OWASP ASVS, CIS Controls, NIST SP 800-53 Comparison

Detailed Breakdown

1. OWASP ASVS

- **Purpose:** A **standard for verifying** the security of web applications and APIs. It's a list of security requirements (what to check for) rather than how to implement them.
- **Use Case:**
  - Creating a secure development lifecycle (SDLC) checklist.
  - Defining security requirements for developers.
  - Guiding penetration tests and security code reviews.
  - Procurement (e.g., "Must achieve ASVS Level 2").
- **Key Traits:**
  - **Granular & technical:** Goes deep into specific vulnerabilities (crypto, auth, injection).
  - **Outcome-focused:** Describes *what* a secure application should do/not do.
  - **Tiered:** Levels 1-3 allow scaling based on app risk profile.

2. CIS Critical Security Controls

- **Purpose:** A **prioritized set of actionable safeguards** to defend against the most common cyber attacks. It's focused on **implementation** and **operations**.
- **Use Case:**
  - Building a foundational cybersecurity program ("cyber hygiene").
  - Remediating common weaknesses post-assessment.
  - Guiding IT and security teams on daily operational tasks.
- **Key Traits:**
  - **Prioritized & practical:** Starts with Inventory (CIS Safeguard 1), then Secure Config (2), etc.
  - **Offense-informed:** Based on real-world attack patterns.
  - **Actionable:** Specific recommendations (e.g., "Deploy and automate asset discovery").

3. NIST SP 800-53

- **Purpose:** A **comprehensive catalog** of security and privacy controls for federal information systems. It is **risk management and compliance-oriented**.
- **Use Case:**
  - Compliance with FISMA, FedRAMP, and other U.S. government regulations.
  - Building a robust, auditable security program in highly regulated environments.
  - As a source for deriving organizational control baselines.
- **Key Traits:**
  - **Comprehensive & granular:** Covers technical, operational, and management controls.
  - **Risk-based:** Offers baselines (Low, Moderate, High) based on system impact.

  - **Framework-agnostic:** Can be mapped to others; part of the larger NIST Cybersecurity Framework (CSF) and RMF.

How They Work Together (Mapping & Synergy)

These frameworks are **complementary, not competitive**. A mature organization uses them in concert:

1. **Strategic Foundation:** Use **NIST 800-53** (or the NIST CSF) to establish your overarching **risk management program** and fulfill compliance mandates.
2. **Operational Execution:** Use **CIS Controls** as the **practical implementation guide** for your IT infrastructure and operations (e.g., how to manage inventories, harden systems, monitor logs).
3. **Application-Specific Deep Dive:** Use **OWASP ASVS** to define and verify **secure software development practices** and the security of your custom applications.

Common Mapping Example:

- **NIST 800-53 Control:** `SI-3 Malicious Code Protection` (requires a capability to detect and eradicate malicious code).
- **CIS Safeguard:** `8.5: Deploy and Maintain Anti-Malware Software` (provides specific steps to implement SI-3).
- **OWASP ASVS:** Does not cover endpoint AV. However, for a malicious upload, **ASVS Chapter 7 (Malicious Controls Verification)** would have requirements for checking file types and scanning uploaded files.

Which One to Choose?

- **You are a developer, appsec professional, or testing an application?** → Start with **OWASP ASVS**.
- **You are building or improving your IT security operations (SOC) and need clear priorities?** → Start with **CIS Controls**.
- **You are in a U.S. federal agency, a government contractor, or a highly regulated industry needing formal compliance? → NIST SP 800-53** is likely required.
- **For most organizations:** Use **CIS Controls for operational hygiene** and **OWASP ASVS for software security**, and map your efforts back to **NIST 800-53/CSF** for governance and reporting.

Analogy

Think of securing a castle:

- **NIST 800-53** is the **architectural blueprint and building code** (comprehensive, covers walls, moat, armory, guard routines).

- **CIS Controls** is the **garrison commander's checklist** (prioritized tasks: post guards, inventory weapons, check gate strength, train soldiers).
- **OWASP ASVS** is the **specialist's guide to securing the royal vault's lock mechanism** (deep, technical, specific to a critical asset).

You need all three perspectives for a truly secure defense.