TUGAS KELOMPOK

AUDIT SISTEM INFORMASI

……

Dosen Pengampu : Hasdi Putra, ST., MT

Disusun Oleh:

1.	Daffa Abdillah	(2111521001)
2.	Shabrina Elfani Gucy	(2111521005)
3.	Nadia Nur Saida	(2111521007)
4.	Syadza Intan Benya	(2111521011)
5.	Annisa Gita Subhi	(2111522011)
6.	Nadini Annisa Byant	(2111522021)
7.	Vania Zerlina Utami	(2111523003)

KELOMPOK 2

KELAS A (01)

PROGRAM STUDI S1 SISTEM INFORMASI

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS ANDALAS

2024

A. IT Governance and IT Strategy

3. What is the PRIMARY consideration for an IS auditor reviewing the prioritization and coordination of IT projects and program management?

A. Projects are aligned with the organization's strategy.

B. Identified project risk is monitored and mitigated.

C. Controls related to project planning and budgeting are appropriate.

D. IT project metrics are reported accurately.

5. Which of the following factors is MOST critical when evaluating the effectiveness of an IT governance implementation?

A. Ensure that assurance objectives are defined.

B. Determine stakeholder requirements and involvement.

C. Identify relevant risk and related opportunities.

D. Determine relevant enablers and their applicability.

23. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. A. Lack of investment in technology

B. Lack of a methodology for systems development

C. Technology not aligning with organization objectives

D. Absence of control over technology contracts

26. Involvement of senior management is MOST important in the development of:

A. Strategic plans.

B. IT policies.

C. IT procedures.

D. Standards and guidelines.

27. Effective IT governance ensures that the IT plan is consistent with the organization's:

A. Business plan.

B. Audit plan.

C. Security plan.

D. Investment plan.

29. IT governance is PRIMARILY the responsibility of the:

A. chief executive officer.

B. board of directors.

C. IT steering committee.

D. audit committee.

39. To support an organization's goals, an IT department should have:

A. A low-cost philosophy.

B. Long- and short-term plans.

C. Leading-edge technology.

D. Plans to acquire new hardware and software.

40. In reviewing the IT short-range (tactical) plan, an IS auditor should determine whether:

A. There is an integration of IT and business personnel within projects.

B. There is a clear definition of the IT mission and vision.

C. A strategic information technology planning scorecard is in place.

D. The plan correlates business objectives to IT goals and objectives.

42. Which of the following goals do you expect to find in an organization's strategic plan?

A. Results of new software testing

B. An evaluation of information technology needs

C. Short-term project plans for a new planning system

D. Approved suppliers for products offered by the company

43.Which of the following does an IS auditor consider to be MOST important when evaluating an organization's IT strategy? That it:

A. Was approved by line management.

B. Does not vary from the IT department's preliminary budget.

C. Complies with procurement procedures.

D. Supports the business objectives of the organization

45. When reviewing the IT strategy, an IS auditor can BEST assess whether the strategy supports the organizations' business objectives by determining whether IT:

A. Has all the personnel and equipment it needs.

B. Plans are consistent with management strategy.

C. Uses its equipment and personnel efficiently and effectively.

D. Has sufficient excess capacity to respond to changing directions.

60. IS control objectives are useful to IS auditors because they provide the basis for understanding the:

A. Desired result or purpose of implementing specific control procedures

B. Best IS security control practices relevant to a specific entity.

C. Techniques for securing information

D. Security policy

89. Which of the following is the MOST important element for successful implementation IT governance?

A. IT scorecard implementation

B. Identify the organization's strategy

C. Conduct risk assessments

D. Create a formal security policy

90. To assist management in achieving IT and business alignment, IS auditors should recommend the use of:

A.control self-evaluation.

B.business impact analysis.

C.TI balanced scorecard.

D.business process reengineering.

95. To gain an understanding of the effectiveness of organizational planning and investment management on IT assets, IS auditors should review:

A.enterprise data model.

B.TI balanced scorecard.

C. Structure IT organization.

D. report historical finance.

99. When reviewing the IT strategic planning process, IS auditors should ensure that the plan:

A.combines advanced technology.

B.handle necessary operational controls.

C.articulate its mission and vision.

D.define project management practices.

