Security Assessments

Author	KH Lai
Tags	General
Status	Reviewed

Security Assessments

Every organization must, in a way perform various types of security assessments on their network infrastructure, end-point devices or even the software applications that are used within the organization. The main purpose of conducting security assessments is for identifying and confirming vulnerabilities that are present so that they can be patched, mitigated and removed. Determining what types of security assessments to conduct is primarily based on the business model of the client organization. Each organization has different compliance requirements and faces different types of threats. Typically, determining what types of security assessment to perform is based on the security maturity of the organization. Some larger organizations have very matured security postures and is able to focus on much more advanced assessments like Red Team Assessments. On the other hand, organizations that have less mature security posture are less suited for conducting advanced security assessments because what they should be doing is establishing a baseline security. For example, choosing an appropriate security standard that are suitable for the organization’s use case. Conducting security assessments without having a security standard on place is like finding a specific tree in the Amazon forest without been given a general area to look for.

Client’s Point of View

When a client organization wants to conduct a security assessment. The executives asks for an assessment on their infrastructure from their third-party vendors. An infrastructure consists of many components like Network, Database, Active Directory (AD), Enterprise Resource Planning (ERP) and so on. Conducting a full infrastructure assessment will take a long time and cost a bunch. The client then discusses and narrow down the scope of the assessment to just the crucial areas of the organization that are of the most concern. Security assessment should only be done when there is a compliance requirements in place. Before finding a third-party vendor to conduct a security assessment, the following factors have to be clear:

- The Goal of the assessment
- The Scope of the assessment

Consultant’s Point of View

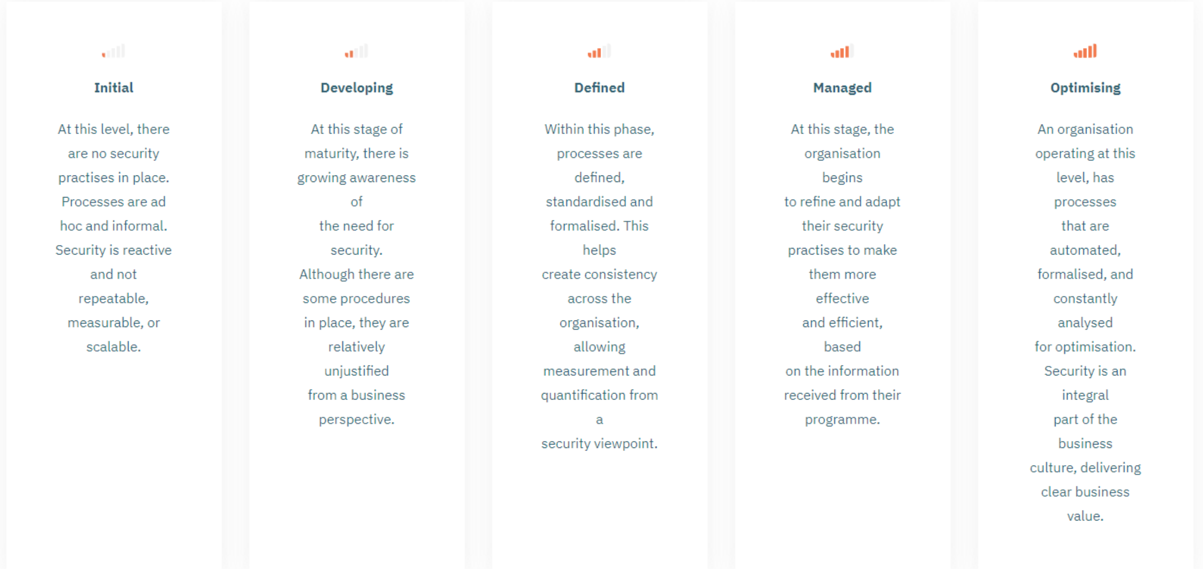
When a consultant is being asked to conduct a security assessment, the client will be most probably be unsure about how the security assessment can help them be more secured and also does not know which area to focus on for the assessment. The consultant’s job is to help the clients understand the issues that they are facing and how to fix them. The consultant must understand the client’s business ins and outs. Every business faces different risks and threats. A financial institution will face completely different risks and threats than a production company. Moreover, compliance and regulations will also differ for every business which determines what types of security assessment to perform.

What is Security Maturity?

