Governance and Management of IT I

Enterprise Governance of Information and Technology (EGIT)

1. Which of the following best describes Enterprise Governance of IT?

   The process of aligning IT strategy with business objectives, ensuring that IT investments deliver value and support organisational goals.

2. Which of the following best describes IT Portfolio Management?

   the process of managing an organisation's IT projects and resources to ensure alignment with business objectives and optimal return on investment.

3. The effectiveness of an IT governance implementation can be most effectively determined by

   ensuring the involvement of stakeholders.

4. The IS auditor noted that roles and responsibilities in terms of IT governance and management are not properly documented and defined. What is the most appropriate recommendation?

   to define the accountability of each critical function.

5. The primary reason for reviewing the organisational chart is as follows

   to understand the roles and responsibilities of individuals.

6. Which of the following is the prime consideration in determining whether IT adds value to the business?

   the alignment of the IT strategy with the organisational strategy

7. A major risk associated with a lack of top management support in terms of IT strategic planning is the following?

   a lack of alignment between the technology and business objectives.

8. The greatest concern with respect to an organisation's governance model is the following

   senior management does not review information security policy.

9. For sound IT governance, the IT plan should be consistent with the following

   the organisation's business plan

10. Who among the following is responsible for IT governance?

    directors

11. To achieve the organisation's objective, the most important consideration for an IT department is to have which of the following

    long- and short - term strategies.

12. While reviewing IT structure, a major concern revolves around which of the following

    the alignment of IT and business requirements.

13. Which of the following is related to strategic planning?

    an approved suppliers for the company's products.

14. The most important consideration when evaluating the IT strategy of an organisation is

    support for the objectives of the business

15. The most important method for ensuring alignment of the IT strategy with the organisation's business objectives is

    to review the compatibility of the IT plan and the business plan

16. Strategic alignment can best be improved by

    involvement of top management in aligning business and technology requirements.

17. Which of the following best ensure effective IT governance?

    alignment of the IT strategy with the organisation's strategies and objectives.

18. The most important factor regarding the effective implementation of IT governance is

    Identified organisational strategies

19. An IT strategies plan should contain

    a mission and vision

20. Which of the following is the main objective of IT governance?

    the optimal use of technology resources

21. Which of the following is the primary purpose of corporate governance?

    to provide a strategic direction

22. Which of the following is a prime indicator in deciding the area of priority for IT governance?

    business risks

23. An IS auditor evaluating an IT governance framework will be more concerned about

    the limited involvement of senior management

IT Standards, Policies and Procedures

1. Which of the following best describes a policy?

   a high-level document that outlines the principles and rules governing an organisation’s actions and decisions.

2. Which of the following best describes a standard?

   a document that defines mandatory technical or operational requirements to ensure consistency and compliance.

3. Which of the following best describes a procedure?

   a detailed set of instructions that outlines the exact steps to be followed to accomplish a specific task.

4. Which of the following is a first step for the auditor having observed that IT policies are not approved by management?

