Vulnerability Assessment:
6 Best Steps to Better Security

EC-Council's Cyber Research team would like to thank **Gabriel Mandefu, Operational Business Analyst, Tenke Fungurume Mining S.A.R.L.,** for authoring this White Paper.

EC-Council Cyber Research

Index

Abstract

Some of the key concepts in the information security world have two aspects: technical, which refers to use of technology-based methodology to secure your business, and non-technical, which refers to the governance aspect of the security of a company. Risk and vulnerability assessment are part of those concepts. These terminologies are taught no matter which career path you choose in InfoSec. Tons of free material are available online, as well as formal training courses on this subject. However, as with any business, the audience is the first consideration. Those material are written with a target reader/student in mind. Hence, most of the time, just one aspect of the concept is emphasized. The aim of this paper is to encourage:

- *Students/readers to learn both sides of risk and vulnerability assessment in order to master these concepts.*
- *Security professionals to consider both sides of risk and vulnerability assessment to ensure effectiveness of security measures they put in place.*

Keywords: *Risk & Vulnerability Assessment*

Introduction

Information security is all about protecting your company's information. To do this, it's crucial to know what kind of risks it is exposed to. To know this, you need to do a risk and vulnerability assessment.

I once met an IT manager of a medium-sized company who was searching for technologies to protect the overall company assets: IT infrastructure, digital, and non-digital data. He went and meet a security professional to ask for assistance on this exercise.

Manager	"What should I do to protect my company's information?"
SecProf	"Hire a trained ethical hacker and let him do a pen testing exercise. He will provide a report at the end of the exercise and based on that, you should know how to proceed."

What do you think about the SecProf's advice? Is it enough to achieve the manager's requirement? Do you think a pen testing exercise will provide insight on how to secure non-digital data? Absolutely, pen testing will help find vulnerabilities and risks related to IT infrastructure and digital information. Not sure how an ethical hacker can protect non-digital information when performing an assessment according to the penetration testing life cycle methodology.

Non-digital information is out of scope of the IT security concept and cannot be assessed through an ethical hacking methodology. Fortunately, there are international standards that look after these kinds of concerns. For instance, ISO 2700, NIST, etc. These standards also define methodology to conduct risk and vulnerability assessment to protect the company's overall information security.

Newbies are confused when reading about risk and vulnerability assessment in training material for security engineers and in non-technical material like ISO 27001 courseware. Also, some security professionals interchangeably use the words risk assessment and vulnerability assessment. Indeed, there's confusion in the information security world regarding these two concepts. The scope of this paper is to clear confusion by discussing the influence of training course curriculum.

When you start thinking about the security of your company, you need to know where to focus your security investments and resources. Without visibility into potential exposures, it is difficult to define effective security measures and controls. A vulnerability management program helps a lot in this regard.

Risk and vulnerability assessments are vital building blocks in your integrated risk management program. When properly conducted, they bring to light weaknesses and threats that exist in your environment and the likelihood that they will be exploited. This, in turn, will give you an idea of their impact on your organization's activities.

1. Check Your Knowledge

Scenario 1: An ethical hacker is running an assessment test on your networks and systems. The assessment test includes the following items:

- Inspecting physical security.
- Checking open ports on network devices and router configurations.
- Scanning for Trojans, spyware, viruses, and malware.
- Evaluating remote management processes.
- Determining flaws and patches on the internal network systems, devices, and servers.

Which of the following assessment tests is being performed?

a
Internal assessment

b
Active assessment

c
Passive assessment

d
External assessment

Scenario 2: You are an ethical hacker contracting with a medical clinic to evaluate their environment. Which of the following is the first thing you should do?

- Choose the best security assessment tools for the systems you choose to test.
- Create reports that clearly identify the problem areas to present to management.
- Define the effectiveness of the current security policies and procedures.
- Decide the best times to test in order to limit the risk of having shutdowns during peak business hours.

Scenario 3: A disgruntled system administrator intentionally disables your core application and deletes your most important databases. Is that an IT issue?

a True **b** False

2. Information Security Roles in an Organization

Cybersecurity career pathways are complex and confusing for newbies. Most of the time, course content is defined based on the skills required to fit a specific role in an organization. Based on the role, we can distinguish two main career pathways in cybersecurity: technical and non-technical.

