Contents

[Vulnerability Prioritization Frameworks 1](#_Toc202210102)

[Exploit Prediction Scoring System (EPSS) 3](#_Toc202210103)

[NIST Risk Management Framework (RMF) 6](#_Toc202210104)

[NIST IR 8286r1 7](#_Toc202210105)

[Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) 10](#_Toc202210106)

[FAIR (Factor Analysis of Information Risk) framework 11](#_Toc202210107)

[VULCON System 12](#_Toc202210108)

[Stakeholder-Specific Vulnerability Categorization (SSVC) 13](#_Toc202210109)

[SSVC Decision Tree 14](#_Toc202210110)

[Table of factors with references 15](#_Toc202210111)

[OWASP Risk Rating Methodology 17](#_Toc202210112)

## Vulnerability Prioritization Frameworks

There are several well-known risk assessment frameworks used for **vulnerability remediation**, each designed to help organizations prioritize and mitigate security risks effectively. Here are some of the most widely recognized frameworks:

**1. NIST Risk Management Framework (RMF)**

* Developed by **NIST SP 800-37**, RMF provides a structured approach to managing cybersecurity risks.
* Focuses on **categorizing, selecting, implementing, assessing, authorizing, and monitoring** security controls.

**2. Factor Analysis of Information Risk (FAIR)**

* A **quantitative** risk assessment model that translates cybersecurity risks into **financial impact**.
* Helps organizations prioritize vulnerabilities based on **monetary loss potential**.

**3. Common Vulnerability Scoring System (CVSS)**

* A standardized framework for assessing the **severity** of vulnerabilities.
* Uses metrics such as **exploitability, impact, and environmental factors** to prioritize remediation.

**4. Exploit Prediction Scoring System (EPSS)**

* Developed to estimate the **likelihood** of a vulnerability being exploited in the wild.
* Helps organizations focus on **high-risk vulnerabilities** that are more likely to be targeted.

**5. Stakeholder-Specific Vulnerability Categorization (SSVC)**

* A decision-tree-based framework used by **CISA** to prioritize vulnerabilities.
* Considers factors like **exploitation status, safety impact, and system prevalence**.

**6. Cyber Kill Chain Framework**

* Developed by **Lockheed Martin**, this framework maps out the **stages of a cyber attack**.
* Helps organizations assess vulnerabilities based on their role in an attack sequence.

**7. MITRE ATT&CK Framework**

* A knowledge base of **adversary tactics and techniques** used in cyber attacks.
* Helps organizations assess vulnerabilities based on **real-world attack scenarios**.

**8. VULCON System**

* A **multi-objective optimization** framework for vulnerability remediation.
* Uses **resource allocation modeling** to prioritize fixes based on **business impact**.

**9. CISA SSVC Methodology**

* A structured approach to **vulnerability prioritization** based on **risk exposure**.
* Helps organizations **triage vulnerabilities** efficiently.

**10. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**

* A **self-directed risk assessment methodology** developed by **CERT**.
* Focuses on **organizational risk management** rather than just technical vulnerabilities.

These frameworks provide different approaches to **risk assessment and remediation**, helping organizations **prioritize vulnerabilities** based on **impact, exploitability, and business risk**. Let me know if you need more details on any of these!

## Exploit Prediction Scoring System (EPSS)

The **Exploit Prediction Scoring System (EPSS)** is a **data-driven framework** designed to estimate the likelihood that a software vulnerability will be exploited in the wild. Unlike traditional vulnerability scoring systems like **CVSS**, which focus on severity, EPSS helps organizations **prioritize remediation efforts** based on real-world exploitability.

**Key Features of EPSS**

* **Probability-Based Scoring**: EPSS assigns a score between **0 and 1 (0-100%)**, indicating the likelihood of exploitation.
* **Real-Time Threat Intelligence**: Uses **CVE data, exploit trends, and security telemetry** to refine predictions.
* **Dynamic Updates**: EPSS scores are continuously updated based on **new threat intelligence**.
* **Complementary to CVSS**: While CVSS measures **intrinsic severity**, EPSS focuses on **actual exploitation risk**.

**Why EPSS Matters**

* Helps organizations **prioritize patching efforts** based on **real-world attack likelihood**.
* Reduces **false urgency** by focusing on vulnerabilities that are **actively exploited**.
* Supports **efficient resource allocation** for cybersecurity teams.

EPSS is widely used by **security researchers, enterprises, and government agencies** to enhance vulnerability management strategies.

