ISACA

SAMPLE EXAM DISCUSSION SLIDES

QUESTION 1

Which of the following choices would provide the **BEST** measure of the effectiveness of the security strategy?

A. Minimizing risk across the enterprise

B. Countermeasures existing for all known threats

C. Losses consistent with annual loss expectations

D. The extent to which control objectives are met

QUESTION 2

Which of the following situations would MOST inhibit the effective implementation of security governance?

A. The complexity of technology

B. Budgetary constraints

C. Conflicting business priorities

D. Lack of high-level sponsorship

QUESTION 3

Management requests that an information security manager determine which regulations regarding disclosure, reporting and privacy are the most important for the organization to address. The recommendations for addressing these legal and regulatory requirements will be **MOST** useful if based on which of the following choices?

A. The extent of enforcement actions

B. The probability and consequences

C. The sanctions for noncompliance

D. The amount of personal liability

QUESTION 4

The classification level of an asset must be **PRIMARILY** based on which of the following choices?

A. Criticality and sensitivity

B. Likelihood and impact

C. Valuation and replacement cost

D. Threat vector and exposure

ISACA®

QUESTION 5

If a security incident is not the result of the failure of a control, then it is **MOST** likely the result of which of the following choices?

A. An incomplete risk analysis

B. The absence of a control

C. A zero-day attack

D. A user error

QUESTION 6

When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the **MOST** important topics to include in the contract from a security standpoint?

A. Compliance with international security standards

B. Use of a two-factor authentication system

C. Existence of an alternate hot site in case of business disruption

D. Compliance with the organization's information security requirements

QUESTION 7

Which of the following would be **MOST** effective in successfully implementing restrictive password policies?

A. Regular password audits

B. Single sign-on system

C. Security awareness program

D. Penalties for noncompliance

QUESTION 8

Assuming that the value of information assets is known, which of the following gives the information security manager the **MOST** objective basis for determining that the information security program is delivering value?

A. Number of controls

B. Cost of achieving control objectives

C. Effectiveness of controls

D. Test results of controls

QUESTION 9

A risk management process is **MOST** effective in achieving organizational objectives if:

A. asset owners perform risk assessments.

B. the risk register is updated regularly.

C. the process is overseen by a steering committee.

D. risk activities are embedded in business processes.

QUESTION 10

A business impact analysis is the **BEST** tool for determining:

A. total cost of ownership.

B. priority of restoration.

C. annual loss expectancy.

D. residual risk.

QUESTION 11

An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees flood the IT help desk with complaints of being unable to perform business functions on Internet sites. This is an example of:

A. conflicting security controls with organizational needs.

B. strong protection of information resources.

C. implementing appropriate controls to reduce risk.

D. proving information security's protective abilities.

QUESTION 12

Which of the following should be performed **FIRST** in the aftermath of a denial-of-service (DoS) attack?

A. Restore servers from backup media stored offsite.

B. Conduct an assessment to determine system status.

C. Perform an impact analysis of the outage.

D. Isolate the screened subnet.

QUESTION 13

Which of the following metrics would be the **MOST** useful in measuring how well information security is monitoring violation logs?

A. Penetration attempts investigated

B. Violation log reports produced

C. Violation log entries

D. Frequency of corrective actions taken

QUESTION 14

Who should be responsible for enforcing access rights to application data?

A. Data owners

B. Business process owners

C. The security steering committee

D. Security administrators

QUESTION 15

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following items would be of **MOST** value?

A. Examples of genuine incidents at similar organizations

B. Statement of generally accepted good practices

C. Associating realistic threats to corporate objectives

D. Analysis of current technological exposures

QUESTION 16

Which of the following choices would be the **MOST** significant key risk indicator?

A. A deviation in employee turnover

B. The number of packets dropped by the firewall

C. The number of viruses detected

D. The reporting relationship of IT

QUESTION 17

Why should the analysis of risk include consideration of potential impact?

A. Potential impact is a central element of risk.

B. Potential impact is related to asset value.

C. Potential impact affects the extent of mitigation.

D. Potential impact helps determine the exposure.

QUESTION 18

A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the **GREATEST** weakness in recovery capability?

A. Exclusive use of the hot site is limited to six weeks.

B. The hot site may have to be shared with other customers.

C. The time of declaration determines site access priority.

D. The provider services all major companies in the area.

QUESTION 19

Which of the following would be the **BEST** indicator of effective information security governance within an organization?

A. The steering committee approves security projects.

B. Security policy training is provided to all managers.

C. Security training is available to all employees on the intranet.

D. IT personnel are trained in testing and applying required patches.

QUESTION 20

When developing an information security program, what is the **MOST** useful source of information for determining available human resources?