2.1. Security governance, risk, and compliance

Pathway for people who are responsible for strategic vision, scoping of requirements, system design, security project management, policy creation and maintenance, governance (security and compliance reviews), and audit response and attestations.

This career pathway teaches you how to align your business with the security framework that better corresponds to your company's core activities. For instance, organizations that handle cardholders may choose the PCI-DSS standard; a public company might choose SOX, etc. Typically, people in this group do not have an IT technical background — for example, executives and managers who work with IT security. So, let's tag this pathway as "non-technical."

2.2. Information security engineers

Pathway for people dedicated to dealing with cybersecurity issues on a technical level as well as day-to-day activities in a security operations center, including the maintenance and monitoring of a live environment. This pathway teaches technical roles such as blue team, red team, and pen testers. It's mostly chosen by people with an IT technical background like network engineers, system administrators, DBA, etc. Let's tag this as "technical."

3. Vulnerability Management Life Cycle and Cybersecurity Courseware

Vulnerability management training is strongly influenced by the background of people choosing the pathway.

3.1. "Technical" pathway

The emphasis is put on security of IT-related services. Training is conducted in such a way that information security is treated as an IT-related problem to fix. So, a security engineer develops the mindset of a problem resolver. The recommended frameworks in this pathway used to be LPT (Master), OSCP, and so on. As a consequence, security engineers think risk and vulnerability assessment is all about IT-related services.

At this stage, let's review your answers to the two first questions asked above. What was your answer to scenario 1? The correct answer is **internal assessment.**

Scenario 1's explanation

An ***internal assessment*** is an evaluation of a network that is created by testing and analyzing processes and systems inside the network. This assessment may include:

- Inspecting physical security.
- Checking open ports on network devices and router configurations.
- Scanning for Trojans, spyware, viruses, and malware.
- Evaluating remote management processes.
- Determining flaws and patches on the internal network systems, devices, and servers.

An ***active assessment*** is an evaluation of a network that is created by actively testing the network for weaknesses. Specifically created packets are sent to target nodes to determine the OS of the domain, the host, services, and vulnerabilities in the network.

A ***passive assessment*** is an evaluation of a network that is created by looking for weaknesses through observation and no direct interaction with the network. Using sniffer traces from a remote system, the operating system of the remote host can be determined, as well as a list of the current users of the network.

An ***external assessment*** is an evaluation of a network that is created by testing external systems and testing from outside the network. This assessment may include:

- Determining if maps exist for network and external service devices.
- Checking for vulnerabilities in web applications.
- Examining the rule set for external network router configurations and firewalls.
- Detecting open ports on the external network and services.
- Identifying DNS zones.

I like the wording of scenario 2. It provides a good opportunity to introduce the non-IT aspects of the security of the company. Unfortunately, see the answer below.

Scenario 2's explanation

During the create a baseline phase, you start by defining the effectiveness of the current security policies and procedures. Establish the risks with how the security procedures are enforced and what may be overlooked. Try to see what the organization looks like from an outsider's perspective, as well as from an insider's point of view. No organization is immune to security gaps. Set goals with management with start dates and end dates. Determine which systems to begin with, set up testing standards, get approval in writing, and keep management informed as you go.

During the vulnerability assessment phase, it is important to decide the best times to test, as you don't want to risk having systems shut down during peak business hours or other sensitive times. You must also choose the best security assessment tools for the systems you choose to test.

During the risk assessment phase, you create reports that clearly identify the problem areas to present to management.

Note: For those with an IT technical background (network engineers, system admin, developer, etc.) and who select the technical pathway of the security course, risk and vulnerability assessment sounds to be all about IT security.

3.2. "Non-technical" pathway

Training flies over the vulnerability management process in a purely theoretical way. Training is conducted in such a way that risk and vulnerability analysis is set as a "high-level project plan" with a set goal to design and implement a security management system. A trainee develops the mindset of project manager. Favorite frameworks here are OSI 27001, NIST, COBIT, PCI DSS, etc. The focus is on information security in a purely procedural way and security of IT-related services is a simple checklist to validate.

Let's review scenario 3 now and discuss Dejan Kosutic's answer in his book 9 steps to cybersecurity.