   to include this as non-compliance in an audit report

5. An area of most concern while reviewing HR policy is the absence of a

   termination process

6. The best reason for a policy that restrict a second employment is

   to prevent a conflict of interest

7. The greatest concern for an IS auditor reviewing an information security policy is the fact that

   the policy is not approved by senior management

8. Policy compliance can be best ensured by

   an existing IT mechanism that support compliance

9. Which of the following is the most important action following the dismissal of an employee?

   disabling access rights on the part of the employee

10. A major risk of an unstructured policy regarding data and system ownership is the fact that

    access can be granted to unauthorised users

11. Which of the following is a major risk when employees are not aware of the information security policy?

    the unintentional disclosure of sensitive information

12. Information security policy should be approved by

    Board of directors

13. Information security policy should include

    the basis of access control authorisation

14. The most important factor for successful implementation of a security policy is

    assimilation and intent of all users

15. Which of the following is most critical in terms of being addressed by an email policy?

    email retention

16. Development of an information security program starts with

    development of a corporate information security policy statement

17. The risk of the unavailability of electronic evidence is reduced by

    Email archive policy

18. The most important concern while reviewing information security policy is the fact that

    IT department objectives drive IT policy

19. The development of operational policies by means of a top-down approach helps

    to make them consistent across the organisation

20. The most important factor while developing information security policy is

    consideration of business requirements

21. The most important factor in determining the appropriate level of protection is

    the outcome of a risk assessment

22. The first point of reference for an IS auditor conducting an audit is

    approved policies

23. The most important factor in developing an information security policy is

    the appetite for risk on the part of an enterprise

24. The most important aspect in ensuring that an organisation's policy complies with legal requirement is to

    have a periodic review of policy conducted by a subject matter expert.

Roles and Responsibilities

1. Which of the following best describes a Strategy Committee?

    a committee that provides guidance on aligning IT strategy with overall business goals and ensures IT investments support the organisation's long term objectives.

2. Which of the following best describes a Steering Committee?

    a committee that oversees the execution of IT projects and ensures that these projects align with the organisation's strategic goals.

3. Final responsibility for the development of an information security policy rests with

    the Board of Directors

4. Participation on the part of senior management is most important as regards the development of

    strategic plans

5. The IS steering committee is primarily responsible for

    approving and monitoring major projects, the status of IS plans and budgets.

6. Ultimate responsibility for IT governance rests with

    the Board of Directors

7. Overall responsibility for system development project is assumed by

    the project steering committee

8. Ownership of a project should be assumed by

    User management

9. A request for proposal (RFP) to purchase a new system will most likely to approved by

    Project steering committee

10. The ultimate responsibility for internal lies with

    Senior management

11. The ultimate responsibility for requirement specifications rests with

    the project sponsor

12. Which of the following is a function of the steering committee?

    to escalate project issues.

13. Who is accountable for ensuring relevant controls over IS resources?

    resource owners

14. Ownership of a system development project and the system proposed is assumed by

    user management

15. The roles of the IT committee is

    to approve and control funds for IT initiatives

16. Responsibility for monitoring project milestones and aligning a project with business requirements rests with

    IT steering committee

17. The role of the IT steering committee is

    to prioritise IT projects as per business requirements

18. The most suitable person to be appointed as chair of the steering committee is

    an executive-level officer

19. An IS steering committee comprises

    key executives officers

20. The primary role of the IT steering committee is

    to monitor the IT project's priorities and milestones.

21. The IT steering committee is primarily required to determine

    that the IT processes are aligned with business requirements.

22. In a system development project, which of the following is considered a major control weakness?

    the organisation does not have a project steering committee

23. An IT steering committee should

    update the board about the activities the committee

Enterprise Architecture

1. Which of the following best describes Enterprise Architecture?

   a framework that outlines the organisation's IT infrastructure and ensures alignment between IT and business strategies.

2. An IS auditor finds that the organisation has two separate Enterprise Architectures, one for current-state representation and a new project has been initiated to build a future-state representation. The IS auditor should

   report this problem in the audit report as an observation

3. The main advantage of an EA initiative is to

   allow the company to invest in the technology that is most suitable

4. Which of the following is a major concern when IT is not involved in a system selection procedure?

   the application technologies may be incompatible with the architecture of the organisation.

5. A vendor has been hired by a company to find a software solution for their electronic toll collection system (ECTS). As part of the solution, the vendor has developed their own application software. The contract will include

   the inclusion of source code in escrow

6. Which of the following factors is the most valuable on account of the technology transition rate?

   sound processes

7. An enterprise is considering investing significantly in infrastructure improvements. Which of the following are the most critical options to consider?

   a risk analysis

8. Which of the following is the most important advantage of open system architecture?

   it facilitates interoperability within different systems

9. Which of the following steps should be carried out first before designing a security architecture?

   define a security policy

10. Compliance risk is not directly addressed by

    risk transfer

11. Following the merger of two companies, a new common interface would replace several self-developed legacy applications. Which of the following options constitutes the biggest risk?

    the substitute plan consists of several independent projects without incorporating resource allocation in an approach to portfolio management

12. The best recommendation for securing an organisation's software investment is to

    include a source code escrow arrangement in the service level agreement.

