vce trainer



CISM.469q

CISM

CISM

Certified Information Security Manager

Licensed to Berend Post berend.post@it-university.nl

Score: 800/1000

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Exam A (469 questions)

Question 1

A test plan to validate the security controls of a new system should be developed during which phase of the project?

- ☐ Testing
- ☐ Initiation
- ☐ Design
- ☐ Development

Question 2

A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

- ☐ rebuild the server from the last verified backup.
- ☐ place the web server in quarantine.
- ☐ shut down the server in an organized manner.
- ☐ rebuild the server with original media and relevant patches.

Question 3

Which of the following would BEST address the risk of data leakage?

- ☐ File backup procedures
- ☐ Database integrity checks
- ☐ Acceptable use policies
- ☐ Incident response procedures

Question 4

Information security managers should use risk assessment techniques to:

- ☐ justify selection of risk mitigation strategies.
- ☐ maximize the return on investment (ROD.
- ☐ provide documentation for auditors and regulators.
- ☐ quantify risks that would otherwise be subjective.

Licensed to Berend Post berend.post@it-university.nl

Question 5

Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

- ☐ Effective security eliminates risk to the business
- ☐ Adopt a recognized framework with metrics
- ☐ Security is a business product and not a process
- ☐ Security supports and protects the business

Question 6

Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

- ☐ Systems operation procedures are not enforced
- ☐ Change management procedures are poor
- ☐ Systems development is outsourced
- ☐ Systems capacity management is not performed

Question 7

Quantitative risk analysis is MOST appropriate when assessment data:

- ☐ include customer perceptions.
- ☐ contain percentage estimates.
- ☐ do not contain specific details.
- ☐ contain subjective information.

Question 8

Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

- ☐ Annual loss expectancy (ALE) of incidents
- ☐ Frequency of incidents
- ☐ Total cost of ownership (TCO)
- ☐ Approved budget for the project

Licensed to Berend Post berend.post@it-university.nl

Question 9

An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

- ☐ Security in storage and transmission of sensitive data
- ☐ Provider's level of compliance with industry standards
- ☐ Security technologies in place at the facility
- ☐ Results of the latest independent security review

Question 10

During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

- ☐ baseline security controls.
- ☐ cost-benefit analyses.
- ☐ benchmarking security metrics.
- ☐ security objectives.

Question 11

On which of the following should a firewall be placed?

- ☐ Web server
- ☐ Intrusion detection system (IDS) server
- ☐ Screened subnet
- ☐ Domain boundary

Question 12

To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

- ☐ set their accounts to expire in six months or less.
- ☐ avoid granting system administration roles.
- ☐ ensure they successfully pass background checks.
- ☐ ensure their access is approved by the data owner.

Question 13

A business impact analysis (BIA) is the BEST tool for calculating:

- ☐ total cost of ownership.
- ☐ priority of restoration.
- ☐ annualized loss expectancy (ALE).
- ☐ residual risk.

Licensed to Berend Post berend.post@it-university.nl

Question 14

Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

- ☐ An intrusion prevention system (IPS)
- ☐ An intrusion detection system (IDS)
- ☐ A host-based intrusion detection system (HIDS)
- ☐ A host-based firewall

Question 15

Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

- ☐ Programming
- ☐ Specification
- ☐ User testing
- ☐ Feasibility

Question 16

Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

- ☐ are compatible with the provider's own classification.
- ☐ are communicated to the provider.
- ☐ exceed those of the outsourcer.
- ☐ are stated in the contract.

Question 17

Which of the following defines the triggers within a business continuity plan (BCP)?

- ☐ Disaster recovery plan
- ☐ Needs of the organization
- ☐ Gap analysis
- ☐ Information security policy

Question 18

When performing an information risk analysis, an information security manager should FIRST:

- ☐ establish the ownership of assets.
- ☐ evaluate the risks to the assets.
- ☐ take an asset inventory.
- ☐ categorize the assets.

Licensed to Berend Post berend.post@it-university.nl

Question 19

Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

- ☐ Gap analysis
- ☐ Regression analysis
- ☐ Risk analysis
- ☐ Business impact analysis

Question 20

A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

- ☐ Access control policy
- ☐ Data classification policy
- ☐ Encryption standards
- ☐ Acceptable use policy

Question 21

Which of the following will BEST prevent an employee from using a USB drive to copy files from desktop computers?

- ☐ Restrict the available drive allocation on all PCs
- ☐ Disable universal serial bus (USB) ports on all desktop devices
- ☐ Conduct frequent awareness training with noncompliance penalties
- ☐ Establish strict access controls to sensitive information

Question 22

An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

- ☐ Inform senior management.
- ☐ Determine the extent of the compromise.
- ☐ Report the incident to the authorities.
- ☐ Communicate with the affected customers.

Licensed to Berend Post berend.post@it-university.nl

Question 23

In order to ensure separation of duties, which of the following activities is BEST performed by someone other than the system administrator?

- ☐ Deleting system logs
- ☐ Using system utilities
- ☐ Monitoring system utilization
- ☐ Defining system recovery procedures

Question 24

An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

- ☐ document and report the root cause of the incidents for senior management.
- ☐ identify security program gaps or systemic weaknesses that need correction.
- ☐ prepare properly vetted notifications regarding the incidents to external parties.
- ☐ identify who should be held accountable for the security incidents.

Question 25

A multinational organization wants to monitor outbound traffic for data leakage from the use of unapproved cloud services. Which of the following should be the information security manager's GREATEST consideration when implementing this control?

- ☐ Security of cloud services
- ☐ Data privacy regulations
- ☐ Resistance from business users
- ☐ Allocation of monitoring resources

Question 26

Which of the following would be MOST helpful when justifying the funding required for a compensating control?

- ☐ Threat assessment
- ☐ Business impact analysis
- ☐ Business case
- ☐ Risk analysis

Licensed to Berend Post berend.post@it-university.nl

Question 27

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

- ☐ Countermeasure cost-benefit analysis
- ☐ Penetration testing
- ☐ Frequent risk assessment programs
- ☐ Annual loss expectancy (ALE) calculation

Question 28

An e-commerce order fulfillment web server should generally be placed on which of the following?

- ☐ Internal network
- ☐ Demilitarized zone (DMZ)
- ☐ Database server
- ☐ Domain controller

Question 29

Detailed business continuity plans should be based PRIMARILY on:

- ☐ consideration of different alternatives.
- ☐ the solution that is least expensive.
- ☐ strategies that cover all applications.
- ☐ strategies validated by senior management.

Question 30

Which of the following presents the GREATEST challenge in calculating return on investment (ROI) in the security environment?

- ☐ Number of incidents cannot be predetermined
- ☐ Project cost overruns cannot be anticipated
- ☐ Cost of security tools is difficult to estimate
- ☐ Costs of security incidents cannot be estimated

Question 31

What is the FIRST action an information security manager should take when a company laptop is reported stolen?

- ☐ Evaluate the impact of the information loss
- ☐ Update the corporate laptop inventory
- ☐ Ensure compliance with reporting procedures
- ☐ Disable the user account immediately

Licensed to Berend Post berend.post@it-university.nl

Question 32

Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

- ☐ Request a list of the software to be used
- ☐ Provide clear directions to IT staff
- ☐ Monitor intrusion detection system (IDS) and firewall logs closely
- ☐ Establish clear rules of engagement

Question 33

What is the BEST way to ensure data protection upon termination of employment?

- ☐ Retrieve identification badge and card keys
- ☐ Retrieve all personal computer equipment
- ☐ Erase all of the employee's folders
- ☐ Ensure all logical access is removed

Question 34

When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

- ☐ calculating the residual risk.
- ☐ enforcing the security standard.
- ☐ redesigning the system change.
- ☐ implementing mitigating controls.

Question 35

Which of the following is MOST important in developing a security strategy?

- ☐ Creating a positive business security environment
- ☐ Understanding key business objectives
- ☐ Having a reporting line to senior management
- ☐ Allocating sufficient resources to information security

Licensed to Berend Post berend.post@it-university.nl

Question 36

Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

- ☐ policy.
- ☐ strategy.
- ☐ guideline
- ☐ baseline.

Question 37

The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

- ☐ Mitigating controls
- ☐ Visibility of impact
- ☐ Likelihood of occurrence
- ☐ Incident frequency

Question 38

An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

- ☐ Research best practices
- ☐ Meet with stakeholders
- ☐ Establish change control procedures
- ☐ Identify critical systems

Question 39

An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

- ☐ Restrict account access to read only
- ☐ Log all usage of this account
- ☐ Suspend the account and activate only when needed
- ☐ Require that a change request be submitted for each download

Licensed to Berend Post berend.post@it-university.nl

Question 40

Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

- ☐ Business continuity coordinator
- ☐ Chief operations officer (COO)
- ☐ Information security manager
- ☐ Internal audit

Question 41

What is the BEST defense against a Structured Query Language (SQL) injection attack?

- ☐ Regularly updated signature files
- ☐ A properly configured firewall
- ☐ An intrusion detection system
- ☐ Strict controls on input fields

Question 42

Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

- ☐ Signal strength
- ☐ Number of administrators
- ☐ Bandwidth
- ☐ Encryption strength

Question 43

The return on investment of information security can BEST be evaluated through which of the following?

- ☐ Support of business objectives
- ☐ Security metrics
- ☐ Security deliverables
- ☐ Process improvement models

Licensed to Berend Post berend.post@it-university.nl

Question 44

An information security manager is asked to provide evidence that the organization is fulfilling its legal obligation to protect personally identifiable information (PII).

Which of the following would be MOST helpful for this purpose?

- ☐ Metrics related to program effectiveness
- ☐ Written policies and standards
- ☐ Privacy awareness training
- ☐ Risk assessments of privacy-related applications

Question 45

An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

- ☐ Intrusion detection system
- ☐ SIEM tool
- ☐ Antivirus software
- ☐ File integrity monitoring software

Question 46

The PRIMARY objective of a risk management program is to:

- ☐ minimize inherent risk.
- ☐ eliminate business risk.
- ☐ implement effective controls.
- ☐ minimize residual risk.

Question 47

The security responsibility of data custodians in an organization will include:

- ☐ assuming overall protection of information assets.
- ☐ determining data classification levels.
- ☐ implementing security controls in products they install.
- ☐ ensuring security measures are consistent with policy.

Licensed to Berend Post berend.post@it-university.nl

Question 48

Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

- ☐ Historical cost of the asset
- ☐ Acceptable level of potential business impacts
- ☐ Cost versus benefit of additional mitigating controls
- ☐ Annualized loss expectancy (ALE)

Question 49

An organization plans to allow employees to use their own devices on the organization's network. Which of the following is the information security manager's BEST course of action?

- ☐ Implement automated software
- ☐ Assess associated risk
- ☐ Conduct awareness training
- ☐ Update the security policy

Question 50

Which of the following groups would be in the BEST position to perform a risk analysis for a business?

- ☐ External auditors
- ☐ A peer group within a similar business
- ☐ Process owners
- ☐ A specialized management consultant

Question 51

Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

- ☐ Tree diagrams
- ☐ Venn diagrams
- ☐ Heat charts
- ☐ Bar charts

Licensed to Berend Post berend.post@it-university.nl

Question 52

Which of the following function is the MOST critical when initiating the removal of system access for terminated employees?

- ☐ Human resources
- ☐ Legal
- ☐ Help desk
- ☐ Information security

Question 53

Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

- ☐ Utilize an intrusion detection system.
- ☐ Establish minimum security baselines.
- ☐ Implement vendor recommended settings.
- ☐ Perform periodic penetration testing.

Question 54

An organization has to comply with recently published industry regulatory requirements — compliance that potentially has high implementation costs. What should the information security manager do FIRST?

- ☐ Implement a security committee.
- ☐ Perform a gap analysis.
- ☐ Implement compensating controls.
- ☐ Demand immediate compliance.

Question 55

An information security manager has been asked to create a strategy to protect the organization's information from a variety of threat vectors. Which of the following should be done FIRST?

- ☐ Perform a threat modeling exercise
- ☐ Develop a risk profile
- ☐ Design risk management processes
- ☐ Select a governance framework

Licensed to Berend Post berend.post@it-university.nl

Question 56

One way to determine control effectiveness is by determining:

- ☐ whether it is preventive, detective or compensatory.
- ☐ the capability of providing notification of failure.
- ☐ the test results of intended objectives.
- ☐ the evaluation and analysis of reliability.

Question 57

An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

- ☐ corporate data privacy policy.
- ☐ data privacy policy where data are collected.
- ☐ data privacy policy of the headquarters' country.
- ☐ data privacy directive applicable globally.

Question 58

A business case for investment in an information security management infrastructure MUST include:

- ☐ evidence that the proposed infrastructure is certified.
- ☐ specifics on the security applications needed.
- ☐ data management methods currently in use.
- ☐ impact of noncompliance with applicable standards.

Question 59

Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

- ☐ Business impact analysis
- ☐ Organizational risk appetite
- ☐ Independent security audit
- ☐ Security risk assessment

Question 60

Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

- ☐ Strategic business plan
- ☐ Upcoming financial results
- ☐ Customer personal information
- ☐ Previous financial results

Licensed to Berend Post berend.post@it-university.nl

Question 61

Which of the following represents a PRIMARY area of interest when conducting a penetration test?