Scenario 3's explanation

Is this an IT issue? No, this is hardly an IT issue; more like an HR issue. Could this have been prevented by IT safeguards? No. The person in this position is required to have direct access to all your systems. So, the way to prevent this type of scenario falls outside the technology area and comes down to how to select your employees, how to supervise them, which kind of legal documents have been signed, how this person is treated within the company, and so on.

Don't get me wrong — information technology and IT safeguards are extremely important in cybersecurity, but they alone are not enough. These measures must be combined with other types of safeguards to be effective.

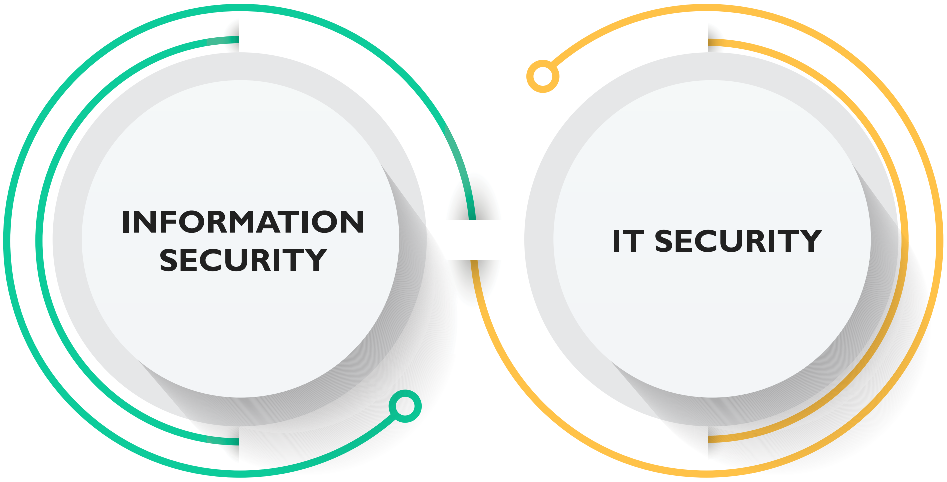
Note: What we can learn from this scenario: 1) IT controls are important in the cybersecurity world, but they are not enough. 2) IT controls must be combined with other type of safeguards to be effective. 3) However, as noticed in the '9 steps to cybersecurity' book like many other "non-technical" courseware material, IT-related measures are not as detailed when compared to technical pathway. The technical aspect of the security is a "project's deliverable" that can be assigned to a third party (internal or external resource)

Why is it important to understand the difference between IT security and information security?

IT security and information technology are terminologies security professionals need to master. A clear understanding of these concepts will help them define clearly IT-related controls and non-IT controls to ensure effectiveness of their company's security posture.

Information security, also called "infosec," doesn't focus on technology and networking security alone; rather it encompasses anything that a company considers to be its intellectual property and private data. The main goal in infosec is to protect the business' activities as a whole.

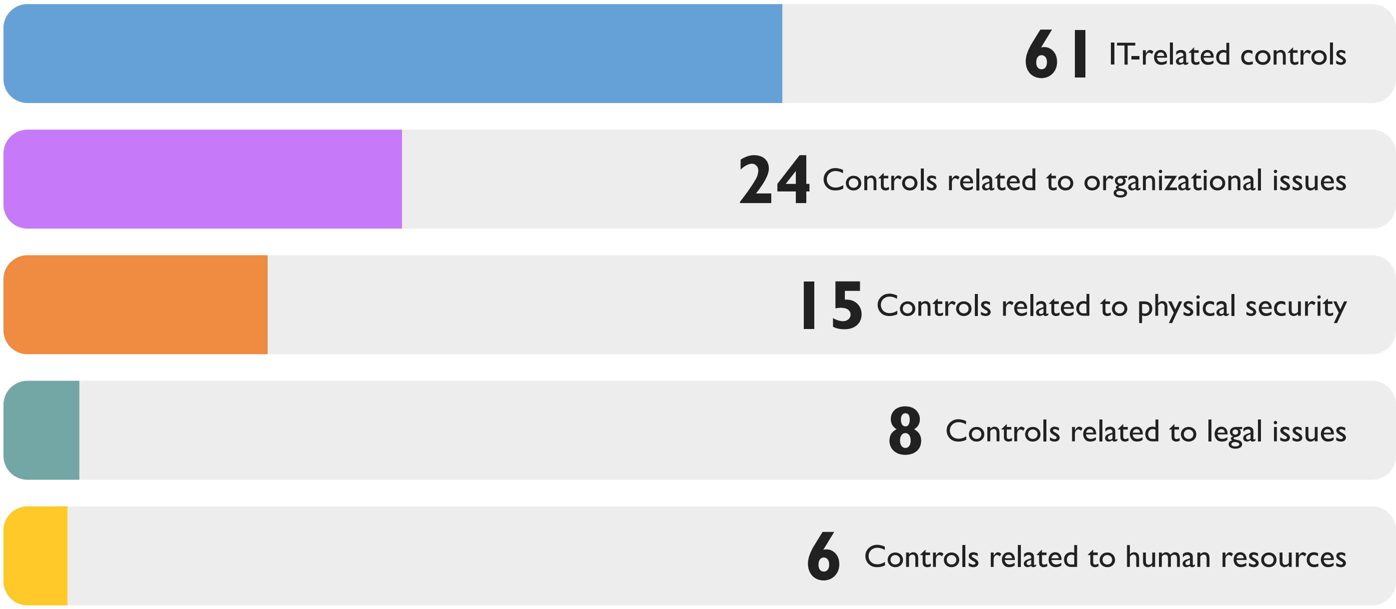
IT security or ITsec focuses on protecting digital assets located on the company's IT infrastructure. Infosec's scope goes beyond ITsec.



