CHAPTER

Information Security and Risk Management

This domain includes questions from the following topics:

- Security management responsibilities
- Difference between administrative, technical, and physical controls
- Three main security principles
- Risk management and risk analysis
- Security policies
- Information classification
- Security-awareness training

A security professional's responsibilities extend well beyond reacting to the virus and hacker news that make headlines. Their day-to-day responsibilities are far less exciting on the surface but are vital to keeping organizations protected against intrusions so that their companies don't become the next headline. The role of security within an organization is a complex one, as it touches every employee and must be managed companywide. It is important that you have an understanding of security beyond the technical details to include management and business issues, both for the CISSP exam and for your role in the field.

QUESTIONS

1. Which of the following best describes the relationship between CobiT and ITIL?

   A. CobiT is a model for IT governance, whereas ITIL is a model for corporate governance.

   B. CobiT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.

   C. CobiT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.

   D. CobiT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals.

2. Jane has been charged with ensuring that clients' personal health information is adequately protected before it is exchanged with a new European partner. What data security requirements must she adhere to?

   A. HIPAA

   B. NIST SP 800-66

   C. Safe Harbor

   D. European Union Principles on Privacy

3. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?

   A. Committee of Sponsoring Organizations of the Treadway Commission

   B. The Organisation for Economic Co-operation and Development

   C. CobiT

   D. International Organization for Standardization

4. Steve, a department manager, has been asked to join a committee that is responsible for defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What committee is he joining?

   A. Security policy committee

   B. Audit committee

   C. Risk management committee

   D. Security steering committee

5. As head of sales, Jim is the information owner for the sales department. Which of the following is not Jim's responsibility as information owner?

A. Assigning information classifications

B. Dictating how data should be protected

C. Verifying the availability of data

D. Determining how long to retain data

6. Assigning data classification levels can help with all of the following except:

A. The grouping of classified information with hierarchical and restrictive security

B. Ensuring that nonsensitive data is not being protected by unnecessary controls

C. Extracting data from a database

D. Lowering the costs of protecting data

7. Which of the following is not included in a risk assessment?

A. Discontinuing activities that introduce risk

B. Identifying assets

C. Identifying threats

D. Analyzing risk in order of cost or criticality

8. Sue has been tasked with implementing a number of security controls, including antivirus and antispam software, to protect the company's e-mail system. What type of approach is her company taking to handle the risk posed by the system?

A. Risk mitigation

B. Risk acceptance

C. Risk avoidance

D. Risk transference

9. The integrity of data is not related to which of the following?

A. Unauthorized manipulation or changes to data

B. The modification of data without authorization

C. The intentional or accidental substitution of data

D. The extraction of data to share with unauthorized entities

10. There are several methods an intruder can use to gain access to company assets. Which of the following best describes masquerading?

A. Changing an IP packet's source address

B. Elevating privileges to gain access

C. An attempt to gain unauthorized access as another user

D. Creating a new authorized user with hacking tools

11. A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?

    A. The asset's value in the external marketplace

    B. The level of insurance required to cover the asset

    C. The initial and outgoing costs of purchasing, licensing, and supporting the asset

    D. The asset's value to the organization's production operations

12. Jill is establishing a companywide sales program that will require different user groups with different privileges to access information on a centralized database. How should the security manager secure the database?

    A. Increase the database's security controls and provide more granularity.

    B. Implement access controls that display each user's permissions each time they access the database.

    C. Change the database's classification label to a higher security status.

    D. Decrease the security so that all users can access the information as needed.

13. As his company's CISO, George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?

    A. threats × vulnerability × asset value = residual risk

    B. SLE × frequency = ALE, which is equal to residual risk

    C. (threats × asset value × vulnerability) × control gap = residual risk

    D. (total risk – asset value) × countermeasures = residual risk

14. Authorization creep is to access controls what scope creep is to software development. Which of the following is not true of authorization creep?

    A. Users have a tendency to request additional permissions without asking for others to be taken away.

    B. It is a violation of "least privilege."

    C. It enforces the "need-to-know" concept.

    D. It commonly occurs when users transfer to other departments or change positions.

15. For what purpose was the COSO framework developed?

    A. To address fraudulent financial activities and reporting

    B. To help organizations install, implement, and maintain CobiT controls

C. To serve as a guideline for IT security auditors to use when verifying compliance

D. To address regulatory requirements related to protecting private health information

16. Susan, an attorney, has been hired to fill a new position at Widgets Inc. The position is Chief Privacy Officer (CPO). What is the primary function of her new role?

A. Ensuring the protection of partner data

B. Ensuring the accuracy and protection of company financial information

C. Ensuring that security policies are defined and enforced

D. Ensuring the protection of customer, company, and employee data

17. Jared plays a role in his company's data classification system. In this role, he must practice due care when accessing data and ensure that the data is used only in accordance with allowed policy while abiding by the rules set for the classification of the data. He does not determine, maintain, or evaluate controls, so what is Jared's role?

A. Data owner

B. Data custodian

C. Data user

D. Information systems auditor

18. Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?

A. FAP

B. OCTAVE

C. ANZ 4360

D. NIST SP 800-30

19. Which of the following is not a characteristic of a company with a security governance program in place?

A. Board members are updated quarterly on the company's state of security.

B. All security activity takes place within the security department.

C. Security products, services, and consultants are deployed in an informed manner.

D. The organization has established metrics and goals for improving security.

20. Michael is charged with developing a classification program for his company. Which of the following should he do first?

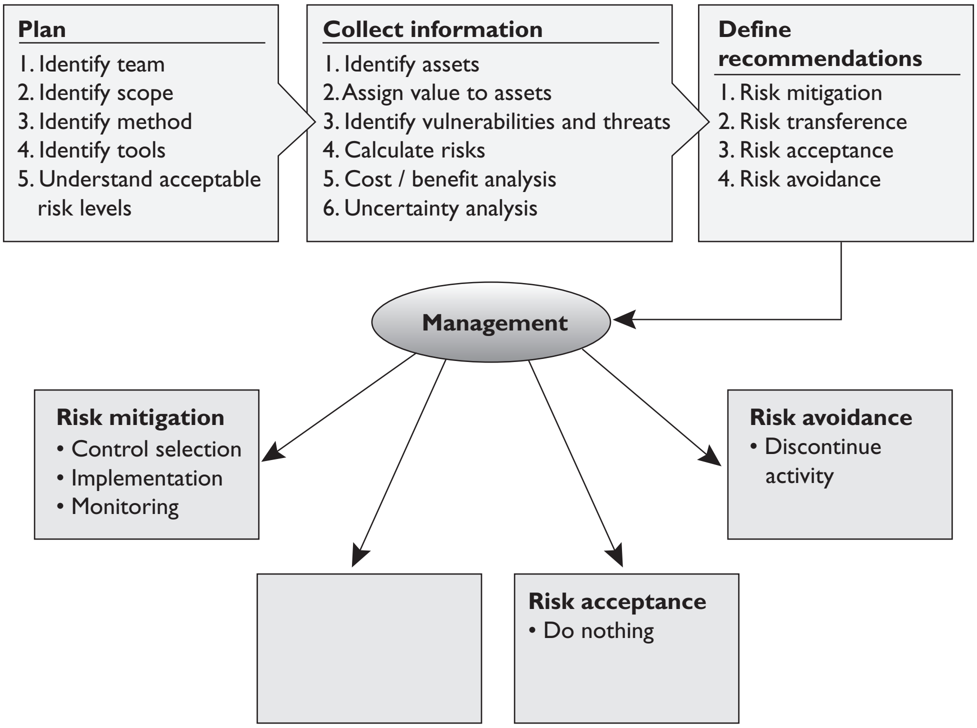
    A. Understand the different levels of protection that must be provided.

    B. Specify data classification criteria.

    C. Identify the data custodians.

    D. Determine protection mechanisms for each classification level.

21. There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?



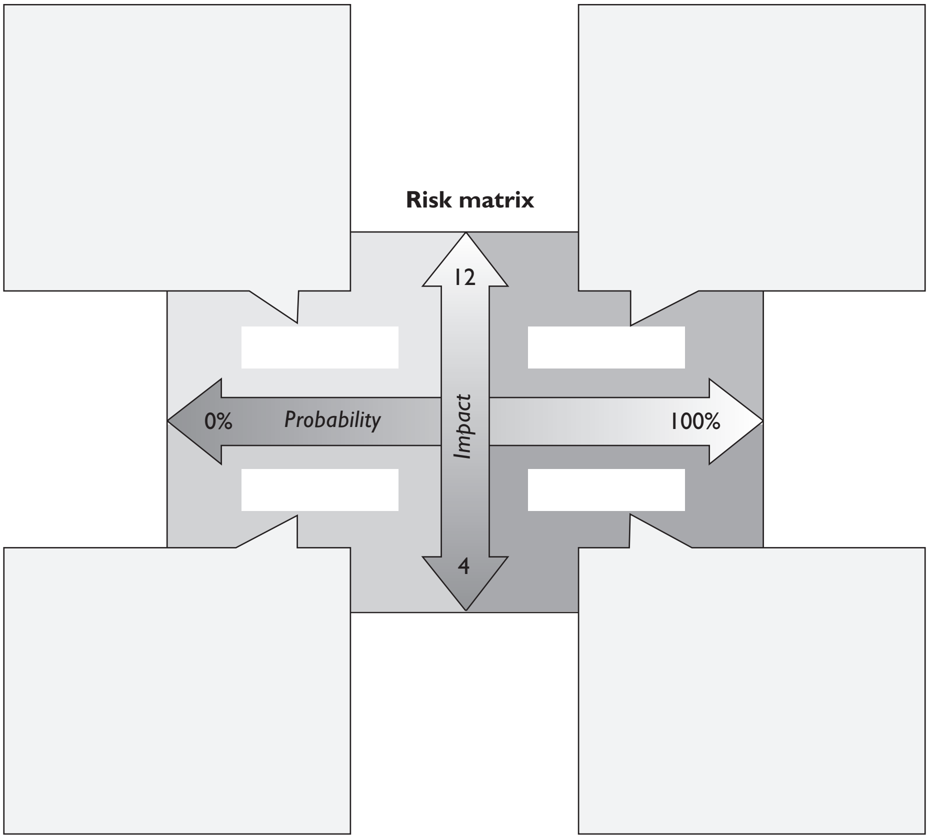
A. Risk transference. Share the risk with other entities.

B. Risk reduction. Reduce the risk to an acceptable level.

C. Risk rejection. Accept the current risk.

D. Risk assignment. Assign risk to a specific owner.

22. The following graphic contains a commonly used risk management scorecard. Identify the proper quadrant and its description.



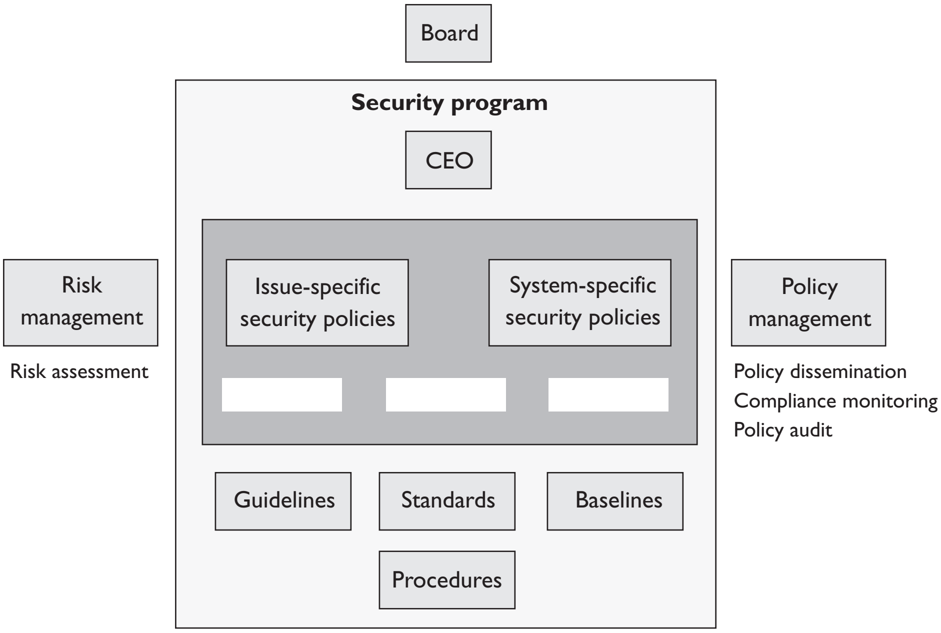
A. Top-right quadrant is high impact, low probability.

B. Top-left quadrant is high impact, medium probability.

C. Bottom-left quadrant is low impact, high probability.

D. Bottom-right quadrant is low impact, high probability.

23. What are the three types of policies that are missing from the following graphic?



A. Regulatory, Informative, Advisory

B. Regulatory, Mandatory, Advisory

C. Regulatory, Informative, Public

D. Regulatory, Informative, Internal Use

24. List in the proper order from the table on the top of the next page the learning objectives that are missing and their proper definitions.

A. Understanding, recognition and retention, skill

B. Skill, recognition and retention, skill

C. Recognition and retention, skill, understanding

D. Skill, recognition and retention, understanding

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning objective:			
Example teaching method:	**Media** • Videos • Newsletters • Posters	**Practical instruction** • Lecture and/or demo • Case study • Hands-on practice	**Theoretical instruction** • Seminar and discussion • Reading and study • Research
Test measure:	True/False Mutiple choice (Identify learning)	Problem solving, i.e., recognition and resolution (Apply learning)	Essay (Interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

25. What type of risk analysis approach does the following graphic provide?

High	7–10	7–10
Medium	4–6	4–6
Low	0–3	0–3

0	10	20	30	40	50	60	70	80	90	100
0	9	18	27	36	45	54	63	72	81	90
0	8	16	24	32	40	48	56	64	72	80
0	7	14	21	28	35	42	49	56	63	70
0	6	12	18	24	30	36	42	48	54	60
0	5	10	15	20	25	30	35	40	45	50
0	4	8	12	16	20	24	28	32	36	40
0	3	6	9	12	15	18	21	24	27	30
0	2	4	6	8	10	12	14	16	18	20
0	1	2	3	4	5	6	7	8	9	10

41–100	High
20–40	Medium
0–19	Low

A. Quantitative

B. Qualitative

C. Operationally Correct

D. Operationally Critical

QUICK ANSWER KEY

1. C
2. C
3. B
4. D
5. C
6. C
7. A
8. A
9. D
10. C
11. B
12. A
13. C
14. C
15. A
16. D
17. C
18. C
19. B
20. A
21. A
22. D
23. A
24. C
25. B

1. Which of the following best describes the relationship between CobiT and ITIL?

   A. CobiT is a model for IT governance, whereas ITIL is a model for corporate governance.

   B. CobiT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.

   C. CobiT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.

   D. CobiT provides a framework for achieving security goals, whereas ITIL defines a framework for achieving IT service-level goals.

   ☑ **C.** The Control Objectives for Information and related Technology (CobiT) is a framework developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and ensure IT maps to business needs, not specifically just security needs. The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. A customizable framework, ITIL provides the goals, the general activities necessary to achieve these goals, and the input and output values for each process required to meet these determined goals. In essence, CobiT addresses "what is to be achieved," while ITIL addresses "how to achieve it."

   ☒ **A** is incorrect because, while CobiT can be used as a model for IT governance, ITIL is not a model for corporate governance. Actually, Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a model for corporate governance. CobiT is derived from the COSO framework. You can think of CobiT as a way to meet many of the COSO objectives, but only from the IT perspective. In order to achieve many of the objectives addressed in CobiT, an organization can use ITIL, which provides process-level steps for achieving IT service management objectives.

   ☒ **B** is incorrect because, as previously stated, CobiT can be used as a model for IT governance, not corporate governance. COSO is a model for corporate governance. The second half of the answer is correct. ITIL is a customizable framework that is available as a series of books or online, for IT service management.

   ☒ **D** is incorrect because CobiT defines goals for the controls that should be used to properly manage IT and ensure IT maps to business needs, not just IT security needs. ITIL provides steps for achieving IT service management goals as they relate to business needs. ITIL was created because of the increased dependence on information technology to meet business needs.

2. Jane has been charged with ensuring that clients' personal health information is adequately protected before it is exchanged with a new European partner. What data security requirements must she adhere to?

   A. HIPAA

   B. NIST SP 800-66

   C. Safe Harbor

   D. European Union Principles on Privacy

   ☑ **C.** The Safe Harbor requirements were created to harmonize the data privacy practices of the U.S. with the European Union's stricter privacy controls, and to prevent accidental information disclosure and loss. The framework outlines how any entity that is going to move private data to and from Europe must go about protecting it. By certifying against this rule base, U.S. companies that work with European entities can more quickly and easily transfer data.

   ☒ **A** is incorrect because the Health Insurance Portability and Accountability Act (HIPAA) does not specifically address data protection for the purposes of sharing it with European entities. HIPAA provides a framework and guidelines to ensure security, integrity, and privacy when handling confidential medical information within the U.S. The U.S. federal regulation also outlines how security should be managed for any facility that creates, accesses, shares, or destroys medical information.

   ☒ **B** is incorrect because NIST SP 800-66 is a risk assessment methodology. It does not point out specific data privacy requirements. NIST SP 800-66 does apply to health care. It was originally designed to be implemented in the health care field and can be used by HIPAA clients to help achieve compliance.

   ☒ **D** is incorrect because the European Union Principles on Privacy are the foundation for the European Union's strict laws pertaining to data that is considered private. The purpose of the principles is not to prepare data specifically for its exchange with U.S. companies, nor are the requirements mandated for U.S. companies. This set of principles has six areas that address using and transmitting sensitive information, and all European states must abide by these principles to be in compliance.

3. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?

A. Committee of Sponsoring Organizations of the Treadway Commission

B. The Organisation for Economic Co-operation and Development

C. CobiT

D. International Organization for Standardization

☑ **B.** Almost every country has its own rules pertaining to what constitutes private data and how it should be protected. As the digital and information age came upon us, these different laws started to negatively affect business and international trade. Thus, the Organisation for Economic Co-operation and Development (OECD) developed guidelines for various countries so that data is properly protected and everyone follows the same rules.

☒ **A** is incorrect because the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 to provide sponsorship for the National Commission on Fraudulent Financial Reporting, an organization that studies deceptive financial reports and what elements lead to them. The acronym COSO refers to a model for corporate governance that addresses IT at a strategic level, company culture, financial accounting principles, and more.

☒ **C** is incorrect because the Control Objectives for Information and related Technology (CobiT) is a framework that defines goals for the controls that should be used to properly manage IT and ensure that IT maps to business needs. It is an international open standard that provides requirements for the control and security of sensitive data and a reference framework.

☒ **D** is incorrect because the International Organization for Standardization (ISO) is an international standard-setting body consisting of representatives from national standards organizations. Its objective is to establish global standardizations. However, its standardizations go beyond the privacy of data as it travels across international borders. For example, some standards address quality control, while others address assurance and security.

4. Steve, a department manager, has been asked to join a committee that is responsible for defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What committee is he joining?

A. Security policy committee

B. Audit committee

C. Risk management committee

D. Security steering committee

☑ **D.** Steve is joining a security steering committee, which is responsible for making decisions on tactical and strategic security issues within the enterprise. The committee should consist of individuals from throughout the organization and meet at least quarterly. In addition to the responsibilities listed in the question, the security steering committee is responsible for establishing a clearly defined vision statement that works with and supports the organizational intent of the business. It should provide support for the goals of confidentiality, integrity, and availability as they pertain to the organization's business objectives. This vision statement should, in turn, be supported by a mission statement that provides support and definition to the processes that will apply to the organization and allow it to reach its business goals.

☒ **A** is incorrect because a security policy committee is a committee chosen by senior management to produce security policies. Usually senior management has this responsibility unless they delegate it to a board or committee. Security policies dictate the role that security plays within the organization. They can be organizational, issue-specific, or system-specific. The steering committee does not directly create policies but reviews and approves them if acceptable.

☒ **B** is incorrect because the audit committee's goal is to provide independent and open communications among the board of directors, management, internal auditors, and external auditors. Its responsibilities include the company's system of internal controls, the engagement and performance of independent auditors, and the performance of the internal audit function. The audit committee would report its findings to the steering committee, but not be responsible for overseeing and approving any part of a security program.

☒ **C** is incorrect because the purpose of a risk management committee is to understand the risks that the organization faces as a whole and work with senior management to reduce these risks to acceptable levels. This committee does not oversee the security program. The security steering committee usually reports its findings to the risk management committee as it relates to information security. A risk management committee must look at overall business risks, not just IT security risks.

5. As head of sales, Jim is the information owner for the sales department. Which of the following is not Jim's responsibility as information owner?

A. Assigning information classifications

B. Dictating how data should be protected

C. Verifying the availability of data

D. Determining how long to retain data

☑ **C.** The responsibility of verifying the availability of data is the only responsibility listed that does not belong to the information owner. Rather, it is the responsibility of the information custodian. The information custodian is also responsible for maintaining and protecting data as dictated by the information owner. This includes performing regular backups of data, restoring data from backup media, retaining records of activity, and fulfilling information security and data protection requirements in the company's policies, guidelines, and standards. Information owners work at a higher level than the custodians. The owners basically state, "This is the level of integrity, availability, and confidentiality that needs to be provided—now go do it." The custodian must then carry out these mandates and follow up with the installed controls to make sure they are working properly.

☒ **A** is incorrect because as information owner Jim is responsible for assigning information classifications. (The question asked which of the following Jim is not responsible for.)

☒ **B** is incorrect because information owners such as Jim are responsible for dictating how information should be protected. The information owner has the organizational responsibility for data protection and is liable for any negligence when it comes to protecting the organization's information assets. This means that Jim must make decisions regarding how information is protected and ensure that the information custodian (a role usually filled by IT or security) is carrying out these decisions.

☒ **D** is incorrect because determining how long to retain data is the responsibility of the information owner. The information owner is also responsible for determining who can access the information and ensuring that proper access rights are being used. He can approve access requests himself or delegate the function to business unit managers, who will approve requests based on user access criteria defined by the information owner.

6. Assigning data classification levels can help with all of the following except:

A. The grouping of classified information with hierarchical and restrictive security

B. Ensuring that nonsensitive data is not being protected by unnecessary controls

C. Extracting data from a database

D. Lowering the costs of protecting data

☑ **C.** Data classification does not involve the extraction of data from a database. However, data classification can be used to dictate who has access to read and write data that is stored in a database. Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed. For example, in a corporation, confidential information may only be accessed by senior management. Auditing could be very detailed and its results monitored daily, and degaussing or zeroization procedures may be required to erase the data. On the other hand, information classified as public may be accessed by all employees, and no special auditing or destruction methods required.

☒ **A** is incorrect because assigning data classification levels can help with the grouping of classified information with hierarchical and restrictive security. Data that shares the same classification, for example, can be grouped together and assigned the same handling requirements and procedures pertaining to how it is accessed, used, and destroyed.

☒ **B** is incorrect because assigning data classification levels can help ensure that nonsensitive data is being protected by the necessary controls. Data classification directly deals with ensuring that the different levels of sensitive data are being protected by the necessary controls. This answer is very tricky because of all the negatives, so make sure to read questions and answers slowly.

☒ **D** is incorrect because data classification helps ensure data is protected in the most cost-effective manner. Protecting and maintaining data costs money, but it is important to spend this money for the information that actually requires protection. For example, data that is classified confidential may require additional access controls as compared to public data to restrict access. It may also require additional auditing and monitoring. This may be appropriate for a soda company's proprietary recipe, but it would be a waste of resources if those same measures were implemented for the soda company's employee directory.

7. Which of the following is not included in a risk assessment?

A. Discontinuing activities that introduce risk

B. Identifying assets

C. Identifying threats

D. Analyzing risk in order of cost or criticality

☑ **A.** Discontinuing activities that introduce risk is a way of responding to risk through avoidance. For example, there are many risks surrounding the use of instant messaging (IM) in the enterprise. If a company decides not to allow IM activity because there is not enough business need for its use, then prohibiting this service is an example of risk avoidance. Risk assessment does not include the implementation of countermeasures such as this.

☒ **B** is incorrect because identifying assets is part of a risk assessment, and the question asks to identify what is not included in a risk assessment. In order to determine the value of assets, those assets must first be identified. Asset identification and valuation are also important tasks of risk management.

☒ **C** is incorrect because identifying threats is part of a risk assessment, and the question asks to identify what is not included in a risk assessment. Risk is present because of the possibility of a threat exploiting a vulnerability. If there were no threats, there would be no risk. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

☒ **D** is incorrect because analyzing risk in order of cost or criticality is part of the risk assessment process, and the question asks to identify what is not included in a risk assessment. A risk assessment researches and quantifies the risk a company faces. Dealing with risk must be done in a cost-effective manner. Knowing the severity of the risk allows the organization to determine how to address it effectively.

8. Sue has been tasked with implementing a number of security controls, including antivirus and antispam software, to protect the company's e-mail system. What type of approach is her company taking to handle the risk posed by the system?

A. Risk mitigation

B. Risk acceptance

C. Risk avoidance

D. Risk transference

☑ **A.** Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it. By implementing security controls such as antivirus and antispam software, Sue is reducing the risk posed by her company's e-mail system. This is also referred to as risk mitigation, where the risk is decreased to a level considered acceptable. In addition to the use of IT security controls and countermeasures, risk can be mitigated by improving procedures, altering the environment, erecting barriers to the threat, and implementing early detection methods to stop threats as they occur, thereby reducing their possible damage.

☒ **B** is incorrect because risk acceptance does not involve spending money on protection or countermeasures, such as antivirus software. When accepting risk, the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to live with it without implementing countermeasures. Many companies accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value.

☒ **C** is incorrect because risk avoidance involves discontinuing the activity that is causing the risk, and in this case Sue's company has chosen to continue to use e-mail. A company may choose to terminate an activity that introduces risk if that risk outweighs the activity's business need. For example, a company may choose to block social media Web sites for some departments because of the risk they pose to employee productivity.

☒ **D** is incorrect because risk transference involves sharing the risks with another entity as in purchasing of insurance to transfer some of the risk to the insurance company. Many types of insurance are available to companies to protect their assets. If a company decides the total or residual risk is too high to gamble with, it can purchase insurance.

9. The integrity of data is not related to which of the following?

A. Unauthorized manipulation or changes to data

B. The modification of data without authorization

C. The intentional or accidental substitution of data

D. The extraction of data to share with unauthorized entities

☑ **D.** The extraction of data to share with unauthorized entities is a confidentiality issue, not an integrity issue. Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of confidentiality should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination. Integrity, on the other hand, is the principle that signifies the data has not been changed or manipulated in an unauthorized manner.

☒ **A** is incorrect because integrity is related to the unauthorized manipulation or changes to data. Integrity is upheld when any unauthorized modification is prevented. Hardware, software, and communication mechanisms must work in concert to maintain and process data correctly and move data to intended destinations without unexpected alteration. The systems and network should be protected from outside interference and contamination.