- ☐ Data mining
- ☐ Network mapping
- ☐ Intrusion Detection System (IDS)
- ☐ Customer data

Question 62

The BEST metric for evaluating the effectiveness of a firewall is the:

- ☐ number of attacks blocked.
- ☐ number of packets dropped.
- ☐ average throughput rate.
- ☐ number of firewall rules.

Question 63

Which of the following events generally has the highest information security impact?

- ☐ Opening a new office
- ☐ Merging with another organization
- ☐ Relocating the data center
- ☐ Rewiring the network

Question 64

There is a time lag 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?

- ☐ Identify the vulnerable systems and apply compensating controls
- ☐ Minimize the use of vulnerable systems
- ☐ Communicate the vulnerability to system users
- ☐ Update the signatures database of the intrusion detection system (IDS)

Question 65

The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

- ☐ hourly billing rate charged by the carrier.
- ☐ value of the data transmitted over the network.
- ☐ aggregate compensation of all affected business users.
- ☐ financial losses incurred by affected business units.

Licensed to Berend Post berend.post@it-university.nl

Question 66

A risk analysis should:

- ☐ include a benchmark of similar companies in its scope.
- ☐ assume an equal degree of protection for all assets.
- ☐ address the potential size and likelihood of loss.
- ☐ give more weight to the likelihood vs. the size of the loss.

Question 67

The MOST important function of a risk management program is to:

- ☐ quantify overall risk.
- ☐ minimize residual risk.
- ☐ eliminate inherent risk.
- ☐ maximize the sum of all annualized loss expectancies (ALEs).

Question 68

Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

- ☐ A bit-level copy of all hard drive data
- ☐ The last verified backup stored offsite
- ☐ Data from volatile memory
- ☐ Backup servers

Question 69

Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

- ☐ Standards
- ☐ Guidelines
- ☐ Security metrics
- ☐ IT governance

Licensed to Berend Post berend.post@it-university.nl

Question 70

Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

- ☐ Reconciliation of the annual systems inventory to the disaster recovery, business continuity plans
- ☐ Periodic audits of the disaster recovery/business continuity plans
- ☐ Comprehensive walk-through testing
- ☐ Inclusion as a required step in the system life cycle process

Question 71

Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

- ☐ Symmetric cryptography
- ☐ Public key infrastructure (PKI)
- ☐ Message hashing
- ☐ Message authentication code

Question 72

To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

- ☐ revise the information security program.
- ☐ evaluate a balanced business scorecard.
- ☐ conduct regular user awareness sessions.
- ☐ perform penetration tests.

Question 73

Which of the following would be the BEST metric for the IT risk management process?

- ☐ Number of risk management action plans
- ☐ Percentage of critical assets with budgeted remedial
- ☐ Percentage of unresolved risk exposures
- ☐ Number of security incidents identified

Licensed to Berend Post berend.post@it-university.nl

Question 74

Information security policy enforcement is the responsibility of the:

- ☐ security steering committee.
- ☐ chief information officer (CIO).
- ☐ chief information security officer (CISO).
- ☐ chief compliance officer (CCO).

Question 75

An information security manager is implementing a bring your own device (BYOD) program. Which of the following would BEST ensure that users adhere to the security standards?

- ☐ Monitor user activities on the network
- ☐ Publish the standards on the intranet landing page
- ☐ Establish an acceptable use policy
- ☐ Deploy a device management solution

Question 76

Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

- ☐ Provide security awareness training to the third-party provider's employees
- ☐ Conduct regular security reviews of the third-party provider
- ☐ Include security requirements in the service contract
- ☐ Request that the third-party provider comply with the organization's information security policy

Question 77

A message* that has been encrypted by the sender's private key and again by the receiver's public key achieves:

- ☐ authentication and authorization.
- ☐ confidentiality and integrity.
- ☐ confidentiality and nonrepudiation.
- ☐ authentication and nonrepudiation.

Licensed to Berend Post berend.post@it-university.nl

Question 78

Which of the following is MOST effective in preventing security weaknesses in operating systems?

- ☐ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Configuration management

Question 79

Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?

- ☐ Return on investment
- ☐ Organizational culture
- ☐ Compliance requirements
- ☐ Criticality of information

Question 80

Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

- ☐ the parties to the agreement can perform.
- ☐ confidential data are not included in the agreement.
- ☐ appropriate controls are included.
- ☐ the right to audit is a requirement.

Question 81

An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

- ☐ Key performance indicators (KPIs)
- ☐ Business impact analysis (BIA)
- ☐ Gap analysis
- ☐ Technical vulnerability assessment

Licensed to Berend Post berend.post@it-university.nl

Question 82

Obtaining senior management support for establishing a warm site can BEST be accomplished by:

- ☐ establishing a periodic risk assessment.
- ☐ promoting regulatory requirements.
- ☐ developing a business case.
- ☐ developing effective metrics.

Question 83

In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

- ☐ develop an operational plan for achieving compliance with the legislation.
- ☐ identify systems and processes that contain privacy components.
- ☐ restrict the collection of personal information until compliant.
- ☐ identify privacy legislation in other countries that may contain similar requirements.

Question 84

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the information security manager?

- ☐ Follow the outsourcer's response plan.
- ☐ Alert the appropriate law enforcement authorities.
- ☐ Refer to the organization's response plan.
- ☐ Notify the outsourcer of the privacy breach.

Question 85

An information security manager is reviewing the impact of a regulation on the organization's human resources system. The NEXT course of action should be to:

- ☐ perform a gap analysis of compliance requirements.
- ☐ assess the penalties for non-compliance.
- ☐ review the organization's most recent audit report.
- ☐ determine the cost of compliance.

Licensed to Berend Post berend.post@it-university.nl

Question 86

Which of the following would be the FIRST step in establishing an information security program?

- ☐ Develop the security policy.
- ☐ Develop security operating procedures.
- ☐ Develop the security plan.
- ☐ Conduct a security controls study.

Question 87

Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

- ☐ map the major threats to business objectives.
- ☐ review available sources of risk information.
- ☐ identify the value of the critical assets.
- ☐ determine the financial impact if threats materialize.

Question 88

What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

- ☐ Periodic review of network configuration
- ☐ Review intrusion detection system (IDS) logs for evidence of attacks
- ☐ Periodically perform penetration tests
- ☐ Daily review of server logs for evidence of hacker activity

Question 89

A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

- ☐ Run a port scan on the system
- ☐ Disable the logon ID
- ☐ Investigate the system logs
- ☐ Validate the incident

Question 90

Which resource is the MOST effective in preventing physical access tailgating/piggybacking?

- ☐ Card key door locks
- ☐ Photo identification
- ☐ Awareness training
- ☐ Biometric scanners

Licensed to Berend Post berend.post@it-university.nl

Question 91

When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the BEST method to determine the priority of system recovery in the event of a disaster?

- ☐ Evaluating the cost associated with each system's outage
- ☐ Reviewing the business plans of each department
- ☐ Comparing the recovery point objectives
- ☐ Reviewing each system's key performance indicators

Question 92

Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

- ☐ SWOT analysis
- ☐ Waterfall chart
- ☐ Gap analysis
- ☐ Balanced scorecard

Question 93

An outcome of effective security governance is:

- ☐ business dependency assessment
- ☐ strategic alignment.
- ☐ risk assessment.
- ☐ planning.

Question 94

Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

- ☐ Incident response metrics
- ☐ Periodic auditing of the incident response process
- ☐ Action recording and review
- ☐ Post incident review

Licensed to Berend Post berend.post@it-university.nl

Question 95

Attackers who exploit cross-site scripting vulnerabilities take advantage of:

- ☐ a lack of proper input validation controls.
- ☐ weak authentication controls in the web application layer.
- ☐ flawed cryptographic secure sockets layer (SSL) implementations and short key lengths.
- ☐ implicit web application trust relationships.

Question 96

A CIO has asked the organization's information security manager to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

- ☐ To create formal requirements to meet projected security needs for the future
- ☐ To create and document a consistent progression of security capabilities
- ☐ To prioritize risks on a longer scale than the one-year plan
- ☐ To facilitate the continuous improvement of the IT organization

Question 97

The PRIMARY reason for using metrics to evaluate information security is to:

- ☐ identify security weaknesses.
- ☐ justify budgetary expenditures.
- ☐ enable steady improvement.
- ☐ raise awareness on security issues.

Question 98

Which of the following steps should be performed FIRST in the risk assessment process?

- ☐ Staff interviews
- ☐ Threat identification
- ☐ Asset identification and valuation
- ☐ Determination of the likelihood of identified risks

Licensed to Berend Post berend.post@it-university.nl

Question 99

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

- ☐ Examples of genuine incidents at similar organizations
- ☐ Statement of generally accepted best practices
- ☐ Associating realistic threats to corporate objectives
- ☐ Analysis of current technological exposures

Question 100

Which of the following would be the BEST indicator that an organization is appropriately managing risk?

- ☐ The number of security incident events reported by staff has increased
- ☐ Risk assessment results are within tolerance
- ☐ A penetration test does not identify any high-risk system vulnerabilities
- ☐ The number of events reported from the intrusion detection system has declined

Question 101

A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

- ☐ Representation by regional business leaders
- ☐ Composition of the board
- ☐ Cultures of the different countries
- ☐ IT security skills

Question 102

When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

- ☐ Centralizing security management
- ☐ Implementing sanctions for noncompliance
- ☐ Policy enforcement by IT management
- ☐ Periodic compliance reviews

Licensed to Berend Post berend.post@it-university.nl

Question 103

Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

- ☐ Patch management
- ☐ Change management
- ☐ Security metrics
- ☐ Version control

Question 104

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

- ☐ Senior management support
- ☐ Results of a cost-benefit analysis
- ☐ Results of a risk assessment
- ☐ Impact on the risk profile

Question 105

When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity/disaster recovery plans is because:

- ☐ this is a requirement of the security policy.
- ☐ software licenses may expire in the future without warning.
- ☐ the asset inventory must be maintained.
- ☐ service level agreements may not otherwise be met.

Question 106

What will have the HIGHEST impact on standard information security governance models?

- ☐ Number of employees
- ☐ Distance between physical locations
- ☐ Complexity of organizational structure
- ☐ Organizational budget

Question 107

Which of the following is the PRIMARY advantage of desk checking a business continuity plan (BCP)?

- ☐ Assesses the availability and compatibility a backup hardware
- ☐ Allows for greater participation be management and the IT department
- ☐ Ensures that appropriate follow-up work is performed on noted issues
- ☐ Provides a low-cost method of assessing the BCP's completeness

Licensed to Berend Post berend.post@it-university.nl

Question 108

A major trading partner with access to the internal network is unwilling or unable to remediate serious information security exposures within its environment. Which of the following is the BEST recommendation?

- ☐ Sign a legal agreement assigning them all liability for any breach
- ☐ Remove all trading partner access until the situation improves
- ☐ Set up firewall rules restricting network traffic from that location
- ☐ Send periodic reminders advising them of their noncompliance

Question 109

During the restoration of several servers, a critical process that services external customers was restored late due to a failure, resulting in lost revenue. Which of the following would have BEST help to prevent this occurrence?

- ☐ Validation of senior management's risk tolerance
- ☐ Updates to the business impact analysis (BIA)
- ☐ More effective disaster recovery plan (DRP) testing
- ☐ Improvements to incident identification methods

Question 110

In order to highlight to management, the importance of network security, the security manager should FIRST:

- ☐ develop a security architecture.
- ☐ install a network intrusion detection system (NIDS) and prepare a list of attacks.
- ☐ develop a network security policy.
- ☐ conduct a risk assessment.

Question 111

Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

- ☐ Boundary router
- ☐ Strong encryption
- ☐ Internet-facing firewall
- ☐ Intrusion detection system (IDS)

Licensed to Berend Post berend.post@it-university.nl

Question 112

The MOST important factor in ensuring the success of an information security program is effective:

- ☐ communication of information security requirements to all users in the organization.
- ☐ formulation of policies and procedures for information security.
- ☐ alignment with organizational goals and objectives.
- ☐ monitoring compliance with information security policies and procedures.

Question 113

What is the PRIMARY role of the information security manager in the process of information classification within an organization?

- ☐ Defining and ratifying the classification structure of information assets
- ☐ Deciding the classification levels applied to the organization's information assets
- ☐ Securing information assets in accordance with their classification
- ☐ Checking if information assets have been classified properly

Question 114

Which of the following architectures for e-business BEST ensures high availability?

- ☐ Availability of an adjacent hot site and a standby server with mirrored copies of critical data
- ☐ Intelligent middleware to direct transactions from a downed system to an alternative
- ☐ A single point of entry allowing transactions to be received and processed quickly
- ☐ Automatic failover to the web site of another e-business that meets the user's needs

Question 115

The PRIMARY objective of security awareness is to:

- ☐ ensure that security policies are understood.
- ☐ influence employee behavior.
- ☐ ensure legal and regulatory compliance
- ☐ notify of actions for noncompliance.

Question 116

The criticality and sensitivity of information assets is determined on the basis of:

- ☐ threat assessment.
- ☐ vulnerability assessment.
- ☐ resource dependency assessment.
- ☐ impact assessment.

