PCOS Security Assessment Plan (SAP)

7 Dec 2025

Aligned to NIST SP 800-30 and internal PCOS Risk Assessment Methodology and NIST SP 800-30 Rev. 1.

Authored By	Reece Niemuth
System Identifier	PCOS-Homelab
Date of Latest Revision	7 Dec 2025
Publication Version	Revision 1 (1.0.0)

CONTAINS NO CLASSIFIED OR SENSITIVE INFORMATION. THIS ARTIFACT SERVES TO DOCUMENT, IN PROFESSIONAL MANNER, A TRAINING RESOURCE FOR SELF-EDUCATION IN THE FIELD OF FEDERAL SYSTEMS ENGINEERING, MAINTENANCE, CYBERSECURITY RESEARCH, AND RELATED.

Security Assessment Plan (SAP) **: Revision History**

Revision / Version	Date	Description / Notes
Rev. 1 (1.0.0)	7 Dec 2025	Publication Inception / Creation

1. Introduction and Purpose

- The System Assessment Plan (SAP) defines the scope, objectives, and methods used to assess risks and evaluate the security posture of the PCOS environment.
- This SAP is based on the PCOS Risk Assessment Methodology and provides the procedural foundation for conducting threat analysis, vulnerability analysis, risk scoring, and mitigation planning.
- Outputs from this SAP will feed directly into the System Assessment Report (SAR) and Risk Assessment Report (RAR) to support iterative engineering improvements within the PCOS lab.

2. Assessment Scope

- Applies to all PCOS components: hypervisors, virtual machines, NAS, monitoring infrastructure, endpoint systems, container hosts, networking equipment, and administrative workstations.
- Includes remote-access mechanisms (SSH, RDP, RealVNC, WireGuard) and internal trust zones (compute, storage, management, monitoring).
- Includes software platforms: Splunk, Nessus, virtualization platforms, endpoint security, configuration tooling, and automation scripts.
- Excludes any external networks beyond the home network boundary.

3. Assessment Objectives

- Identify internal and external risks affecting confidentiality, integrity, and availability.
- Validate the accuracy and completeness of system description, threat identification, and vulnerability analysis.
- Generate consistent risk ratings using qualitative (H/M/L) and semi-quantitative (1–5) scoring.
- Evaluate and document mitigation plans mapped to RMF treatment categories.
- Support continuous refinement of architecture, segmentation, monitoring, and baseline enforcement.

4. Assessment Methodology (Aligned to RA Methodology)

4.1 System Characterization

- Confirm architecture, components, data types, and boundaries.

- Validate system diagrams, trust zones, and expected data flows.

4.2 Threat Identification

- Evaluate relevant threats based on NIST SP 800-30 categories: adversarial, accidental, structural, environmental.
- Map threats to system components and operational behaviors.

4.3 Vulnerability Analysis

- Conduct technical vulnerability scans (Nessus), configuration inspections, baseline reviews, and manual data flow evaluations.
- Identify weaknesses in segmentation, trust inheritance, VM baselines, authentication, patching, and monitoring coverage.

4.4 Risk Scoring

- Assign likelihood (1–5) and impact (1–5) values.
- Produce qualitative ratings (High / Moderate / Low).
- Document rationale and trace each score to supporting evidence.

4.5 Mitigation Planning

- Map mitigations to RMF control families and formal treatment categories: mitigate, avoid, accept, or transfer.
- Prioritize improvements that reduce residual risk to acceptable levels.
- Validate feasibility in the PCOS lab environment.

5. Risk Categories & Assessment Tables

5.1 Risk Category: Safety & Physical Environment

Description of Risk	Likelihood	Impact	Mitigation Actions
Residential power outage causing system downtime	Medium	Low	UPS system, VM snapshots, scheduled backups
Overheating of equipment in home office	Low	Low	Ensure ventilation, monitor temperature sensors
Accidental physical disconnection or equipment damage	Low	Low	Cable management, equipment placement

5.2 Risk Category: Achievement of Lab Objectives

Description of Risk	Likelihood	Impact	Mitigation Actions
Misconfigured services undermining test results or engineering learning	Medium	Medium	Apply baselines, document configs, validate against known-good states
Lack of visibility in monitoring stack leading to missed findings	Medium	Medium	Expand Splunk ingestion, validate data sources
VM or container corruption impacting long-term projects	Low	Medium	Use snapshots, maintain image templates

5.3 Risk Category: Technical / Cybersecurity Risks

Description of Risk	Likelihood	Impact	Mitigation Actions
External threat activity exploiting misconfigured or exposed services	Low	High	Firewall rules, WireGuard-only remote access, baseline hardening
Unpatched systems increasing vulnerability exposure	Medium	Medium	Routine patch cycle, Nessus scanning
Weak segmentation allowing unintended lateral movement	Medium	High	Refine VLANs, enforce internal firewall rules

5.4 Risk Category: Information Technology & Data Risks

Description of Risk	Likelihood	Impact	Mitigation Actions
Loss of test data or configurations	Medium	Medium	NAS backups, VM export rotation
Credential compromise for lab accounts	Low	Medium	MFA where possible, password manager
Monitoring or logging gaps	Medium	Low	Validate Splunk ingestion, enforce TA coverage

6. Assessment Schedule & Frequency

- Full RA/SAP → SAR/RAR cycle performed biannually or after major architectural changes.
- Interim checks conducted after significant updates (new hypervisor, new segmentation, new tooling).
- Nessus scans performed at least monthly.
- Baseline and configuration reviews performed quarterly.

7. Deliverables

- System Assessment Report (SAR) — consolidates all findings, risks, and evidence.

- Risk Assessment Report (RAR) — provides final risk determination, scoring, and treatment recommendations.
- Updated Architecture Diagrams — reflect any material changes discovered during assessment.
- Mitigation Tracking List — PCOS equivalent of a POA&M.

8. Output Statement

The SAP defines the procedures, scope, and analytical steps used to evaluate the PCOS environment's security posture. It operationalizes the Risk Assessment Methodology by detailing how threats, vulnerabilities, risks, and mitigations are identified and assessed. SAP outputs serve as source material for the SAR and RAR, ensuring consistent traceability between system characterization, risk analysis, documented findings, and planned remediation activities.