☒ **B** is incorrect because the modification of data without authorization is related to integrity. Integrity is about protecting data so that it cannot be changed either by users or other systems that do not have the rights to do so.

☒ **C** is incorrect because the intentional or accidental substitution of data is related to integrity. Along with the assurance that data is not modified by unauthorized entities, integrity is upheld when the assurance of the accuracy and reliability of the information and systems is provided. An environment that enforces integrity prevents attackers, for example, from inserting a virus, logic bomb, or backdoor into a system that could corrupt or replace data. Users usually affect a system or its data's integrity by mistake (although internal users may also commit malicious deeds). For example, a user may insert incorrect values into a data processing application that ends up charging a customer $3,000 instead of $300.

10. There are several methods an intruder can use to gain access to company assets. Which of the following best describes masquerading?

A. Changing an IP packet's source address

B. Elevating privileges to gain access

C. An attempt to gain unauthorized access as another user

D. Creating a new authorized user with hacking tools

☑ **C.** Masquerading is an attempt to gain unauthorized access by impersonating an authorized user. Masquerading is commonly used by attackers carrying out phishing attacks and has been around for a long time. For example, in 1996 hackers posed as AOL staff members and sent messages to victims asking for their passwords in order to verify correct billing information or verify information about the AOL accounts. Today, phishers often masquerade as large banking companies and well-known Internet entities like Amazon.com and eBay. Masquerading is a type of active attack because the attacker is actually doing something instead of sitting back and gathering data.

☒ **A** is incorrect because changing an IP packet's source address is an example of masquerading and not a definition of masquerading. IP spoofing is the act of presenting false information within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.

☒ **B** is incorrect because elevating privileges is not part of masquerading. Elevating privileges is often the next step after being able to penetrate a system successfully, but it does not have anything to do directly with fooling a user or system about the attacker's true identity.

☒ **D** is incorrect because masquerading involves commonly posing as an authorized user that already exists in the system the attacker is attempting to access. It is common for the attacker then to attempt to create a new authorized user account on a compromised system, but successful masquerading has to happen first.

11. A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?

A. The asset's value in the external marketplace

B. The level of insurance required to cover the asset

C. The initial and outgoing costs of purchasing, licensing, and supporting the asset

D. The asset's value to the organization's production operations

☑ **B.** The level of insurance required to cover the asset is not a consideration when assigning values to assets. It is actually the other way around: By knowing the value of an asset, an organization can more easily determine the level of insurance coverage to purchase for that asset. In fact, understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. This knowledge can also help companies perform effective cost/benefit analyses, understand exactly what is at risk, and comply with legal and regulatory requirements.

☒ **A** is incorrect because the asset's value in the external marketplace is a factor that should be considered when determining the value of an asset. It should also include the value the asset might have to competitors or what others are willing to pay for a given asset.

☒ **C** is incorrect because the initial and outgoing costs of purchasing, licensing, and supporting the asset are considerations when determining the cost and value of an asset. The asset must be cost-effective to the business directly. If the supporting requirements of maintaining the asset outweighs the business need for the asset, its value will decrease.

☒ **D** is incorrect because it is a factor to be considered when determining an asset's value. The asset's value to the organization's production operations is the determination of cost to an organization if the asset is not available for a certain period of time. Along these same lines, the asset's usefulness and role in the organization should be considered as well as the operational and production activities affected if the asset is unavailable. If the asset helps operations it is valuable; the trick is to figure out how valuable.

12. Jill is establishing a companywide sales program that will require different user groups with different privileges to access information on a centralized database. How should the security manager secure the database?

    A. Increase the database's security controls and provide more granularity.

    B. Implement access controls that display each user's permissions each time they access the database.

    C. Change the database's classification label to a higher security status.

    D. Decrease the security so that all users can access the information as needed.

    ☑ **A.** The best approach to securing the database in this situation would be to increase the controls and assign very granular permissions. These measures would ensure that users cannot abuse their privileges and the confidentiality of the information would be maintained. Granularity of permissions gives network administrators and security professionals additional control over the resources they are charged with protecting, and a fine level of detail enables them to give individuals just the precise level of access they need.

    ☒ **B** is incorrect because implementing access controls that display each user's permissions each time they access the database is an example of one control. It is not the overall way of dealing with user access to a full database of information. This may be an example of increasing database security controls, but it is only one example and more would need to be put into place.

    ☒ **C** is incorrect because the classification level of the information in the database was previously determined based on its confidentiality, integrity, and availability levels. These levels do not change simply because more users need access to the data. Thus, you would never increase or decrease the classification level of information when more users or groups need to access that information. Increasing the classification level would only mean a smaller subset of users could access the database.

    ☒ **D** is incorrect because it puts data at risk. If security is decreased so that all users can access it as needed, then users with lower privileges will be able to access data of higher classification levels. Lower security also makes it easier for intruders to break into the database. As stated in answer C, a classification level is not changed just because the number of users who need to access the data increases or decreases.

13. As his company's CISO, George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?

A. threats × vulnerability × asset value = residual risk

B. SLE × frequency = ALE, which is equal to residual risk

C. (threats × asset value × vulnerability) × control gap = residual risk

D. (total risk – asset value) × countermeasures = residual risk

☑ **C.** Countermeasures are implemented to reduce overall risk to an acceptable level. However, no system or environment is 100 percent secure, and with every countermeasure some risk remains. The leftover risk after countermeasures are implemented is called residual risk. Residual risk differs from total risk, which is the risk companies face when they choose not to implement any countermeasures. While the total risk can be determined by calculating threats × vulnerability × asset value = total risk, residual risk can be determined by calculating (threats × vulnerability × asset value) × control gap = residual risk. Control gap is the amount of protection the control cannot provide.

☒ **A** is incorrect because threats × vulnerability × asset value does not equal residual risk. It is the equation to calculate total risk. Total risk is the risk a company faces in the absence of any security safeguards or actions to reduce the overall risk exposure. The total risk is reduced by implementing safeguards and countermeasures, leaving the company with residual risk—or the risk left over after safeguards are implemented.

☒ **B** is incorrect because SLE × frequency is the equation to calculate the annualized loss expectancy (ALE) as a result of a threat exploiting a vulnerability and the business impact. The frequency is the threat's annual rate of occurrence (ARO). The ALE is not equal to residual risk. ALE indicates how much money a specific type of threat is likely to cost the company over the course of a year. Knowing the real possibility of a threat and how much damage, in monetary terms, the threat can cause is important in determining how much should be spent to try and protect against that threat in the first place.

☒ **D** is incorrect and is a distracter answer. There is no such formula like this used in risk assessments. The actual equations are threats × vulnerability × asset value = total risk; and (threats × vulnerability × asset value) × control gap = residual risk.

14. Authorization creep is to access controls what scope creep is to software development. Which of the following is not true of authorization creep?

