**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 \o "1-3" \h \z \u**

*Right-click and select 'Update Field' to update the table of contents after opening this document 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 (including SP 800-53, Cybersecurity Framework, and SP 800-171) 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.

This document includes detailed control mappings, implementation guidance, expert insights, and practical resources to help organizations effectively implement these security controls.

## Key Benefits of the Integrated Approach

* Comprehensive coverage across organizational and technical security domains
* Improved alignment between management requirements and development team implementation
* Enhanced compliance posture while addressing real-world security threats
* Efficient resource allocation based on risk prioritization
* More effective security controls validated through multiple perspectives

# 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. The framework is regularly updated, with the latest being Revision 5 (2020).

**Key characteristics of NIST frameworks include:**

* Comprehensive coverage of security and privacy controls
* Risk-based approach to control selection and implementation
* Flexible framework that can be tailored to organization needs
* Regular updates to address emerging threats and technologies
* Strong emphasis on organizational risk management

## 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. The OWASP Top 10 provides specific guidance for addressing common web application vulnerabilities.

**Key characteristics of OWASP Top 10 include:**

* Focus on web application security risks
* Based on real-world data and attack patterns
* Practical guidance for developers and security professionals
* Updated periodically to reflect emerging threats
* Community-driven approach to security awareness

## Integration Benefits

Combining both frameworks creates a stronger, more comprehensive security program that addresses both organizational and technical aspects of cybersecurity. The integration provides:

* Comprehensive coverage across organizational and technical domains
* Better alignment between management and development teams
* Improved compliance alongside practical security implementation
* More efficient resource allocation based on risk assessment
* Enhanced security validation through multiple perspectives

# 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. Each OWASP risk is mapped to primary and supporting NIST controls to provide comprehensive coverage.

## 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.
* **AC-16 - Security and Privacy Attributes:** Provides explicit security and privacy attributes that can be used for access control decisions.

### Supporting NIST Controls

* **AC-4 - Information Flow Enforcement:** Controls the flow of information within the system and between interconnected systems.
* **AC-17 - Remote Access:** Establishes and enforces security requirements for remote access sessions.
* **CM-7 - Least Functionality:** Configures systems to provide only essential capabilities required for operation.
* **SC-23 - Session Authenticity:** Protects the authenticity of communications sessions by validating session identifiers.

### Implementation Guidance

* Implement centralized access control mechanisms that enforce all user access policies
* Use role-based access control (RBAC) with proper separation of duties
* Implement session management controls to prevent unauthorized access
* Regularly audit and review access control configurations and logs
* Deny by default except for public resources
* Implement access control mechanisms once and reuse them
* Enforce record ownership rather than accepting user-controlled data

## 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 the confidentiality and integrity of 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 and secure protocols.
* **SC-12 - Cryptographic Key Establishment and Management:** Establishes and manages cryptographic keys throughout their lifecycle in accordance with established policies.

### Implementation Guidance

* Use strong, industry-standard encryption algorithms (AES-256, RSA-2048)
* Implement proper key management procedures including secure key storage
* Encrypt all sensitive data in transit using TLS 1.3
* Classify data and apply appropriate protection based on sensitivity
* Use secure hashing algorithms (SHA-256 or better) for password storage
* Enforce HTTPS with secure protocols (TLS 1.2+)
* Store passwords using strong adaptive hashing functions

# 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.

**Key implementation steps:**

1. Complete risk assessment and prioritization
2. Establish governance framework
3. Select appropriate NIST framework (CSF, 800-53, 800-171)
4. Map OWASP Top 10 risks to relevant NIST controls
5. Develop an implementation roadmap with defined phases and milestones

### 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.

**Key implementation steps:**

1. Implement critical controls for A01 (Broken Access Control) and A02 (Cryptographic Failures)
2. Establish secure coding standards
3. Deploy static application security testing (SAST)
4. Implement controls for A03-A06
5. Set up monitoring and logging capabilities
6. Implement remaining controls for A07-A10

### Validation Phase

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

**Key implementation steps:**

1. Conduct vulnerability assessments and penetration testing
2. Perform security control assessments
3. Validate control effectiveness against OWASP Top 10 risks
4. Review and analyze security testing results
5. Address identified gaps and weaknesses

### Maintenance Phase

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

**Key implementation steps:**

1. Establish continuous monitoring program
2. Conduct periodic security assessments
3. Update controls based on new threats and vulnerabilities
4. Perform regular security training and awareness
5. Continuously improve security controls and processes

# Best Practices and Recommendations

This section provides best practices and expert recommendations for implementing an integrated NIST and OWASP security framework.

## Secure By Design

Integrate security throughout the system development lifecycle. Address security requirements, architecture, and design before implementation begins.

*Related NIST Controls: SA-3, SA-8, SA-15*

## Defense in Depth

Implement multiple layers of controls to protect against various attack vectors. Don't rely on a single security measure for critical systems.

*Related NIST Controls: SC-7, SI-3, SI-4*

## Continuous Monitoring

Implement ongoing security monitoring to detect and respond to potential security incidents and vulnerabilities as they emerge.

*Related NIST Controls: AU-6, CA-7, SI-4*

## Regular Assessment

Perform regular security assessments and testing to validate control effectiveness and identify new vulnerabilities.

*Related NIST Controls: CA-2, RA-5, SA-11*

## Integration Approach

Choose an implementation tier based on your organization's risk assessment, available resources, and security program maturity. Start with the Basic tier for critical controls and progressively enhance implementation as resources allow.

*Related NIST Controls: PL-2, PM-4, RA-3*

# 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.

Implementing this integrated framework requires a structured approach that includes thorough planning, phased implementation, rigorous validation, and ongoing maintenance. By following the guidance provided in this document, organizations can establish a strong security posture that addresses both compliance requirements and real-world security threats.

Remember that security is an ongoing process, not a one-time project. Continuously improve your security controls and processes to address evolving threats and changes in your organization's environment.

## References and Resources

* NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
* NIST Cybersecurity Framework (CSF)
* OWASP Top 10 - 2021
* OWASP Application Security Verification Standard (ASVS)
* NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations