

ASSALAMU'ALAIKUM

Chapt 2

Approaches to Defining Risk

DR. RAHMAD KURNIAWAN, ST., MIT., MTA., CISDV.

- ❖ **Definition of Risk**
- ❖ **Types of Risks**
- ❖ **Computer Risk**


- ❖ Oxford English Dictionary → a chance or possibility of **danger, loss, injury** or other **adverse consequences**', and the definition of at risk is 'exposed to danger'.
 - negative consequences
- ❖ The Institute of Risk Management (IRM) → The combination of the probability of an event and its consequence. Consequences can range from positive to negative.
- ❖ ISO Guide 73 → effect of **uncertainty** on objectives

- ❖ The Institute of Internal Auditors (IIA) →
The uncertainty of an event occurring that could have an impact on the achievement of objectives.
 - Risk is measured in terms of consequences and likelihood.
- ❖ Risk → An event with the ability to impact (inhibit, enhance or cause doubt about) the effectiveness and efficiency of the core processes of an organization.



Types of Risks

- ❖ Compliance (or mandatory) risks;
- ❖ Hazard (or pure) risks;
- ❖ Control (or uncertainty) risks;
- ❖ Opportunity (or speculative) risks.
- ❖ In general terms, organizations will seek to **minimize** compliance risks, **mitigate** hazard risks, **manage** control risks and **embrace** opportunity risks.



Range of computer risks

In order to understand the distinction between compliance, hazard, control and opportunity risks, the example of the use of computers is helpful. Operating a computer system involves fulfilling certain legal obligations; in particular, data protection requirements and these are the compliance risks. Virus infection is an operational or hazard risk and there will be no benefit to an organization suffering a virus attack on its software programs. When an organization installs or upgrades a software package, control risks will be associated with the upgrade project.

The selection of new software is also an opportunity risk, where the intention is to achieve better results by installing the new software, but it is possible that the new software will fail to deliver all of the functionality that was intended and the opportunity benefits will not be delivered. In fact, the failure of the functionality of the new software system may substantially undermine the operations of the organization.



Inherent level of risk

An example of how inherently high-risk activities are reduced to a lower level of risk by the application of sensible and practical risk response options.

Crossing the road

Crossing a busy road would be inherently dangerous if there were no controls in place and many more accidents would occur. When a risk is inherently dangerous, greater attention is paid to the control measures in place, because the perception of risk is much higher. Pedestrians do not cross the road without looking and drivers are always aware that pedestrians may step into the road. Often, other traffic calming control measures are necessary to reduce the speed of the motorists or increase the risk awareness of both motorists and pedestrians.



❖ **Thank you**