A. Users have a tendency to request additional permissions without asking for others to be taken away.

B. It is a violation of "least privilege."

C. It enforces the "need-to-know" concept.

D. It commonly occurs when users transfer to other departments or change positions.

☑ **C.** The "need-to-know" concept is based on the idea that users are only given access rights to resources that they need in order to fulfill their job responsibilities. If access is not explicitly allowed, it should be implicitly denied. Instead of giving access to everything, and then taking privileges away based on "need-to-know," the better approach is to start with nothing and add privileges based on need to know. Authorization creep is contrary to this concept. It is about the accumulation of access rights over time, particularly those that the user does not have a need to know.

☒ **A** is incorrect because it correctly describes a cause of authorization creep and the question asks which statement is not true. Authorization creep often occurs due to users' tendency to request additional permissions without asking for others to be taken away. As a result, users have far more access rights and permissions than they require. This can pose a significant risk because too many users have too much privileged access to company assets.

☒ **B** is incorrect because authorization creep is a violation of "least privilege" and the question asks which statement is not true. Least privilege is a principle that states users should be given the least amount of privileges necessary to be productive when carrying out tasks. Enforcing least privilege on user accounts should be an ongoing job, which means each user's permissions should be reviewed to ensure the company is not putting itself at risk.

☒ **D** is incorrect because it correctly describes a cause of authorization creep, and the question asks which statement is not true. When users transfer to other departments or change positions, they are often assigned more access rights and permissions—far more than they need to get their jobs done. These rights and permissions are commonly added to their original ones, and their access to resources can be too vast and dangerous.

15. For what purpose was the COSO framework developed?

A. To address fraudulent financial activities and reporting

B. To help organizations install, implement, and maintain CobiT controls

C. To serve as a guideline for IT security auditors to use when verifying compliance

D. To address regulatory requirements related to protecting private health information

☑ **A.** COSO is an acronym for the Committee of Sponsoring Organizations of the Treadway Commission, which was formed in 1985 to provide sponsorship for the National Commission on Fraudulent Financial Reporting, an organization that studies deceptive financial reports and the elements that lead to them. Thus, the COSO framework was essentially developed to deal with fraudulent financial activities and reporting. Basically, COSO helps ensure that public companies who report their financial information to the Security Exchange Commission (SEC) are telling the truth and not "cooking the books."

☒ **B** is incorrect because COSO preceded CobiT; therefore, COSO was not developed to help organizations install, implement, and maintain CobiT controls. CobiT was derived from the COSO framework and offers a way to meet many of the COSO objectives from an IT perspective. COSO is a model for corporate governance on a strategic level, while CobiT is a model for IT governance on an operational level.

☒ **C** is incorrect because COSO was not developed to serve as a guideline to help IT security auditors. However, CobiT, which was derived from the COSO framework and defines goals for the controls that should be used to properly manage IT and ensure IT maps to business needs, is often used by auditors. CobiT lays out executive summaries, management guidelines, frameworks, control objectives, an implementation toolset, and audit guidelines. A majority of regulation compliance and audits are built on the CobiT framework.

☒ **D** is incorrect because COSO was not developed to address regulatory requirements related to private health information. However, NIST SP 800-66 is a risk assessment methodology that is designed to be implemented in the healthcare field or other regulated industries.

16. Susan, an attorney, has been hired to fill a new position at Widgets Inc. The position is Chief Privacy Officer (CPO). What is the primary function of her new role?

A. Ensuring the protection of partner data

B. Ensuring the accuracy and protection of company financial information

C. Ensuring that security policies are defined and enforced

D. Ensuring the protection of customer, company, and employee data

☑ **D.** The Chief Privacy Officer (CPO) position is being created by companies in response to the increasing demands on organizations to protect myriad types of data. The CPO is responsible for ensuring the security of customer, company, and employee data, which keeps the company free from legal prosecution and—hopefully—out of the headlines. Thus, the CPO is directly involved with setting policies on how data is collected, protected, and distributed to third parties. The CPO is usually an attorney and reports to the Chief Security Officer.

☒ **A** is incorrect because protecting partner data is just a small subset of all the data the CPO is responsible for protecting. CPOs are responsible for ensuring the protection of customer, company, and employee data. Partner data is among the various types of data that the CPO is responsible for protecting. In addition, the CPO is responsible for knowing how its company's suppliers, partners, and other third parties are protecting its sensitive information. Many times, companies will need to review these other parties (which have copies of data needing protection).

☒ **B** is incorrect because the accuracy of financial information is the responsibility of its data owner—the Chief Financial Officer (CFO). The CFO is responsible for the corporation's account and financial activities, and the overall financial structure of the organization. The CPO is responsible for helping to ensure the secrecy of this data, but not the accuracy of the data. The financial information is also a small subset of all the data types the CPO is responsible for protecting.

☒ **C** is incorrect because the definition and enforcement of security policies is the responsibility of senior management, commonly delegated to the CISO or CSO—not the CPO. A security policy is an overall general statement that dictates what role security plays within the organization. The CPO's responsibilities as they relate to policies are to contribute to the setting of data protection policies, including how data is collected, protected, and distributed to third parties.

17. Jared plays a role in his company's data classification system. In this role, he must practice due care when accessing data and ensure that the data is used only in accordance with allowed policy while abiding by the rules set for the classification of the data. He does not determine, maintain, or evaluate controls, so what is Jared's role?

A. Data owner

B. Data custodian

C. Data user

D. Information systems auditor

☑ **C.** Any individual who routinely uses data for work-related tasks is a data user. Users must have the necessary level of access to the data to perform the duties within their position and are responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others. This means that users must practice due care and act in accordance with both security policy and data classification rules.

☒ **A** is incorrect because the data owner has a greater level of responsibility in the protection of the data. Data owners are responsible for classifying the data, regularly reviewing classification levels, and delegating the responsibility of the data protection duties to the data custodian. The data owner is typically a manager or executive in the organization and is held responsible when it comes to protecting the company's information assets.

☒ **B** is incorrect because the data custodian is responsible for the implementation and maintenance of security controls as dictated by the data owner. In other words, the data custodian is the technical caretaker of the controls that protects the data. Her duties include making backups, restoring data, implementing and maintaining countermeasures, and administering controls.

☒ **D** is incorrect because an information systems auditor is responsible for evaluating controls. After evaluating the controls, the auditor provides reports to management, illustrating the mapping between the set acceptable risk level of the organization and her findings. This does not have to do with using the data or practicing due care with the use of data.

18. Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?

A. FAP

B. OCTAVE

C. ANZ 4360

D. NIST SP 800-30

☑ **C.** While ANZ 4360 can be used to analyze security risks, it was not created for that purpose. It takes a much broader approach to risk management than other risk assessment methodologies, such as NIST and OCTAVE, which focus on IT threats and information security risks. ANZ 4360 can be used to understand a company's financial, capital, human safety, and business decisions risks.

☒ **A** is incorrect because there is no formal FAP risk analysis approach. It is a distracter answer.