104. When implementing an IT governance framework in an organization, the MOST important objectives are:

A. Alignment of IT with business

B. Accountability

C.Realizing value with IT

D.Increase return on investment

106. The ultimate goal of IT governance is to:

A.encourage optimal use of IT.

B.reduce IT costs.

C.decentralize IT resources across the organization.

D.centralize IT control.

110. In the context of effective information security governance, the MAIN objective of delivering value is to:

A.Optimize security investments to support business objectives.

B.Implement a set of standard security practices.

C.Institute standards-based solutions.

D.Implement a culture of continuous improvement.

111. As a driver of IT governance, transparency of IT's cost, value and risk is primarily achieved through:

A. performance measurement.

B. strategic alignment.

C. value delivery.

D. resource management.

112. Which of the following should be the MOST important consideration when deciding on areas of priority for IT governance implementations?

A. Process maturity

B. Performance indicators

C Business risk

D. Assurance reports

113. Responsibility for the governance of IT should rest with the:

A. IT strategy committee.

B. Chief information officer.

C. Audit committee.

D. Board of directors.

115. When developing a formal enterprise security program, the MOST critical success factor is the:

A. Establishment of a review board.

B. Creation of a security unit.

C. Effective support of an executive sponsor.

D. Selection of a security process owner.

116. When reviewing an organization's strategic IT plan, an IS auditor should expect to find:

A. An assessment of the fit of the organization's application portfolio with business objectives.

B. Actions to reduce hardware procurement cost.

C. A listing of approved suppliers of IT contract resources.

D. A description of the technical architecture for the organization's network perimeter security.32

138. An IS auditor is evaluating the IT governance framework of an organization. Which of the following would be the **GREATEST** concern?

A. Senior management has limited involvement.

B. Return on investment (ROI) is not measured.

C. Chargeback of IT cost is not consistent.

D. Risk appetite is not quantified.

146. The MOST important point of consideration for an IS auditor while reviewing an enterprise's project portfolio is that it

A. does not exceed the existing IT budget.

B. is aligned with the investment strategy.

C. has been approved by the IT steering committee.

D. is aligned with the business plan.

148. An enterprise's risk appetite is **BEST** established by

A. the chief legal officer.

B. security management.

C. the audit committee.

D. the steering committee.

150. A financial enterprise has had difficulties establishing clear responsibilities between its IT strategy committee and its IT steering committee. Which of the following responsibilities would MOST likely be assigned to its IT steering committee?

A. Approving IT project plans and budgets

B. Aligning IT to business objectives

C. Advising on IT compliance risk

D. Promoting IT governance practices

B. IT-related Frameworks

20. Value delivery from IT to the business is MOST effectively achieved by:

A. Aligning the IT strategy with the enterprise strategy

B. Embedding accountability in the enterprise

C. Providing a positive return on investment

D. Establishing an enterprise wide risk management process

C. IT Standards, Policies, and Procedures

2. An IS auditor is verifying IT policies and finds that some of the policies have not been approved by management (as required by policy), but the employees strictly follow the policies. What should the IS auditor do FIRST?

A. Ignore the absence of management approval because employees follow the policies.

B. Recommend immediate management approval of the policies.

C. Emphasize the importance of approval to management.

D. Report the absence of documented approval.

6. Which of the following is the BEST reason to implement a policy that places conditions on secondary employment for IT employees?

A. To prevent the misuse of corporate resources

B. To prevent conflicts of interest

C. To prevent employee performance issues

D To prevent theft of IT assets

19. An IS auditor discovers several IT-based projects were implemented and not approved by the steering committee. What is the GREATEST concern for the IS auditor?

A. The IT department's projects will not be adequately funded.

B. IT projects are not following the system development life cycle process.

C. IT projects are not consistently formally approved.

D. The IT department may not be working toward a common goal.

22. An IS auditor is evaluating a newly developed IT policy for an organization. Which of the following factors does the IS auditor consider MOST important to facilitate compliance with the policy upon its implementation?

A. Existing IT mechanisms enabling compliance

B. Alignment of the policy to the business strategy

C. Current and future technology initiatives

D. Regulatory compliance objectives defined in the policy

25. An IS auditor is performing a review of an organization's governance model. Which of the following should be of MOST concern to the auditor?

A. The information security policy is not periodically reviewed by senior management.

B. A policy ensuring systems are patched in a timely manner does not exist.

C. The audit committee did not review the organization's mission statement.

D. An organizational policy related to information asset protection does not exist.

47. Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.

