Patriot Command Operations System (PCOS)

"Fortiter et Fideliter"

A living testbed for secure configuration, continuous monitoring, and automation — engineered to elevate my ability to protect information, sustain operations, and support the mission of the DoD cyber landscape

PCOS Risk Assessment Methodology

7 Dec 2025

A documented, repeatable process for identifying, analyzing, and prioritizing risks affecting the PCOS environment in accordance with 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.

[Publication Title] : Revision History

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

1. System Description

- PCOS is a home-office cybersecurity laboratory used for systems engineering practice, RMF methodology training, and evaluation of security tooling (Splunk, Nessus, endpoint protection, automation frameworks, container platforms).
- Core components include multiple hypervisors, virtualized Windows/Linux hosts, a NAS device, and lightweight monitoring infrastructure. All of which accessed over SSH, RDP, RealVNC by personal device on the same private network, or remotely via encrypted WireGuard VPN Tunnel.
- The system boundary is defined by the residential home network, with a single administrative enclave consisting of all PCOS-managed hosts and internally segmented trust zones (compute, monitoring, storage, management).
- All data processed is unclassified, test-generated, and used solely for education, experimentation, and validation of ISSE-aligned engineering patterns.
- Architectural assumptions include internal segmentation intent, consolidated logging to Splunk, periodic patching and baseline application, dependency on home networking and power availability, and use of virtualized or containerized subsystems for experimentation.

2. Threat Identification

- Uses NIST SP 800-30 threat categories: adversarial, accidental, structural, and environmental.
- **Adversarial threats:** commodity malware, automated internet scanning, credential compromise attempts, and exploitation of exposed or misconfigured services.
- **Accidental threats:** user misconfiguration, unintended data deletion, improper patching, credential mishandling, or disruptions caused by administrative errors.
- **Structural threats:** hardware failure, VM corruption, degraded storage devices, OS/service defects, or dependency stack instability.
- **Environmental threats:** residential power loss, network outages, overheating, or external service disruptions affecting cloud-integrated components.
- Threat relevance is evaluated based on system exposure, architectural design, and operational behaviors within the PCOS environment.

3. Vulnerability Analysis

- Focuses on **technical weaknesses** and **architecture-level weaknesses** directly affecting confidentiality, integrity, or availability.
- **Technical vulnerabilities include:** unpatched OS or applications, outdated virtual machine snapshots, weak or default configurations, incomplete STIG/CIS baseline alignment, insufficient logging coverage, and weak authentication practices.
- **Architecture-level vulnerabilities include:** inadequate segmentation between trust zones, unclear or overly permissive data paths, insufficient boundary enforcement, centralized single points of failure, or inconsistent application of security baselines across hosts.
- Vulnerabilities are identified through Nessus scanning, manual configuration review, log analysis, architecture inspection, dependency verification, and review of system/service configurations.

4. Risk Scoring

- Uses the NIST SP 800-30 qualitative scale (**High / Moderate / Low**) as the primary risk descriptor.
- Supplements with a **semi-quantitative scoring model**:
  - Likelihood scored 1–5 based on exposure, exploitability, control maturity, and historical observation.
  - Impact scored 1–5 based on system downtime potential, loss of test data, interruption of the lab environment, and cost/time of restoration.
- Combines likelihood × impact to produce a numerical index supporting consistent and defensible prioritization.
- Each risk is mapped to both numerical and qualitative categories to maintain interpretability and repeatability.
- Risk scoring is applied uniformly across all identified threat–vulnerability pairings and updated periodically as configuration, tooling, or architecture changes.

5. Mitigation Planning

- Aligns mitigations with high-level RMF control families (AC, CM, IA, PL, SC, SI, MP, CP) and PCOS-specific architecture constructs.
- Each mitigation is assigned an RMF-aligned treatment strategy: **mitigate, avoid, accept, or transfer** (transfer typically not applicable in a personal lab context).