A. Proficiency test

B. Job descriptions

C. Organization chart

D. Skills inventory

QUESTION 21

Quantitative risk analysis is **MOST** appropriate when assessment results:

A. include customer perceptions.

B. contain percentage estimates.

C. lack specific details.

D. contain subjective information.

ISACA

QUESTION 22

During the security review of organizational servers it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. What is the **FIRST** step the security manager should perform?

A. Copy sample files as evidence.

B. Remove access privileges to the folder containing the data.

C. Report this situation to the data owner.

D. Train the HR team on properly controlling file permissions.

QUESTION 23

What is the **MOST** important contractual element when contracting with an outsourcer to provide security administration?

A. The right-to-terminate clause

B. Limitations of liability

C. The service level agreement

D. The financial penalties clause

QUESTION 24

There is a delay between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out **FIRST** to mitigate the risk during this time period?

A. Identify the vulnerable systems and apply compensating controls.

B. Minimize the use of vulnerable systems.

C. Communicate the vulnerability to system users.

D. Update the signatures database of the intrusion detection system.

QUESTION 25

Which of the following should be included in a good privacy statement?

A. A notification of liability on accuracy of information

B. A notification that information will be encrypted

C. A statement of what the company will do with information it collects

D. A description of the information classification process

QUESTION 26

Which of the following techniques **MOST** clearly indicates whether specific risk-reduction controls should be implemented?

A. Cost-benefit analysis

B. Penetration testing

C. Frequent risk assessment programs

D. Annual loss expectancy calculation

QUESTION 27

How does knowledge of risk appetite help to increase security control effectiveness?

A. It shows senior management that you understand their needs.

B. It provides a basis for redistributing resources to mitigate risk above the risk appetite.

C. It requires continuous monitoring because the entire risk environment is constantly changing.

D. It facilitates communication with management about the importance of security.

QUESTION 28

Which of the following is one of the **BEST** metrics an information security manager can employ to effectively evaluate the results of a security program?

A. Number of controls implemented

B. Percent of control objectives accomplished

C. Percent of compliance with the security policy

D. Reduction in the number of reported security incidents

QUESTION 29

Which of the following is the **MOST** appropriate use of gap analysis?

A. Evaluating a business impact analysis

B. Developing a business balanced scorecard

C. Demonstrating the relationship between controls

D. Measuring current state versus desired future state

QUESTION 30

Which of the following actions should be taken when an online trading company discovers a network attack in progress?

A. Shut off all network access points

B. Dump all event logs to removable media

C. Isolate the affected network segment

D. Enable trace logging on all events

QUESTION 31

To achieve effective strategic alignment of information security initiatives, it is important that:

A. steering committee leadership rotates among members.

B. major organizational units provide input and reach a consensus.

C. the business strategy is updated periodically.

D. procedures and standards are approved by all departmental heads.

QUESTION 32

An information security manager determines that management of risk is inconsistent across a mature organization, creating a weak link in overall protection. The **MOST** appropriate initial response for the information security manager is to:

A. escalate to the steering committee.

B. review compliance with standards.

C. write more stringent policies.

D. increase enforcement.

QUESTION 33

The **PRIMARY** concern of an information security manager documenting a formal data retention policy is:

A. generally accepted industry good practices.

B. business requirements.

C. legislative and regulatory requirements.

D. storage availability.

QUESTION 34

Control objectives are **MOST** closely aligned with:

A. risk tolerance.

B. criticality.

C. risk appetite.

D. sensitivity.

QUESTION 35

An information security manager is advised by contacts in law enforcement that there is evidence that the company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The **FIRST** step that the security manager should take is to:

A. perform a comprehensive assessment of the organization's exposure to the hackers' techniques.

B. initiate awareness training to counter social engineering.

C. immediately advise senior management of the elevated risk.

D. increase monitoring activities to provide early detection of intrusion.

QUESTION 36

Which of the following is the **FIRST** step after the intrusion detection system sends out an alert about a possible attack?

A. Assess the type and severity of the attack.

B. Determine whether it is an actual incident.

C. Contain the damage to minimize the risk.

D. Minimize the disruption of computer resources.

QUESTION 37

Which of the following choices should be assessed after the likelihood of a loss event has been determined?

A. The magnitude of impact

B. Risk tolerance

C. The replacement cost of assets

D. The book value of assets

ISACA®

QUESTION 38

The **MOST** timely and effective approach to detecting nontechnical security violations in an organization is:

A. the development of organizationwide communication channels.

B. periodic third-party auditing of incident reporting logs.

C. an automated policy compliance monitoring system.

D. deployment of suggestion boxes throughout the organization.

QUESTION 39

An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage cross-training. Which type of authorization policy would **BEST** address this practice?