B. Specific user accountability cannot be established.

C. Unauthorized users may have access to modify data.

D. Audit recommendations may not be implemented.

50. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that :

A. This lack of knowledge may lead to unintentional disclosure of sensitive information.

B. Information security is not critical to all functions.

C. Is audit should provide security training to the employees.

D.The audit finding will cause management to provide continuous training to staff.

53. Which of the following should be included in an organization's information security policy?

A. A list of key IT resources to be secured

B. The basis for access control authorization

C. Identity of sensitive security assets

D. Relevant software security features

56. Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

57. A comprehensive and effective email policy should address the issues of email structure, policy enforcement, monitoring and:

A. recovery.

B. retention.

C. rebuilding.

D. reuse.

61. The initial step in establishing an information security program is the:

A. Development and implementation of an information security standards manual

B. Performance of a comprehensive security control review by the IS auditor

C. Adoption of a corporate information security policy statement

D. Purchase of security access control software

102. Which of the following does an IS auditor refer to first when conducting an IS audit?

A.Procedures implemented

B.Approved policy

C.Internal standards

D.Documented practice

114. Which of the following is normally a responsibility of the chief information security officer?

A. Periodically reviewing and evaluating the security policy

B. Executing user application and software testing and evaluation

C. Granting and revoking user access to IT resources

D. Approving access to data and applications

119. The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

A. Alignment of the IT activities with IS audit recommendations

B. Enforcement of the management of security risk

C. Implementation of the chief information security officer's recommendations

D. Reduction of the cost for IT security

131. The MOST important element for the effective design of an information security policy is the:

A. threat landscape.

B. prior security incidents.

C. emerging technologies.

D. enterprise risk appetite.

D. Organizational Structure

9. When auditing the IT governance framework and IT risk management practices existing within an organization, the IS auditor identified some undefined responsibilities regarding IT management and governance roles. Which of the following recommendations is the MOST appropriate?

A. Review the strategic alignment of IT with the business.

B. Implement accountability rules within the organization.

C. Ensure that independent IS audits are conducted periodically.

D. Create a chief risk officer role in the organization.

15. An IS auditor reviews an organizational chart PRIMARILY for:

A. Understanding of the complexity of the organizational structure.

B. Investigating various communication channels.

C. Understanding the responsibilities and authority of individuals.

D. Investigating the network connected to different employees.

24. Which of the following is a function of an IT steering committee?

A. Monitoring vendor-controlled change control and testing

B. Ensuring a separation of duties within the information's processing environment

C. Approving and monitoring the status of IT plans and budgets

D. Liaising between the IT department and end users

30. From a control perspective, the key element in job descriptions is that they:

A. Provide instructions on how to do the job and define authority.

B. Are current, documented and readily available to the employee.

C. Communicate management's specific job performance expectations.

D. Establish responsibility and accountability for the employee's actions.

46. An IS auditor of a large organization is reviewing the roles and responsibilities of the IT function and finds some individuals serving multiple roles. Which one of the following combinations of roles should be of GREATEST concern for the IS auditor?

A. Network administrators are responsible for quality assurance.

B. System administrators are application programmers.

C. End users are security administrators for critical applications.

D. Systems analysts are database administrators.

59. Which of the following choices is the PRIMARY benefit of requiring a steering committee to oversee IT investment?

A. To conduct a feasibility study to demonstrate IT value

B. To ensure that investments are made according to business requirements

C. To ensure that proper security controls are enforced

D. To ensure that a standard development methodology is implemented

108. The MAIN objective of implementing corporate governance is to:

A. provide strategic direction.

B.control business operations.

C.align IT with business.

D.implement good practices.

117. When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures

B. Defining a security policy

C. Specifying an access control methodology

D. Defining roles and responsibilities

123. An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

A. User acceptance testing occurs for all reports before release into production

B. Organizational data governance practices are put in place

C. Standard software tools are used for report development

D. Management signs off on requirements for new reports

E. Enterprise Architecture

11. An IS auditor found that the enterprise architecture (EA) recently adopted by an organization has an adequate current-state representation. However, the organization has started a separate project to develop a future-state representation. The IS auditor should:

A. Recommend that this separate project be completed as soon as possible.

B. Report this issue as a finding in the audit report.

C. Recommend the adoption of the Zachmann framework.

D. Rescope the audit to include the separate project as part of the current audit.

13. The PRIMARY benefit of an enterprise architecture initiative is to:

A. Enable the organization to invest in the most appropriate technology.

B. Ensure security controls are implemented on critical platforms.

C. Allow development teams to be more responsive to business requirements.

D. Provide business units with greater autonomy to select it solutions that fit their needs.

33. A business unit has selected a new accounting application and did not consult with IT early in the selection process. The PRIMARY risk is that:

A. The security controls of the application may not meet requirements.

B. The application may not meet the requirements of the business users.

C. The application technology may be inconsistent with the enterprise architecture.

D. The application may create unanticipated support issues for IT.

halo

66. A benefit of open system architecture is that it:

A. Facilitates interoperability within different systems.

B. Facilitates the integration of proprietary components.

C. Will be a basis for volume discounts from equipment vendors.

D.Allows for the achievement of more economies of scale for equipment.

136. Which of the following is of **MOST** interest to an IS auditor reviewing an organization's risk strategy?

A. All risk is mitigated effectively

B. Residual risk is zero after control implementation

C. All likely risk is identified and ranked.

D. The organization uses an established risk framework

F. Enterprise Risk Management

1. Organizations requiring employees to take a mandatory vacation each year PRIMARILY want to ensure:

A. adequate cross-training exists between functions.

B. an effective internal control environment is in place by increasing morale.

C. potential irregularities in processing are identified by a temporary replacement.

D. the risk of processing errors is reduced.

4. In a review of the human resources policies and procedures within an organization, an IS auditor is MOST concerned with the absence of a:

A. requirement for periodic job rotations.

B. process for formalized exit interviews.

C. termination checklist.

D. requirement for new employees to sign a nondisclosure agreement.

7. An IS auditor has been assigned to review an organization's information security policy. Which of the following issues represents the HIGHEST potential risk?

A. The policy has not been updated in more than one year.

B. The policy includes no revision history.

C. The policy is approved by the security administrator.

D. The company does not have an information security policy committee.

8. When performing a review of a business process reengineering (BPR) effort, which of the following is of PRIMARY concern?

A. Controls are eliminated as part of the streamlining BPR effort.

B. Resources are not adequate to support the BPR process.

C. The audit department does not have a consulting role in the BPR effort.

D. The BPR effort includes employees with limited knowledge of the process area.

12. An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

A. Controls in place.

B. Effectiveness of the controls.

C. Mechanism for monitoring the risk.

D. Threats/vulnerabilities affecting the assets.

14. Which of the following situations is addressed by a software escrow agreement?

A. The system administrator requires access to software to recover from a disaster.

B. A user requests to have software reloaded onto a replacement hard drive.

C. The vendor of custom-written software goes out of business.

D. An IS auditor requires access to software code written by the organization.

16. Sharing risk is a key factor in which of the following methods of managing risk?

A. Transferring risk

B. Tolerating risk

C. Terminating risk

D. Treating risk

17. A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential impact, the team should:

A. Compute the amortization of the related assets.

B. Calculate a return on investment.

C. Apply a qualitative approach.

D. Spend the time needed to define the loss amount exactly.

28. Establishing the level of acceptable risk is the responsibility of:

A. Quality assurance management.

B. Senior business management.

C. The chief information officer.

D. The chief security officer.

92. To address the risk of operations staff failing to perform daily backups, management requires the system administrator signs off on daily backups. This is an example of a risk:

A. Avoidance.

B. Transfer.

C. Mitigation.

D. Acceptance.

93. Poor password choices and unencrypted data transmission over unprotected communication lines are example from:

A. vulnerability.

B. threats.

C. probability.

D. impact.

98. The PRIMARY control objectives of mandatory vacation or job rotation are to:

A. allows cross-training for development.

B. helps maintain employee morale.

C. detect inappropriate employee actions or

D. illegal. provide competitive employee benefits.

100. A small organization has only one database administrator (DBA) and one system administrator. DBAs has root access to the UNIX server, which hosts the database application. How the separation of duties should be enforced in this scenario?

A.Hire a second DBA and divide the duties between the two individuals.

B.Remove DBA root access on all UNIX servers.

C.Make sure all DBA actions are logged and all logs are backed up to tape.

D.Make sure the database logs are forwarded to a UNIX server where the DBA does not have root access.