Enterprise Risk Management

1. Which of the following best describes an example of risk mitigation?

   implementing multi-factor authentication to reduce the likelihood of unauthorised access

2. Which of the following best describes an example of risk acceptance?

   deciding to proceed with a project despite known risks as the potential benefits outweigh the risks.

3. Which of the following best describes an example of risk avoidance?

   declining to enter a new market due to the high potential for regulatoly challenges.

4. Which of the following should be reviewed first while evaluating an organisation's risk management procedure?

   threats or vulnerabilities effecting the assets

5. Which of the following treatments indicates the exchange of risk?

   to transfer risk

6. A team performing a risk analysis has difficulty anticipating the financial losses that might result from a risk. To evaluate the potential impact, the team should

   apply a qualitative approach

7. Establishing the level of acceptable risk is the responsibility of

   senior business management

8. Performance of the process of risk management is an input for

   security policy decisions

9. The first duty of the IS auditor is to review any current e-business program in search of vulnerabilities. What should the nest task be?

   to identify risks and the possibility of occurrence

10. An assessment of IT risk is best achieved by

    an assessment of those risks and vulnerabilities relevant to current IT infrastructure and IT programs.

11. A poor choice of passwords and unencrypted data transmissions over protected communication lines are examples of

    vulnerabilities

12. The first step in implementing a risk management program is to

    determine the threat, vulnerability and risk profiles of the organisation.

13. What is the best recommendation for a small-sized IT organisation that does not have an independent risk management function and where the organisation's operational risk reporting includes only a few forms of IT risk that are commonly defined?

    establish regular IT risk management meetings to define and assess risk and develop a contingency plan as an approach to controlling risk within the company

14. Which of the following types of insurance cover a risk rising from employees' fraudulent actions?

    fidelity coverage

15. Which of the following is of greatest interest to an IS auditor evaluating the risk strategy of an organisation?

    all risks are identified and categorised

16. The most important consideration while reviewing a risk management program is

    the fact that IT risk is presented from a business perspective

17. The risk appetite of an enterprise is best ascertained by

    the steering committee

18. You are reviewing the risk management procedures of HDA Inc. You should primarily focus on

    whether all likely risks are documented and prioritised

19. Which of the following is the best way to assess the IT risk

    determine the threats to the organisation's current IT environment.

Laws and Regulations

1. Which of the following best describes a Governance, Risk, and Compliance (GRC) program?

   a framework that integrates the assurance functions to achieve organisational objectives and ensure regulatory compliance.

2. Which of the following is a determining factor in not maintaining customer data at an offshore location?

   privacy laws could prevent the flow of information across borders

3. Which of the following is a major concern for an IS auditor when reviewing regulatory compliance of an organisation?

   no list of applicable laws and regulations is maintained

4. The most important factor to consider in terms of the success of IT activities is

   to analyze IT support for compliance with regulatory requirements.

5. A Major concern regarding the storage of sensitive data in the cloud as

   data confidentiality

6. The most important concern regarding the use of cloud services is

   compliance with laws and regulations

IT Resource Management

1. What is the primary objective of background screening of new staff?

   assurance about the integrity of the staff

2. Which of the following is the primary consideration when reviewing the IT priorities and co-ordination?

   alignment of the project with business objectives.

3. A software escrow agreement is intended primarily to address which of the following?

   the risk of business closure of a vendor of custom-written software

4. The prime objective of mandatory holidays for employees is which of the following?

   reduce the opportunity for fraud or illegal acts

5. Which of the following roles, taken together, should not be trusted to a single individual?

   system administrator and application developer

6. The integrity of new staff can be determined by which of the following?

   conducting background verification

7. Which of the following dual roles is an area of major concern?

   system administrator and application programmer

8. The rate of change in technology increases the importance of which of the following?

   implementing and enforcing sound processes

9. The most important consideration when planning to implement a new technology is which of the following?

   a risk analysis

10. The best compensatory control for a lack of segregation of duties between IT staff and end users is which of the following?