Licensed to Berend Post berend.post@it-university.nl

Question 117

Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

- ☐ Integrating the risk assessment into the internal audit program
- ☐ Applying global security standards to the IT projects
- ☐ Training project managers on risk assessment
- ☐ Having the information security manager participate on the project setting committees

Question 118

It is important to classify and determine relative sensitivity of assets to ensure that:

- ☐ cost of protection is in proportion to sensitivity.
- ☐ highly sensitive assets are protected.
- ☐ cost of controls is minimized.
- ☐ countermeasures are proportional to risk.

Question 119

After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

- ☐ increase its customer awareness efforts in those regions.
- ☐ implement monitoring techniques to detect and react to potential fraud.
- ☐ outsource credit card processing to a third party.
- ☐ make the customer liable for losses if they fail to follow the bank's advice.

Question 120

What is an appropriate frequency for updating operating system (OS) patches on production servers?

- ☐ During scheduled rollouts of new applications
- ☐ According to a fixed security patch management schedule
- ☐ Concurrently with quarterly hardware maintenance
- ☐ Whenever important security patches are released

Licensed to Berend Post berend.post@it-university.nl

Question 121

The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

- ☐ IT assets in key business functions are protected.
- ☐ business risks are addressed by preventive controls.
- ☐ stated objectives are achievable.
- ☐ IT facilities and systems are always available.

Question 122

Which of the following is the MOST important element of an information security strategy?

- ☐ Defined objectives
- ☐ Time frames for delivery
- ☐ Adoption of a control framework
- ☐ Complete policies

Question 123

When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

- ☐ services delivery objective.
- ☐ recovery time objective (RTO).
- ☐ recovery window.
- ☐ maximum tolerable outage (MTO).

Question 124

An information security organization should PRIMARILY:

- ☐ support the business objectives of the company by providing security-related support services.
- ☐ be responsible for setting up and documenting the information security responsibilities of the information security team members.
- ☐ ensure that the information security policies of the company are in line with global best practices and standards.
- ☐ ensure that the information security expectations are conveyed to employees.

Licensed to Berend Post berend.post@it-university.nl

Question 125

Who should drive the risk analysis for an organization?

- ☐ Senior management
- ☐ Security manager
- ☐ Quality manager
- ☐ Legal department

Question 126

Which of the following would be the MOST significant security risk in a pharmaceutical institution?

- ☐ Compromised customer information
- ☐ Unavailability of online transactions
- ☐ Theft of security tokens
- ☐ Theft of a Research and Development laptop

Question 127

When security policies are strictly enforced, the initial impact is that:

- ☐ they may have to be modified more frequently.
- ☐ they will be less subject to challenge.
- ☐ the total cost of security is increased.
- ☐ the need for compliance reviews is decreased.

Question 128

A digital signature using a public key infrastructure (PKI) will:

- ☐ not ensure the integrity of a message.
- ☐ rely on the extent to which the certificate authority (CA) is trusted.
- ☐ require two parties to the message exchange.
- ☐ provide a high level of confidentiality.

Question 129

Which if the following would be the MOST important information to include in a business case for an information security project in a highly regulated industry?

- ☐ Compliance risk assessment
- ☐ Critical audit findings
- ☐ Industry comparison analysis
- ☐ Number of reported security incidents

Licensed to Berend Post berend.post@it-university.nl

Question 130

Which of the following would MOST likely require a business continuity plan to be invoked?

- ☐ An unauthorized visitor discovered in the data center
- ☐ A distributed denial of service attack on an e-mail server
- ☐ An epidemic preventing staff from performing job functions
- ☐ A hacker holding personally identifiable information hostage

Question 131

To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRS T crucial step an information security manager would take in ensuring business continuity planning?

- ☐ Conducting a qualitative and quantitative risk analysis.
- ☐ Assigning value to the assets.
- ☐ Weighing the cost of implementing the plan vs. financial loss.
- ☐ Conducting a business impact analysis (BIA).

Question 132

A global organization processes and stores large volumes of personal data. Which of the following would be the MOST important attribute in creating a data access policy?

- ☐ Availability
- ☐ Integrity
- ☐ Reliability
- ☐ Confidentiality

Question 133

Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

- ☐ Certificate-based authentication of web client
- ☐ Certificate-based authentication of web server
- ☐ Data confidentiality between client and web server
- ☐ Multiple encryption algorithms

Licensed to Berend Post berend.post@it-university.nl

Question 134

The MAIN reason for continuous monitoring of a security strategy is to:

- ☐ optimize resource allocation.
- ☐ confirm benefits are being realized.
- ☐ evaluate the implementation of the strategy.
- ☐ allocate funds for information security

Question 135

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

- ☐ Results from a gap analysis
- ☐ Results from a business impact analysis
- ☐ Deadlines and penalties for noncompliance
- ☐ An inventory of security controls currently in place

Question 136

The PRIMARY advantage of single sign-on (SSO) is that it will:

- ☐ support multiple authentication mechanisms.
- ☐ increase the security related applications.
- ☐ strengthen user password.
- ☐ increase efficiency of access management.

Question 137

Risk management programs are designed to reduce risk to:

- ☐ a level that is too small to be measurable.
- ☐ the point at which the benefit exceeds the expense.
- ☐ a level that the organization is willing to accept.
- ☐ a rate of return that equals the current cost of capital.

Licensed to Berend Post berend.post@it-university.nl

Question 138

To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

- ☐ end users.
- ☐ legal counsel.
- ☐ operational units.
- ☐ audit management.

Question 139

Priority should be given to which of the following to ensure effective implementation of information security governance?

- ☐ Consultation
- ☐ Negotiation
- ☐ Facilitation
- ☐ Planning

Question 140

Logging is an example of which type of defense against systems compromise?

- ☐ Containment
- ☐ Detection
- ☐ Reaction
- ☐ Recovery

Question 141

Which of the following presents the GREATEST exposure to internal attack on a network?

- ☐ User passwords are not automatically expired
- ☐ All network traffic goes through a single switch
- ☐ User passwords are encoded but not encrypted
- ☐ All users reside on a single internal subnet

Question 142

Which of the following would present the GREATEST risk to information security?

- ☐ Virus signature files updates are applied to all servers every day
- ☐ Security access logs are reviewed within five business days
- ☐ Critical patches are applied within 24 hours of their release
- ☐ Security incidents are investigated within five business days

Licensed to Berend Post berend.post@it-university.nl

Question 143

Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

- ☐ Screened subnets
- ☐ Information classification policies and procedures
- ☐ Role-based access controls
- ☐ Intrusion detection system (IDS)

Question 144

An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

- ☐ Right to audit
- ☐ Nondisclosure agreement
- ☐ Proper firewall implementation
- ☐ Dedicated security manager for monitoring compliance

Question 145

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. As a FIRST step, the security manager should:

- ☐ copy sample files as evidence.
- ☐ remove access privileges to the folder containing the data.
- ☐ report this situation to the data owner.
- ☐ train the HR team on properly controlling file permissions.

Question 146

Which of the following is the MOST important risk associated with middleware in a client-server environment?

- ☐ Server patching may be prevented
- ☐ System backups may be incomplete
- ☐ System integrity may be affected
- ☐ End-user sessions may be hijacked

Licensed to Berend Post berend.post@it-university.nl

Question 147

Which of the following metrics would provide management with the MOST useful information about the progress of a security awareness program?

- ☐ Increased number of downloads of the organization's security policy
- ☐ Increased reported of security incidents
- ☐ Completion rate of user awareness training within each business unit
- ☐ Decreased number of security incidents

Question 148

An organization has decided to implement a security information and event management (SIEM) system. It is MOST important for the organization to consider:

- ☐ industry best practices.
- ☐ data ownership.
- ☐ log sources.
- ☐ threat assessments.

Question 149

Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

- ☐ baseline.
- ☐ strategy.
- ☐ procedure.
- ☐ policy.

Question 150

Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

- ☐ Mantrap
- ☐ Biometric lock
- ☐ Closed-circuit television (CCTV)
- ☐ Security guard

Licensed to Berend Post berend.post@it-university.nl

Question 151

Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

- ☐ Interoffice a system-generated complex password with 30 days expiration
- ☐ Give a dummy password over the telephone set for immediate expiration
- ☐ Require no password but force the user to set their own in 10 days
- ☐ Set initial password equal to the user ID with expiration in 30 days

Question 152

In assessing risk, it is MOST essential to:

- ☐ provide equal coverage for all asset types.
- ☐ use benchmarking data from similar organizations.
- ☐ consider both monetary value and likelihood of loss.
- ☐ focus primarily on threats and recent business losses.

Question 153

To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

- ☐ review the functionalities and implementation requirements of the solution.
- ☐ review comparison reports of tool implementation in peer companies.
- ☐ provide examples of situations where such a tool would be useful.
- ☐ substantiate the investment in meeting organizational needs.

Question 154

When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

- ☐ IP spoofing
- ☐ Man-in-the-middle attack
- ☐ Repudiation
- ☐ Trojan

Question 155

Which of the following should be of MOST concern to an information security manager reviewing an organization's data classification program?

- ☐ The program allows exceptions to be granted.
- ☐ Labeling is not consistent throughout the organization.
- ☐ Data retention requirement are not defined.
- ☐ The classifications do not follow industry best practices.

Licensed to Berend Post berend.post@it-university.nl

Question 156

Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

- ☐ Intrusion detection system (IDS)
- ☐ IP address packet filtering
- ☐ Two-factor authentication
- ☐ Embedded digital signature

Question 157

The PRIMARY benefit of performing an information asset classification is to:

- ☐ link security requirements to business objectives.
- ☐ identify controls commensurate to risk.
- ☐ define access rights.
- ☐ establish ownership.

Question 158

Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

- ☐ Include security responsibilities in the job description
- ☐ Require the administrator to obtain security certification
- ☐ Train the system administrator on penetration testing and vulnerability assessment
- ☐ Train the system administrator on risk assessment

Question 159

Nonrepudiation can BEST be ensured by using:

- ☐ strong passwords.
- ☐ a digital hash.
- ☐ symmetric encryption.
- ☐ digital signatures.

Licensed to Berend Post berend.post@it-university.nl

Question 160

An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers and maintaining all core business functions house. The information security manager has determined a defense in depth strategy should be used. Which of the following BEST describes this strategy?

- ☐ Multi-factor login requirements for cloud service applications, timeouts, and complex passwords
- ☐ Deployments of nested firewalls within the infrastructure
- ☐ Separate security controls for applications, platforms, programs, and endpoints
- ☐ Strict enforcement of role-based access control (RBAC)

Question 161

Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

- ☐ Delivery path tracing
- ☐ Reverse lookup translation
- ☐ Out-of-band channels
- ☐ Digital signatures

Question 162

What is the PRIMARY objective of a post-event review in incident response?

- ☐ Adjust budget provisioning
- ☐ Preserve forensic data
- ☐ Improve the response process
- ☐ Ensure the incident is fully documented

Question 163

The PRIMARY objective of an Internet usage policy is to prevent:

- ☐ access to inappropriate sites.
- ☐ downloading malicious code.
- ☐ violation of copyright laws.
- ☐ disruption of Internet access.

Licensed to Berend Post berend.post@it-university.nl

Question 164

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

- ☐ Warm
- ☐ Redundant
- ☐ Shared
- ☐ Mobile

Question 165

The PRIMARY reason for initiating a policy exception process is when:

- ☐ operations are too busy to comply.
- ☐ the risk is justified by the benefit.
- ☐ policy compliance would be difficult to enforce.
- ☐ users may initially be inconvenienced.

Question 166

Which of the following are the essential ingredients of a business impact analysis (B1A)?

- ☐ Downtime tolerance, resources and criticality
- ☐ Cost of business outages in a year as a factor of the security budget
- ☐ Business continuity testing methodology being deployed
- ☐ Structure of the crisis management team

Question 167

Which of the following would be MOST important to include in a bring your own device (BYOD) policy with regard to lost or stolen devices? The need for employees to:

- ☐ initiate the company's incident reporting process.
- ☐ seek advice from the mobile service provider.
- ☐ notify local law enforcement.
- ☐ request a remote wipe of the device.

Question 168

Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

- ☐ Tuning
- ☐ Patching
- ☐ Encryption
- ☐ Packet filtering

Licensed to Berend Post berend.post@it-university.nl

Question 169

Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

- ☐ removed into the custody of law enforcement investigators.
- ☐ kept in the tape library' pending further analysis.
- ☐ sealed in a signed envelope and locked in a safe under dual control.
- ☐ handed over to authorized independent investigators.

Question 170

When outsourcing data to a cloud service provider, which of the following should be the information security manager's MOST important consideration?

- ☐ Roles and responsibilities have been defined for the subscriber organization.
- ☐ Cloud servers are located in the same country as the organization.
- ☐ Access authorization includes biometric security verification.
- ☐ Data stored at the cloud service provider is not co-mingled.

