

TNI Audit-as-a-Service - RMF Implementation Guide

TNI Audit-as-a-Service - RMF Implementation Guide

□□ Detailed Implementation Instructions · Legendary Precision □□

Organization : True North Insights, LLC Date : 2025-05-04 Version : 1.0

##

Introduction

True
North's RMF
Accelerators
True North
Insights offers
several
accelerators
that can speed
your RMF
implementation:

1. Control
Implementation
Statements
Library

Our pre-written
control
implementation
statements
cover the
complete
FedRAMP
Moderate
baseline. Each
statement is: -
Written in clear,
assessor-
friendly
language -
Technically
accurate and
implementation-
neutral -
Designed for
easy
customization
to your
environment

2.
Document
Templates

##

**Introduction**

- System
Security Plan
(SSP)
Template with
OSCAL export
capability -
Privacy
Threshold
Analysis (PTA)
and Privacy
Impact
Assessment
(PIA) -
Incident
Response Plan
with tabletop
exercise
scenarios -
Contingency
Plan template
with BIA
worksheet

2025-05-04

American Excellence

3.

Automation
Tools
- GitLab
CI/CD
Templates for
control
validation -
Docker-based
scanning tools
pre-configured
for FedRAMP
requirements -
Terraform
modules for
compliant
infrastructure -
Python scripts
for generating
OSCAL JSON
evidence

4.

Assessment
Tools

##



Introduction

- Control testing procedures mapped to NIST SP 800-53A - Evidence collection checklist by control family - POA&M tracking system with risk scoring - RMF readiness assessment toolkit

2025-05-04
American Excellence

Common Pitfalls and How to Avoid Them

Scope Creep

Problem: System boundaries expand during implementation, invalidating security documentation. **Solution:** Document and control boundaries clearly at the start; use configuration management to track changes.

Insufficient Evidence

Problem: Controls are implemented but evidence is inadequate for assessment. **Solution:** Design evidence collection into implementation; use True North's evidence matrix to ensure completeness.

Control Conflicts

Problem: Some security controls conflict with operational requirements. **Solution:** Identify conflicts early and document risk-based decisions for alternative implementations.

Policy-Practice Gap

Problem: Written policies don't match actual practices. **Solution:** Develop policies based on implementable practices; update both in tandem.

Additional Resources

- NIST SP 800-37 Rev 2:
<https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final> - FedRAMP Documentation:
<https://www.fedramp.gov/documents/> - OSCAL Resources:
<https://pages.nist.gov/OSCAL/> - True North Knowledge Base:
<https://truenorthinsights.com/kb>

True North Insights · Veteran-Owned Small Business · CAGE: 8NEX1

Contact: jeffreysanford@gmail.com · Website: www.truenorthinsights.com

Hoorah! Bringing legendary commitment to your security mission from America's heartland.