EPSS calculates **Probability-Based Scoring** using a **machine-learning model** that analyzes various factors to estimate the likelihood of a vulnerability being exploited in the next **30 days**. The scoring process involves several key steps:

**EPSS Calculation Process**

1. **Data Gathering** – Collects vulnerability details from sources like **MITRE CVE, NVD, CWE, Exploit-DB, and security scanners**.
2. **Exploit Activity Analysis** – Examines real-world exploitation evidence from **honeypots, intrusion detection systems (IDS/IPS), and malware analysis platforms**.
3. **Machine Learning Training** – Uses AI models to identify patterns between vulnerability characteristics and exploitation likelihood.
4. **Optimization & Accuracy Testing** – Evaluates prediction accuracy using metrics like **true positives (TP), false positives (FP), false negatives (FN), and true negatives (TN)**.
5. **Daily Score Updates** – Continuously refines predictions based on **new threat intelligence**.

**EPSS Score Interpretation**

* **Scores range from 0 to 1 (0-100%)**, indicating the probability of exploitation.
* **Higher scores** mean a vulnerability is more likely to be exploited.
* **Lower scores** suggest a lower risk of exploitation.

EPSS helps organizations **prioritize patching efforts** by focusing on vulnerabilities that are **actively exploited** rather than just severe ones.

A graph with a blue line and a blue line

AI-generated content may be incorrect.

## NIST Risk Management Framework (RMF)

The **NIST Risk Management Framework (RMF)** is a **structured, risk-based approach** to managing cybersecurity, privacy, and supply chain risks across an organization's **system development life cycle (SDLC)**. It is outlined in **NIST SP 800-37** and integrates security controls from **NIST SP 800-53** to ensure comprehensive risk management.

**Key Steps in the RMF Process**

1. **Prepare** – Establish the organization's risk management strategy and readiness.
2. **Categorize** – Define the system's security impact based on data sensitivity and operational importance.
3. **Select** – Choose appropriate security controls from **NIST SP 800-53** based on risk assessment.
4. **Implement** – Deploy and document security controls within the system.
5. **Assess** – Evaluate the effectiveness of security controls to ensure they function as intended.
6. **Authorize** – Senior officials make a **risk-based decision** on whether the system can operate.
7. **Monitor** – Continuously track security controls and emerging threats to maintain compliance.

**Why RMF Matters**

* **Integrates cybersecurity into the SDLC**, ensuring security is considered from the start.
* **Provides a flexible, scalable framework** applicable to **government, private sector, and critical infrastructure**.
* **Aligns with regulatory requirements**, including **FISMA (Federal Information Security Modernization Act)**.

For a deeper dive, you can explore the official [**NIST RMF guide**](https://csrc.nist.gov/Projects/risk-management/about-rmf).

## NIST IR 8286r1

Cybersecurity risk prioritization in **NIST IR 8286r1** focuses on integrating cybersecurity risk management into **enterprise risk management (ERM)** to ensure that organizations can effectively assess, prioritize, and mitigate cybersecurity threats in alignment with business objectives.

**Key Aspects of Cybersecurity Risk Prioritization in NIST IR 8286r1**

1. **Risk Aggregation & Prioritization**
   * Organizations must **aggregate cybersecurity risks** across different business units to create a **comprehensive risk profile**.
   * Prioritization is based on **business impact, likelihood of exploitation, and operational dependencies**.
2. **Cybersecurity Risk Register (CSRR)**
   * The **Cybersecurity Risk Register (CSRR)** is a structured repository for tracking cybersecurity risks.
   * Risks are categorized based on **severity, potential impact, and mitigation strategies**.
3. **Risk Response Selection**
   * Organizations must evaluate **risk response options**, including **acceptance, mitigation, transfer, or avoidance**.
   * The selection process considers **cost-benefit analysis, regulatory requirements, and mission-critical dependencies**.
4. **Integration with Enterprise Risk Register (ERR)**
   * Cybersecurity risks are **mapped to enterprise risk categories**, ensuring alignment with **strategic business objectives**.
   * This integration helps executives **make informed decisions** about cybersecurity investments.
5. **Continuous Monitoring & Risk Conditioning**

* Organizations must implement **continuous monitoring** to track evolving threats and adjust risk prioritization accordingly.
* **Risk conditioning** ensures that cybersecurity risks are **regularly reassessed** based on new threat intelligence.

**Why This Matters**

* **Improves cybersecurity governance** by aligning risk management with enterprise-wide strategies.
* **Enhances decision-making** by providing structured methodologies for prioritizing cybersecurity risks.
* **Supports regulatory compliance** by ensuring cybersecurity risks are documented and managed effectively.