Question 171

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

- ☐ Risk analysis process
- ☐ Business impact analysis (BIA)
- ☐ Risk management balanced scorecard
- ☐ Risk-based audit program

Question 172

It is MOST important for an information security manager to ensure that security risk assessments are performed:

- ☐ consistently throughout the enterprise
- ☐ during a root cause analysis
- ☐ as part of the security business case
- ☐ in response to the threat landscape

Licensed to Berend Post berend.post@it-university.nl

Question 173

Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

- ☐ Never use open source tools
- ☐ Focus only on production servers
- ☐ Follow a linear process for attacks
- ☐ Do not interrupt production processes

Question 174

Who can BEST approve plans to implement an information security governance framework?

- ☐ Internal auditor
- ☐ Information security management
- ☐ Steering committee
- ☐ Infrastructure management

Question 175

Which program element should be implemented FIRST in asset classification and control?

- ☐ Risk assessment
- ☐ Classification
- ☐ Valuation
- ☐ Risk mitigation

Question 176

A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

- ☐ Enable access through a separate device that requires adequate authentication
- ☐ Implement manual procedures that require password change after each use
- ☐ Request the vendor to add multiple user IDs
- ☐ Analyze the logs to detect unauthorized access

Licensed to Berend Post berend.post@it-university.nl

Question 177

Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

- ☐ Ease of installation
- ☐ Product documentation
- ☐ Available support
- ☐ System overhead

Question 178

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

- ☐ Risk management metrics
- ☐ External audit findings
- ☐ Results of vulnerability assessments
- ☐ The organization's security incident trends

Question 179

An organization is planning to open a new office in another country. Sensitive data will be routinely sent between two offices. What should be the information security manager's FIRST course of action?

- ☐ Identify applicable regulatory requirements to establish security policies.
- ☐ Update privacy policies to include the other country's laws and regulations.
- ☐ Apply the current corporate security policies to the new office.
- ☐ Encrypt the data for transfer to the head office based on security manager approval.

Question 180

Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

- ☐ corporate internal auditor.
- ☐ System developers/analysts.
- ☐ key business process owners.
- ☐ corporate legal counsel.

Licensed to Berend Post berend.post@it-university.nl

Question 181

A risk management approach to information protection is:

- ☐ managing risks to an acceptable level, commensurate with goals and objectives.
- ☐ accepting the security posture provided by commercial security products.
- ☐ implementing a training program to educate individuals on information protection and risks.
- ☐ managing risk tools to ensure that they assess all information protection vulnerabilities.

Question 182

Which of the following would the BEST demonstrate the added value of an information security program?

- ☐ Security baselines
- ☐ A SWOT analysis
- ☐ A gap analysis
- ☐ A balanced scorecard

Question 183

Who is MOST important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data loss?

- ☐ An independent auditor for identification of control deficiencies
- ☐ A damage assessment expert for calculating losses
- ☐ A forensics expert for evidence management
- ☐ A penetration tester to validate the attack

Question 184

An information security manager uses security metrics to measure the:

- ☐ performance of the information security program.
- ☐ performance of the security baseline.
- ☐ effectiveness of the security risk analysis.
- ☐ effectiveness of the incident response team.

Licensed to Berend Post berend.post@it-university.nl

Question 185

Access control to a sensitive intranet application by mobile users can BEST be implemented through:

- ☐ data encryption.
- ☐ digital signatures.
- ☐ strong passwords.
- ☐ two-factor authentication.

Question 186

Which of the following will BEST prevent external security attacks?

- ☐ Static IP addressing
- ☐ Network address translation
- ☐ Background checks for temporary employees
- ☐ Securing and analyzing system access logs

Question 187

Which of the following BEST describes the scope of risk analysis?

- ☐ Key financial systems
- ☐ Organizational activities
- ☐ Key systems and infrastructure
- ☐ Systems subject to regulatory compliance

Question 188

An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

- ☐ mitigate the impact by purchasing insurance.
- ☐ implement a circuit-level firewall to protect the network.
- ☐ increase the resiliency of security measures in place.
- ☐ implement a real-time intrusion detection system.

Licensed to Berend Post berend.post@it-university.nl

Question 189

Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

- ☐ conduct a risk assessment and allow or disallow based on the outcome.
- ☐ recommend a risk assessment and implementation only if the residual risks are accepted.
- ☐ recommend against implementation because it violates the company's policies.
- ☐ recommend revision of current policy.

Question 190

An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

- ☐ Shut down and power off the server.
- ☐ Duplicate the hard disk of the server immediately.
- ☐ Isolate the server from the network.
- ☐ Copy the database log file to a protected server.

Question 191

The MAIN reason why asset classification is important to a successful information security program is because classification determines:

- ☐ the priority and extent of risk mitigation efforts.
- ☐ the amount of insurance needed in case of loss.
- ☐ the appropriate level of protection to the asset.
- ☐ how protection levels compare to peer organizations.

Question 192

When personal information is transmitted across networks, there MUST be adequate controls over:

- ☐ change management.
- ☐ privacy protection.
- ☐ consent to data transfer.
- ☐ encryption devices.

Licensed to Berend Post berend.post@it-university.nl

Question 193

When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

- ☐ Number of controls
- ☐ Cost of achieving control objectives
- ☐ Effectiveness of controls
- ☐ Test results of controls

Question 194

Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

- ☐ Termination conditions
- ☐ Liability limits
- ☐ Service levels
- ☐ Privacy restrictions

Question 195

Of the following, who should have PRIMARY responsibility for assessing the security risk associated with an outsourced cloud provider contract?

- ☐ Information security manager
- ☐ Compliance manager
- ☐ Chief information officer
- ☐ Service delivery manager

Question 196

Which of the following BEST reduces the likelihood of leakage of private information via email?

- ☐ Email encryption
- ☐ User awareness training
- ☐ Strong user authentication protocols
- ☐ Prohibition on the personal use of email

Licensed to Berend Post berend.post@it-university.nl

Question 197

Isolation and containment measures for a compromised computer has been taken and information security management is now investigating. What is the MOST appropriate next step?

- ☐ Run a forensics tool on the machine to gather evidence
- ☐ Reboot the machine to break remote connections
- ☐ Make a copy of the whole system's memory
- ☐ Document current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/ I'DP) ports

Question 198

Why is "slack space" of value to an information security manager as pan of an incident investigation?

- ☐ Hidden data may be stored there
- ☐ The slack space contains login information
- ☐ Slack space is encrypted
- ☐ It provides flexible space for the investigation

Question 199

Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

- ☐ Database administrator (DBA)
- ☐ Finance department management
- ☐ Information security manager
- ☐ IT department management

Question 200

Which of the following results from the risk assessment process would BEST assist risk management decision making?

- ☐ Control risk
- ☐ Inherent risk
- ☐ Risk exposure
- ☐ Residual risk

Licensed to Berend Post berend.post@it-university.nl

Question 201

Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

- ☐ System analyst
- ☐ System user
- ☐ Operations manager
- ☐ Data security officer

Question 202

After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

- ☐ transferred.
- ☐ treated.
- ☐ accepted.
- ☐ terminated.

Question 203

At what stage of the applications development process should the security department initially become involved?

- ☐ When requested
- ☐ At testing
- ☐ At programming
- ☐ At detail requirements

Question 204

Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

- ☐ Batch patches into frequent server updates
- ☐ Initially load the patches on a test machine
- ☐ Set up servers to automatically download patches
- ☐ Automatically push all patches to the servers

Licensed to Berend Post berend.post@it-university.nl

Question 205

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

- ☐ Communicating specially drafted messages by an authorized person
- ☐ Refusing to comment until recovery
- ☐ Referring the media to the authorities
- ☐ Reporting the losses and recovery strategy to the media

Question 206

Which of the following would BEST assist an IS manager in gaining strategic support from executive management?

- ☐ Annual report of security incidents within the organization
- ☐ Research on trends in global information security breaches
- ☐ Rating of the organization's security, based on international standards
- ☐ Risk analysis specific to the organization

Question 207

Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

- ☐ Defining job roles
- ☐ Performing a risk assessment
- ☐ Identifying data owners
- ☐ Establishing data retention policies

Question 208

The PRIMARY purpose of using risk analysis within a security program is to:

- ☐ justify the security expenditure.
- ☐ help businesses prioritize the assets to be protected.
- ☐ inform executive management of residual risk value.
- ☐ assess exposures and plan remediation.

Licensed to Berend Post berend.post@it-university.nl

Question 209

Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

- ☐ Disclosure of personal information
- ☐ Sufficient coverage of the insurance policy for accidental losses
- ☐ Intrinsic value of the data stored on the equipment
- ☐ Replacement cost of the equipment

Question 210

Which of the following would be the BEST defense against sniffing?

- ☐ Password protect the files
- ☐ Implement a dynamic IP address scheme
- ☐ Encrypt the data being transmitted
- ☐ Set static mandatory access control (MAC) addresses

Question 211

The PRIMARY purpose for continuous monitoring of security controls is to ensure:

- ☐ system availability.
- ☐ control gaps are minimized.
- ☐ effectiveness of controls.
- ☐ alignment with compliance requirements.

Question 212

Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization's technical infrastructure?

- ☐ An intrusion detection system
- ☐ Established security baselines
- ☐ Penetration testing
- ☐ Log aggregation and correlation

Question 213

To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

- ☐ Security breach frequency
- ☐ Annualized loss expectancy (ALE)
- ☐ Cost-benefit analysis
- ☐ Peer group comparison

Licensed to Berend Post berend.post@it-university.nl

Question 214

Who is responsible for ensuring that information is classified?

- ☐ Senior management
- ☐ Security manager
- ☐ Data owner
- ☐ Custodian

Question 215

Security awareness training is MOST likely to lead to which of the following?

- ☐ Decrease in intrusion incidents
- ☐ Increase in reported incidents
- ☐ Decrease in security policy changes
- ☐ Increase in access rule violations

Question 216

Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

- ☐ The program's governance oversight mechanisms
- ☐ Information security periodicals and manuals
- ☐ The program's security architecture and design
- ☐ Training and certification of the information security team

Question 217

An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

- ☐ Rewrite the application to conform to the upgraded operating system
- ☐ Compensate for not installing the patch with mitigating controls
- ☐ Alter the patch to allow the application to run in a privileged state
- ☐ Run the application on a test platform; tune production to allow patch and application

Licensed to Berend Post berend.post@it-university.nl

Question 218

When designing an information security quarterly report to management, the MOST important element to be considered should be the:

- ☐ information security metrics.
- ☐ knowledge required to analyze each issue.
- ☐ linkage to business area objectives.
- ☐ baseline against which metrics are evaluated.

Question 219

A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

- ☐ Understand the business requirements of the developer portal
- ☐ Perform a vulnerability assessment of the developer portal
- ☐ Install an intrusion detection system (IDS)
- ☐ Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Question 220

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organization’s information security manager?

- ☐ The change did not include a proper assessment of risk.
- ☐ Documentation of the change was made after implementation.
- ☐ The information security manager did not review the change prior to implementation.
- ☐ The operations team implemented the change without regression testing.

Question 221

In order to highlight to management, the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

- ☐ prepare a security budget.
- ☐ conduct a risk assessment.
- ☐ develop an information security policy.
- ☐ obtain benchmarking information.

Licensed to Berend Post berend.post@it-university.nl

Question 222

Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

- ☐ Number of controls implemented
- ☐ Percent of control objectives accomplished
- ☐ Percent of compliance with the security policy
- ☐ Reduction in the number of reported security incidents

Question 223

Which of the following devices should be placed within a demilitarized zone (DMZ)?

- ☐ Network switch
- ☐ Web server
- ☐ Database server
- ☐ File/print server

Question 224

Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

- ☐ Budget allocation
- ☐ Technical skills of staff
- ☐ User acceptance
- ☐ Password requirements

Question 225

Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

- ☐ Daily
- ☐ Weekly
- ☐ Concurrently with O/S patch updates
- ☐ During scheduled change control updates

Question 226

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

- ☐ Steering committee leadership be selected by rotation.
- ☐ Inputs be obtained and consensus achieved between the major organizational units.
- ☐ The business strategy be updated periodically.
- ☐ Procedures and standards be approved by all departmental heads.

Licensed to Berend Post berend.post@it-university.nl

Question 227

Which of the following authentication methods prevents authentication replay?

- ☐ Password hash implementation
- ☐ Challenge/response mechanism
- ☐ Wired Equivalent Privacy (WEP) encryption usage
- ☐ HTTP Basic Authentication

Question 228

Information security policies should:

- ☐ address corporate network vulnerabilities.
- ☐ address the process for communicating a violation.
- ☐ be straightforward and easy to understand.
- ☐ be customized to specific groups and roles.

Question 229

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

- ☐ Evaluating a business impact analysis (BIA)
- ☐ Developing a balanced business scorecard
- ☐ Demonstrating the relationship between controls
- ☐ Measuring current state vs. desired future state

Question 230

An information security program should focus on:

- ☐ best practices also in place at peer companies.
- ☐ solutions codified in international standards.
- ☐ key controls identified in risk assessments.
- ☐ continued process improvement.

Question 231

The recovery point objective (RPO) requires which of the following?

- ☐ Disaster declaration
- ☐ Before-image restoration
- ☐ System restoration
- ☐ After-image processing

Licensed to Berend Post berend.post@it-university.nl

Question 232

Ensuring that activities performed by outsourcing providers comply with information security policies can BEST be accomplished through the use of:

- ☐ service level agreements.
- ☐ explicit contract language.
- ☐ local regulations.
- ☐ independent audits.