- **Configuration and Patch Management:** routine updates, baseline reapplication, automated hardening enforcement, configuration monitoring, and periodic review of services and permissions.
- **Segmentation and Boundary Controls:** refining trust zones, restricting east–west traffic, improving firewall rules, isolating monitoring and storage layers, and validating ingress/egress constraints.
- **Monitoring and Visibility Enhancements:** expanding Splunk log sources, improving alert logic, validating Nessus coverage, integrating new hosts into monitoring pipelines, and tuning thresholds.
- **Architecture Hardening:** reducing single points of failure, validating backup/restore procedures, strengthening hypervisor controls, and ensuring consistent baseline inheritance.
- Mitigation steps directly reference the associated risk score, expected effectiveness, and resulting reduction in residual risk.

6. Conclusion and Lifecycle Integration

- Findings map into SAR/RAR-style documentation to support repeatable engineering practice, though without formal AO decisions or mandated Continuous Monitoring cycles.
- Risk information feeds into periodic environment reviews, baseline updates, infrastructure changes, and tooling enhancements as part of an informal—but structured—engineering lifecycle.
- The methodology supports iterative learning, experimentation, and continuous improvement across RMF, ISSE, and security engineering disciplines.
- This process maintains coherence, traceability, and maturity improvement across assessment iterations, even within a personal learning and development environment.

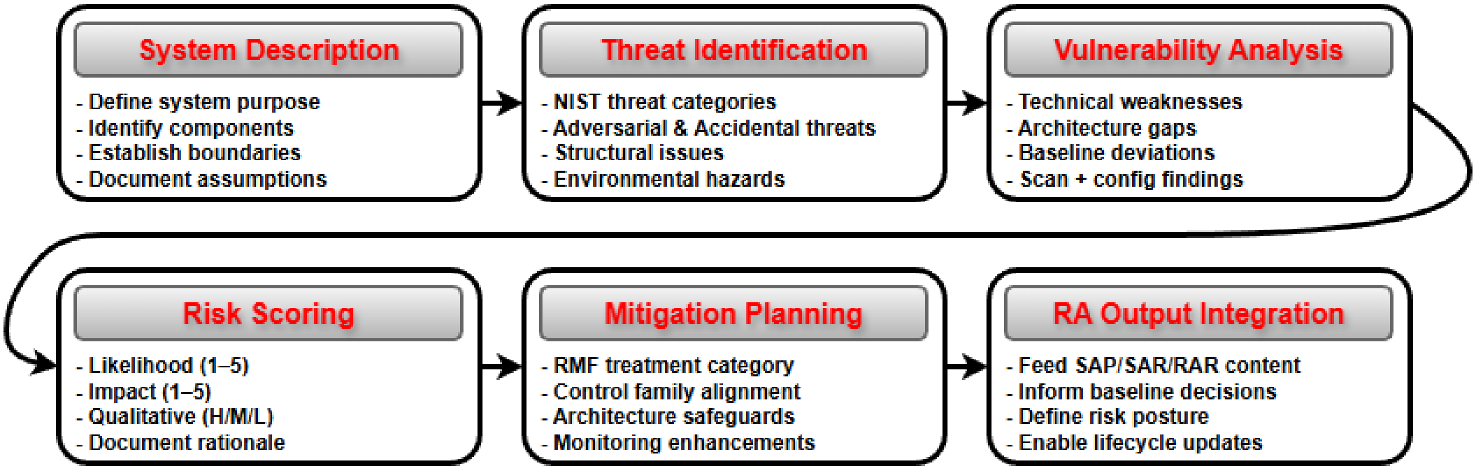

Figure 1 – Logical Flow of Risk Assessment Conducted on the PCOS

6. Output & Statement of Purpose

The output of this Risk Assessment Methodology provides a structured, defensible basis for identifying system risks, determining their significance, and selecting appropriate mitigation strategies for the PCOS environment. The results directly inform development of the System Assessment Plan (SAP), System Assessment Report (SAR), and Risk Assessment Report (RAR) by supplying the foundational threat, vulnerability, and risk scoring data required for evaluation activities. This methodology ensures traceability between system characterization, identified weaknesses, associated risks, and planned treatments, enabling consistent documentation, repeatability of assessments, and alignment with RMF-inspired engineering practices. Although PCOS does not operate under a formal Authorization process, the RA outputs support disciplined decision-making, baseline refinement, and continuous improvement of system security posture.