101. Which of the following user profiles does an IS auditor MOST concern about when conducting audit of electronic funds transfer systems?

A. Three users with the ability to capture and verify their own messages

B.Five users with the ability to capture and send their own messages

C.Five users with the ability to verify other users and send their own messages

D.Three users with the ability to capture and verify other users' messages and send their own messages

105. The IS auditor is reviewing the IT security risk management program. Security risk measures should:

A. address all network risks.

B.tracked over time based on the IT strategic plan.

C.consider the entire IT environment.

D.resulting in the identification of vulnerability tolerances.

109. Which of the following should be considered first when implementing a risk management program?

A.Understanding of the organization's threats, vulnerabilities and risk profile

B.Understanding of risk exposure and potential consequences of compromise

C.Determining risk management priorities based on potential impacts

D.Adequate risk mitigation strategies to keep risk consequences at acceptable levels

.

120. An organization has a well-established risk management process. Which of the following risk management practices would MOST likely expose the organization to the greatest amount of compliance risk?

A. Risk reduction

B. Risk transfer

C. Risk avoidance

D. Risk mitigation

121. An employee who has access to highly confidential information resigned. Upon departure, which of the following should be done FIRST?

A. Conduct an exit interview with the employee.

B. Ensure succession plans are in place.

C. Revoke the employee’s access to all systems.

D. Review the employee’s job history.

124. Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment

B. Information systems audit

C. Investment portfolio analysis

D. Business risk assessment

127. During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described types of IT risk. What is the MOST appropriate recommendation in this situation?

A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
B. Use common industry standard aids to divide the existing risk documentation into several individual types of risk which will be easier to handle.
C. No recommendation is necessary because the current approach is appropriate for a medium-sized organization.
D. Establish regular IT risk management meetings to identify and assess risk and create a mitigation plan as input to the organization's risk management.

128. Overall quantitative business risk for a particular threat can be expressed as:

A. A product of the likelihood and magnitude of the impact if a threat successfully exploits a vulnerability.
B. The magnitude of the impact if a threat source successfully exploits the vulnerability.
C. The likelihood of a given threat source exploiting a given vulnerability.
D. The collective judgment of the risk assessment team.

132. As result of profitability pressure, senior management of an enterprise decided to keep investments in information security at an inadequate level, which of the following is the **BEST** recommendation of an IS auditor?

A. Use cloud providers for low-risk operations.
B. Revise compliance enforcement processes.
C. Request that senior management accepts the risk.
D. Postpone low-priority security procedures.

G. Maturity Models

54. Which of the following is the initial step in creating a firewall policy?

A. A cost-benefit analysis of methods for securing the applications

B. Identification of network applications to be externally accessed

C. Identification of vulnerabilities associated with network applications to be externally accessed

D. Creation of an application traffic matrix showing protection methods

58. An organization is considering making a major investment to upgrade technology. Which of the following choices is the MOST important to consider?

A. A cost analysis

B. The security risk of the current technology

C. Compatibility with existing systems

D. A risk analysis

151. Which of the following is the BEST enabler for strategic alignment between business and IT?

A. A maturity model

B. Goals and metrics

C. Control objectives

D. A responsible, accountable, consulted and informed (RACI) chart

lo dh selesai??

lo ajak on

H. Laws, Regulations and Industry Standards Affecting the Organization

51. Which of the following is responsible for the approval of an information security policy?

A. IT department

B. Security committee

C. Security administrator

D. Board of directors

97. For a healthcare organization, which of the following reasons MOST likely indicates that Patient benefits data warehouse should remain in-house and not outsourced to overseas operations?

A. There are regulations regarding data privacy.

B.The cost of training member service representatives will be much higher.

C.It is more difficult to monitor remote databases.

D.Time zone differences can hinder customer service.

125. Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. Claims to meet or exceed industry security standards.

B. Agrees to be subject to external security reviews.

C. Has a good market reputation for service and experience.

D. Complies with security policies of the organization.

141. Which of the following is the BEST way to ensure that organizational security policies comply with data security regulatory requirements?

