**NIST to OWASP Security Controls Mapping**

Comprehensive Security Framework

A Complete Guide to Integrating NIST Controls with OWASP Top 10

April 28, 2025

# **Table of Contents**

TOC Placeholder - Will be populated automatically when opened in Word

# **Executive Summary**

This comprehensive document provides a detailed mapping between the National Institute of Standards and Technology (NIST) cybersecurity controls and the Open Web Application Security Project (OWASP) Top 10 web application security risks. The integration of these two frameworks offers organizations a robust approach to addressing both organizational and technical aspects of cybersecurity.

The NIST frameworks provide broad organizational security controls, while the OWASP Top 10 focuses specifically on critical web application vulnerabilities. By mapping these frameworks together, organizations can develop a more comprehensive security program that addresses both organizational governance and technical implementation requirements.

# **NIST vs. OWASP Comparison**

This section provides a comparison between NIST frameworks and OWASP Top 10, highlighting their complementary nature and how they can be integrated to create a comprehensive security program.

## **NIST Framework Overview**

NIST SP 800-53 is a comprehensive security control catalog with over 1,000 controls across 20 families. It provides detailed specifications for security and privacy controls for federal information systems and organizations.

## **OWASP Top 10 Overview**

The OWASP Top 10 is a focused list of the 10 most critical web application security risks based on real-world data. It is periodically updated, with the latest version released in 2021.

# **NIST Controls to OWASP Top 10 Mapping**

This section provides a detailed mapping between NIST SP 800-53 controls and OWASP Top 10 web application security risks.

## **A01:2021 - Broken Access Control**

Risk Description: Restrictions on authenticated users aren't properly enforced. Attackers can exploit flaws to access unauthorized functionality/data.

### **Primary NIST Controls:**

* **AC-3 - Access Enforcement:** Enforces approved authorizations for logical access to information and system resources.
* **AC-5 - Separation of Duties:** Prevents any single individual from having complete control over critical processes.
* **AC-6 - Least Privilege:** Implements the principle of least privilege, allowing only authorized access necessary to accomplish assigned tasks.

## **A02:2021 - Cryptographic Failures**

Risk Description: Failures related to cryptography that often lead to sensitive data exposure or system compromise.

### **Primary NIST Controls:**

* **SC-13 - Cryptographic Protection:** Implements FIPS-validated or NSA-approved cryptography for protecting information.
* **SC-28 - Protection of Information at Rest:** Protects the confidentiality and integrity of information at rest through appropriate cryptographic mechanisms.
* **SC-8 - Transmission Confidentiality and Integrity:** Protects the confidentiality and integrity of transmitted information through encryption.

# **Implementation Guide**

This section provides a step-by-step guide for implementing an integrated security program using both NIST and OWASP frameworks.

## **Implementation Phases**

### **Planning Phase**

The planning phase establishes the foundation for your integrated security program, ensuring alignment with organizational needs, proper scoping, and clear objectives.

### **Implementation Phase**

During the implementation phase, security controls are deployed according to the roadmap established in the planning phase, with a focus on addressing high-priority risks first.

### **Validation Phase**

The validation phase ensures that implemented controls are effective at mitigating the identified risks through testing, assessment, and evaluation.

### **Maintenance Phase**

The maintenance phase focuses on continuous monitoring, periodic reassessment, and ongoing improvement of security controls to address evolving threats.

# **Conclusion**

The integration of NIST controls and OWASP Top 10 provides organizations with a comprehensive approach to addressing both organizational and technical aspects of cybersecurity. By mapping these frameworks together, organizations can develop a more robust security program that protects against a wide range of threats and vulnerabilities.