☒ **B** is incorrect because OCTAVE focuses on IT threats and information security risks. OCTAVE is meant to be used in situations where people manage and direct the risk evaluation for information security within their organization. The organization's employees are given the power to determine the best approach for evaluating security.

☒ **D** is incorrect because NIST SP 800-30 is specific to IT threats and how they relate to information security risks. It focuses mainly on systems. Data is collected from network and security practice assessments, and from people within the organization. The data is then used as input values for the risk analysis steps outlined in the 800-30 document.

19. Which of the following is not a characteristic of a company with a security governance program in place?

A. Board members are updated quarterly on the company's state of security.

B. All security activity takes place within the security department.

C. Security products, services, and consultants are deployed in an informed manner.

D. The organization has established metrics and goals for improving security.

☑ **B.** If all security activity takes place within the security department, then security is working within a silo and is not integrated throughout the organization. In a company with a security governance program, security responsibilities permeate the entire organization, from executive management down the chain of command. A common scenario would be executive management holding business unit managements responsible for carrying out risk management activities for their specific business units. In addition, employees are held accountable for any security breaches they participate in, either maliciously or accidentally.

☒ **A** is incorrect because security governance is a set of responsibilities and practices exercised by the board and executive management of an organization with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the organization's resources are used responsibly. An organization with a security governance program in place has a board of directors that understands the importance of security and is aware of the organization's security performance and breaches.

☒ **C** is incorrect because security governance is a coherent system of integrated security components that includes products, personnel, training, processes, etc. Thus, an organization with a security governance program in place is likely to purchase and deploy security products, managed services, and consultants in an informed manner. They are also constantly reviewed to ensure they are cost-effective.

☒ **D** is incorrect because security governance requires performance measurement and oversight mechanisms. An organization with a security governance program in place continually reviews its processes, including security, with the goal of continued improvement. On the other hand, an organization that lacks a security governance program is likely to march forward without analyzing its performance and therefore repeatedly makes similar mistakes.

20. Michael is charged with developing a classification program for his company. Which of the following should he do first?

A. Understand the different levels of protection that must be provided.

B. Specify data classification criteria.

C. Identify the data custodians.

D. Determine protection mechanisms for each classification level.

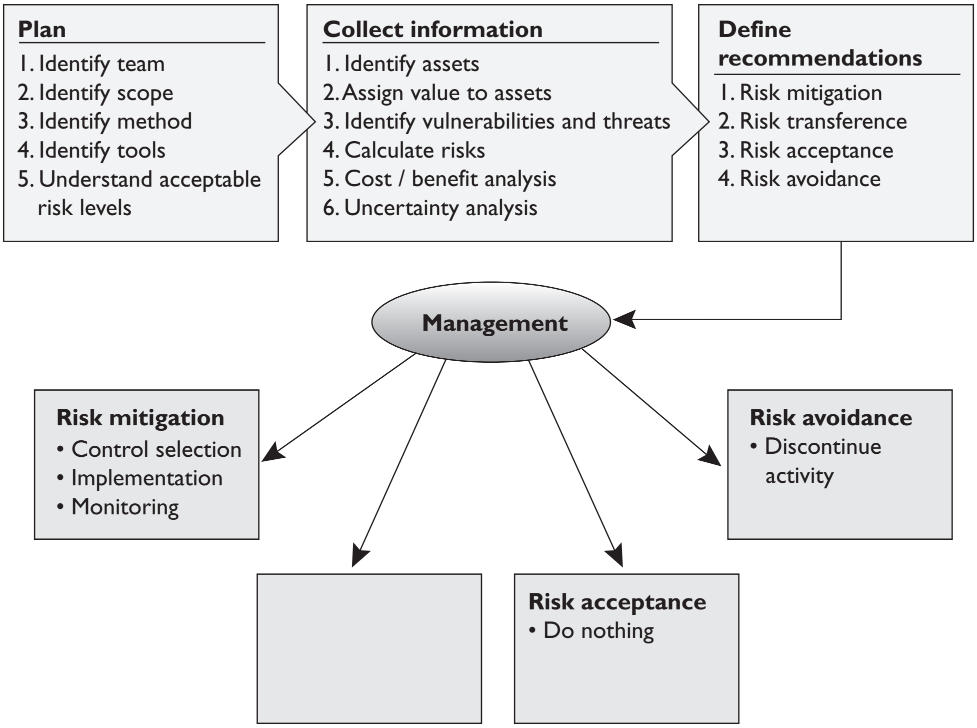
☑ **A.** Before Michael begins developing his company's classification program, he must understand the different levels of protection that must be provided. Only then can he develop the necessary classification levels and their criteria. One company may choose to use only two layers of classification, while another may choose to use more. Regardless, when developing classification levels, he should keep in mind that too many or too few classification levels will render the classification ineffective; there should be no overlap in the criteria definitions between classification levels; and classification levels should be developed for both data and software.

☒ **B** is incorrect because data classification criteria cannot be established until the classification levels themselves have been defined. The classification criteria are used by data owners to know what classification should be assigned to specific data. Basically, the classifications are defined buckets and the criteria help data owners determine what bucket each data set should be put into.

☒ **C** is incorrect because there is no need to identify the data custodians until classification levels are defined, criteria are determined for how data are classified, and the data owner has indicated the classification of the data she is responsible for. Remember, the data custodian is responsible for implementing and maintaining the controls specified by the data owner.

☒ **D** is incorrect because protection mechanisms for each classification level cannot be determined until the classification levels themselves are defined based on the different levels of protection that are required. The types of controls implemented per classification will depend upon the level of protection that management and the security team have determined is needed.

