

ABS Vulnerability Risk Management for the Financial Industry in Singapore



April 2025

abs

Table of Contents

1. Introduction	1
1.1 Objective	1
2. Asset Management	2
2.1 Asset Category	2
2.2 Asset Context	3
3. Vulnerability Identification	4
3.1 Vulnerability Data Sources	4
3.2 Vulnerability Risk Analysis	5
3.3 Vulnerability Assessment	5
3.4 Vulnerability Remediation Prioritisation	6
3.5 Remediation Timeline	7
3.6 Risk Response Scenarios	7
4. Vulnerability Remediation	8
4.1 Considerations for Effective Vulnerability Remediation	8
4.2 Process Managing Zero-Day Vulnerability	8
4.3 Information Gathering Prior to Remediation	9
4.4 Testing of Patches or Vulnerabilities Remediation Solution	9
4.5 Remediation Timelines	10
4.6 Managing Mitigation in case of unavailability of Patch(es) for vulnerability	11
4.7 System Obsolescence	11
4.8 Post Deployment / Remediation Verification	11
4.9 Measurement / Metrics	12
4.10 Consequence Management	12
5. Appendix	13
6. References	14
7. Glossary	15

1. Introduction

1.1 Objective

With the focus on digitalisation, Financial Institutions (FIs) have been rapidly growing their IT hardware / software footprint. Concurrently, security vulnerabilities identified continue to increase year-on-year. In 2022, National Vulnerability Database announced 25,043 new vulnerabilities. In 2023, new vulnerabilities increased further by 15% to 28,822¹. These new unique vulnerabilities then multiplied by assets and environments in FI, making the absolute vulnerabilities to increase in tandem.

Traditionally, each vulnerability needs to be risk-assessed by human who understand severity of the affected assets and prioritised for remediation according to its risk profile. This approach demands huge number of resources to assess and address these vulnerabilities and consequently, prevents focus on the vulnerabilities that truly matter.

With the diligent efforts of the regulators and FIs in Singapore to uplift the cyber maturity, any FI today has a higher level of cyber readiness and layered defences to protect against most vulnerabilities. The layered defences allow a FI to balance between resilience and security as aggressive patching without sufficient testing may result in service disruption.

This paper is intended to provide guidance to FIs in Singapore to adopt or to modernise their vulnerability management processes using widely adopted best practices.

The guidance is set out in the following sections:

- Section 2 addresses the identification of IT asset that provides visibility over hardware and software critical for supporting the IT operations and its attack surface.
- Section 3 addresses the strategy and approach in identifying and prioritising the treatment of vulnerabilities.
- Section 4 addresses the strategy in vulnerabilities remediation and mitigations.

¹ Total of new vulnerability obtained from National Vulnerability Database

2. Asset Management

Vulnerability management requires a complete and accurate inventory of assets within the FI computing infrastructure and applications. A common method for achieving this is by utilising a configuration management database (CMDB). Regularly scanning and discovering assets is important to identify any potential security vulnerabilities that may require patching. The inventory serves as the foundation for identifying assets that may need patching for security vulnerabilities.

It is important to note that the range of assets spans across various categories, a few examples of which are provided below. This paper does not aim to provide an exhaustive list of asset categories, and as technology continues to advance, new asset categories will undoubtedly emerge.

2.1 Asset Category

The asset category list can guide the prioritisation of vulnerabilities and subsequently determine the appropriate remediation procedures based on the nature of the assets. The following is a high-level grouping of assets. The FI should consider its situation and adjust the grouping as necessary.

- a. **Operating Systems:** All types of operating systems used for servers, endpoints (including laptops), and mobile platforms.
- b. **Open-Source Application, Middleware, and Database Services:** A variety of services including web servers, file servers, middleware, and database servers maintained as an Open-Sourced project.
- c. **Proprietary Business Application Software and Libraries:** A variety of business applications and libraries maintained by a software vendor and whose source codes is not available to the FI.
- d. **Security and Networking Devices:** Network devices such as routers, switches, and firewalls.
- e. **Firmware:** Programs or microcode embedded into hardware devices like PC Basic Input/Output System (BIOS).
- f. **Internet-of-Things (IoT):** Any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which can be connected to the FI's network or the Internet.
- g. **Virtualisation and Cloud Services:** Encompassing various categories mentioned above, including on-prem virtualised platform (e.g. VMware), cloud platforms, services, and containers across Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions.

