CYBER MANAGEMENT ALLIANCE

CISSP Domain 1

Security& Risk Management Review Notes

Information Security Governance

Security governance is the set of responsibilities and practices exercised by the Board and Executive Management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

Information Security Management

Information Security Management includes the following:

- Risk management;
- Information security;
- Policies and procedures;
- Standards;
- Guidelines;
- Baselines;
- Information classification;
- Security organisation; and
- Security education.

Due Care - Development and implementation of policies and procedures to aid in protecting the company, its assets and its people from threats.

Due Diligence - Act of investigating and understanding the risk. Another way of understanding these terms is to think of Due Care as doing the right thing, and Due Diligence as evaluating the results of Due Care measures to ensure that they are performing as intended.

An Ideal Policy – should be:

- Strategic in nature;
- Supported by management;
- Aligned to business objectives;
- Very generic and non-technical;
- Forceful with directive wording;
- Communicated properly;
- Reviewed at least once in a year or with any change to the organisation; and
- Updated at least every three years.

Standards – should include:

- Mandatory activities, actions and rules or regulations; and
- A means to ensure that specific technologies, applications, parameters and procedures are implemented in a uniform manner across the organization.
- Example: ISO 27001.

Guidelines – are:

- Recommended actions and operational guides to users, IT staff, operations staff and others when a specific standard does not apply; and
- To help ensure that security measures are observed.
- Example: Password guidelines.

Procedures – are:

- Detailed step-by-step tasks that should be performed to achieve a certain goal; and
- To spell out how the policy, standards and guidelines will be implemented in an operating environment.
- Example: Incident Response Procedure.

Separation of Duties – The design of sensitive processes requiring two or more people to complete them.

Job Rotation - Good for cross-training and reduces the likelihood that employees will collude for personal gain.

Mandatory Vacations - Detect/prevent irregularities that violate policy and practices.

Split Knowledge - Someone who only has enough knowledge to perform part of a task.

Dual Control - Two or more people must be available and active to perform an action.

Senior Management - Has the ultimate responsibility for security.

Chief InfoSec Officer – has:

- Functional responsibility for security;
- Responsibility for understanding the business objectives of the organisation;
- Ensures that a risk assessment is performed; and
- Communicates the risks to Executive Management.

Data Owner - Determines the data classification.

Data Custodian - Preserves the information CIA.

System Owner – Is responsible for the security of the system containing data.

System Administrator - looks after:

- Patch management;
- User ID creation and deletion; and
- Monitors logs of the Security Administrator.

Risk Analysis – works to:

- Identify assets and assign values to them;
- Identify vulnerabilities and threats; quantifies the impact of potential threats;
- Provides an economic balance between the impact of a risk and the cost of safeguards; and
- Calculates quantitative analysis use risks to attempt to predict the level of monetary losses, and the percentage chance for each type of threat. The qualitative analysis does not use calculations but is more situation and scenario-based.

Single Loss Expectancy (SLE) – is:

A dollar amount that is assigned to a single event representing the company's potential loss amount if a specific threat were to take place. Example:

SLE = Asset value ($) x EF (%)

(Example 1000 $ (value of server) * 0.4 (Probability of Fire)

Exposure Factor (EF) - Represents the percentage of loss a realised threat could have on a certain asset.

Annualized Loss Expectancy (ALE) - ALE = SLE x Annualized Rate of Occurrence (ARO)

Annualized Rate of Occurrence (ARO) - The value which represents the estimated frequency of a specific threat taking place within a one year time frame.

Delphi Method – two types:

Consensus Delphi method:

- Experts help to identify the highest priority security and corresponding counter-measures.
- A systematic interactive forecasting method based on independent inputs of selected experts.

Modified Delphi method:

- A silent form of brainstorming in which participants develop ideas individually and silently, with no group interaction. The ideas are submitted to a group of decision-makers for consideration and action.
- This technique is similar to the Consensus Delphi method in terms of procedures (a series of rounds with selected experts), and intent (to predict future events, arriving at a consensus).

Hiring Practices – comprises:

- Perform background checks (prior employment, education, criminal history and financial history);
- Requirement of confidentiality agreements (Non-Disclosure Agreement);
- An Intellectual Property Agreement;
- Conflict of Interest Agreements for positions handling competitive information; and
- Non-Compete Agreements for positions in charge of unique corporate processes.

TOGAF

The TOGAF framework enables organisations to effectively address critical business needs by:

- Ensuring that everyone speaks the same language;
- Avoiding lock-in to proprietary solutions by standardising on open methods for Enterprise Architecture;
- Saving time and money, and utilising resources more effectively; and
- Achieving demonstrable ROI.

SABSA - SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for enterprise security architecture and service management. It was developed independently from the Zachman Framework but has a similar structure.

Stages in Business Continuity Management – they are:

- Phase I: Project Management and Initiation.
- Phase II: Business Impact Analysis (BIA).
- Phase III: Recovery Strategy.
- Phase IV: Plan Design & Development.
- Phase V: Implementation.
- Phase VI: Testing.
- Phase VII: Maintenance, Awareness and Training.

Business Continuity Planning (BCP) – comprises:

- Addressing the preservation and recovery of business in the event of outages to normal business operations;
- Is an approved set of arrangements and procedures that enables an organisation to:
- Facilitate the recovery of business operations;
- Minimise loss;
- Repair or replace the damaged facilities or components as soon as possible.

Business Impact Analysis (BIA) - The process of determining the impact of an IT service disruption to business operations in terms of financial loss. It is a part of BCP.

BCP Coordinator Roles and Responsibilities – include:

- Responsible for the development of BCP;
- To serve as the liaison between the Planning Development team and management;
- Has direct access and authority to interact with all employees;
- Possessing a thorough business knowledge and understanding how an outage can affect the organisation:
- Be familiar with the entire organisation and the position within the organisation;
- Has easy access to executive management; and
- Understands the Charter, Mission Statement and executive viewpoint.

Mean Time Between Failure (MTBF) – Is the estimated lifetime of a piece of equipment, calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced.

Mean Time to Repair (MTTR) - Is an estimate of how long it will take to fix a piece of equipment and have it back in production.

Recovery Time Objective (RTO) - Is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Recovery Point Objective (RPO) - Is defined by Business Continuity Planning and is the maximum targeted period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit within which to work.

Intellectual Property Law Patent – is:

- A patent granting the owner a legally-enforceable right to exclude others from practicing the invention covered;
- Usually twenty years from the filing date;
- Legal ownership, the strongest form of IP protection, granted by a government; and
- Protects novel, useful and non-obvious inventions.

Trademark – is:

- A word, name, symbol, colour, sound, product shape or combination of these used to identified goods and distinguish them from those made or sold by others;
- Is used in relation to services rather than products, and ca sometimes be called a “service mark”.

Copyright – is:

- A set of exclusive rights regulating the use of a particular expression of ideas (i.e. “original works of authorship”);
- To protect the expression of an idea, not the resource itself; and
- A computer program that can be protected under copyright law.

Trade Secret – is:

- A secret that does not expire as would a patent;
- A secret that provides a company with a competitive value or advantage;
- A development that requires special skills, ingenuity and/or expenditure of money or effort; and
- Proprietary to the company (e.g. the formula for Coca-Cola or Pepsi).

Student Notes: