INFORMATION SECURITY GOVERNANCE

Assignment no 1 **Prepared by: Dr. Manoj Kumar**

Submitted by: Kashish Srivastava | R134218079 | 500067405

Q1: Explain information security governance and GRC and its importance as per IT security prospectus?

Information security governance is a sustainable security culture based on four features requiring care and feeding for the organization.

- Have a better security that is deliberate in nature
- Must be enjoyable since it is a culture, every member of the organization should have a happy and challengable environment for participation in security
- The input provided by an individual should also be aware of the output to be received
- It provides a return on investment. The reason anyone does security is to improve an offering and lower vulnerabilities; we must return a multiple of the effort invested.

GRC- Governance, Risk and Compliance

It is the collection of capabilities an organization should hold to achieve the objectives along with the act of integrity. This includes the work done by departments like internal audit, compliance, risk, legal, finance, IT, HR as well as the lines of business, executive suite and the board itself.

Q2: Design a Framework for analyzing information security key forces?

The security of information systems is a serious issue because computer abuse is increasing. It is important, therefore, that systems analysts and designers develop expertise in methods for specifying information systems security. The characteristics found in three generations of general information system design methods provide a framework for comparing and understanding current security design methods. These methods include approaches that use checklists of controls, divide functional requirements into engineering partitions, and create abstract models of both the problem and the solution.

Threat of barrier

Supplier power employee, Consultant, Vendor

Substitutes consultant

Customer Power

Compliances and Internal audits

Q3: Why SWOT is important. What are the types of security strategies?

SWOT is strengths, weakness, ooportunities and threats

There are 2 types of security strategies:

Threat Management and Digital Trust (Compliance)

-Identify and respond to threats with speed and confidence

-Govern and protect your business, data, users and assets.

Provision, audit and report user access

- Increase end-user satisfaction
- Achieve regulatory compliance
- Reduce business risk and costs
- Provide insight on risky users

Q4: How many numbers of security competencies are there in CSF, elaborate each?

There are 7 security competencies present in CSF.

These competencies are based on effective security leadership.

Understand the organization culture - Involve within the environent happily and adapt it positively

Communicate real risk - Understanding real time challenges

Engage associated at all organizational levels - Creating awareness at all the organizational levels via association

Pay attention to technical competence - Technically organization has to be comparably strong

Be an insider - Confidentiallity has to be maintained

Set realistic but aggressive goals

Collaborate and network outside the company - Maintaining network outside the

company to stay aware of the updates ,policies and friendly relations

Q5: Discuss C suite in detail? Explain security council representation?

Executing effective security governance and defining the strategic security objectives of an organization is an arduous task, but can be accomplished through C-Suite interaction. It requires leadership and ongoing support from executive management and other departments to succeed and develop an information security governance. Effective information security management also requires integration with and cooperation from organizational and business unit management.

Security council representation is as followed(Top-bottom):

Human resources, Information Tehnology, Legal, Basic units, Information security,Internal Audit, Compliance and ethics, physical security and risk management. The purpose of the working group is to develop a set of recommendations. Foster communication, promote awareness and education about information security with the goal of reducing the risk of unauthorized or malicious compromise of data and services.

Activities are focused on four audiences: faculty, students, technical staff and non-technical staff. Note, activities will be measured.

Provide communications, education and awareness support, recommendations and expertise to information security council initiatives (and working groups).

The Research Data Working Group will provide good practice and resource information to researchers regarding data protection.

Q6: ***The risk can impact an organization many ways. What are those ways to analyses the risks?***
Differentiate with the help of example?

Risk can be analysed in two forms:

Qualitative Analysis
Quantitative Analysis

Threat assessment
Vulnerability assessment
Impact assessment

It is clear that vulnerability assessment is a key input into risk assessment, so both exercises are crucial in securing an organization's information assets and increasing its likelihood of achieving its mission and objectives. Proper identification and addressing of vulnerabilities can go a long way towards reducing the probability and impact of threats materializing at system, human, or process levels. Performing one without the other, however, is leaving your company more exposed to the unknown.