With the wide adoption of cloud deployments, asset management practice and tooling capability must be refreshed or upgraded to ensure accuracy of the assets under management.

2.2 Asset Context

The presence of contextual information associated with each asset instance are important in organizing and prioritising the vulnerability management process. Examples of relevant details include:

- a. **Impact and value of the asset:** Importance of the asset to the FI such as core banking systems.
- b. **Sensitivity of data:** The level of sensitivity of the data processed by and/or store in the asset in view of legal, compliance, and business impact, for example, personally identifiable information (PII).
- c. **Location and exposure level:** Whether the asset is internet-facing, intranet, or operates in an air-gapped environment. The reachability to the asset serves as a key factor for prioritisation.
- d. **Regulatory requirements:** Compliance obligations of the assets, such as those designated as Critical Information Infrastructure (CII) system.
- e. **Uptime and availability considerations:** Factors related to the asset's availability and the impact of patching on its uptime.
- f. **Non patchable:** Hardware or software that cannot be patched due to lack of support or end of life product.
- g. **Exclusion:** Hardware or software that is not connected to network or has no logical means to access over the network. Exclusion can also be past source codes residing in repository not being used for production.

Combining the contextual information and asset categories allows FI to create a vulnerability management strategy for their assets.

3. Vulnerability Identification

Vulnerability discovery involves actively scanning systems and networks to uncover potential weaknesses that could be exploited. Once vulnerabilities are identified, FI should prioritise their remediation efforts based on the severity and exploitability of the vulnerabilities, likelihood of exploitation, as well as the potential impact on the FI. By prioritizing remediation based on these factors, FI can allocate resources more effectively and address the more critical vulnerabilities first to enhance overall security posture.

3.1 Vulnerability Data Sources

a. Vendor Patch Updates

Effective vulnerability management requires proactive and timely monitoring of vendor released patches. Some information like zero-day vulnerability may be privileged and released only to software customers. FI should subscribe to vendor software release announcement for timely assessment and remediation.

b. Vulnerability Advisories Subscription

To effectively manage the increasing number of vulnerabilities disclosed each year, FI should establish a process for tracking vulnerability advisories, assessing their relevance to the environment, and prioritizing remediation based on severity and existing controls.

Subscribing to a reputable central vulnerability repository service is recommended to ensure timely notification of security advisories related to vulnerabilities used by FI. This subscription should provide essential information such as vulnerability details, initial scoring, exploit availability, vendor solutions or workarounds, affected products and versions. The FI should stay updated on patch releases and recommended workarounds from their vendors.

Additionally, monitoring security advisory notifications from Computer Emergency Response Teams (CERTs), community-maintained vulnerability lists, and subscribing to relevant security social media platforms can provide valuable insights and awareness of ongoing discussions related to vulnerabilities.

c. Vulnerability Data - Comparative Evaluation and Tracking

FI should establish a data prioritisation process for comparing vulnerability data from multiple sources. This ensures consistency by relying on a primary data source while considering secondary sources. Additionally, FI should consistently track updates to vulnerability data, including new exploitation methods discovered by researchers or threat actors.

d. Vulnerability from cyber security assessments

Security assessment highlights the security weaknesses of an FI and allows FI to perform proactive risk treatment. FI should include vulnerabilities identified from security assessments such as vulnerability assessment, penetration testing and adversarial attack and simulation exercise.

e. **Bug Bounty or Vulnerability Disclosure Program**

For in-house developed software, FI should consider establishing a bug bounty program and/or vulnerability disclosure program to encourage responsible reporting for the FI's timely resolution.

For vulnerability that is validated as false positive by the FI or principal vendor who provides Commercial-Off-The-Shelf product, it should be excluded from remediation. As the state of false positive vulnerability may change due to the design or implementation changes over time, it should be tracked and reviewed periodically to determine if false positive remains relevant.

3.2 Vulnerability Risk Analysis

FI should employ a risk-based approach to evaluate the relevance of vulnerability advisories and its risk exposure. To ensure timely identification of vulnerable assets, FI should conduct periodic vulnerability assessments, with the frequency determined by the criticality of the assets.

