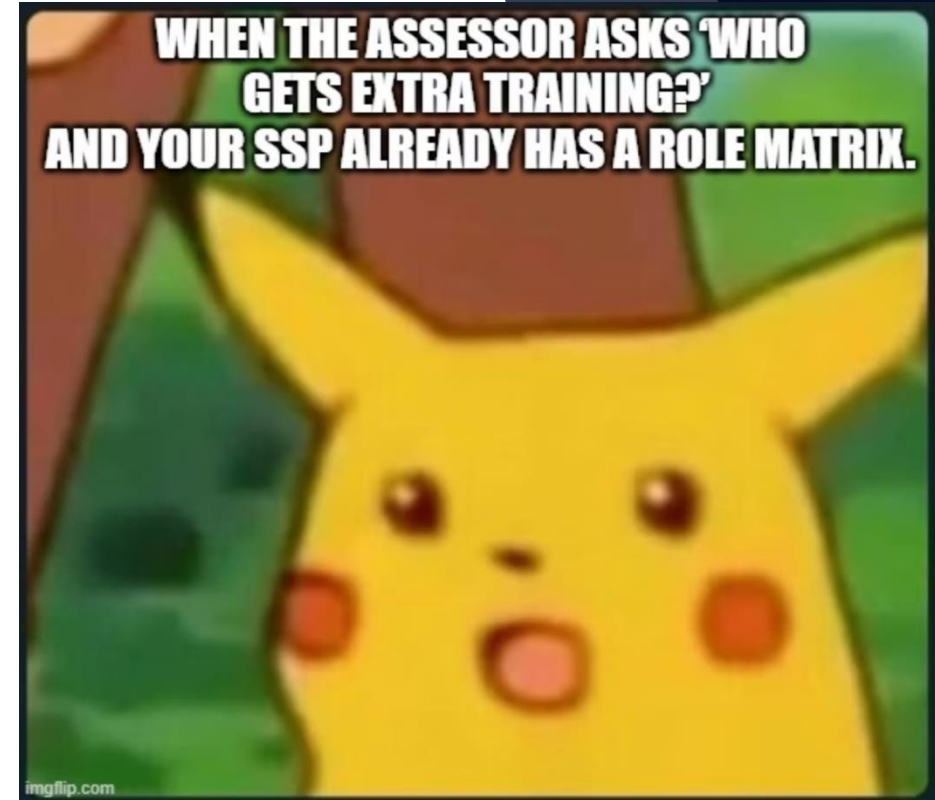
Administrative AO Example – Governance

- **Who:** vCISO owns the SSP; ISSO maintains it; Change Advisory Board reviews major updates.
- **What:** SSP documents:
 - System boundary, in-scope CUI & SPA assets, external service providers.
- **When:** Updated:
 - After significant changes (new CSP, new enclave, major tool changes).
 - After annual self-assessment or formal C3PAO assessment.
- **Where:** Stored in GCC High SharePoint library /CMMC/SSP, versioned (Doc ID).
- **How:**
 - Changes tracked as tickets in CRM/PSA (e.g., ConnectWise, Autotask) tagged SSP-Update.

AO-Level Example – AT.L2-3.2.2 [Role-Based Training]

People / Training AO Example

- **Who:** HR + Security Awareness Lead.
- **What:** Role-based training:
 - All users: annual security awareness and basic CUI handling module.
 - MSP engineers/admins: secure remote access, privileged account handling, client CUI handling rules.
 - SOC team: incident response runbooks and simulated exercises.
- **When:** Initial within 30 days of hire; annually thereafter; additional when major changes or incidents occur.
- **Where:** Delivered via LMS (e.g., KnowBe4); completion recorded in LMS and mirrored into CRM contact records/HRIS.
- **How:**
 - Course completion ($\geq 80\%$ passing score) required before granting elevated access.
 - Monthly report reconciles LMS completions vs CRM "role = admin" records.



AO-Level Example – PE.L2-3.10.x [Physical Access & Visitor Control]

Physical / Facilities AO Example

- **Who:** Facilities Manager manages access control; SOC Lead reviews logs.
- **What:**
 - CUI assets reside in MDF-01 closet and XYZ Datacenter co-lo cage.
 - Badge access required for all entry points; visitors must sign in, wear badges, and be escorted.
- **When:**
 - Visitor logs reviewed quarterly.
 - Badge/access list reconciled monthly against HR/CRM staff roster.
- **Where:**
 - Badging system (Lenel, HID, etc.); visitor logs stored in SharePoint folder /Facilities/Visitor Logs.
- **How:**
 - Escort procedure defined in Physical Security SOP; SOC retains 90+ days of camera footage covering CUI racks and entrances.