    reviewing transaction and application logs

11. Which of the following risks should be assessed by an IS auditor reviewing an organisation that uses cross-training practices?

    all parts of a system being known to one person

12. The most important consideration when reviewing an approved software product list is which of the following?

    whether the risk associated with each product is reviewed periodically

13. The primary control objective of job rotation is to achieve which of the following?

    to detect improper or illegal employee acts

14. Which of the following should be done as a priority when an employee with access to highly confidential information resigns?

    revoke the employee's access to all systems

15. The primary control objective of implementing a vacation policy is which of the following?

    to identify potential errors or inconsistencies in business processes

16. Which of the following best describes Segregation of Duties?

    the process of dividing responsibilities among different individuals to reduce the risk of error or fraud.

Key Points

- Enterprise Governance of Information and Technology (EGIT) encompasses the framework and processes that ensure IT delivers value and manages risk effectively.
- IT Portfolio Management involves managing the organisation's IT projects, applications, and resources as a portfolio to ensure they align with the organisation's goals and deliver the expected value,.
- IT Portfolio Management aims to optimise IT investments and resource allocation.
- The effectiveness of IT governance implementation can be determined most effectively by involving stakeholders and addressing their requirements.
- The primary reason for reviewing the organisation chart is to understand the roles, responsibilities and authority of the individual.
- This helps in determining whether there is proper segregation of functions.
- Investment in IT will be of no value if IT does not support the business objectives.
- Participation by top management is critical in ensuring that information security policy complies with business requirements.
- IT governance is primarily the obligation of the Board of Directors.
- The Board of Directors is required to ensure that IT activities are moving in the desired direction and that IT is adding value to the business.
- To achieve an organisation's objectives, the most important consideration for an IT department is to have long - and short - term plans.
- Selecting suppliers for the company's products constitutes strategic level planning, aims to provide direction to the business function.

- The involvement of top management in mediating between the imperative of business and technology is the best option when it comes to improving strategic alignment.
- Identification of the business strategy is the most important factor as regards the effective implementation of IT governance.
- The IT strategic plan must contain a clear statement regarding the mission and vision of IT.
- IT governance is intended to ensure the optimal use of IT resources and thereby support the business strategy.
- Corporate governance provides strategic direction to the organisation as a whole and thereby aligns the efforts of all the functions in the same direction with a view to achieving a common business goal.
- IT governance should concentrate on those areas with a high business risk.
- It is essential to ensure that senior management is involved in the implementation of an IT governance framework.
- Policy defines what should be done but not how to do it detail.
- A documented termination process is important in ensuring information security on the part of the organisation.
- The main reason for restricting second employment is to prevent conflicts of interest and thereby safeguard the organisations' sensitive information.
- Senior management is responsible for developing, reviewing, approving and evaluating security policy.
- Without proper ownership of data and systems, there is an increased risk of providing access to individuals who are not otherwise authorised.
- Board of Directors responsible for the approval of the information security policy.
- The IT department is responsible for the execution of the policy.
- The steering committee monitors IT projects.
- The audit committee oversees the audit function.
- The security policy includes a broad framework of security arrangements as approved by top management.
- This includes an overall basis for access control authorisation.
- The email policy should address the issue of email retention as per business and legal requirements.

- This, in turn, will help to retain electronic evidence as per the organisation's requirements.
- In a top-down approach, all the policies are derived from corporate level policy to ensure that is consistent across the organisation.
- The outcome of a risk assessment determines the critically of the assets.
- Appropriateness of control is considered on the basis of risk associated with assets.
- A risk assessment considers risk on the basis of probability and impact.
- The strategy Committee is tasked with ensuring that the IT strategy is aligned with the broader business objectives, guiding IT investments to support the organisation's long term goals.
- User management is involved in requirement specifications and is regard as the owner of the project.
- User management conducts user acceptance testing and approves projects as they are defined and accomplished.
- The project steering committee includes top-level officers from each function, and is best suited to approving Request for Proposal (RFP).
- The organisation's senior management is responsible for effective internal control mechanisms.
- The project sponsor is generally regarded as being in charge of the business function for which a system is to be developed.
- The project sponsor is responsible for finalising the functional specifications for the new system under development.
- In the case of any issues or concerns impacting anticipated results, the steering committee should escalate them.
- Resource owners are responsible for maintaining appropriate security measures over information assets.
- Asset owners should make decisions relating to classification and access rights.
- System administrators, network administrators and database administrators provide support in terms of asset security.
- IT executives will review the outsourcing of contracts and the IT framework.
- The IT strategy committee advises the board on IT strategy.
- Board members generally are not expected to be involved in implementation.