3.3 Vulnerability Assessment

The severity of a disclosed software vulnerability is determined by the Common Vulnerability Scoring System (CVSS) when it is registered with the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) program. With the ever increase of vulnerabilities, FI should focus on prioritising and assessing the risk of the vulnerability.

FI should conduct a vulnerability risk assessment, considering the vulnerability's exploitability and whether it is actively exploited by threat actors. During the assessment, FI can use the existing CVSS framework or create a risk-based vulnerability management scoring framework to prioritise vulnerabilities based on the FI's specific requirements. The framework may include aggregation of the following criteria:

a. **Vulnerability Severity Information**

If the vendor's reassessed severity differs from the severity published in the NVD, the FI should adopt the vendor's assessment. For example, in relation to vulnerabilities in code libraries, software vendors may provide a different severity scoring compared to the raw score as different software vendors may utilise the libraries differently.

b. **Threat Intelligence / Exploit Information**

Threat intelligence provides important context to prioritise remediation efforts. FI should subscribe to threat intelligence feeds that provide information on widely and actively exploited vulnerabilities, as well as availability of Proof-of-Concept (POC) exploit codes. The effectiveness of the exploitation may also depend on the threat actor's capabilities. Threat actors can be classified based on motivation and skill level, ranging from nation-state actors to script kiddies. FI should profile and assess the threat actor groups targeting its industry and their common attack tactics regularly. FI may test POC exploit codes internally to aid in the assessment.

This intelligence should be incorporated into the FI's risk-based vulnerability management.

c. Asset Placement/ Application Criticality Information

FI should recalculate the severity score by considering the environmental controls in place to mitigate the risk. For example, a vulnerable system in an isolated environment would have a lower risk compared to a system accessible from the internet.

3.4 Vulnerability Remediation Prioritisation

FI should use a risk-based approach to prioritise vulnerability remediation, considering the asset's reachability and vulnerability exploitability. Prioritisation can be determined with the following parameters.

a. Vulnerability severity

FI should assess the vulnerability characteristics using an industry adopted standard such as Common Vulnerability Scoring System (CVSS) or composite vulnerability score. Vulnerability severity rating is based on vulnerability score from rated between 0.1 and 10.

b. Asset Reachability

FI should regularly scan for internet-accessible vulnerabilities and prioritise their remediation. If there are no controls to reduce exposure, emergency patching should be prioritised.

c. Exploitability

FI should review if vulnerability is exploitable in their assets. This is greatly varied based on the asset's components or configurations in place. The vulnerability may not be relevant if the vulnerable component has been removed or has not been deployed. Absence of these vulnerable components or configurations effectively removed attack surface and deprioritise the remediation.

d. Asset Criticality

FI should assess asset criticality based on security risk. For example, systems like VPN gateways that are accessible from the internet pose a higher risk in terms of reachability and exploitability. Additionally, FI should prioritise systems with higher business impact, such as those providing critical services to their customers.

FI should simplify categorisation of vulnerabilities into high-priority patching and routine patching to minimise impact to business services and minimise tracking overheads on an ongoing basis. High-priority patching is required to address vulnerabilities where there is no effective control, whereby routine patching is required for vulnerabilities that have been mitigated by layered defences.

Criticality of asset	Critical exposure vulnerability	
	High-priority patching	Routine patching
Internet facing system	✓	
Critical system	✓	
Other system		✓

A reassessment is necessary if the values of the parameters change significantly.

3.5 Remediation Timeline

FI should establish a remediation timeline as per their risk appetite. The status of remediation should be tracked till the remediation actions are completed.

3.6 Risk Response Scenarios

FI can choose to respond to risk of vulnerability through the following means:

- a. **Accept the risk** of the vulnerability by relying on existing layered defences to prevent exploitation of the vulnerability.
- b. **Mitigate the risk** by eliminating the vulnerability such as applying software patching, software upgrade, enhancing security configuration to reduce attack surface and likelihood of exploitation.
- c. **Transfer the risk** by softening the impact when the exploitation occurs such as cyber insurance and allow third party to manage the vulnerability (such as Software-As-A-Service).
- d. **Avoid the risk** through eliminating the attack surface such as removal of the vulnerable software, removal of the affected components, removal of libraries and disabling the vulnerable services.