It is important that regular vulnerability and risk assessments become a culture in every organization. A committed, ongoing capacity should be created and supported, so that everyone within the organization understands their role in supporting these key activities.

Q7: Put some light on Risk Assessment Process with the help of risk mitigation options (draw a figure).

Risk mitigation strategy

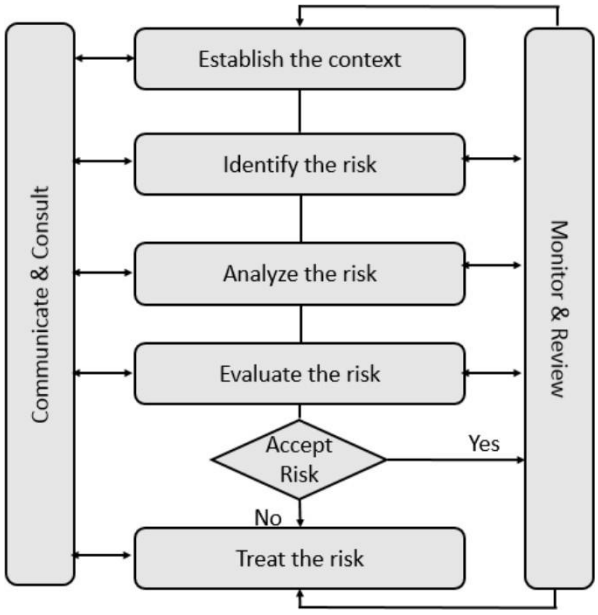
Establishing the context

Identification & Anayzing and evaluate risks

Treat the risks

Tracking & reporting

Communication and controls and Monitor and Review



Look critically at your organization's context in terms of sector, operational processes and assets, sources of risks, and the outcome should they materialize. For example, an insurance company might handle customer information in a cloud database. In this cloud environment, sources of risks might include ransomware attacks, and impact might include loss of business and litigation. Once you've identified risks, keep track of them in a risk log or registry.

Here, you'll estimate the likelihood of the risk materializing as well as the scale of the impact to the organization. For example, a pandemic might have a low probability of occurring but a very high impact

on employees and customers should it arise. Analysis can be qualitative (using scales, e.g. low, medium, or high) or quantitative (using numeric terms e.g. financial impact, percentage probability etc.)

In this phase, evaluate the results of your risk analysis with the documented risk acceptance criteria. Then, prioritize risks to ensure that investment is focused on the most important risks (see Figure 2 below). Prioritized risks might be ranked in a 3-band level, i.e.:

- Upper band for intolerable risks.
- Middle band where consequences and benefits balance.
  A lower band where risks are considered negligible.

Q8: Explain various security Control Methodologies?

Security control methodlogies are:

ISO/IEC 27001 – Information Security Management Standard

NIST – Measurement Standard

COBIT – IT Governance Framework

HIPPA

SO/IEC 27001:2013 controls

The Standard doesn't mandate that all 114 Annex A controls be implemented. A risk assessment should determine which controls are required, and a justification provided as to why other controls are excluded from the ISMS.

Below are the list of control sets.

- A.5 Information security policies
- A.6 Organisation of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

Q9: Design a table with respect to various risk controls?

Identification.	Determine all critical assets of the technology infrastructure. Next, diagnose sensitive data that is created, stored, or transmitted by these assets. Create a risk profile for each.
Assessment.	Administer an approach to assess the identified security risks for critical assets. After careful evaluation and assessment, determine how to effectively and efficiently allocate time and resources towards risk mitigation. The assessment approach or methodology must analyze the correlation between assets, threats, vulnerabilities, and mitigating controls.
Mitigation.	Define a mitigation approach and enforce security controls for each risk.
Prevention.	Implement tools and processes to minimize threats and vulnerabilities from occurring in your firm's resources.