- The steering committee should consist of key executives and representatives from user management.
- Only user management and IT members will not serve the aims of the committee.
- Keeping the board informed ensures alignment with the organisation's strategic goals and provides oversight on IT initiatives and investments.
- Enterprise Architecture is a comprehensive framework that defines the structure and operation of an organisation's IT infrastructure.
- It is important for the Enterprise Architecture to consider the entire future outcome as IT strategic and tactical plans will be determined by the difference between the present state and the future state.
- Enterprise Architecture's primary focus is to ensure that the technology initiatives are compatible with the IT organisation's framework, data and implementation standards.
- For fields such as the use of common systems, repositories, or programming language, the Enterprise Architecture describes both a current and future state.
- Change control includes the application and execution of good change management systems.
- An organisation should carry out a risk assessment before implementing new technology, which will then be presented to the management of the business unit for review and acceptance.
- An open system is a system in which the components and protocols conform to standards independent of a particular supplier.
- Open system facilitate interoperability between systems made by different vendors.
- The first step in developing a security architecture is to establish a security policy for information and related technology.
- A security policy provides customers, administrators, and technical staff with a consistent security framework.
- Transferring risk usually covers financial risk.
- The measures for maintaining compliance with the post-merger organisation's overall strategy should be streamlined.

- When resource management is not distributed, there is a danger that independent initiatives may overestimate the availability of essential information tools for the legacy applications built in-house.
- Risk mitigation involves taking actions to reduce the likelihood or impact of a risk.
- Risk transfer for instance, when taking out an instance policy is a form of risk sharing.
- The method of risk management involves making specific security-related choices, such as acceptable risk rates.
- To measure IT risk, it is important to analyse risks and weaknesses using qualitative or quantitative risk evaluation methods.
- Establishing regular IT risk management meetings in a medium-sized organisation is the best way of identifying and evaluating IT-related risk, identifying responsibilities on the part of the respective management, and updating the risk register and mitigation plans.
- Fidelity insurance is taken out by an employer against losses incurred as an result of dishonest actions by employees.
- Governance, Risk and Compliance (GRC) program is a framework that integrates assurance functions (such as audit, risk management, and compliance) to help the organisation achieve its objectives and ensure it adheres to regulatory requirements.
- Some privacy law restrict the movement of data outside the jurisdiction.
- In the absence of a list of all relevant laws and regulations, the level of compliance and consistency with specific laws and regulations cannot be monitored.
- Compliance with regulatory requirements will be the most effective and necessary choice.
- Considering various laws and regulations that require privacy or confidentiality of customer information, unauthorised access to information and data leakage are major concerns.
- The primary objective of background screening is to ensure that the new staff members are trustworthy and have a history of integrity.
- An escrow agreement is entered into between a service provider and a client to ensure the permanent availability of the client’s source code.

- Mandatary holidays aim to hand over the processes that employee was responsible for to another employee, thereby unearthing any fraud or process lapses committed by the employee on holiday.
- Ideally, all of the roles should be segregated, but the major concern is about the system administrator and application developer. This person can do almost anything, including creating the back door.
- It is essential to implement sound IT process and policies to cope with frequent and rapid IT changes.
- In cross-training, individuals are trained on other aspects of the jobs in addition to their routing function.
- It is important to ensure that cross-training does not lead to potential exposures related to abuse of privilege.