- As per a 27001 Academy article which details IT-related controls and non-IT controls based on ISO 270011,"There are 114 ISO 27001 information security controls listed in its Annex A in the current 2013 revision of the standard (compared to 133 from the previous 2005 revision of the standard). Here is a breakdown of what type of controls are included:

- Controls related to organizational issues: 24
- Controls related to human resources: 6
- IT-related controls: 61
- Controls related to physical security: 15
- Controls related to legal issues: 8"

Breakdown of ISO 27001 controls



This gives an idea on what should be considered when planning a risk and vulnerability assessment exercise. Ensure the scope of work is well defined and meets business requirements, then follow the vulnerability assessment methodology.

4. Vulnerability Management Life Cycle

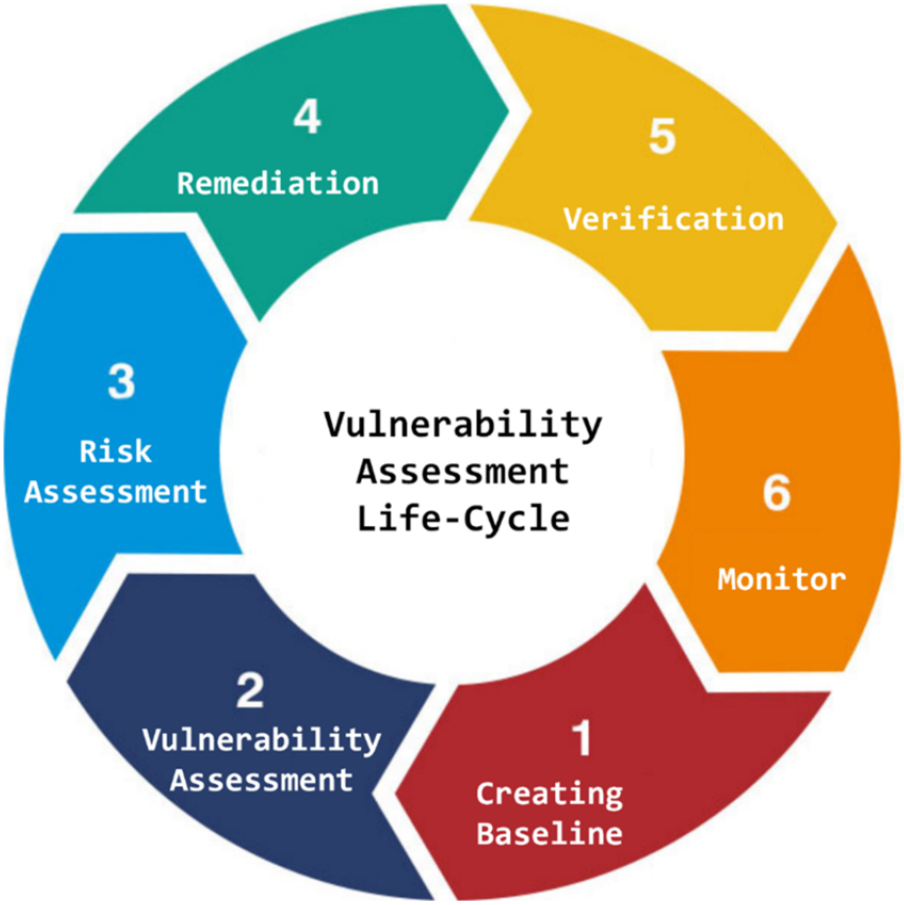
As stated in the introduction, risk and vulnerability assessments are vital building blocks in your integrated risk management program. Let's make it clear and show how these two concepts are linked.