You can explore the full document [here](https://csrc.nist.gov/pubs/ir/8286/r1/ipd).

The **Cybersecurity Risk Register (CSRR)** is a structured repository used by organizations to **identify, document, and track cybersecurity risks**. It serves as a centralized record of potential threats, vulnerabilities, and associated risk mitigation strategies.

**Key Components of a CSRR**

* **Risk Description** – A detailed explanation of the identified cybersecurity risk.
* **Threat Source** – The origin or actor responsible for the risk (e.g., cybercriminals, insider threats).
* **Likelihood** – The probability of the risk materializing.
* **Impact** – The potential consequences on business operations, financials, or reputation.
* **Risk Owner** – The individual or team responsible for managing the risk.
* **Mitigation Strategy** – Actions taken to reduce or eliminate the risk.
* **Residual Risk** – The remaining risk after mitigation efforts.
* **Review & Update Frequency** – A schedule for reassessing and updating risk entries.

**Purpose of a CSRR**

* **Enhances cybersecurity governance** by providing visibility into risk exposure.
* **Supports risk prioritization** by aligning cybersecurity risks with enterprise risk management (ERM).
* **Facilitates decision-making** by helping executives allocate resources effectively.

You can explore more details on the **Cybersecurity Risk Register** [here](https://csrc.nist.gov/glossary/term/cybersecurity_risk_register).

## Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

The **Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)** framework is a **risk assessment methodology** designed to help organizations identify, evaluate, and mitigate cybersecurity risks. Developed by **Carnegie Mellon University** for the **U.S. Department of Defense**, OCTAVE focuses on **organizational risk management** rather than just technical vulnerabilities.

**Key Features of OCTAVE**

* **Self-Directed Approach**: Organizations conduct their own risk assessments using internal teams.
* **Business-Centric**: Prioritizes **critical assets** and their impact on business operations.
* **Threat & Vulnerability Identification**: Helps organizations **map threats to assets** and assess security gaps.
* **Flexible Methodology**: Includes variations like **OCTAVE-S** (for smaller organizations) and **OCTAVE Allegro** (for complex environments).

**Three Phases of OCTAVE**

1. **Build Asset-Based Threat Profiles**: Identify critical assets and define security requirements.
2. **Identify Infrastructure Vulnerabilities**: Assess weaknesses in IT systems and network access paths.
3. **Develop a Risk Mitigation Strategy**: Prioritize remediation efforts based on business impact.

**Why OCTAVE Matters**

* **Aligns cybersecurity with business objectives**.
* **Empowers organizations** to manage their own risk assessments.
* **Provides a structured, repeatable process** for vulnerability remediation.

OCTAVE is widely used in **government, financial, and healthcare sectors** to enhance **cyber resilience**.

## FAIR (Factor Analysis of Information Risk) framework

The **FAIR (Factor Analysis of Information Risk) framework** is a **quantitative** risk assessment methodology designed to help organizations measure and manage cybersecurity and operational risks in **financial terms**. Unlike traditional risk assessment models that rely on subjective ratings (e.g., "high," "medium," "low"), FAIR provides a structured approach to **risk quantification**, enabling more informed decision-making.

**Key Components of FAIR**

1. **Loss Event Frequency (LEF)** – Estimates how often a risk event is likely to occur.
2. **Loss Magnitude (LM)** – Measures the financial impact of a risk event.
3. **Threat Event Frequency (TEF)** – Evaluates how often a threat actor attempts an attack.
4. **Vulnerability (V)** – Assesses the probability that an attack will succeed.
5. **Primary & Secondary Losses** – Differentiates between direct financial losses (e.g., system downtime) and indirect losses (e.g., reputational damage).

**Why FAIR is Revolutionary**

* **Quantifies risk in financial terms**, making it easier for executives to prioritize cybersecurity investments.
* **Provides a common language** for risk discussions across technical and business teams.
* **Supports risk-based decision-making**, helping organizations allocate resources effectively.

FAIR is recognized as an **international standard** by **The Open Group** and is widely used in cybersecurity risk management. If you’d like a deeper dive into FAIR’s methodology, you can check out [this resource](https://www.fairinstitute.org/what-is-fair). Let me know if you need more details!

## VULCON System

The VULCON System (VULnerability CONtrol) is a vulnerability prioritization, mitigation, and management framework designed to optimize cybersecurity remediation efforts. It was developed to address the challenge of efficiently allocating resources for vulnerability patching while minimizing security risks.