Question 233

The PRIMARY focus of the change control process is to ensure that changes are:

- ☐ authorized.
- ☐ applied.
- ☐ documented.
- ☐ tested.

Question 234

The FIRST step in developing an information security management program is to:

- ☐ identify business risks that affect the organization.
- ☐ clarify organizational purpose for creating the program.
- ☐ assign responsibility for the program.
- ☐ assess adequacy of controls to mitigate business risks.

Question 235

When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

- ☐ Business continuity plan
- ☐ Disaster recovery plan
- ☐ Incident response plan
- ☐ Vulnerability management plan

Question 236

A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

- ☐ there are sufficient safeguards in place to prevent this risk from happening.
- ☐ the needed countermeasure is too complicated to deploy.
- ☐ the cost of countermeasure outweighs the value of the asset and potential loss.
- ☐ The likelihood of the risk occurring is unknown.

Licensed to Berend Post berend.post@it-university.nl

Question 237

Which of the following should be in place before a black box penetration test begins?

- ☐ IT management approval
- ☐ Proper communication and awareness training
- ☐ A clearly stated definition of scope
- ☐ An incident response plan

Question 238

The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

- ☐ Data owner
- ☐ Data custodian
- ☐ Systems programmer
- ☐ Security administrator

Question 239

Which of the following is the BEST method to securely transfer a message?

- ☐ Password-protected removable media
- ☐ Facsimile transmission in a secured room
- ☐ Using public key infrastructure (PKI) encryption
- ☐ Steganography

Question 240

Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

- ☐ The number of false positives increases
- ☐ The number of false negatives increases
- ☐ Active probing is missed
- ☐ Attack profiles are ignored

Question 241

The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

- ☐ contribute cost-effective expertise not available internally.
- ☐ be made responsible for meeting the security program requirements.
- ☐ replace the dependence on internal resources.
- ☐ deliver more effectively on account of their knowledge.

Licensed to Berend Post berend.post@it-university.nl

Question 242

What is the BEST technique to determine which security controls to implement with a limited budget?

- ☐ Risk analysis
- ☐ Annualized loss expectancy (ALE) calculations
- ☐ Cost-benefit analysis
- ☐ Impact analysis

Question 243

Which of the following is the PRIMARY benefit of implementing a maturity model for information security management?

- ☐ Information security management costs will be optimized.
- ☐ Information security strategy will be in line with industry best practice.
- ☐ Gaps between current and desirable levels will be addressed.
- ☐ Staff awareness of information security compliance will be promoted.

Question 244

In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

- ☐ testing time window prior to deployment.
- ☐ technical skills of the team responsible.
- ☐ certification of validity for deployment.
- ☐ automated deployment to all the servers.

Question 245

Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

- ☐ Baseline security standards
- ☐ System access violation logs
- ☐ Role-based access controls
- ☐ Exit routines

Licensed to Berend Post berend.post@it-university.nl

Question 246

Which of the following has the MOST direct impact on the usability of an organization's asset classification program?

- ☐ The granularity of classifications in the hierarchy
- ☐ The frequency of updates to the organization's risk register
- ☐ The business objectives of the organization
- ☐ The support of senior management for the classification scheme

Question 247

Which of the following will BEST protect against malicious activity by a former employee?

- ☐ Preemployment screening
- ☐ Close monitoring of users
- ☐ Periodic awareness training
- ☐ Effective termination procedures

Question 248

The BEST strategy for risk management is to:

- ☐ achieve a balance between risk and organizational goals.
- ☐ reduce risk to an acceptable level.
- ☐ ensure that policy development properly considers organizational risks.
- ☐ ensure that all unmitigated risks are accepted by management.

Question 249

Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

- ☐ determining the extent of property damage.
- ☐ preserving environmental conditions.
- ☐ ensuring orderly plan activation.
- ☐ reducing the extent of operational damage.

Licensed to Berend Post berend.post@it-university.nl

Question 250

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

- ☐ enable independent and objective review of the root cause of the incidents.
- ☐ obtain support for enhancing the expertise of the third-party teams.
- ☐ identify lessons learned for further improving the information security management process.
- ☐ obtain better buy-in for the information security program.

Question 251

Which of the following guarantees that data in a file have not changed?

- ☐ Inspecting the modified date of the file
- ☐ Encrypting the file with symmetric encryption
- ☐ Using stringent access control to prevent unauthorized access
- ☐ Creating a hash of the file, then comparing the file hashes

Question 252

Security audit reviews should PRIMARILY:

- ☐ ensure that controls operate as required.
- ☐ ensure that controls are cost-effective.
- ☐ focus on preventive controls.
- ☐ ensure controls are technologically current.

Question 253

The implementation of a capacity plan would prevent:

- ☐ file system overload arising from distributed denial-of-service attacks
- ☐ system downtime for scheduled security maintenance
- ☐ software failures arising from exploitation of buffer capacity vulnerabilities
- ☐ application failures arising from insufficient hardware resources

Question 254

The MOST important reason for formally documenting security procedures is to ensure:

- ☐ processes are repeatable and sustainable.
- ☐ alignment with business objectives.
- ☐ auditability by regulatory agencies.
- ☐ objective criteria for the application of metrics.

Licensed to Berend Post berend.post@it-university.nl

Question 255

Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

- ☐ User assessments of changes
- ☐ Comparison of the program results with industry standards
- ☐ Assignment of risk within the organization
- ☐ Participation by all members of the organization

Question 256

A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

- ☐ A penetration test
- ☐ A security baseline review
- ☐ A risk assessment
- ☐ A business impact analysis (BIA)

Question 257

Which of the following is a potential indicator of inappropriate Internet use by staff?

- ☐ Increased help desk calls for password resets
- ☐ Reduced number of pings on firewalls
- ☐ Increased reports of slow system performance
- ☐ Increased number of weakness from vulnerability scans

Question 258

Which of the following is the MOST important prerequisite for establishing information security management within an organization?

- ☐ Senior management commitment
- ☐ Information security framework
- ☐ Information security organizational structure
- ☐ Information security policy

Licensed to Berend Post berend.post@it-university.nl

Question 259

Risk assessment is MOST effective when performed:

- ☐ at the beginning of security program development.
- ☐ on a continuous basis.
- ☐ while developing the business case for the security program.
- ☐ during the business change process.

Question 260

Which of the following is MOST essential for a risk management program to be effective?

- ☐ Flexible security budget
- ☐ Sound risk baseline
- ☐ New risks detection
- ☐ Accurate risk reporting

Question 261

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

- ☐ Security' awareness training
- ☐ Achievable goals and objectives
- ☐ Senior management sponsorship
- ☐ Adequate start-up budget and staffing

Question 262

A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

- ☐ higher costs in supporting end users
- ☐ impact on network capacity
- ☐ decrease in end user productivity
- ☐ lack of a device management solution

Question 263

In implementing information security governance, the information security manager is PRIMARILY responsible for:

- ☐ developing the security strategy.
- ☐ reviewing the security strategy.
- ☐ communicating the security strategy.
- ☐ approving the security strategy

Licensed to Berend Post berend.post@it-university.nl

Question 264

Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:

- ☐ ensure the controls are regularly tested for ongoing effectiveness.
- ☐ hand over the controls to the relevant business owners.
- ☐ prepare to adapt the controls for future system upgrades.
- ☐ perform testing to compare control performance against industry levels.

Question 265

In business-critical applications, user access should be approved by the:

- ☐ information security manager.
- ☐ data owner.
- ☐ data custodian.
- ☐ business management.

Question 266

An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

- ☐ Unsure that critical data on the server are backed up.
- ☐ Shut down the compromised server.
- ☐ Initiate the incident response process.
- ☐ Shut down the network.

Question 267

If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

- ☐ obtaining evidence as soon as possible.
- ☐ preserving the integrity of the evidence.
- ☐ disconnecting all IT equipment involved.
- ☐ reconstructing the sequence of events.

Licensed to Berend Post berend.post@it-university.nl

Question 268

Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

- ☐ Filter media access control (MAC) addresses
- ☐ Use a Wi-Fi Protected Access (WPA2) protocol
- ☐ Use a Wired Equivalent Privacy (WEP) key
- ☐ Web-based authentication

Question 269

Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

- ☐ Theft of purchased software
- ☐ Power outage lasting 24 hours
- ☐ Permanent decline in customer confidence
- ☐ Temporary loss of e-mail due to a virus attack

Question 270

Phishing is BEST mitigated by which of the following?

- ☐ Security monitoring software
- ☐ Encryption
- ☐ Two-factor authentication
- ☐ User awareness

Question 271

Managing the life cycle of a digital certificate is a role of a(n):

- ☐ system administrator.
- ☐ security administrator.
- ☐ system developer.
- ☐ independent trusted source.

Question 272

A security risk assessment exercise should be repeated at regular intervals because:

- ☐ business threats are constantly changing.
- ☐ omissions in earlier assessments can be addressed.
- ☐ repetitive assessments allow various methodologies.
- ☐ they help raise awareness on security in the business.

Licensed to Berend Post berend.post@it-university.nl

Question 273

While implementing information security governance an organization should FIRST:

- ☐ adopt security standards.
- ☐ determine security baselines.
- ☐ define the security strategy.
- ☐ establish security policies.

Question 274

What is the MOST important success factor in launching a corporate information security awareness program?

- ☐ Adequate budgetary support
- ☐ Centralized program management
- ☐ Top-down approach
- ☐ Experience of the awareness trainers

Question 275

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

- ☐ users can gain direct access to the application ID and circumvent data controls.
- ☐ when multiple sessions with the same application ID collide, the database locks up.
- ☐ the database becomes unavailable if the password of the application ID expires.
- ☐ an incident involving unauthorized access to data cannot be tied to a specific user.

Question 276

Of the following, whose input is of GREATEST importance in the development of an information security strategy?

- ☐ End users
- ☐ Corporate auditors
- ☐ Process owners
- ☐ Security architects

Question 277

A risk assessment should be conducted:

- ☐ once a year for each business process and subprocess.
- ☐ every three to six months for critical business processes.
- ☐ by external parties to maintain objectivity.
- ☐ annually or whenever there is a significant change.

Licensed to Berend Post berend.post@it-university.nl

Question 278

An organization shares customer information across its globally dispersed branches. Which of the following should be the GREATEST concern to information security management?

- ☐ Cross-cultural differences between branches
- ☐ Conflicting data protection regulations
- ☐ Insecure wide area networks (WANs)
- ☐ Decentralization of information security

Question 279

Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

- ☐ Conduct awareness sessions on intellectual property policy
- ☐ Require all employees to sign a nondisclosure agreement
- ☐ Promptly remove all access when an employee leaves the organization
- ☐ Restrict access to a need-to-know basis

Question 280

The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

- ☐ periodically testing the incident response plans.
- ☐ regularly testing the intrusion detection system (IDS).
- ☐ establishing mandatory training of all personnel.
- ☐ periodically reviewing incident response procedures.

Question 281

When messages are encrypted and digitally signed to protect documents transferred between trading partners, the GREATEST concern is that:

- ☐ trading partners can repudiate the transmission of messages.
- ☐ hackers can eavesdrop on messages.
- ☐ trading partners can repudiate the receipt of messages.
- ☐ hackers can introduce forgery messages.

Licensed to Berend Post berend.post@it-university.nl

Question 282

The decision as to whether a risk has been reduced to an acceptable level should be determined by:

- ☐ organizational requirements.
- ☐ information systems requirements.
- ☐ information security requirements.
- ☐ international standards.

Question 283

An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

- ☐ Ethics
- ☐ Proportionality
- ☐ Integration
- ☐ Accountability

Question 284

Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

- ☐ Setting up a backup site
- ☐ Maintaining redundant systems
- ☐ Aligning with recovery time objectives (RTOs)
- ☐ Data backup frequency

Question 285

Which of the following is the MOST effective, positive method to promote security awareness?

- ☐ Competitions and rewards for compliance
- ☐ Lock-out after three incorrect password attempts
- ☐ Strict enforcement of password formats
- ☐ Disciplinary action for noncompliance

Question 286

Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

- ☐ Stress testing
- ☐ Patch management
- ☐ Change management
- ☐ Security baselines

Licensed to Berend Post berend.post@it-university.nl

Question 287

The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

- ☐ helps ensure that communications are secure.
- ☐ increases security between multi-tier systems.
- ☐ allows passwords to be changed less frequently.
- ☐ eliminates the need for secondary authentication.

Question 288

Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

- ☐ Authentication
- ☐ Hardening
- ☐ Encryption
- ☐ Nonrepudiation

Question 289

The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

- ☐ determining the scope for inclusion in an information security program.
- ☐ defining the level of access controls.
- ☐ justifying costs for information resources.
- ☐ determining the overall budget of an information security program.

Question 290

What of the following is MOST important to include in an information security policy?

- ☐ Maturity levels
- ☐ Best practices
- ☐ Management objectives
- ☐ Baselines

Question 291

Which of the following will BEST protect confidential data when connecting large wireless networks to an existing wired-network infrastructure?

