A. ensure the provider is made liable for losses.
B. recommend not renewing the contract upon expiration.
C. recommend the immediate termination of the contract.
D. determine the current level of security.

Correct Answer: D
Explanation:
It is important to ensure that adequate levels of protection are written into service level agreements (SLAs) and other outsourcing contracts. Information must be obtained from providers to determine how that outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

QUESTION 250
Information security managers should use risk assessment techniques to:

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

Correct Answer: A
Explanation:
Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.

QUESTION 251
Which of the following BEST indicates a successful risk management practice?

A. Overall risk is quantified
B. Inherent risk is eliminated
C. Residual risk is minimized
D. Control risk is tied to business units

Correct Answer: C
Explanation:
A successful risk management practice minimizes the residual risk to the organization. Choice A is incorrect because the fact that overall risk has been quantified does not necessarily indicate the existence of a successful risk management practice. Choice B is incorrect since it is virtually impossible to eliminate inherent risk. Choice D is incorrect because, although the tying of control risks to business may improve accountability, this is not as desirable as minimizing residual risk.

QUESTION 252
A risk mitigation report would include recommendations for:

A. assessment.
B. acceptance
C. evaluation.
D. quantification.

Correct Answer: B

Explanation:
Acceptance of a risk is an alternative to be considered in the risk mitigation process. Assessment. evaluation and risk quantification are components of the risk analysis process that are completed prior to determining risk mitigation solutions.

QUESTION 253
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:

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

Correct Answer: C
Explanation:
An organization may decide to live with specific risks because it would cost more to protect themselves than the value of the potential loss. The safeguards need to match the risk level. While countermeasures could be too complicated to deploy, this is not the most compelling reason. It is unlikely that a global financial institution would not be exposed to such attacks and the frequency could not be predicted.

QUESTION 254
An information security manager is advised by contacts in law enforcement that there is evidence that his/ her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

A. perform a comprehensive assessment of the organization's exposure to the hacker's techniques.
B. initiate awareness training to counter social engineering.
C. immediately advise senior management of the elevated risk.
D. increase monitoring activities to provide early detection of intrusion.

Correct Answer: C
Explanation:
Information about possible significant new risks from credible sources should be provided to management along with advice on steps that need to be taken to counter the threat. The security manager should assess the risk, but senior management should be immediately advised. It may be prudent to initiate an awareness campaign subsequent to sounding the alarm if awareness training is not current. Monitoring activities should also be increased.

QUESTION 255
Which of the following is MOST essential for a risk management program to be effective?

A. Flexible security budget
B. Sound risk baseline
C. New risks detection
D. Accurate risk reporting

Correct Answer: C
Explanation:

All of these procedures are essential for implementing risk management. However, without identifying new risks, other procedures will only be useful for a limited period.

QUESTION 256
What is the BEST technique to determine which security controls to implement with a limited budget?

A. Risk analysis
B. Annualized loss expectancy (ALE) calculations
C. Cost-benefit analysis
D. Impact analysis

Correct Answer: C
Explanation:
Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh it's benefit and that the best safeguard is provided for the cost of implementation. Risk analysis identifies the risks and suggests appropriate mitigation. The annualized loss expectancy (ALE) is a subset of a cost-benefit analysis. Impact analysis would indicate how much could be lost if a specific threat occurred.

QUESTION 257
Which program element should be implemented FIRST in asset classification and control?

A. Risk assessment
B. Classification
C. Valuation
D. Risk mitigation

Correct Answer: C
Explanation:
Valuation is performed first to identify and understand the assets needing protection. Risk assessment is performed to identify and quantify threats to information assets that are selected by the first step, valuation. Classification and risk mitigation are steps following valuation.

QUESTION 258
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

A. Business continuity coordinator
B. Chief operations officer (COO)
C. Information security manager
D. Internal audit

Correct Answer: B
Explanation:
The recovery point objective (RPO) is the processing checkpoint to which systems are recovered. In addition to data owners, the chief operations officer (COO) is the most knowledgeable person to make this decision. It would be inappropriate for the information security manager or an internal audit to determine the RPO because they are not directly responsible for the data or the operation.

QUESTION 259

The BEST strategy for risk management is to:

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

Correct Answer: B
Explanation:
The best strategy for risk management is to reduce risk to an acceptable level, as this will take into account the organization's appetite for risk and the fact that it would not be practical to eliminate all risk. Achieving balance between risk and organizational goals is not always practical. Policy development must consider organizational risks as well as business objectives. It may be prudent to ensure that management understands and accepts risks that it is not willing to mitigate, but that is a practice and is not sufficient to l>e considered a strategy.

QUESTION 260
The valuation of IT assets should be performed by:

A. an IT security manager.
B. an independent security consultant.
C. the chief financial officer (CFO).
D. the information owner.

Correct Answer: D
Explanation:
Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep knowledge of the business processes and of the functional IT requirements. An IT security manager is an expert of the IT risk assessment methodology and IT asset valuation mechanisms. However, the manager could not have a deep understanding of all the business processes of the firm. An IT security subject matter expert will take part of the process to identify threats and vulnerabilities and will collaborate with the business information asset owner to define the risk profile of the asset. A chief financial officer (CFO) will have an overall costs picture but not detailed enough to evaluate the value of each IT asset.

QUESTION 261
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?

A. Implement countermeasures.
B. Eliminate the risk.
C. Transfer the risk.
D. Accept the risk.

Correct Answer: C
Explanation:
Risks are typically transferred to insurance companies when the probability of an incident is low but the impact is high. Examples include: hurricanes, tornados and earthquakes. Implementing countermeasures may not be the most cost-effective approach to security management.

Eliminating the risk may not be possible. Accepting the risk would leave the organization vulnerable to a catastrophic disaster which may cripple or ruin the organization. It would be more cost effective to pay recurring insurance costs than to be affected by a disaster from which the organization cannot financially recover.

QUESTION 262
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:

A. transferred.
B. treated.
C. accepted.
D. terminated.

Correct Answer: C
Explanation:
When the cost of control is more than the cost of the risk, the risk should be accepted. Transferring, treating or terminating the risk is of limited benefit if the cost of that control is more than the cost of the risk itself.

QUESTION 263
For risk management purposes, the value of an asset should be based on:

A. original cost.
B. net cash flow.
C. net present value.
D. replacement cost.

Correct Answer: D
Explanation:
The value of a physical asset should be based on its replacement cost since this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

QUESTION 264
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

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

Correct Answer: B
Explanation:
Identifying the relevant systems and processes is the best first step. Developing an operational plan for achieving compliance with the legislation is incorrect because it is not the first step. Restricting the collection of personal information comes later. Identifying privacy legislation in other countries would not add much value.