4. Vulnerability Remediation

4.1 Considerations for Effective Vulnerability Remediation

- a. The vulnerability management process requires communication and collaboration among multiple stakeholders, both internal and external. This includes security team, infrastructure management team, application team, DevOps team, testing team, and third-party vendors.
- b. Software and hardware vendors play a significant role in the vulnerability management process. To avoid delays, the FI should minimise interdependencies and consider vendor who promptly release of patches and configurations against published vulnerabilities.
- c. When procuring hardware or software, FI should ensure appropriate software maintenance contracts. Vulnerability management approach, communication, patch distribution, frequency, and testing should be considered during the procurement process.
- d. Avoiding conflicting policies that create barriers to implementation, such as inadequate maintenance downtime or varying green zones that hinder patching without disruptions.
- e. Engineering and architectural designs, decisions, policies, and standards should align with the need for rapid deployment of software patches.
- f. Review and standardise tools, integrating them into a common data and reporting platform for accurate reporting and FI-wide visibility of assets, patches, and vulnerabilities. Implement appropriate governance processes for data accuracy, relevance, and comprehensiveness.
- g. Ensure scalability, stability, and security of tools for diverse environments.
- h. Use tools that identify applicable assets for efficient vulnerability remediation scope. Consider unified security and endpoint management products to cover the vulnerabilities management process.
- i. Establish maintenance windows for patching, agreed upon during service or asset go-live. Review knowledge, skills, and resources to prevent delays in patch deployments.
- j. Automate vulnerability remediation and patching processes whenever possible.

4.2 Process Managing Zero-Day Vulnerability

FI should establish a comprehensive procedure to effectively respond to critical zero-day vulnerabilities. This procedure should include a detailed task force description, outlining the roles and responsibilities of personnel from different teams involved. It is crucial to have well-defined processes for notification, authorisation for zero-day risk mitigation or remediation plans, proposed action plans, testing, deployment, and post-deployment actions. Communication within the FI should be escalated appropriately and, on a need-to-know basis.

FI should also assess the exposure and impact of zero-day vulnerabilities, and if these vulnerabilities cannot be resolved within agreed timelines, a risk management procedure should be in place. This procedure should involve risk review, sign-off, and communication at appropriate levels. Patching and remediation standards should clearly specify timelines for addressing critical zero-day vulnerabilities.

It is highly recommended that FI periodically review their readiness, tooling, and processes to address critical zero-day vulnerabilities. In cases where available, FI can consider implementing “virtual patching” as an option.

4.3 Information Gathering Prior to Remediation

FI should aim to:

- a. Avoid using multiple sources of information and instead promote the use of a central platform that combines different datasets. These datasets should include information on vulnerabilities, CVEs, affected assets, severity ratings, remediation methods, testing results, patch movements, remediation progress, exception management, change records, and other auditing information. This information should be accessible to all stakeholders.
- b. Establish consistent and standardised methods for downloading, updating, and distributing patches. These methods should be closely integrated with asset and CMDB systems, as well as vendor sources. It is crucial that the distribution and transportation of patches are carried out securely, with proper signature and hash value verifications.
- c. Implement automation to automatically classify information, detect information gaps, and identify outdated updates based on the specific needs of the FI. Such an information system is particularly important in preventing zero-day attacks and eliminates the need to manually retrieve information from multiple sources within the FI. The principles of having a single pane of glass and a single source of truth should guide these efforts.

4.4 Testing of Patches or Vulnerabilities Remediation Solution

- a. FI should develop an effective testing strategy and incorporate testing processes into the patch deployment procedures for non-production environments. This includes testing the patch/vulnerability mitigation solution in the following environments, depending on the FI's requirements:
 - A dedicated testing environment to analyse the results.
 - A lab/sandbox environment
 - A non-production environment
- b. It is important for testing to consider the interdependencies of applications and avoid conducting isolated tests. FI should prioritise the quality of testing and prevent delays in remediation caused by incorrect interpretation of test results. Additionally, FI should be aware of the limitations of testing when approving or rejecting remediation, such as the inability to replicate a production-like setup in non-production environments.
- c. Successful production patching requires thorough testing in non-production environments.
- d. Testing should also encompass solution roll-back scenarios and identify faulty and incompatible patches.

4.5 Remediation Timelines

It is important to clearly specify vulnerability remediation timelines in overall vulnerability process standards. FI needs to reduce service downtime as well as reduce time to remediate vulnerabilities or deploy patches.