- ☐ Mandatory access control (MAC) address filtering
- ☐ Strong passwords
- ☐ Virtual private network (VPN)
- ☐ Firewall

Licensed to Berend Post berend.post@it-university.nl

Question 292

Which of the following attacks is BEST mitigated by utilizing strong passwords?

- ☐ Man-in-the-middle attack
- ☐ Brute force attack
- ☐ Remote buffer overflow
- ☐ Root kit

Question 293

The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

- ☐ regulatory' requirements.
- ☐ business requirements.
- ☐ financial value.
- ☐ IT resource availability.

Question 294

What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

- ☐ Mandatory
- ☐ Discretionary
- ☐ Walled garden
- ☐ Role-based

Question 295

The MAIN goal of an information security strategic plan is to:

- ☐ develop a risk assessment plan.
- ☐ develop a data protection plan.
- ☐ protect information assets and resources.
- ☐ establish security governance.

Question 296

An intranet server should generally be placed on the:

- ☐ internal network.
- ☐ firewall server.
- ☐ external router.
- ☐ primary domain controller.

Licensed to Berend Post berend.post@it-university.nl

Question 297

Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

- ☐ Business impact analysis (BIA)
- ☐ Penetration testing
- ☐ Audit and review
- ☐ Threat analysis

Question 298

Which of the following threats is prevented by using token-based authentication?

- ☐ Password sniffing attack on the network
- ☐ Denial of service attack over the network
- ☐ Main-in-the middle attack on the client
- ☐ Session eavesdropping attack on the network

Question 299

An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

- ☐ broken authentication.
- ☐ unvalidated input.
- ☐ cross-site scripting.
- ☐ structured query language (SQL) injection.

Question 300

Which of the following documents would be the BEST reference to determine whether access control mechanisms are appropriate for a critical application?

- ☐ User security procedures
- ☐ Business process flow
- ☐ IT security policy
- ☐ Regulatory requirements

Licensed to Berend Post berend.post@it-university.nl

Question 301

What is the MOST important element to include when developing user security awareness material?

- ☐ Information regarding social engineering
- ☐ Detailed security policies
- ☐ Senior management endorsement
- ☐ Easy-to-read and compelling information

Question 302

A risk management program would be expected to:

- ☐ remove all inherent risk.
- ☐ maintain residual risk at an acceptable level.
- ☐ implement preventive controls for every threat.
- ☐ reduce control risk to zero.

Question 303

When performing a risk assessment, the MOST important consideration is that:

- ☐ management supports risk mitigation efforts.
- ☐ annual loss expectations (ALEs) have been calculated for critical assets.
- ☐ assets have been identified and appropriately valued.
- ☐ attack motives, means and opportunities be understood.

Question 304

Which of the following devices should be placed within a DMZ?

- ☐ Proxy server
- ☐ Application server
- ☐ Departmental server
- ☐ Data warehouse server

Question 305

An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

- ☐ Nothing, since a risk assessment was completed during development.
- ☐ A vulnerability assessment should be conducted.
- ☐ A new risk assessment should be performed.
- ☐ The new vendor's SAS 70 type II report should be reviewed.

Licensed to Berend Post berend.post@it-university.nl

Question 306

Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

- ☐ Biometric authentication
- ☐ Embedded steganographic
- ☐ Two-factor authentication
- ☐ Embedded digital signature

Question 307

Which of the following is the MOST effective method of determining security priorities?

- ☐ Impact analysis
- ☐ Threat assessment
- ☐ Vulnerability assessment
- ☐ Gap analysis

Question 308

When supporting an organization's privacy officer, which of the following is the information security manager's PRIMARY role regarding primacy requirements?

- ☐ Monitoring the transfer of private data
- ☐ Conducting privacy awareness programs
- ☐ Ensuring appropriate controls are in place
- ☐ Determining data classification

Question 309

A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's FIRST course of action?

- ☐ Review the current security policy.
- ☐ Inform senior management of the new regulation.
- ☐ Update the security incident management process.
- ☐ Determine impact to the business.

Licensed to Berend Post berend.post@it-university.nl

Question 310

A common concern with poorly written web applications is that they can allow an attacker to:

- ☐ gain control through a buffer overflow.
- ☐ conduct a distributed denial of service (DoS) attack.
- ☐ abuse a race condition.
- ☐ inject structured query language (SQL) statements.

Question 311

What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

- ☐ Business impact analyses
- ☐ Security gap analyses
- ☐ System performance metrics
- ☐ Incident response processes

Question 312

The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

- ☐ service level monitoring.
- ☐ penetration testing.
- ☐ periodically auditing.
- ☐ security awareness training.

Question 313

An organization to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

- ☐ Evaluate the cost of information security integration
- ☐ Assess the business objectives of the processes
- ☐ Identify information security risk associated with the processes
- ☐ Benchmark the processes with best practice to identify gaps

Question 314

Information security awareness programs are MOST effective when they are:

- ☐ customized for each target audience.
- ☐ sponsored by senior management.
- ☐ reinforced by computer-based training.
- ☐ conducted at employee orientation

Licensed to Berend Post berend.post@it-university.nl

Question 315

The PRIMARY objective of a security steering group is to:

- ☐ ensure information security covers all business functions.
- ☐ ensure information security aligns with business goals.
- ☐ raise information security awareness across the organization.
- ☐ implement all decisions on security management across the organization.

Question 316

What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

- ☐ Risk assessment report
- ☐ Technical evaluation report
- ☐ Business case
- ☐ Budgetary requirements

Question 317

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

- ☐ Management requires regular reports.
- ☐ The environment changes constantly.
- ☐ Technology risks must be mitigated.
- ☐ The current threat levels are being assessed.

Question 318

When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

- ☐ The firewall should block all inbound traffic during the outage
- ☐ All systems should block new logins until the problem is corrected
- ☐ Access control should fall back to no synchronized mode
- ☐ System logs should record all user activity for later analysis

Licensed to Berend Post berend.post@it-university.nl

Question 319

An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

- ☐ eliminating the risk.
- ☐ transferring the risk.
- ☐ mitigating the risk.
- ☐ accepting the risk.

Question 320

Which of the following risks is represented in the risk appetite of an organization?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☐ Audit

Question 321

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

- ☐ a strong authentication.
- ☐ IP antispoofing filtering.
- ☐ network encryption protocol.
- ☐ access lists of trusted devices.

Question 322

Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

- ☐ Gantt chart
- ☐ Waterfall chart
- ☐ Critical path
- ☐ Rapid Application Development (RAD)

Question 323

What is the GREATEST risk when there is an excessive number of firewall rules?

- ☐ One rule may override another rule in the chain and create a loophole
- ☐ Performance degradation of the whole network
- ☐ The firewall may not support the increasing number of rules due to limitations
- ☐ The firewall may show abnormal behavior and may crash or automatically shut down

Licensed to Berend Post berend.post@it-university.nl

Question 324

The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

- ☐ create more overhead than signature-based IDSs.
- ☐ cause false positives from minor changes to system variables.
- ☐ generate false alarms from varying user or system actions.
- ☐ cannot detect new types of attacks.

Question 325

An information security manager has completed a risk assessment and has determined the residual risk. Which of the following should be the NEXT step?

- ☐ Conduct an evaluation of controls
- ☐ Determine if the risk is within the risk appetite
- ☐ Implement countermeasures to mitigate risk
- ☐ Classify all identified risks

Question 326

Which of the following is a key area of the ISO 27001 framework?

- ☐ Operational risk assessment
- ☐ Financial crime metrics
- ☐ Capacity management
- ☐ Business continuity management

Question 327

During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

- ☐ Feasibility
- ☐ Design
- ☐ Development
- ☐ Testing

Question 328

The MOST effective use of a risk register is to:

- ☐ identify risks and assign roles and responsibilities for mitigation.
- ☐ identify threats and probabilities.
- ☐ facilitate a thorough review of all IT-related risks on a periodic basis.
- ☐ record the annualized financial amount of expected losses due to risks.

Licensed to Berend Post berend.post@it-university.nl

Question 329

A newly hired information security manager reviewing an existing security investment plan is MOST likely to be concerned when the plan:

- ☐ is based solely on a review of security threats and vulnerabilities in existing IT systems
- ☐ identifies potential impacts that the implementation may have on business processes
- ☐ focuses on compliance with common international security standards
- ☐ has summarized IT costs for implementation rather than providing detail

Question 330

In the course of responding 10 an information security incident, the BEST way to treat evidence for possible legal action is defined by:

- ☐ international standards.
- ☐ local regulations.
- ☐ generally accepted best practices.
- ☐ organizational security policies.

Question 331

Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

- ☐ Implement countermeasures.
- ☐ Eliminate the risk.
- ☐ Transfer the risk.
- ☐ Accept the risk.

Question 332

The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

- ☐ generally accepted industry best practices.
- ☐ business requirements.
- ☐ legislative and regulatory requirements.
- ☐ storage availability.

Licensed to Berend Post berend.post@it-university.nl

Question 333

How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

- ☐ Give organization standards preference over local regulations
- ☐ Follow local regulations only
- ☐ Make the organization aware of those standards where local regulations causes conflicts
- ☐ Negotiate a local version of the organization standards

Question 334

Which of the following is an inherent weakness of signature-based intrusion detection systems?

- ☐ A higher number of false positives
- ☐ New attack methods will be missed
- ☐ Long duration probing will be missed
- ☐ Attack profiles can be easily spoofed

Question 335

Most security vulnerabilities in software exit because:

- ☐ security features are not tested adequately.
- ☐ software has undocumented features.
- ☐ security is not properly designed.
- ☐ software is developed without adherence to standards.

Question 336

When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

- ☐ Estimated productivity losses
- ☐ Possible scenarios with threats and impacts
- ☐ Value of information assets
- ☐ Vulnerability assessment

Question 337

An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

- ☐ performance measurement.
- ☐ integration.
- ☐ alignment.
- ☐ value delivery.

Licensed to Berend Post berend.post@it-university.nl

Question 338

The MAIN advantage of implementing automated password synchronization is that it:

- ☐ reduces overall administrative workload.
- ☐ increases security between multi-tier systems.
- ☐ allows passwords to be changed less frequently.
- ☐ reduces the need for two-factor authentication.

Question 339

Who in an organization has the responsibility for classifying information?

- ☐ Data custodian
- ☐ Database administrator
- ☐ Information security officer
- ☐ Data owner

Question 340

Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

- ☐ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Acquisition management

Question 341

The MOST basic requirement for an information security governance program is to:

- ☐ be aligned with the corporate business strategy.
- ☐ be based on a sound risk management approach.
- ☐ provide adequate regulatory compliance.
- ☐ provide best practices for security- initiatives.

Question 342

An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

- ☐ Review the procedures for granting access
- ☐ Establish procedures for granting emergency access
- ☐ Meet with data owners to understand business needs
- ☐ Redefine and implement proper access rights

Licensed to Berend Post berend.post@it-university.nl

Question 343

A good privacy statement should include:

- ☐ notification of liability on accuracy of information.
- ☐ notification that information will be encrypted.
- ☐ what the company will do with information it collects.
- ☐ a description of the information classification process.

Question 344

Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

- ☐ Use security tokens for authentication
- ☐ Connect through an IPSec VPN
- ☐ Use https with a server-side certificate
- ☐ Enforce static media access control (MAC) addresses

Question 345

The information classification scheme should:

- ☐ consider possible impact of a security breach.
- ☐ classify personal information in electronic form.
- ☐ be performed by the information security manager.
- ☐ classify systems according to the data processed.

Question 346

The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

- ☐ verify the decision with the business units.
- ☐ check the system's risk analysis.
- ☐ recommend update after post implementation review.
- ☐ request an audit review.

Licensed to Berend Post berend.post@it-university.nl

Question 347

In business critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

- ☐ ensure access to individual functions can be granted to individual users only.
- ☐ implement role-based access control in the application.
- ☐ enforce manual procedures ensuring separation of conflicting duties.
- ☐ create service accounts that can only be used by authorized team members.

Question 348

Who is responsible for raising awareness of the need for adequate funding for risk action plans?

- ☐ Chief information officer (CIO)
- ☐ Chief financial officer (CFO)
- ☐ Information security manager
- ☐ Business unit management

Question 349

Which of the following is MOST important for a successful information security program?

- ☐ Adequate training on emerging security technologies
- ☐ Open communication with key process owners
- ☐ Adequate policies, standards and procedures
- ☐ Executive management commitment

Question 350

The configuration management plan should PRIMARILY be based upon input from:

- ☐ business process owners.
- ☐ the information security manager.
- ☐ the security steering committee.
- ☐ IT senior management.

Question 351

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

- ☐ ensure the provider is made liable for losses.
- ☐ recommend not renewing the contract upon expiration.
- ☐ recommend the immediate termination of the contract.
- ☐ determine the current level of security.

Licensed to Berend Post berend.post@it-university.nl

Question 352

Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

- ☐ Alignment with industry best practices
- ☐ Business continuity investment
- ☐ Business benefits
- ☐ Regulatory compliance

Question 353

It is important to develop an information security baseline because it helps to define:

- ☐ critical information resources needing protection.
- ☐ a security policy for the entire organization.
- ☐ the minimum acceptable security to be implemented.
- ☐ required physical and logical access controls.