A. Multilevel

B. Role-based

C. Discretionary

D. Mandatory

QUESTION 40

At what point in the risk management process is residual risk determined?

A. When evaluating the results of the application of new or existing controls or countermeasures

B. When identifying and classifying information resources or assets that need protection

C. When assessing threats and the consequences of a compromise

D. After the elements of risk have been established, when combining them to form an overall view of risk

QUESTION 41

Which of the following should be reviewed to ensure that security controls are effective?

A. Risk assessment policies

B. Return on security investment

C. Security metrics

D. User access rights

ISACA

QUESTION 42

A security operations center detected an attempted structured query language injection, but could not determine if it was successful. Which of the following resources should the information security manager approach to assess the possible impact?

A. Application support team

B. Business process owner

C. Network management team

D. System administrator

QUESTION 43

Which person or group should have final approval of an organization’s information technology (IT) security policies?

A. Business unit managers

B. Chief information security officer

C. Senior management

D. Chief information officer

QUESTION 44

Which of the following is the **BEST** metric for evaluating the effectiveness of security awareness training?

A. The number of password resets

B. The number of reported incidents

C. The number of incidents resolved

D. The number of access rule violations

QUESTION 45

Which of the following steps should be **FIRST** in developing an information security plan?

A. Perform a technical vulnerabilities assessment.

B. Analyze the current business strategy.

C. Perform a business impact analysis.

D. Assess the current levels of security awareness.

QUESTION 46

The information security policies of an organization require that all confidential information must be encrypted while communicating to external entities. A regulatory agency insisted that a compliance report must be sent without encryption. The information security manager should:

A. extend the information security awareness program to include employees of the regulatory authority.

B. send the report without encryption on the authority of the regulatory agency.

C. initiate an exception process for sending the report without encryption.

D. refuse to send the report without encryption.

QUESTION 47

The fact that an organization may suffer a significant disruption as the result of a distributed denial-of service (DDoS) attack is considered:

A. an intrinsic risk.

B. a systemic risk.

C. a residual risk.

D. an operational risk.

QUESTION 48

The effectiveness of managing business risk is **BEST** measured by the number of:

A. significant IT-related incidents that were not identified during risk assessment.

B. security assessments compliant with organizational standards and guidelines.

C. vulnerabilities identified by risk assessment and not properly mitigated.

D. security incidents causing significant financial loss or business disruption.

QUESTION 49

Which of the following is the **MOST** important consideration for an organization interacting with the media during a disaster?

A. Communicating specially drafted messages by an authorized person

B. Refusing to comment until recovery

C. Referring the media to the authorities

D. Reporting the losses and recovery strategy to the media

QUESTION 50

Which of the following is the **BEST** approach to dealing with inadequate funding of the security program?

A. Eliminate low-priority security services.

B. Require management to accept the increased risk.

C. Prioritize risk mitigation and educate management.

D. Reduce monitoring and compliance enforcement activities.

QUESTION 51

Which of the following should be determined **FIRST** when establishing a business continuity program?

A. Cost to rebuild information processing facilities

B. Incremental daily cost of the unavailability of systems

C. Location and cost of offsite recovery facilities

D. Composition and mission of individual recovery teams

QUESTION 52

Reducing exposure of a critical asset is an effective mitigation measure because it reduces:

A. the impact of a compromise.

B. the likelihood of being exploited.

C. the vulnerability of the asset.

D. the time needed for recovery.

QUESTION 53

Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awareness.

B. It is easier to manage and control.

C. It is more responsive to business unit needs.

D. It provides a faster turnaround for security requests.

QUESTION 54

After a service interruption of a critical system, the incident response team finds that it needs to activate the warm recovery site. Discovering that throughput is only half of the primary site, the team nevertheless notifies management that it has restored the critical system. This is **MOST** likely because it has achieved the:

A. recovery point objective.

B. recovery time objective.

C. service delivery objective.

D. maximum tolerable outage.

QUESTION 55

The enactment of policies and procedures for preventing hacker intrusions is an example of an activity that belongs to:

A. risk management.

B. compliance.

C. IT management.

D. governance.

QUESTION 56

A new email virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed **FIRST** in response to this threat?

A. Quarantine all picture files stored on file servers.

B. Block all emails containing picture file attachments.

C. Quarantine all mail servers connected to the Internet.

D. Block incoming Internet mail but permit outgoing mail.

QUESTION 57

The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the **MOST** critical security consideration?