FI should explore and test alternative methods to avoid system reboots. One option is to download and patch systems ahead of time, scheduling the system reboot for a later stage. Careful consideration should be given to the timing of this approach. Additionally, FI should establish deployment policies and procedures based on specific metrics. These can be one of or combination of –

a. **Immediate Deployment Policy**

FI should prioritise patching as soon as a patch becomes available. This approach is especially relevant for zero-day vulnerabilities but can also be applied to highly mature products. It is commonly implemented when FI aims to enforce a "zero trust" security policy. However, FI needs to carefully consider the trade-off between service availability, cost, and the benefits associated with these deployment strategies.

b. **Time Based Policy**

FI should adopt a patching policy that involves regular intervals, such as leveraging Microsoft's "Patch Tuesday" and initiating patching activities after the release of monthly patches. It is crucial to coordinate the timelines of patch releases from other vendors to bundle deployments effectively. This approach can be applied to services, products, or workloads that have designated monthly downtime or maintenance windows available.

c. **Patch Based Policy** – Patch when predefined number of outstanding critical patches are outstanding. FI can adopt this to trigger patching where downtime is a concern and want to bundle patches within stipulated timeframes.

d. **Controlled Deployment Policy** – When the cumulative security risk surpasses a specific level or set of metrics, a patch should be implemented. This approach, known as the "patch when cumulative security risk exceeds a certain level" policy, can be adopted if it aligns well with the FI's context. To initiate patching, FI must establish crucial metrics that determine the acceptable threshold of cumulative security risk for each of their information systems.

e. **Hybrid Policy** – Different combinations of the approaches can be implemented for various information systems within the FI.

Before deciding the order of patch deployments, FI should consider various factors such as testing on non-production, production, and disaster recovery environments. It is important to follow standard ITIL guidelines and consider IT Disaster Recovery procedures. By doing so, FI can determine the appropriate sequence for deploying patches, ensuring that proper testing and safeguards are in place before moving to critical production and disaster recovery environments.

4.6 Managing Mitigation in case of unavailability of Patch(es) for vulnerability

When a new vulnerability becomes publicly known, the risk increases as attackers are more likely to develop exploits targeting the vulnerable software. In cases where known solutions or patches are unavailable for remediation, and the risk exposure is high, FI should consider disabling the vulnerable feature(s) or component(s) to minimise immediate exposure. Alternatively, FI can explore mitigation approach through layered defences, if feasible, to mitigate or reduce the risk of exploitation. This may involve isolating the vulnerable assets, implementing network-based security controls to restrict access, segmenting the network, and enforcing physical and logical access restrictions.

Additionally, FI should implement enhanced network monitoring to detect anomalies and potential exploitation attempts. Any suspicious behaviour should be promptly blocked to prevent further attack paths.

During the implementation of mitigation measures, FI should determine whether the mitigation should be temporary and rolled back once a future solution or patch becomes available, or if it should be applied permanently. It is crucial for FI to have plans and procedures in place to take assets offline in situations where the risk is elevated, and systems cannot be patched.

FI should have clearly laid out processes to seek remediation timeline extension. Risk acceptance frameworks should be in place to address such the residual risk.

4.7 System Obsolescence

Obsolete systems within FI may be unable to receive patches or updates. It is important for FI to regularly identify these assets and review existing contracts with software and hardware vendors to understand their policies regarding zero-day and non-zero-day vulnerabilities. This will help determine what level of support is covered by these contracts. For assets that cannot be patched, FI should plan for long-term risk mitigation using various methods outlined in section 4.6.

4.8 Post Deployment / Remediation Verification

Post-deployment vulnerability remediation requires adherence to both service performance and availability standards, as well as the successful resolution of underlying vulnerabilities.

To ensure efficiency, FI should automate the verification process after deployment by scanning and confirming the status of remediated vulnerabilities. It is advisable for FI to utilise the same centralised tools for viewing patching status as those used during deployment. These tools should possess the capability to automatically detect the remediation status of vulnerabilities and, if necessary, blacklist problematic patches. Artefacts resulting of the application of patches or mitigations against the vulnerabilities should be made available to all stakeholders and reviewed for accuracy and completeness.