Question 354

Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

- ☐ Platform security
- ☐ Entitlement changes
- ☐ Intrusion detection
- ☐ Antivirus controls

Question 355

An information security manager wishing to establish security baselines would:

- ☐ include appropriate measurements in the system development life cycle.
- ☐ implement the security baselines to establish information security best practices.
- ☐ implement the security baselines to fulfill laws and applicable regulations in different jurisdictions.
- ☐ leverage information security as a competitive advantage.

Question 356

A successful risk management program should lead to:

- ☐ optimization of risk reduction efforts against cost.
- ☐ containment of losses to an annual budgeted amount.
- ☐ identification and removal of all man-made threats.
- ☐ elimination or transference of all organizational risks.

Licensed to Berend Post berend.post@it-university.nl

Question 357

When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

- ☐ to a higher false reject rate (FRR).
- ☐ to a lower crossover error rate.
- ☐ to a higher false acceptance rate (FAR).
- ☐ exactly to the crossover error rate.

Question 358

A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

- ☐ Denial of service (DoS) attacks
- ☐ Traffic sniffing
- ☐ Virus infections
- ☐ IP address spoofing

Question 359

An information security manager must understand the relationship between information security and business operations in order to:

- ☐ support organizational objectives.
- ☐ determine likely areas of noncompliance.
- ☐ assess the possible impacts of compromise.
- ☐ understand the threats to the business.

Question 360

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

- ☐ The complexity of technology
- ☐ Budgetary constraints
- ☐ Conflicting business priorities
- ☐ High-level sponsorship

Licensed to Berend Post berend.post@it-university.nl

Question 361

Which of the following are the MOST important individuals to include as members of an information security steering committee?

- ☐ Direct reports to the chief information officer
- ☐ IT management and key business process owners
- ☐ Cross-section of end users and IT professionals
- ☐ Internal audit and corporate legal departments

Question 362

Which of the following steps in conducting a risk assessment should be performed FIRST?

- ☐ Identity business assets
- ☐ Identify business risks
- ☐ Assess vulnerabilities
- ☐ Evaluate key controls

Question 363

The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

- ☐ escalate issues to an external third party for resolution.
- ☐ ensure that senior management provides authority for security to address the issues.
- ☐ insist that managers or units not in agreement with the security solution accept the risk.
- ☐ refer the issues to senior management along with any security recommendations.

Question 364

What does a network vulnerability assessment intend to identify?

- ☐ 0-day vulnerabilities
- ☐ Malicious software and spyware
- ☐ Security design flaws
- ☐ Misconfiguration and missing updates

Licensed to Berend Post berend.post@it-university.nl

Question 365

To prevent computers on the corporate network from being used as part of a distributed denial of service attack, the information security manager should use:

- ☐ incoming traffic filtering
- ☐ outgoing traffic filtering
- ☐ IT security policy dissemination
- ☐ rate limiting

Question 366

To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

- ☐ Service level agreements (SLAs)
- ☐ Right to audit clause
- ☐ Intrusion detection system (IDS) services
- ☐ Spam filtering services

Question 367

To determine the selection of controls required to meet business objectives, an information security manager should:

- ☐ prioritize the use of role-based access controls.
- ☐ focus on key controls.
- ☐ restrict controls to only critical applications.
- ☐ focus on automated controls.

Question 368

On a company's e-commerce web site, a good legal statement regarding data privacy should include:

- ☐ a statement regarding what the company will do with the information it collects.
- ☐ a disclaimer regarding the accuracy of information on its web site.
- ☐ technical information regarding how information is protected.
- ☐ a statement regarding where the information is being hosted.

Licensed to Berend Post berend.post@it-university.nl

Question 369

Which of the following has the highest priority when defining an emergency response plan?

- ☐ Critical data
- ☐ Critical infrastructure
- ☐ Safety of personnel
- ☐ Vital records

Question 370

Which two components PRIMARILY must be assessed in an effective risk analysis?

- ☐ Visibility and duration
- ☐ Likelihood and impact
- ☐ Probability and frequency
- ☐ Financial impact and duration

Question 371

What is the MOST appropriate change management procedure for the handling of emergency program changes?

- ☐ Formal documentation does not need to be completed before the change
- ☐ Business management approval must be obtained prior to the change
- ☐ Documentation is completed with approval soon after the change
- ☐ All changes must follow the same process

Question 372

Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

- ☐ define the circumstances where cryptography should be used.
- ☐ define cryptographic algorithms and key lengths.
- ☐ describe handling procedures of cryptographic keys.
- ☐ establish the use of cryptographic solutions.

Question 373

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- ☐ Automation of controls
- ☐ Documentation of control procedures
- ☐ Integration of assurance efforts
- ☐ Standardization of compliance requirements

Licensed to Berend Post berend.post@it-university.nl

Question 374

Good information security procedures should:

- ☐ define the allowable limits of behavior.
- ☐ underline the importance of security governance.
- ☐ describe security baselines for each platform.
- ☐ be updated frequently as new software is released.

Question 375

Identification and prioritization of business risk enables project managers to:

- ☐ establish implementation milestones.
- ☐ reduce the overall amount of slack time.
- ☐ address areas with most significance.
- ☐ accelerate completion of critical paths.

Question 376

The MOST important success factor to design an effective IT security awareness program is to:

- ☐ customize the content to the target audience.
- ☐ ensure senior management is represented.
- ☐ ensure that all the staff is trained.
- ☐ avoid technical content but give concrete examples.

Question 377

Which of the following is the MOST usable deliverable of an information security risk analysis?

- ☐ Business impact analysis (BIA) report
- ☐ List of action items to mitigate risk
- ☐ Assignment of risks to process owners
- ☐ Quantification of organizational risk

Question 378

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?

- ☐ Compliance with international security standards.
- ☐ Use of a two-factor authentication system.
- ☐ Existence of an alternate hot site in case of business disruption.
- ☐ Compliance with the organization's information security requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 379

When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

- ☐ Business management
- ☐ Operations manager
- ☐ Information security manager
- ☐ System users

Question 380

In an organization that has undergone an expansion through an acquisition which of the following would BEST secure the enterprise network?

- ☐ Using security groups
- ☐ Log analysis od system access
- ☐ Business or role-based segmentation
- ☐ Encryption of data traversing networks

Question 381

Good information security standards should:

- ☐ define precise and unambiguous allowable limits.
- ☐ describe the process for communicating violations.
- ☐ address high-level objectives of the organization.
- ☐ be updated frequently as new software is released.

Question 382

In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

- ☐ original cost to acquire.
- ☐ cost of the software stored.
- ☐ annualized loss expectancy (ALE).
- ☐ cost to obtain a replacement.

Licensed to Berend Post berend.post@it-university.nl

Question 383

An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

- ☐ threat.
- ☐ loss.
- ☐ vulnerability.
- ☐ probability.

Question 384

The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

- ☐ Secure Sockets Layer (SSL).
- ☐ Secure Shell (SSH).
- ☐ IP Security (IPSec).
- ☐ Secure/Multipurpose Internet Mail Extensions (S/MIME).

Question 385

The MOST important characteristic of good security policies is that they:

- ☐ state expectations of IT management.
- ☐ state only one general security mandate.
- ☐ are aligned with organizational goals.
- ☐ govern the creation of procedures and guidelines.

Question 386

An information security program should be sponsored by:

- ☐ infrastructure management.
- ☐ the corporate audit department.
- ☐ key business process owners.
- ☐ information security management.

Question 387

Which of the following is the PRIMARY reason for implementing a risk management program?

- ☐ Allows the organization to eliminate risk
- ☐ Is a necessary part of management's due diligence
- ☐ Satisfies audit and regulatory requirements
- ☐ Assists in incrementing the return on investment (ROD

Licensed to Berend Post berend.post@it-university.nl

Question 388

Without prior approval, a training department enrolled the company in a free cloud-based collaboration site and invited employees to use it. Which of the following is the BEST response of the information security manager?

- ☐ Conduct a risk assessment and develop an impact analysis.
- ☐ Update the risk register and review the information security strategy.
- ☐ Report the activity to senior management.
- ☐ Allow temporary use of the site and monitor for data leakage.

Question 389

Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

- ☐ Justification of the security budget must be continually made.
- ☐ New vulnerabilities are discovered every day.
- ☐ The risk environment is constantly changing.
- ☐ Management needs to be continually informed about emerging risks.

Question 390

Risk acceptance is a component of which of the following?

- ☐ Assessment
- ☐ Mitigation
- ☐ Evaluation
- ☐ Monitoring

Question 391

Data owners are normally responsible for which of the following?

- ☐ Applying emergency changes to application data
- ☐ Administering security over database records
- ☐ Migrating application code changes to production
- ☐ Determining the level of application security required

Licensed to Berend Post berend.post@it-university.nl

Question 392

An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's FIRST step to support this strategy?

- ☐ Incorporate social media into the security awareness program.
- ☐ Develop a guideline on the acceptable use of social media.
- ☐ Develop a business case for a data loss prevention solution.
- ☐ Employ the use of a web content filtering solution.

Question 393

After logging in to a web application, further password credentials are required at various application points. Which of the following is the PRIMARY reason for such an approach?

- ☐ To ensure access is granted to the authorized person
- ☐ To enforce strong two-factor authentication
- ☐ To ensure session management variables are secure
- ☐ To implement single sign-on

Question 394

When developing an incident response plan, the information security manager should:

- ☐ include response scenarios that have been approved previously by business management.
- ☐ determine recovery time objectives (RTOs).
- ☐ allow IT to decide which systems can be removed from the infrastructure.
- ☐ require IT to invoke the business continuity plan.

Question 395

Secure customer use of an e-commerce application can BEST be accomplished through:

- ☐ data encryption.
- ☐ digital signatures.
- ☐ strong passwords.
- ☐ two-factor authentication.

Licensed to Berend Post berend.post@it-university.nl

Question 396

Which of the following would a security manager establish to determine the target for restoration of normal processing?

- ☐ Recover time objective (RTO)
- ☐ Maximum tolerable outage (MTO)
- ☐ Recovery point objectives (RPOs)
- ☐ Services delivery objectives (SDOs)

Question 397

The MOST useful way to describe the objectives in the information security strategy is through:

- ☐ attributes and characteristics of the 'desired state."
- ☐ overall control objectives of the security program.
- ☐ mapping the IT systems to key business processes.
- ☐ calculation of annual loss expectations.

Question 398

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

- ☐ Fallback processes are tested the weekend before changes are made.
- ☐ The development manager migrates programs into production.
- ☐ A manual rather than an automated process is used to compare program versions.
- ☐ Users are not notified of scheduled system changes.

Question 399

Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

- ☐ Information security officer
- ☐ Security steering committee
- ☐ Data owner
- ☐ Data custodian

Licensed to Berend Post berend.post@it-university.nl

Question 400

Which of the following is the BEST indicator that an effective security control is built into an organization?

- ☐ The monthly service level statistics indicate a minimal impact from security issues.
- ☐ The cost of implementing a security control is less than the value of the assets.
- ☐ The percentage of systems that is compliant with security standards.
- ☐ The audit reports do not reflect any significant findings on security.

Question 401

Which of the following is the MOST important to keep in mind when assessing the value of information?

- ☐ The potential financial loss
- ☐ The cost of recreating the information
- ☐ The cost of insurance coverage
- ☐ Regulatory requirement

Question 402

The recovery time objective (RTO) is reached at which of the following milestones?

- ☐ Disaster declaration
- ☐ Recovery of the backups
- ☐ Restoration of the system
- ☐ Return to business as usual processing

Question 403

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

- ☐ Define security metrics
- ☐ Conduct a risk assessment
- ☐ Perform a gap analysis
- ☐ Procure security tools

Licensed to Berend Post berend.post@it-university.nl

Question 404

What should be an organization's MAIN concern when evaluating an Infrastructure as a Service (IaaS) cloud computing model for an e-Commerce application?

- ☐ Availability of provider's services
- ☐ Internal about requirements
- ☐ Where the application resides
- ☐ Application ownership

Question 405

Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

- ☐ it implies compliance risks.
- ☐ short-term impact cannot be determined.
- ☐ it violates industry security practices.
- ☐ changes in the roles matrix cannot be detected.

Question 406

A border router should be placed on which of the following?

- ☐ Web server
- ☐ IDS server
- ☐ Screened subnet
- ☐ Domain boundary

Question 407

The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

- ☐ sales department.
- ☐ database administrator.
- ☐ chief information officer (CIO).
- ☐ head of the sales department.

Question 408

Who is ultimately responsible for the organization's information?

- ☐ Data custodian
- ☐ Chief information security officer (CISO)
- ☐ Board of directors
- ☐ Chief information officer (CIO)

Licensed to Berend Post berend.post@it-university.nl

Question 409

When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

- ☐ Evaluate productivity losses
- ☐ Assess the impact of confidential data disclosure
- ☐ Calculate the value of the information or asset
- ☐ Measure the probability of occurrence of each threat

Question 410

To implement a security framework, an information security manager must FIRST develop:

- ☐ security standards.
- ☐ security procedures.
- ☐ a security policy.
- ☐ security guidelines.

Question 411

Which of the following characteristics is MOST important to a bank in a high-value online financial transaction system?

