Tata Kelola TI (IT Governance)

IT Security Risk

RISKY BUSINESS

- Referensi : Evan Wheeler (2011). **Security Risk Management: Building an Information Security Risk Management Program from the Ground Up 1st Edition.** Elsevier Inc, ISBN: 978-1-59749-615-5.

MISSION OF IT SECURITY

- ❑ The Information Security field is all about managing the risks to sensitive data and critical resources.
- ❑ The goal of Information Security should be to ensure that the confidentiality, integrity, availability, and accountability of the organization’s resources (tangible and intangible assets) are maintained at an acceptable level.

GOAL OF RISK MANAGEMENT

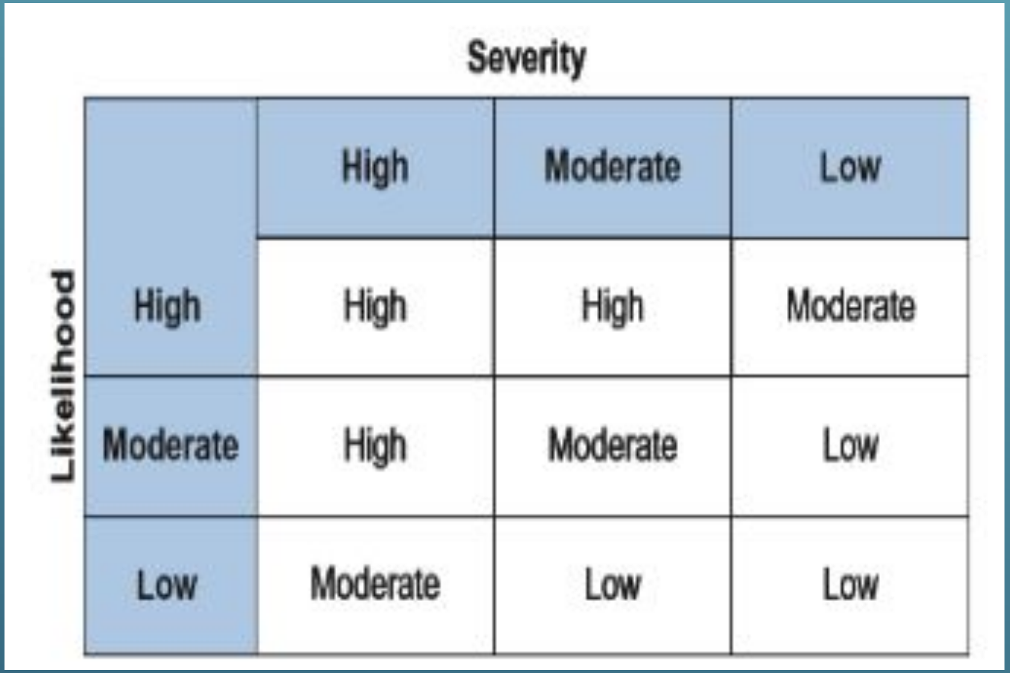
- The goal of risk management is to maximize the output of the organization (in terms of services, products, and revenue) while minimizing the chance of unexpected negative outcomes.

ARCHITECTING A SECURITY PROGRAM

- ❑ The building blocks of a security program are policies, standards, guidelines, procedures, and baselines, which you use to establish expectations about how to secure the sensitive resources.
- ❑ Some of the topics that need to be covered in policies and standards are as follows:
  - How the critical resources will be identified ?
  - The roles responsible for conducting risk assessments.
  - The process that will be followed for risk assessments.
  - How often assessments will be conducted ?
  - How findings will be scored and addressed ?
  - The process for requesting an exception.

QUANTITATIVE ANALYSIS

- Qualitative approaches use a relative scale (for example, Low–Moderate–High) to rate risks based on some predefined criteria for each level and rely on the knowledge and experience of the assessor for accuracy.



		Severity		
		High	Moderate	Low
Likelihood	High	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

QUANTITATIVE ANALYSIS

- ❑ Single Loss Expectancy× Average Rate of Occurrence = Annualized Loss Expectancy

- ❑ It calculates an Annual Loss Expectancy based on a Single Loss Expectancy and Annual Rate of Occurrence.

For example, if you expect to lose five BlackBerries this year, and the cost to replace one BlackBerry is $50, then your ALE is 5 × $50 = $250.

If you only lost one blackberry every 2 years, your ALE 0.5 × $50 = $25.

QUANTITATIVE ANALYSIS

Most of the models take advantage of probability theory and statistics to measure risk exposure. Many formulas for risk have been proposed, including:

- Sensitivity × Severity × Likelihood = Risk Exposure

- Exposure Rating = Severity2 × Threat

QUANTITATIVE ANALYSIS

One industry researcher has even offered a formula that includes six variables:

- Vulnerability
- Popularity
- Exposure
- Threats
- Asset Value
- System

THANK YOU