A. Laws and regulations of the country of origin may not be enforceable in the foreign country.

B. A security breach notification might get delayed due to the time difference.

C. Additional network intrusion detection sensors should be installed, resulting in an additional cost.

D. The company could lose physical control over the server and be unable to monitor the physical security posture of the servers.

QUESTION 58

Senior management commitment and support for information security can **BEST** be obtained through presentations that:

A. use illustrative examples of successful attacks.

B. explain the technical risk to the organization.

C. evaluate the organization against good security practices.

D. tie security risk to key business objectives.

QUESTION 59

Which of the following recommendations is the **BEST** one to promote a positive information security governance culture within an organization?

A. Strong oversight by the audit committee

B. Organizational governance transparency

C. Collaboration across business lines

D. Positive governance ratings by stock analysts

QUESTION 60

What is the **PRIMARY** purpose of installing an intrusion detection system?

A. To identify weaknesses in network security

B. To identify patterns of suspicious access

C. To identify how an attack was launched on the network

D. To identify potential attacks on the internal network

QUESTION 61

After obtaining commitment from senior management, which of the following should be completed **NEXT** when establishing an information security program?

A. Define security metrics.

B. Conduct a risk assessment.

C. Perform a gap analysis.

D. Procure security tools.

QUESTION 62

Information security governance is **PRIMARILY** driven by:

A. technology constraints.

B. regulatory requirements.

C. litigation potential.

D. business strategy.

QUESTION 63

Assuming all options are technically feasible, which of the following would be the **MOST** effective approach for the information security manager to address excessive exposure of a critical customer-facing server?

A. Develop an incident response plan

B. Reduce the attack surface

C. Initiate compartmentalization

D. Implement compensating controls

QUESTION 64

The **BEST** approach to developing an information security program is to use a:

A. process.

B. framework.

C. model.

D. guideline.

QUESTION 65

Which of the following is **MOST** important to the success of an information security program?

A. Security awareness training

B. Achievable goals and objectives

C. Senior management sponsorship

D. Adequate start-up budget and staffing

QUESTION 66

Which of the following activities **MUST** a financial-services organization do with regard to a web-based service that is gaining popularity among its customers?

A. Perform annual vulnerability mitigation.

B. Maintain third-party liability insurance.

C. Conduct periodic business impact analyses.

D. Architect a real-time failover capability.

QUESTION 67

Which of the following is **MOST** important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

A. Cost to build a redundant processing facility and location

B. Daily cost of losing critical systems and recovery time objectives

C. Infrastructure complexity and system sensitivity

D. Criticality results from the business impact analysis

QUESTION 68

What is the goal of risk aggregation?

A. To combine homogenous elements to reduce overall risk

B. To influence the organization’s risk acceptance methodologies

C. To group individual acceptable risk events for simplified risk reporting

D. To identify significant overall risk from a single threat vector

QUESTION 69

Which of the following internal or external influences on an organization is the **MOST** difficult to estimate?

A. Vulnerability posture

B. Compliance requirements

C. Outsourcing expenses

D. Threat landscape

QUESTION 70

The **FIRST** step to create an internal culture that embraces information security is to:

A. implement stronger controls.

B. conduct periodic awareness training.

C. actively monitor operations.

D. gain endorsement from executive management.

QUESTION 71

The **PRIMARY** purpose of involving third-party teams for carrying out postincident reviews of information security incidents is to:

A. enable independent and objective review of the root cause of the incidents.

B. obtain support for enhancing the expertise of the third-party teams.

C. identify lessons learned for further improving the information security management process.

D. obtain better buy-in for the information security program.

QUESTION 72

Which of the following situations presents the **GREATEST** information security risk for an organization with multiple, but small, domestic processing locations?

A. Systems operation guidelines are not enforced.

B. Change management procedures are poor.

C. Systems development is outsourced.

D. Systems capacity management is not performed.

QUESTION 73

In the process of deploying a new email system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the **MOST** appropriate method to ensure data confidentiality in a new email system implementation?

A. Encryption

B. Strong authentication

C. Digital signature

D. Hashing algorithm

QUESTION 74

An information security manager wants to implement a security information and event management (SIEM) system not funded in the current budget. Which of the following choices is **MOST** likely to persuade management of this need?

A. A comprehensive risk assessment

B. An enterprisewide impact assessment

C. A well-developed business case

D. Computing the net present value of future savings

QUESTION 75

Which of the following is the **MOST** cost-effective type of access control?

A. Centralized

B. Role-based

C. Decentralized

D. Discretionary

ISACA