Security Maturity is an organization’s security stance in relation to its risk environment. The risk scenarios differs for each organization as each organization has its own security risks. Therefore, the security maturity of an organization depends on how efficiently they implement security procedures to counter these risks. A good security posture takes years to develop. Having a high security maturity involves many factors.

- Well-designed security protocols/policies
- Good regulatory compliance
- An effective cyber incident response plan
- A strong CSIRT Team
- Frequent security testing
- A strong security culture (Among Employees)

Based on the security maturity model, there are different stages of security maturity. Below is an image to better illustrate the different stages



Initial

At this level, there are no security practises in place. Processes are ad hoc and informal. Security is reactive and not repeatable, measurable, or scalable.

Developing

At this stage of maturity, there is growing awareness of the need for security. Although there are some procedures in place, they are relatively unjustified from a business perspective.

Defined

Within this phase, processes are defined, standardised and formalised. This helps create consistency across the organisation, allowing measurement and quantification from a security viewpoint.

Managed

At this stage, the organisation begins to refine and adapt their security practises to make them more effective and efficient, based on the information received from their programme.

Optimising

An organisation operating at this level, has processes that are automated, formalised, and constantly analysed for optimisation. Security is an integral part of the business culture, delivering clear business value.

Obtained from https://www.nedapsecurity.com/what-is-your-security-maturity/

Vulnerability Assessments

Vulnerability Assessments are suited for all organizations whether big or small. Vulnerability Assessments are based on a particular security standard and it determines whether the organization is compliant with the security standard. The security standard implemented is depending on the organization and business model. Vulnerability assessments aims to discover vulnerabilities in an infrastructure without simulating cyber attacks. Moreover, vulnerability assessments identifies whether the organization has met the security standard and/or does the organization have the configurations that are compliant with the security standard. Typically during a vulnerability assessment, a vulnerability scan is run to validate on critical and high vulnerabilities but will not perform simulated attacks like privilege escalation or post-exploitation. Vulnerability Assessments are mostly automated by using vulnerability scanning tools. It identifies and categorizes the risks that are present in the defined scope of assessment and provides remediation steps to fix the issues.

Penetration Testing

Penetration Testing is a type of security assessment that is conducted to simulate a cyber attack. Conducting penetration tests are more appropriate for organizations with high security maturity. Organizations that has a lower security level are more suited for conducting vulnerability assessments due to the reason that conducting a penetration test may find too many vulnerabilities and may overwhelm the client with remediations. Therefore, before considering conducting penetration tests, a track record of vulnerability assessments should be present.

The Difference

Vulnerability Assessments and Penetration Testing often get confused. Both are completely different types of security assessments. Vulnerability assessments look for vulnerabilities without simulating attacks whereas Penetration tests are often performed manually by simulating cyber attacks to see if and how the system can be penetrated. Both assessments are used for different situations and one is not better than the other. Typically, there are various security standards that can be used for a vulnerability assessments and it goes through a checklist to determine whether the target organization is compliant with the standard in place. It is important to note that it is suggested that penetration tests should only be conducted after some vulnerability assessments have been performed. Below is a table to better illustrate the differences.

Vulnerability Assessments	Penetration Testing
Identifies low hanging vulnerabilities	Identifies business-specific vulnerabilities
May have false positives	Vulnerabilities found are legitimate through manual inspection
A more cost-effective approach	Cost significantly more time and money
Provides generic remediations that may not be relevant	Provides logical and realistic remediations that are suited for the client organization

Performing vulnerability assessments can find common vulnerabilities based on the security standard that the organization should be compliant to. Even though penetration tests must also comply with a specific security standard, conducting penetration tests can identify business-specific vulnerabilities. This is referred to as Business Logic Vulnerabilities. As established earlier, each organization has their own business model and their system/application has their own “custom code” which powers their business logic.

According to the OWASP foundation, “the most serious security issues are the ones that are not generic, but deeply intertwined in your business logic and custom application design”. Running a vulnerability assessment will probably fail to detect these business logic vulnerabilities because vulnerability scanning tools are generic and are not designed for custom application but rather for applications/systems in general. Thus, while they can identify generic issues, they do not have enough knowledge of the application to detect more specific issues.

Types of Compliance Standards

- ISO 27001
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)

Types of Security Standards

- Open Web Application Security Project (OWASP)
- Penetration Testing Execution Standard (PTES)
- National Institute of Standards and Technology (NIST)