MSPs: Make Your SSP Match What You Actually Sell & Deliver

Aligning SSPs with CRMs & Scoping Language

Your CRM/PSA (ConnectWise, Autotask, Salesforce, HubSpot, etc.) usually knows:

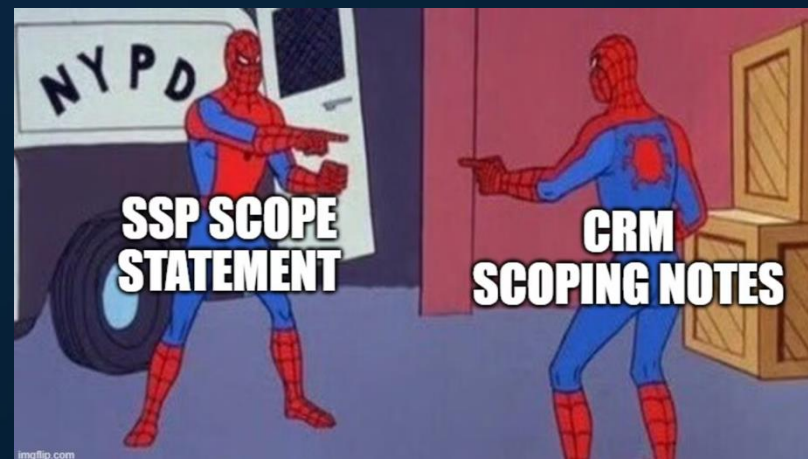
- What services each client has bought.
- Which environments/assets you manage.
- Key contacts and roles.

SSP alignment examples:

- If CRM says "Managed MDR + EDR," SSP should show which 800-171 controls are implemented via this service.
- If CRM says "No physical hosting," SSP shouldn't describe on-prem data centers.

Use CRM fields to drive SSP and scoping language:

- "Has CUI?" yes/no.
- "CMMC scope description" free-text field.
- "Primary CUI systems," "ESP/CSPs in scope," "MDR/EDR/Backup included?"



On-slide example: Simple screenshot mock-up of CRM account fields and an excerpt of SSP text that uses the same boundary language.

If You Write It/Say It, You Must Prove It

Evidence Strategy – Tying It All Together

For each AO, link:

Statement → Tool/service → Evidence.

Evidence types:



Policy / SOP extract



Config screenshots

(GPO, Entra, Intune, EDR, backup jobs)



Logs/reports

(SIEM alerts, backup success reports, training completion)



Physical artifacts

(photos, access logs, sign-in sheets)

Avoid two extremes:

- No evidence ("trust me, bro").
- Evidence dump (30 screenshots with no explanation).



Best practice: 1–3 artifacts per AO, clearly labeled with what they prove and what date/asset they cover.

Hands-On 1: Kill the Checkbox Language

Bad vs Good Rewrite Exercise

Before (Bad):

Backups are performed regularly for critical systems.

After (Workshop Version):

Space for your improved statement

Prompt on screen:

- Identify missing ODPs/ODVs (how often, what retained).
- Add Who/What/When/Where/How.
- Reference tools/services (e.g., Veeam, Azure Backup, Datto).
- Tie to evidence (backup job report, restore test, ticket).



Facilitation note: Ask the room for suggestions; build a short, strong AO statement live.

Hands-On 2: Leave With Real Control Statements

Draft Your Own AO & Practice Statements

Ask participants to pick one technical AO they own (e.g., backups, EDR, patching, log review).

AO-level template:

"[Who] performs [What] on [Where] [When] using [How]. Evidence: [artifacts]."

Practice-level template:

"[a] [Definition/policy/ODP/ODV]. [b] [Implementation across tech types]. [c] [Monitoring/maintenance over time]. Please refer to the AO-level implementation statements for further details."



By the end of this slide, you should have: At least one AO-level and one practice-level statement you can re-use in your SSP.

Assessment Week Tips + Key Takeaways



Assessment Week Tips + Key Takeaways

Use the SSP as Your Script (Not a Prop)

Tips:

- Have the same SSP version open that assessors received.
- Answer directly using your implementation statements; then show mapped evidence/tool.
- Give one good example, then ask: "Would you like another example?"
- Don't improvise new commitments; stay inside your described implementation.

Key Takeaways:

- Avoid "checkbox language" – describe real behaviors and real tools.
- Cover Technology, Facilities, and Personnel where relevant.
- Don't improvise new commitments; stay inside your described implementation.
- Map your stack & services to specific 800-171 controls and show that in the SSP.
- Align SSP scope with CRM/service catalog and scoping notes.
- Use ODP/ODV + Who/What/When/Where/How as your standard template.

**WHEN THE ASSESSOR READS
YOUR AO AND YOU ALREADY
HAVE THE EXACT EVIDENCE OPEN.**

