Unit III

BCA- 602

CYBER LAW & INTERNET SECURITY

Information Security Governance

It involves the identification of an organisation information assets and development, documentation and implementation policy, standard, procedure and guidelines to ensure CIA (Confidentiality, Integrity, Availability).

The **Information Security Governance and Risk Management** domain entails the identification of an organization's **information** assets and the development, documentation, implementation and updating of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability.

Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

Principles

Establish organization wide **information security**. ...

Adopt a risk-based approach. ...

Set the direction of investment decisions. ...

Ensure conformance with internal and external requirements. ...

Foster a **security**-positive environment for all stakeholders. ...

Review performance in relation to business outcomes.

Information security governance ensures that an organization has the correct **information** structure, leadership and guidance.

Governance helps ensure that a company has the proper administrative controls to mitigate risk.

Risk analysis helps ensure that an organization properly identifies, analyzes, and mitigates risk.

In essence, **security governance** is the process of developing a **security** program that adequately meets the strategic needs of the business. ... It then collaborates with the **implementation**/operations level to communicate **security** requirements and create a **cybersecurity** profile.

Three primary goals of information security are preventing the loss of **availability**, the loss of **integrity**, and the loss of **confidentiality** for systems and data. Most security practices and controls can be traced back to preventing losses in one or more of these areas

Information Governance turns that data into business information by setting the policies and **procedures** to ensure that there are as few instances of that information as possible, that it is securely accessible to the people who need it and it is removed from the organisation as quickly as possible to meet regulatory ...

Information Governance is the **responsibility** of every employee. You must treat all personal **information** with respect and regard for confidentiality, **information** security and **information** quality.

“The **Information Governance framework** covers all staff that create, store, share and dispose of **information**. It sets out the procedures for sharing **information** with stakeholders, partners and suppliers.

Governance of **information security** consists of: (1) aligning **information security objectives** and strategies with business **objectives** and strategies; (2) deliver value to stakeholders - this includes any person or organization that may affect, be affected or perceive to be affected by an activity of the organization

Strategic alignment is an outcome of effective security governance.

Where there is good governance, there is likely to be strategic alignment.

Risk assessment is not an outcome of effective security governance; it is a process.

AHIMA's 8 principles of information governance

Principle of **accountability**: One member of the organization's leadership will be responsible for information governance.

Principle of **transparency**: Information governance will be conducted in an open, verifiable manner.

Principle of integrity: Information management will maintain the reliability of the data.

These components of information governance include the following:

Information governance organization component.

Data stewardship component.

Data quality management component.

Metadata management component.

Privacy and security component.

Information life cycle management component.

Risk Management

Cyber risk management is the process of identifying, analysing, evaluating and addressing your organisation's **cyber security** threats. The first part of any **cyber risk management** programme is a **cyber risk assessment**.

The **risk management process** is a framework for the actions that need to be taken. It begins with identifying **risks**, goes on to analyze **risks**, then the **risk** is prioritized, a solution is implemented, and finally, the **risk** is monitored.

Mitigating **cyber risks** and preventing attacks– Implementing a **cyber risk management** strategy helps to identify the threats to an organisation. Developing a **risk** treatment plan also helps to address the **risks** and put the correct defences in place. This reduces the threats from **cyber**-attacks.

There are different types of risks that a firm might face and needs to overcome. Widely, risks can be classified into three types: Business Risk, **Non**-Business Risk, and **Financial Risk**. Business Risk: These types of risks are taken by business enterprises themselves in order to maximize shareholder value and profits.

There are four parts to any good risk assessment and they are **Asset identification**, **Risk Analysis**, Risk likelihood & impact, and **Cost** of Solutions. **Asset Identification** – This is a complete inventory of all of your company's assets, both physical and non-physical.

Step 1: Identify hazards, i.e. anything that may cause harm.

Step 2: Decide who may be harmed, and how.

Step 3: **Assess** the **risks** and take action.

Step 4: Make a record of the findings.

Step **5**: Review the **risk assessment**.

The Transaction **Risk Investigator** position relies on excellent judgment to plan and accomplish goals and will work under very limited supervision of the Manager. Excellent individual problem-solving and analytical skills are used to authenticate customers and complex transactions.

In the following sections four methods of risk mapping will be discussed: Quantitative risk assessment (QRA), Event-Tree **Analysis** (ETA), Risk matrix approach (RMA) and Indicator-based approach (IBA).

**********Thank you**********