Vulnerability assessment or vulnerability analysis is a series of activities a company should perform regularly to identify, quantify, and prioritize the risks and vulnerabilities in order to keep its information security posture effective.

Risk assessment identifies recognized threats, threat actors, and the probability that these factors will result in an exposure or loss. In simple words, risk assessment is a process of looking for bad things that can happen, who can cause them, and what will their impact be on important pieces of the company's information if they rise up.

Vulnerability and risk assessments represent, respectively, step 2 and step 3 in the vulnerability management life cycle

Vulnerability management life cycle starts by defining the effectiveness of the current security policies and procedures. If a company has already set up an information security management system, it is important to establish any risks that may be associated with the implementation of current security procedures and what may have been overlooked.



Try to see what the organization looks like from an outsider's perspective, as well as from an insider's standpoint. Work with management to set goals with start dates and end dates. Determine which systems to begin with, set up testing standards, get approval in writing form, and keep management informed on the progress: what you are doing, how you will do it, and the timing for each phase of the project.

The following steps describe the vulnerability management life cycle that security professionals use to find and remediate security weakness before any attack and/or implement security controls.

4.1. Creating Baseline

In this phase, the following activities take place: defining the effectiveness of the current security measures and procedures, ensuring that nothing in the scope of information security management system is overlooked, working with management to set goals with a timeframe to complete them, and getting written approval prior to beginning any assessment activity.

4.2. Vulnerability Assessment

In this phase, a vulnerability scan will be performed to identify vulnerabilities in the OS, web application, webserver, and other services. This phase helps identify the category and criticality of the vulnerability and minimizes the level of risk. This is the step where penetration testing begins.

4.3. Risk Assessment

In this phase, risks are identified, characterized, and classified with risk control techniques. Vulnerabilities are categorized based on impact level (like Low, Medium, High). This is where you have to present reports that identify problems and the risk treatment plan to protect the information.

4.4. Remediation

Refer to performing the steps that are used to mitigate the founded vulnerabilities according to impact level. In this phase, the response team designs mitigation processes to cover vulnerabilities.

4.5. Verification

This phase helps verify whether all the previous phases were properly employed or not. It is also where the verification of remedies is performed. This is where you show verifiable evidence that your risk treatment plan was effective and corrected issues.

4.6. Monitor

It’s important to remember that after a while, measures that protected the company need to be closely monitored and kept up to date via a regular vulnerability management plan. Incident monitoring is performed using firewall, IDS/IPS, or SIEM tools.

5. Conclusion

Is there a comprehensive courseware detailing every single concept currently on the market? Not sure if that exists. But it is important to note the following:

- Each courseware is prepared for a target audience and materials, examples, etc., are presented accordingly.
- Course content is prepared based on the course's difficulty level (beginner, intermediate, and advanced)

Hence, be open minded and don't limit yourself to what you learned from one course. As a saying goes: "The only limit is the one you set yourself." No matter the training pathway you decide to take, learn as much as you can on risk and vulnerability management until you feel like you understand both sides of it, from a technical and non-technical standpoint. What you learn from course material is a starting point — go beyond.

6. References

- https://advisera.com/27001academy/iso-27001-controls/
- https://link.springer.com/chapter/10.1007%2F978-3-030-41987-5_12
- https://link.springer.com/chapter/10.1007%2F978-3-319-77028-4_10
- 9 Steps to Cybersecurity- Author: Dejan Kosutic Published by: EPPS Services Ltd, Zagreb. Chap 2: the cybersecurity myths, Myth#1
- http://thehackertips.com/certified-ethical-hacker-ceh-vulnerability-analysis/

EC-Council
Global Services