Risk Management Discussion Points

Presentation

Outline

Risk Appetite

Residual Risk

Documenting Results

Risk Appetite

Risk appetite is the level of risk that an organization is willing to accept in pursuit of its objectives. It reflects the amount and type of risk the organization is prepared to tolerate to achieve its goals and guides decision-making by balancing potential risks and rewards.

Security and Accessibility

Perfect Security: Ensuring maximum protection of data and systems, which often means implementing stringent controls, restrictions, and monitoring. This can reduce the risk of cyberattacks, data breaches, and unauthorized access but can also make systems less user-friendly and harder to access for legitimate users.

Unlimited Accessibility: Allowing easy and unrestricted access to data and systems, which enhances user convenience and productivity. However, this can increase vulnerability to cyber threats, data breaches, and unauthorized access, as fewer controls are in place to safeguard the systems.

Examples

High Risk Appetite:
A tech startup in its early stages might prioritize rapid development and innovation over stringent security measures.

Low Risk Appetite:
A financial services company, such as a bank, typically has a low risk appetite for information security due to the sensitivity of financial data and the regulatory requirements.

Examples

Axie Infinity

Can have a
HIGH RISK APPETITE
and
LOW RISK APPETITE

Examples

Axie Infinity

HIGH RISK APPETITE	LOW RISK APPETITE
Managers Investors	Scholars

Examples

A. 100% chance to get ₱1000

B. 50% chance to get ₱1500
50% chance to get nothing

A. 100% chance to lose ₱1000

B. 50% chance to lose ₱1500
50% chance to lose nothing

Residual Risk

Residual risk refers to the level of risk that persists even after implementing various security measures and control.

It is a combined function of (1) a threat less the effect of threat-reducing safeguards, (2) a vulnerability less the effect of vulnerability-reducing safeguards, and (3) an asset less the effect of asset value-reducing safeguards.”

Calculating Residual Risk

Residual Risk = Initial Risk - Mitigated Risk

Initial Risk

Potential impact and likelihood of an event occuring in the the absence of any risk mitigation

Mitigated Risk

Level of risk that remains after implementing risk management controls or strategies

Managing Residual Risk

Risk Acceptance

Acceptance of residual risk if it falls within the organization's risk appetite and when further mitigation is too costly

Risk Transfer

Organizations can transfer residual risk to a third party through insurance policies or outsourcing arrangements

Managing Residual Risk

Risk Avoidance

There are certain situations where organizations may choose to avoid decisions or activities that carry high level of residual risk

Risk Mitigation

Implement additional risk management controls or strategies to further reduce residual risk

DOCUMENTING RESULT

The results of risk assessment activities can be delivered in a number of ways: a report on a systematic approach to risk control, a project–based risk assessment, or a topic–specific risk assessment.

When the organization is pursuing an overall risk management program, it requires a systematic report that enumerates the opportunities for controlling risk. This report documents a series of proposed controls, each of which has been justified by one or more feasibility or rationalization approaches.

DOCUMENTING RESULT CONTD.

At a minimum, each information asset–threat pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed. Furthermore, each control strategy should articulate which of the four fundamental risk–reducing approaches will be used or how they might be combined, and how that should justify the findings by referencing the feasibility studies. Additional preparatory work for project management should be included where available.