A. Inclusion of a blanket legal statement in each policy

B. Periodic review by subject matter experts

C. Annual sign - off by senior management on organizational policies

D. Policy alignment to the most restrictive regulations

I. IT Resource Management

31. Which of the following BEST provides assurance of the integrity of new staff?

A. Background screening

B. References

C. Bonding

D. Qualifications listed on a resume

32.When an employee is terminated from service, the MOST important action is to:

A. hand over all of the employee's files to another designated employee.

B. complete a backup of the employee's work.

C. notify other employees of the termination.

D. disable the employee's logical access.

34. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. Ensure that the employee maintains a good quality of life, which will lead to greater productivity.
B. Reduce the opportunity for an employee to commit an improper or illegal act.
C. Provide proper cross-training for another employee.
D. Eliminate the potential disruption caused when an employee takes vacation one day at a time.

35.A local area network (LAN) administrator normally is restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

41. Which of the following does an IS auditor consider the MOST relevant to short-term planning for an IT department?

A. Allocating resources
B. Adapting to changing technologies
C. Conducting control self-assessments
D. Evaluating hardware needs

48. An IS audit department is planning to minimize the risk of short-term employees. Activities contributing to this objective are documented procedures, knowledge sharing, cross-training and:

A. Succession planning.
B. Staff job evaluation.
C. Responsibilities definitions.
D. Employee award programs.

140. An IS auditor is reviewing a contract management process to determine the financial viability of a software vendor for a critical business application. An IS auditor should determine whether the vendor being considered

A. can deliver on the immediate contract.

B. is of similar financial standing as the organization.

C. has significant financial obligations that can impose liability to the organization.

D. can support the organization in the long term.

J. IT Service Provider Acquisition and Management

37.During an audit, the IS auditor discovers that the human resources (HR) department uses a cloud-based application to manage employee records. The HR department engaged in a contract outside of the normal vendor management process and manages the application on its own. Which of the following is of GREATEST concern?

A. Maximum acceptable downtime metrics have not been defined in the contract.

B. The IT department does not manage the relationship with the cloud vendor.

C. The help desk call center is in a different country, with different privacy requirements.

D. Organization-defined security policies are not applied to the cloud application.

44. An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. A backup server is available to run ETCS operations with up-to-date data.

B. A backup server is loaded with all relevant software and data.

C. The systems staff of the organization is trained to handle any event.

D. Source code of the ETCS application is placed in escrow.

55. Which of the following is an implementation risk within the process of decision support systems?

A. Management control

B. Semistructured dimensions

C. Inability to specify purpose and usage patterns

D. Changes in decision processes

62. Which of the following is the MOST important function to be performed by IT management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider

B. Participating in systems design with the provider

C. Renegotiating the provider's fees

D. Monitoring the outsourcing provider's performance

63. An organization purchased a third-party application and made significant modifications. While auditing the development process for this critical, customer-facing application, the IS auditor noted that the vendor has been in business for only one year. Which of the following helps to mitigate the risk relating to continued application support?

A. A viability study on the vendor

B. A software escrow agreement

C. Financial evaluation of the vendor

D.A contractual agreement for future enhancements

64. An IS auditor reviewing an outsourcing contract of IT facilities expects it to define the:

A. Hardware configuration.

B. Access control software.

C. Ownership of intellectual property.

D.Application development methodology.

65. While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Because the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

A. Requirement for securely protecting of information can be compromised.

B. Contract may be terminated because prior permission from the outsourcer was not obtained.

C. Other service provider to whom work has been outsourced is not subject to audit.

D.Outsourcer will approach the other service provider directly for furtherwork.

91. Which of the following is the BEST reference for an IS auditor to determine a vendor's capabilities in meet service level agreement requirements for critical IT security services?

A.Compliance with master contracts

B.Agreed key performance indicators

C.Business continuity test results

D.Independent audit report results

94. IS auditors are tasked with reviewing IT structures and activities that have recently been outsourced to various providers. Which of the following should the IS auditor determine first?

A.Audit clauses exist in all contracts.

B.Each contract's service level agreement is evidenced by key performance indicators in accordance.

C. Contract guarantees from the provider support the organization's business needs.

D.Upon termination of the contract, support is guaranteed by each outsourcer for the new outsourcer.

96. Regarding outsourcing of IT services, which of the following conditions should be of concern BIGGEST for IS auditors?

A.Core activities that provide distinct benefits to the organization have been outsourced.

B.Periodic renegotiation is not specified in the outsourcing contract.

C.Outsourcing contracts fail to cover every action required by the business.

D.Similar activities are outsourced to more than one vendor.