Key Features of VULCON

- Multi-Objective Optimization: Uses mixed integer optimization algorithms to prioritize vulnerabilities based on risk exposure, asset criticality, and available personnel resources.

- Time-to-Vulnerability Remediation (TVR): Measures the time required to remediate vulnerabilities, helping organizations optimize their response efforts.

- Total Vulnerability Exposure (TVE): Assesses the cumulative risk posed by unpatched vulnerabilities, allowing organizations to track and reduce overall exposure.

- Real-World Testing: VULCON has been tested on months of real vulnerability scan data from a Cyber-Security Operations Center (CSOC), demonstrating its effectiveness in reducing exposure.

Why VULCON Matters

- Improves vulnerability response efficiency by optimizing remediation workflows.

- Helps organizations allocate cybersecurity resources effectively based on risk impact.

- Provides operational guidance for maintaining a target security posture.

VULCON is a valuable tool for cybersecurity teams, government agencies, and enterprises looking to enhance their vulnerability management strategies.

## Stakeholder-Specific Vulnerability Categorization (SSVC)

The **Stakeholder-Specific Vulnerability Categorization (SSVC)** is a **vulnerability prioritization methodology** developed by **CISA** in collaboration with **Carnegie Mellon University's Software Engineering Institute (SEI)**. It provides a **decision-tree model** to help organizations prioritize vulnerabilities based on **exploitation status, technical impact, automatability, mission prevalence, and public well-being impact**.

**Key Features of SSVC**

* **Decision Tree-Based Approach**: SSVC categorizes vulnerabilities into four possible actions:
  + **Track**: No immediate action required; monitor for updates.
  + **Track**\*: Requires closer monitoring due to specific characteristics.
  + **Attend**: Needs attention from supervisory-level individuals; may require internal/external notifications.
  + **Act**: Requires urgent action from leadership; immediate remediation recommended.
* **Focus on Mission-Critical Systems**: SSVC prioritizes vulnerabilities based on their impact on **critical infrastructure and government entities**.
* **Alternative to CVSS**: Unlike CVSS, which focuses on severity scores, SSVC considers **real-world exploitation and operational impact**.

**Why SSVC Matters**

* Helps organizations **triage vulnerabilities efficiently**.
* Reduces reliance on **generic severity scores** by incorporating **contextual risk factors**.
* Supports **government agencies and critical infrastructure** in making informed remediation decisions.

### SSVC Decision Tree

A diagram of a diagram

AI-generated content may be incorrect.

## Table of factors with references

|  |  |  |  |
| --- | --- | --- | --- |
| **Factor** | **Description** | **Methodology** | **Source** |
| Risk Impact | Evaluates the potential consequences of a vulnerability on enterprise objectives. | Risk assessment frameworks (e.g., FAIR, OCTAVE) | NIST IR 8286r1, p. 12 |
| Likelihood of Exploitation | Assesses the probability that a vulnerability will be exploited. | Threat modeling, historical exploit analysis | NIST SP 800-30r1, p. 25 |
| Security Control Deficiencies | Identifies gaps in security controls that may increase vulnerability risk. | Security audits, compliance assessments | NIST SP 800-53r5, p. 47 |
| Common Vulnerability Scoring System (CVSS) Base Score | Measures the severity of vulnerabilities using standardized metrics. | CVSS scoring methodology | NIST IR 8409, p. 8 |
| Environmental Impact | Adjusts vulnerability severity based on the specific operational environment. | Contextual risk analysis, asset dependency mapping | NIST IR 7435, p. 14 |
| Exploit Prediction Scoring System (EPSS) | Estimates the likelihood of exploitation based on historical data. | Machine learning models, exploit trend analysis | NIST CSWP 41, p. 3 |
| Known Exploited Vulnerabilities (KEV) | Prioritizes vulnerabilities that have been actively exploited in the wild. | Threat intelligence feeds, KEV databases | NIST CSWP 41, p. 5 |
| Threat Intelligence | Incorporates real-time threat data to assess emerging risks. | Threat intelligence platforms, adversary simulation | NIST CSWP 41, p. 7 |
| Asset Criticality | Evaluates the importance of affected systems to business operations. | Business impact analysis, dependency mapping | NVD - Vulnerability Metrics, p. 10 |
| Patch Availability | Determines whether a fix is available and its urgency. | Patch management systems, vendor advisories | NVD - Vulnerability Metrics, p. 12 |
| Temporal Metrics | Adjusts prioritization based on evolving threat landscapes. | Continuous monitoring, real-time risk scoring | NVD - Vulnerability Metrics, p. 15 |
| Likely Exploited Vulnerabilities (LEV) | Enhances KEV and EPSS-based remediation prioritization using probability equations. | Statistical modeling, exploit likelihood estimation | SecurityWeek - LEV Metric |
| Stakeholder-Specific Vulnerability Categorization (SSVC) | Prioritizes vulnerabilities based on exploitation status, safety impact, and system prevalence. | Decision trees, structured risk assessment | CISA SSVC Guide |
| VULCON System | Optimizes vulnerability remediation using multi-objective prioritization. | Mixed integer optimization, resource allocation modeling | PNNL - VULCON |

