# DATA QUALITY & SOURCE OF TRUTH

Vulnerability Management Maturity Model (VMMM v2)

Domain: Identify
Maturity Tier: Foundational

## EXECUTIVE SNAPSHOT

**Why this matters:**

- Multiple scanners produce conflicting vulnerability data requiring manual reconciliation

**What breaks without it:**

- Hours spent investigating conflicting data—analysts paralyzed determining which scanner to trust
- False positives consume remediation capacity—days investigating vulnerabilities that don't exist

**What "good" looks like:**

- Level 3: Source of truth documentation, false positive procedures, validation checks, conflict resolution
- Level 4+: Automated quality checks, false positive library, tracked metrics, systematic improvement

**Who should care:**

- Security teams struggling with conflicting vulnerability data from multiple scanning tools
- Security operations needing authoritative data source when scanners report different severity ratings
- Asset owners frustrated by false positives creating remediation burden for non-existent vulnerabilities

## URGENCY ASSESSMENT

☑ Critical Foundation (prevents conflicting data paralysis)

☐ Compliance Driver

☐ Risk Mitigation

☑ Operational Efficiency (eliminates false positive waste)

☑ Strategic Enhancement (enables confident prioritization)

*(If unchecked at Level 2+, organization wastes resources on inaccurate data and false positives)*

## FRAMEWORK ALIGNMENT EXAMPLES

*This capability supports accountability requirements in commonly adopted security frameworks. These examples illustrate alignment, not exhaustive control coverage.*

**NIST 800-53:** Demonstrates inventory accuracy with vulnerability data validation

**NIST CSF 2.0:** Shows asset management with accurate vulnerability associations

**CIS v8:** Provides asset inventory accuracy through vulnerability data correlation

**ISO 27001:** Demonstrates vulnerability management with documented data quality controls

## MATURITY QUICK CHECK

○ Level 1: No source of truth, conflicting data, reactive false positive handling

○ Level 2: Informal tribal knowledge, ad hoc conflict resolution, individual handling

○ Level 3: **Source of truth docs, false positive procedures, validation checks, conflict resolution**

○ Level 4: Automated checks, false positive library, quality metrics, systematic reviews

○ Level 5: ML-enhanced detection, data lineage, automated correlation, continuous optimization

## DEPENDENCIES & BOUNDARIES

**Depends on:** Asset Inventory, Scanning & Detection Coverage, Risk-Based Prioritization

**Enables:** Confident prioritization, efficient remediation, trusted reporting

**This is NOT:** Universal scanner authority, zero false positive guarantee

Related Resources: Data Quality & Source of Truth Guide · Framework Mapping · Self-Assessment