103. A company selects a vendor to develop and implement a new software system. For ensure that a company's investment in software is protected, which of the following security clauses is MOST important to include in a master services agreement?

A.Limitation of liability

B.Service level requirements

C.Software shelter

D. Control version

107. Which of the following is MOST important for an IS auditor to consider when reviewing agreements service levels with external IT service providers?

A.Terms of payment

B.Uptime guarantee

C.Indemnification clause

D. Resolution default

122. An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement between the organization and vendor should be the provisions for:

A. documentation of staff background checks.

B. independent audit reports or full audit access.

C. reporting the year-to-year incremental cost reductions.

D. reporting staff turnover, development or training

126. After the merger of two organizations, multiple self-developed legacy applications from both organizations are to be replaced by a new common platform. Which of the following is the GREATEST risk?

A. Project management and progress reporting is combined in a project management office that is driven by external consultants.

B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.

C. The resources of each of the organizations are incfficiently allocated while they are being familiarized with the other organization's legacy systems.

D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

129. While conducting an IS audit of a service provider for a government program involving confidential information, an IS auditor noted that the service provider delegated a part of the IS work to another subcontractor. Which of the following provides the MOST assurance that the requirements for protecting confidentiality of information are met?

A. Monthly committee meetings include the subcontractor's IS manager.

B. Management reviews weekly reports from the subcontractor.

C. Permission is obtained from the government agent regarding the contract.

D. Periodic independent audit of the work delegated to the subcontractor.

130. During an audit, which of the following situations are MOST concerning for an organization that significantly outsources IS processing to a private network?

A. The contract does not contain a right-to-audit clause for the third party.

B. The contract was not reviewed by an information security subject matter expert prior to signing.
C. The IS outsourcing guidelines are not approved by the board of directors.
D. There is a lack of well-defined IS performance evaluation procedures.

K. IT Performance Monitoring and Reporting

36. A decision support system is used to help high-level management:

A. Solve highly structured problems.
B. Combine the use of decision models with predetermined criteria.
C. Make decisions based on data analysis and interactive models.
D. Support only structured decision-making tasks.

38. Before implementing an IT balanced scorecard, an organization must:

A. Deliver effective and efficient services.
B. Define key performance indicators.
C. Provide business value to IT projects.
D. Control IT expenses.

49. The rate of change in technology increases the importance of :

A. Outsourcing the IT function.
B. Implementing and enforcing sound processes.
C. Hiring qualified personnel.
D. Meeting user requirement.

52. While reviewing the IT governance processes of an organization, an IS auditor discovers the firm has recently implemented an IT balanced scorecard (BSC). The implementation is complete; however, the IS auditor notices that performance indicators are not objectively measurable. What is the PRIMARY risk presented by this situation?

A. Key performance indicators are not reported to management and management cannot determine the effectiveness of the BSC.
B. IT projects could suffer from cost overruns.
C. Misleading indications of IT performance may be presented to management.
D. IT service level agreements may not be accurate.

118. Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

A. Define a balanced scorecard for measuring performance.

B. Consider user satisfaction in the key performance indicators.

C. Select projects according to business benefits and risk.

D. Modify the yearly process of defining the project portfolio.

152. An IT steering committee should:

A. include a mix of members from different departments and staff levels.

B. ensure that IS security policies and procedures have been executed properly.

C. maintain minutes of its meetings and keep the board of directors informed.

D. be briefed about new trends and products at each meeting by a vendor.

L. Quality Assurance and Quality Management of IT

10. An IS auditor is performing a review of the software quality management process in an organization. The FIRST step should be to:

A. Verify how the organization complies the standards.

B. Identify and report the existing controls.

C. Review the metrics for quality evaluation.

D. Request all standards adopted by the organization.

18. While reviewing a quality management system, the IS auditor should PRIMARILY focus on collecting evidence to show that:

A. Quality management systems comply with good practices.

B. Continuous improvement targets are being monitored.

C. Standard operating procedures of it are updated annually.

D. Key performance indicators are defined.

21. During a feasibility study regarding outsourcing IT processing, the relevance for the IS auditor of reviewing the vendor's business continuity plan is to:

A. Evaluate the adequacy of the service levels that the vendor can provide in a contingency.

B. Evaluate the financial stability of the service bureau and its ability to fulfill the contract.

C. Review the experience of the vendor's staff.

D. Test the business continuity plan.