- ☐ Identification
- ☐ Confidentiality
- ☐ Authentication
- ☐ Audit monitoring

Question 412

When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:

- ☐ give the business a measure of the organization's overall readiness
- ☐ provide participants with situations to ensure understanding of their roles
- ☐ measure management engagement as part of an incident response team
- ☐ challenge the incident response team to solve the problem under pressure

Licensed to Berend Post berend.post@it-university.nl

Question 413

Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

- ☐ Regular review of access control lists
- ☐ Security guard escort of visitors
- ☐ Visitor registry log at the door
- ☐ A biometric coupled with a PIN

Question 414

Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

- ☐ The right to conduct independent security reviews
- ☐ A legally binding data protection agreement
- ☐ Encryption between the organization and the provider
- ☐ A joint risk assessment of the system

Question 415

A security manager meeting the requirements for the international flow of personal data will need to ensure:

- ☐ a data processing agreement.
- ☐ a data protection registration.
- ☐ the agreement of the data subjects.
- ☐ subject access procedures.

Question 416

A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

- ☐ Prevent the system from being accessed remotely
- ☐ Create a strong random password
- ☐ Ask for a vendor patch
- ☐ Track usage of the account by audit trails

Licensed to Berend Post berend.post@it-university.nl

Question 417

The FIRST step in an incident response plan is to:

- ☐ notify- the appropriate individuals.
- ☐ contain the effects of the incident to limit damage.
- ☐ develop response strategies for systematic attacks.
- ☐ validate the incident.

Question 418

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

- ☐ Develop an implementation strategy.
- ☐ Schedule the target end date for implementation activities.
- ☐ Budget the total cost of implementation activities.
- ☐ Calculate the residual risk for each countermeasure.

Question 419

A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

- ☐ meet with stakeholders to decide how to comply.
- ☐ analyze key risks in the compliance process.
- ☐ assess whether existing controls meet the regulation.
- ☐ update the existing security/privacy policy.

Question 420

To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

- ☐ create a separate account for the programmer as a power user.
- ☐ log all of the programmers' activity for review by supervisor.
- ☐ have the programmer sign a letter accepting full responsibility.
- ☐ perform regular audits of the application.

Licensed to Berend Post berend.post@it-university.nl

Question 421

When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

- ☐ the information security steering committee.
- ☐ customers who may be impacted.
- ☐ data owners who may be impacted.
- ☐ regulatory- agencies overseeing privacy.

Question 422

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

- ☐ invite an external consultant to create the security strategy.
- ☐ allocate budget based on best practices.
- ☐ benchmark similar organizations.
- ☐ define high-level business security requirements.

Question 423

Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

- ☐ Customer data stolen
- ☐ An electrical power outage
- ☐ A web site defaced by hackers
- ☐ Loss of the software development team

Question 424

An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

- ☐ ensure that security processes are consistent across the organization.
- ☐ enforce baseline security levels across the organization.
- ☐ ensure that security processes are fully documented.
- ☐ implement monitoring of key performance indicators for security processes.

Licensed to Berend Post berend.post@it-university.nl

Question 425

Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

- ☐ Configuration of firewalls
- ☐ Strength of encryption algorithms
- ☐ Authentication within application
- ☐ Safeguards over keys

Question 426

Which of the following measures would be MOST effective against insider threats to confidential information?

- ☐ Role-based access control
- ☐ Audit trail monitoring
- ☐ Privacy policy
- ☐ Defense-in-depth

Question 427

The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

- ☐ change the root password of the system.
- ☐ implement multifactor authentication.
- ☐ rebuild the system from the original installation medium.
- ☐ disconnect the mail server from the network.

Question 428

What is the BEST way to ensure users comply with organizational security requirements for password complexity?

- ☐ Include password construction requirements in the security standards
- ☐ Require each user to acknowledge the password requirements
- ☐ Implement strict penalties for user noncompliance
- ☐ Enable system-enforced password configuration

Licensed to Berend Post berend.post@it-university.nl

Question 429

What is the MOST important item to be included in an information security policy?

- ☐ The definition of roles and responsibilities
- ☐ The scope of the security program
- ☐ The key objectives of the security program
- ☐ Reference to procedures and standards of the security program

Question 430

Which of the following is the BEST approach to make strategic information security decisions?

- ☐ Establish an information security steering committee.
- ☐ Establish periodic senior management meetings.
- ☐ Establish regular information security status reporting.
- ☐ Establish business unit security working groups.

Question 431

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain any effective information security program?

- ☐ Ensure information security is included in any change control efforts
- ☐ Merge the two information security programs to establish continuity
- ☐ Determine new factors that could influence the information security strategy
- ☐ Implement the current information security program in the acquired company

Question 432

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

- ☐ Proficiency test
- ☐ Job descriptions
- ☐ Organization chart
- ☐ Skills inventory

Licensed to Berend Post berend.post@it-university.nl

Question 433

A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

- ☐ an effective control over connectivity and continuity.
- ☐ a service level agreement (SLA) including code escrow.
- ☐ a business impact analysis (BIA).
- ☐ a third-party certification.

Question 434

After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

- ☐ Senior management
- ☐ Business manager
- ☐ IT audit manager
- ☐ Information security officer (ISO)

Question 435

What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

- ☐ Provide detailed instructions on how to carry out different types of tasks
- ☐ Ensure consistency of activities to provide a more stable environment
- ☐ Ensure compliance to security standards and regulatory requirements
- ☐ Ensure reusability to meet compliance to quality requirements

Question 436

Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

- ☐ Manager
- ☐ Custodian
- ☐ User
- ☐ Owner

Licensed to Berend Post berend.post@it-university.nl

Question 437

What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

- ☐ all use weak encryption.
- ☐ are decrypted by the firewall.
- ☐ may be quarantined by mail filters.
- ☐ may be corrupted by the receiving mail server.

Question 438

Which of the following is the BEST defense against distributed denial of service (DDoS) attacks?

- ☐ Multiple and redundant paths
- ☐ Well-configured routers and firewalls
- ☐ Regular patching
- ☐ Intruder-detection lockout

Question 439

Which of (lie following would be the MOST relevant factor when defining the information classification policy?

- ☐ Quantity of information
- ☐ Available IT infrastructure
- ☐ Benchmarking
- ☐ Requirements of data owners

Question 440

Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?

- ☐ Data ownership
- ☐ Data monitoring
- ☐ Data custodian
- ☐ Data encryption

Question 441

The MOST effective way to incorporate risk management practices into existing production systems is through:

- ☐ policy development.
- ☐ change management.
- ☐ awareness training.
- ☐ regular monitoring.

Licensed to Berend Post berend.post@it-university.nl

Question 442

Which of the following should be PRIMARILY included in a security training program for business process owners?

- ☐ Impact of security risks
- ☐ Application vulnerabilities
- ☐ Application recovery time
- ☐ List of security incidents reported

Question 443

When a significant security breach occurs, what should be reported FIRST to senior management?

- ☐ A summary of the security logs that illustrates the sequence of events
- ☐ An explanation of the incident and corrective action taken
- ☐ An analysis of the impact of similar attacks at other organizations
- ☐ A business case for implementing stronger logical access controls

Question 444

Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

- ☐ Log all account usage and send it to their manager
- ☐ Establish predetermined automatic expiration dates
- ☐ Require managers to e-mail security when the user leaves
- ☐ Ensure each individual has signed a security acknowledgement

Question 445

Which of the following is MOST important for an information security manager to regularly report to senior management?

- ☐ Results of penetration tests
- ☐ Audit reports
- ☐ Impact of unremediated risks
- ☐ Threat analysis reports

Licensed to Berend Post berend.post@it-university.nl

Question 446

In the process of deploying a new e-mail 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 e-mail system implementation?

- ☐ Encryption
- ☐ Digital certificate
- ☐ Digital signature
- ☐ I lashing algorithm

Question 447

The valuation of IT assets should be performed by:

- ☐ an IT security manager.
- ☐ an independent security consultant.
- ☐ the chief financial officer (CFO).
- ☐ the information owner.

Question 448

The PRIMARY reason for using information security metrics is to:

- ☐ achieve senior management commitment.
- ☐ ensure alignment with corporate requirements.
- ☐ adhere to legal and regulatory requirements.
- ☐ monitor the effectiveness of controls.

Question 449

Which of the following is the BEST justification to convince management to invest in an information security program?

- ☐ Cost reduction
- ☐ Compliance with company policies
- ☐ Protection of business assets
- ☐ Increased business value

Question 450

In an organization, information systems security is the responsibility of:

- ☐ all personnel.
- ☐ information systems personnel.
- ☐ information systems security personnel.
- ☐ functional personnel.

Licensed to Berend Post berend.post@it-university.nl

Question 451

An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following would be MOST important to include in the business case?

- ☐ Business impact if threats materialize
- ☐ Availability of unused funds in the security budget
- ☐ Threat information from reputable sources
- ☐ Alignment of the new initiative with the approved business strategy

Question 452

Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

- ☐ Security audit reports
- ☐ Balanced scorecard
- ☐ Capability maturity model (CMM)
- ☐ Systems and business security architecture

Question 453

What is the BEST way to alleviate security team understaffing while retaining the capability in-house?

- ☐ Hire a contractor that would not be included in the permanent headcount
- ☐ Outsource with a security services provider while retaining the control internally
- ☐ Establish a virtual security team from competent employees across the company
- ☐ Provide cross training to minimize the existing resources gap

Question 454

Which of the following is MOST important for measuring the effectiveness of a security awareness program?

- ☐ Reduced number of security violation reports
- ☐ A quantitative evaluation to ensure user comprehension
- ☐ Increased interest in focus groups on security issues
- ☐ Increased number of security violation reports

Licensed to Berend Post berend.post@it-university.nl

Question 455

The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

- ☐ ensure the confidentiality of sensitive material.
- ☐ provide a high assurance of identity.
- ☐ allow deployment of the active directory.
- ☐ implement secure sockets layer (SSL) encryption.

Question 456

When residual risk is minimized:

- ☐ acceptable risk is probable.
- ☐ transferred risk is acceptable.
- ☐ control risk is reduced.
- ☐ risk is transferable.

Question 457

Which would be the BEST recommendation to protect against phishing attacks?

- ☐ Install an antispam system
- ☐ Publish security guidance for customers
- ☐ Provide security awareness to the organization's staff
- ☐ Install an application-level firewall

Question 458

The BEST way to mitirate the risk associated with a social engineering attack is to:

- ☐ deploy an effective intrusion detection system (IDS).
- ☐ perform a business risk assessment of the email filtering system.
- ☐ implement multi-factor authentication on critical business systems.
- ☐ perform a user-knowledge gap assessment of information security practices.

Question 459

A global organization has developed a strategy to share a customer information database between offices in two countries. In this situation, it is MOST important to ensure:

- ☐ data sharing complies with local laws and regulations at both locations.
- ☐ data is encrypted in transit and at rest.
- ☐ a nondisclosure agreement is signed.
- ☐ risk coverage is split between the two locations sharing data.

Licensed to Berend Post berend.post@it-university.nl

Question 460

Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

- ☐ The activities being monitored deviate from what is considered normal.
- ☐ The information regarding monitored activities becomes stale.
- ☐ The pattern of normal behavior changes quickly and dramatically.
- ☐ The environment is complex.

Question 461

Which of the following tasks should be performed once a disaster recovery plan has been developed?

- ☐ Analyze the business impact
- ☐ Define response team roles
- ☐ Develop the test plan
- ☐ Identify recovery time objectives

Question 462

Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

- ☐ Security compliant servers trend report
- ☐ Percentage of security compliant servers
- ☐ Number of security patches applied
- ☐ Security patches applied trend report

Question 463

Which of the following is MOST effective in protecting against the attack technique known as phishing?

- ☐ Firewall blocking rules
- ☐ Up-to-date signature files
- ☐ Security awareness training
- ☐ Intrusion detection monitoring

Licensed to Berend Post berend.post@it-university.nl

Question 464

What would be the MOST significant security risks when using wireless local area network (LAN) technology?

- ☐ Man-in-the-middle attack
- ☐ Spoofing of data packets
- ☐ Rogue access point
- ☐ Session hijacking

Question 465

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

- ☐ Regular password audits
- ☐ Single sign-on system
- ☐ Security awareness program
- ☐ Penalties for noncompliance

Question 466

The MOST important objective of a post incident review is to:

- ☐ capture lessons learned to improve the process.
- ☐ develop a process for continuous improvement.
- ☐ develop a business case for the security program budget.
- ☐ identify new incident management tools.

Question 467

For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

- ☐ Biometrics
- ☐ Symmetric encryption keys
- ☐ Secure Sockets Layer (SSL)-based authentication
- ☐ Two-factor authentication

Licensed to Berend Post berend.post@it-university.nl

Question 468

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?

- ☐ Multilevel
- ☐ Role-based
- ☐ Discretionary
- ☐ Attribute-based

Question 469

Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

- ☐ Encrypting first by receiver's private key and second by sender's public key
- ☐ Encrypting first by sender's private key and second by receiver's public key
- ☐ Encrypting first by sender's private key and second decrypting by sender's public key
- ☐ Encrypting first by sender's public key and second by receiver's private key

Licensed to Berend Post berend.post@it-university.nl