FI should consider implementing automated scanning to confirm remediation of concerned vulnerabilities. Scan results must be interpreted considering the context and limitations of the scan engine, such as the absence of detection rules for certain vulnerabilities or the inaccessibility of vulnerable assets due to network segmentation or traffic filtering.

To effectively manage such situations, FI must establish clear roles, responsibilities, and procedures for handling patch blacklisting. Additionally, thorough tracking of rollbacks should be maintained for future reference.

4.9 Measurement / Metrics

FI should develop actionable remediation Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), or metrics to support an effective patch management process. These measurements should address various levels of responsibility and usage may extend to assist in reviews of regulatory requirements as well as understanding alignment with FI's security policies.

At the enterprise level, metrics should be designed to indicate the overall risk exposure of the FI. They should align with vulnerability rating, prioritisation, asset classes, and remediation timelines specified in the FI's patching standards. These metrics should identify areas of vulnerability and risk mitigation that require improvement, along with associated targets and goals. It may be beneficial for FI to divide these measurements into two levels: lower-level and enterprise-level metrics. Lower-level metrics can provide a comprehensive view, focusing on the speed of patching, while enterprise-level metrics can highlight the impact of patching and risk mitigation. Some examples of metrics are included in Appendix A.

4.10 Consequence Management

Apart from reporting key metrics of the vulnerability and patch management. FI should consider adopting consequence management to improve resilience. Risk exposure increases in the event where patches are unable to be deployed within the vulnerability remediation timeline. Effective risk management should consider limit the risk exposure by limiting additional changes to the environment until the vulnerability is remediated to an acceptable threshold. An example is to prohibit introduction of new system when the vulnerabilities are not remediated in accordance with the required policy.

When creating a consequence management model, the FI should consider the various asset types and their specific use cases. For instance, consequences applied to end-user workstations may not be suitable for business-critical applications.

5. Appendix

The following are examples of lower-level metrics:

- Mean/Median Time to patch any given asset.
- Number/Percentage of systems which could not be patched vs planned in each cycle.
- Number/Percentage of systems fully compliant with patching standard.
- Number/Percentage of pending patches of each severity.
- Number/Percentage of pending security patches vs non-security patches (bug fixes and feature enhancements).
- Number of high impact patches reducing 90 % of attack vectors.
- Patching and compliance trend over time compared against vulnerability detection/patch arrival time.
- Vulnerabilities scan coverage.

The following are examples of Enterprise Level Metrics:

- Number of vulnerability and patch severity classifications (critical/Important/moderate/Low).
- Number/Percentage of compliance for critical/high patches within stipulated remediation/patching timelines for specific assess class.
- Number/Percentage of target compliance for critical/high patches within stipulated remediation/patching timelines.
- Number/Percentage of systems deviating from target compliance for each severity and/or each asset classes.
- Number/Percentage of systems pending Zero-Day vulnerability remediation (with/without mitigation).
- Number/Percentage of vulnerabilities pending patch delivery.
- Number/Percentage of vulnerabilities with mitigation pending.
- Vulnerability remediation past due date.
- Vulnerability churn rate (rate of vulnerabilities being closed vs new arrivals).
- Average vulnerability age.
- Mean time to detect vulnerability.
- Patch age (age of system since last patch was applied).
- Exclusions granted for vulnerabilities from remediation.

6. References

We would like to thank various bodies and communities for developing vulnerability and patch management guidelines, knowledgebase referenced for the development of this paper.

Source	Reference Information
National Institute of Standards and Technology (NIST)	NIST SP800-40 revision 4 "Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology"
Forum of Incident Response and Security Teams (FIRST)	Common Vulnerability Scoring System v3.0 (CVSS) First Organisation Exploit Prediction Scoring System (EPSS)
Monetary Authority of Singapore	Technology Risk Management Guidelines
Nesara Dissanayake	Software Security Patch Management
SANS Institute	Key Metrics and Vulnerability Management Maturity Model

7. Glossary

ABS	Association of Banks in Singapore
DevOps	DevOps combines development (Dev) and operations (Ops) to increase the efficiency, speed, and security of software development and delivery compared to traditional processes.
ITIL	Information Technology Infrastructure Library, is a set of IT best practices designed to assist businesses in aligning their IT services with customer and business needs.
NVD	National Vulnerability Database
VPN	Virtual Private Network