## OWASP Risk Rating Methodology

The OWASP Risk Rating Methodology is a structured approach to assessing the risk associated with vulnerabilities, particularly in web applications. It helps prioritize vulnerabilities based on their potential impact and likelihood of being exploited. Here's how it applies to vulnerability rating:

1. **Identify the Vulnerability**: Determine the specific vulnerability present in the application, such as SQL injection, cross-site scripting (XSS), or insecure direct object references.
2. **Assess Likelihood**: Evaluate how likely it is that the vulnerability will be exploited. This involves considering factors such as:
   * **Skill Level Required**: How skilled does an attacker need to be to exploit the vulnerability?
   * **Motive**: Is there a strong incentive for attackers to exploit this vulnerability?
   * **Opportunity**: Are there many opportunities for attackers to exploit this vulnerability?
   * **Ease of Discovery**: How easy is it for attackers to discover the vulnerability?
3. **Assess Impact**: Determine the potential impact of the vulnerability being exploited. This includes:
   * **Technical Impact**: What damage can be done to the system or data?
   * **Business Impact**: How does the exploitation affect business operations, reputation, or financial standing?
4. **Calculate Risk**: Use the OWASP Risk Rating formula to calculate the overall risk:
   * **Risk = Likelihood x Impact**
   * Assign numerical values to likelihood and impact to derive a risk score.
5. **Prioritize Remediation**: Based on the risk score, prioritize vulnerabilities for remediation. High-risk vulnerabilities should be addressed first to reduce the potential for exploitation.
6. **Document and Review**: Document the findings and review them regularly to ensure that the risk assessment remains current and relevant.

By applying the OWASP Risk Rating Methodology, organizations can systematically evaluate and prioritize vulnerabilities, ensuring that resources are allocated effectively to mitigate the most significant risks.

Start

├── Identify Vulnerability

│ ├── Assess Likelihood

│ │ ├── Skill Level Required

│ │ │ ├── High

│ │ │ │ ├── Low Likelihood

│ │ │ └── Low

│ │ │ ├── High Likelihood

│ │ ├── Motive

│ │ │ ├── High

│ │ │ │ ├── High Likelihood

│ │ │ └── Low

│ │ │ ├── Low Likelihood

│ │ ├── Opportunity

│ │ │ ├── High

│ │ │ │ ├── High Likelihood

│ │ │ └── Low

│ │ │ ├── Low Likelihood

│ │ ├── Ease of Discovery

│ │ │ ├── Easy

│ │ │ │ ├── High Likelihood

│ │ │ └── Difficult

│ │ │ ├── Low Likelihood

├── Assess Impact

│ ├── Technical Impact

│ │ ├── High

│ │ │ ├── High Impact

│ │ └── Low

│ │ ├── Low Impact

│ ├── Business Impact

│ │ ├── High

│ │ │ ├── High Impact

│ │ └── Low

│ │ ├── Low Impact

├── Calculate Risk

│ ├── Risk = Likelihood x Impact

│ │ ├── High Risk

│ │ ├── Medium Risk

│ │ └── Low Risk

└── End

**Explanation:**

1. **Identify Vulnerability**: Start by identifying the specific vulnerability.
2. **Assess Likelihood**: Evaluate the likelihood of exploitation based on:
   * **Skill Level Required**: Determine if high or low skill is needed.
   * **Motive**: Assess the motivation level of potential attackers.
   * **Opportunity**: Evaluate the opportunities available for exploitation.
   * **Ease of Discovery**: Consider how easily the vulnerability can be discovered.
3. **Assess Impact**: Determine the potential impact if the vulnerability is exploited:
   * **Technical Impact**: Evaluate the technical consequences.
   * **Business Impact**: Consider the business implications.
4. **Calculate Risk**: Use the formula "Risk = Likelihood x Impact" to determine the overall risk level:
   * **High Risk**: Requires immediate attention.
   * **Medium Risk**: Needs to be addressed but is less urgent.
   * **Low Risk**: Can be monitored and addressed as needed.