Risk Assessment and Analysis:

Module 3

Risk Assessments

- Risk Assessments focus on **identifying the threats** facing the information systems, networks and data, and assessing the potential consequences face should these adverse events occur.
- Risk analysis is the process of **identifying and analyzing potential issues** that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks.

Environment Knowledge

- Understanding the environment
- Understanding the organization
- Understanding the business
- Understanding IT
- Understanding security
- Understanding threats, vulnerabilities, and risks

Actions

- Implementing risk assessment
- Implementing risk mitigation
- Implementing risk monitoring
- Implementing risk reporting
- Implementing risk awareness, communication, and training programs.

Why is risk analysis important?

- anticipate and reduce the effect of harmful results from adverse events.
- evaluate whether the potential risks of a project are balanced by its benefits to aid in the decision process when evaluating whether to move forward with the project;
- plan responses for technology or equipment failure or loss from adverse events, both natural and human-caused; identify the impact of and prepare for changes in the enterprise environment, including the likelihood of new competitors entering the market or changes to government regulatory policy.

Importance of regular IT security assessments

Conducting a thorough IT security assessment on a regular basis helps organizations develop a solid foundation for ensuring business success. In particular, it enables them to:

- Identify and remediate IT security gaps
- Prevent data breaches
- Choose appropriate protocols and controls to mitigate risks
- Prioritize the protection of the asset with the highest value and highest risk
- Eliminate unnecessary or obsolete control measures
- Evaluate potential security partners
- Establish, maintain and prove compliance with regulations
- Accurately forecast future needs

IT risk assessment components and formula

The four key components

An IT risk assessment involves four key components:

1. **Threat** — A threat is an event that could harm an organization’s people or assets. Examples include natural disasters, website failures.
2. **Vulnerability** — A vulnerability is any potential weak point that could allow a threat to cause damage. For example, outdated antivirus software is a vulnerability that can allow a malware attack to succeed. Having a server room in the basement is a vulnerability that increases the chances of a hurricane or flood ruining equipment and causing downtime.
3. **Impact** — Impact is the total damage the organization would incur if a vulnerability were exploited by a threat. For example, a successful ransomware attack could result in not just lost productivity and data recovery expenses, but also disclosure of customer data or trade secrets resulting in lost business, legal fees, and compliance penalties.

The risk equation

Risk = Threat x Vulnerability x Asset

What is information as an asset?

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently.

Asset Valuation

This is a method of assessing the worth of the organization's information system assets based on its CIA security.

Total Asset Value = Asset Value * Weight of Asset

Assumptions for asset valuation include:

- The value of an asset depends on the sensitivity of data inside the container and their potential impact on CIA.
- CIA of information will have a minimum value of 1 for each.
- The value of levels for CIA are as follows: A rating of 3 is high, 2 is medium and 1 is low.
- The value of the information asset is determined by the sum of the three (C + I + A) attributes.

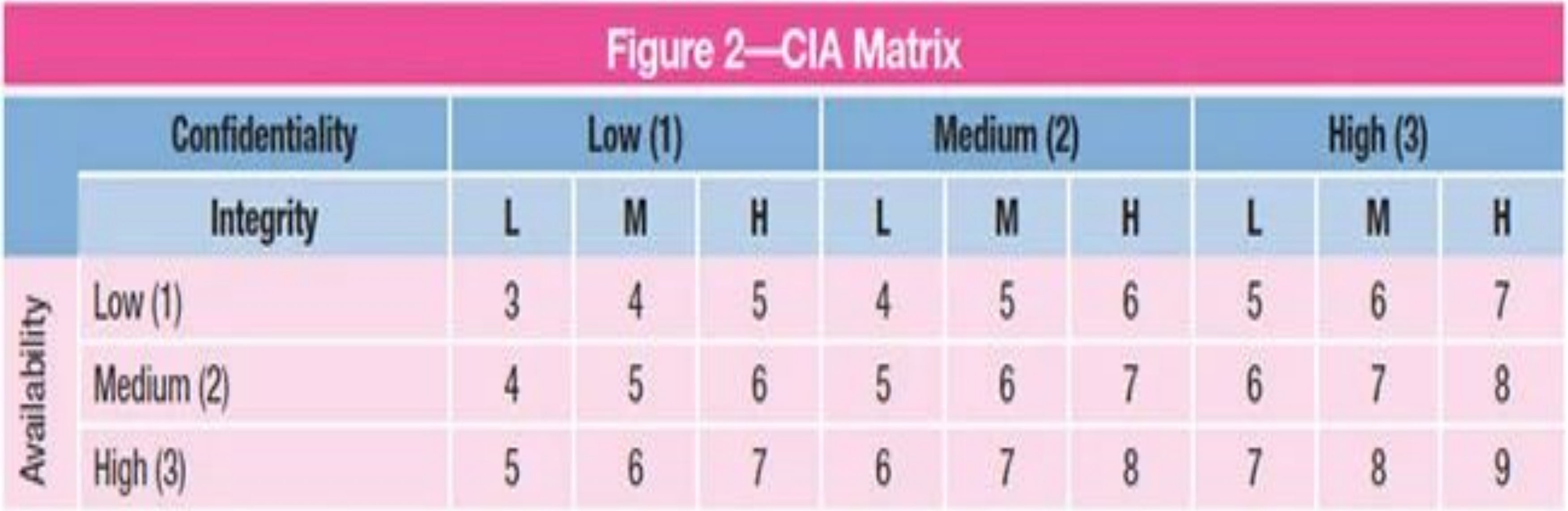

Figure 2—CIA Matrix

	Confidentiality	Low (1)			Medium (2)			High (3)		
	Integrity	L	M	H	L	M	H	L	M	H
Availability	Low (1)	3	4	5	4	5	6	5	6	7
	Medium (2)	4	5	6	5	6	7	6	7	8
	High (3)	5	6	7	6	7	8	7	8	9

Source: Shemlse Gebremedhin Kassa. Reprinted with permission.