21. There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?



A. Risk transference. Share the risk with other entities.

B. Risk reduction. Reduce the risk to an acceptable level.

C. Risk rejection. Accept the current risk.

D. Risk assignment. Assign risk to a specific owner.

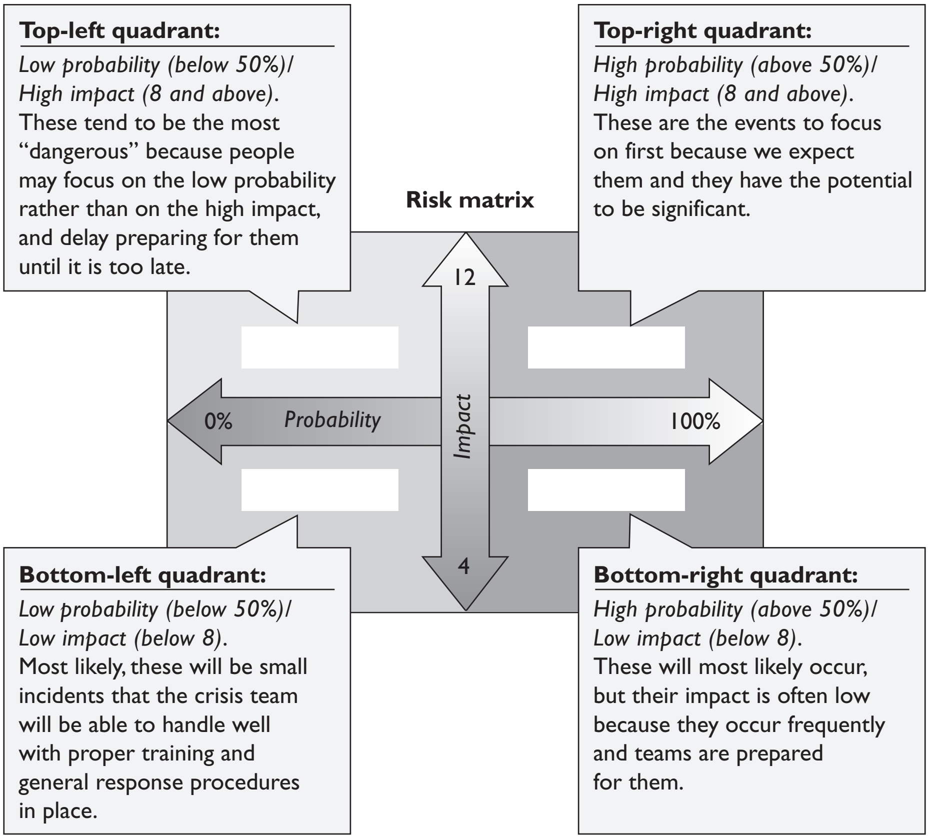
☑ **A.** Once a company knows the amount of total and residual risk it is faced with, it must decide how to handle it. Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it. Many types of insurance are available to companies to protect their assets. If a company decides the total or residual risk is too high to gamble with, it can purchase insurance, which would transfer the risk to the insurance company.

☒ **B** is incorrect because another approach is risk mitigation, where the risk is reduced to a level considered acceptable enough to continue conducting business. The implementation of firewalls, training, and intrusion/detection protection systems represent types of risk mitigation. Risk reduction is the same as risk mitigation, which is already listed in the graphic.

☒ **C** is incorrect because companies should never reject risk, which basically means that they refuse to deal with it. Risk commonly has a negative business impact and if not dealt with properly the company could have to deal with things such as the loss of production resources, legal liability issues, or a negative effect on its reputation. It is important that identified risk be dealt with properly through transferring it, avoiding it, reducing it, or accepting it.

☒ **D** is incorrect because while someone could be delegated to deal with a specific risk, this is not one of the methods that is used to deal with risk. Even if risk was assigned to a specific entity to deal with it, she would still need to either transfer, avoid, reduce, or accept the risk.

22. The following graphic contains a commonly used risk management scorecard. Identify the proper quadrant and its description.



Top-left quadrant:
Low probability (below 50%)/ High impact (8 and above).
These tend to be the most "dangerous" because people may focus on the low probability rather than on the high impact, and delay preparing for them until it is too late.

Top-right quadrant:
High probability (above 50%)/ High impact (8 and above).
These are the events to focus on first because we expect them and they have the potential to be significant.

Bottom-left quadrant:
Low probability (below 50%)/ Low impact (below 8).
Most likely, these will be small incidents that the crisis team will be able to handle well with proper training and general response procedures in place.

Bottom-right quadrant:
High probability (above 50%)/ Low impact (below 8).
These will most likely occur, but their impact is often low because they occur frequently and teams are prepared for them.

A. Top-right quadrant is high impact, low probability.

B. Top-left quadrant is high impact, medium probability.

C. Bottom-left quadrant is low impact, high probability.

D. Bottom-right quadrant is low impact, high probability.

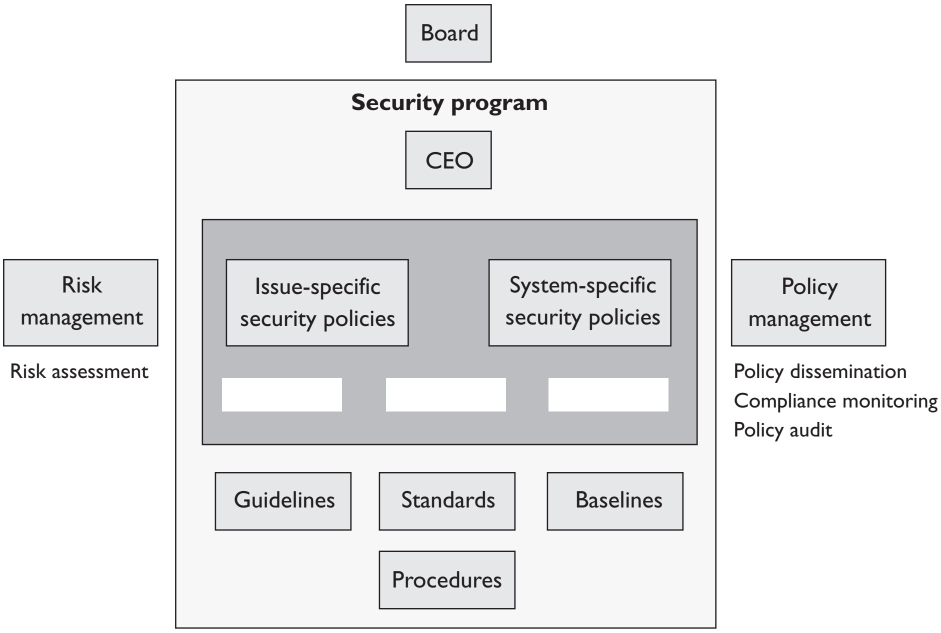
☑ **D.** The bottom-right quadrant contains low impact, high probability risks. This means that there is a high chance that specific threats will exploit specific vulnerabilities. Although these risks are commonly frequent, their business impact is low. Out of the four quadrants, the risks that reside in this quadrant should be dealt with after the first two higher quadrants. An example of a risk that could reside in this quadrant is a virus that infects a user workstation. Since viruses are so common this would mean that this risk has a high probability of taking place. This is only a user workstation and not a production system, so the impact would be low.

☒ **A** is incorrect because the top-right quadrant contains high impact, high probability risks. This means that there is a high chance that specific threats will exploit specific vulnerabilities. These risks are commonly frequent and their business impact is high. Out of the four quadrants, the risks that reside in this quadrant should be dealt with first. An example of a risk that would reside in this quadrant is an attacker compromising an internal mail server. If the proper countermeasures are not in place, there is a high probability that this would occur. Since this is a resource that the whole company depends upon, it would have a high business impact.

☒ **B** is incorrect because the top-left quadrant contains high impact, low probability risks. This means that there is a low chance that specific threats will exploit specific vulnerabilities. These risks are commonly infrequent and their business impact is low. Out of the four quadrants, the risks that reside in this quadrant should be dealt with after the risks that reside in the top-right quadrant. An example of this type of risk is an attacker compromising an internal DNS server. If there is an external-facing DNS server and a DMZ is in place, an attacker being able to access an internal DNS server is low. But if this does happen, this would have a high business impact since all systems depend upon this resource.

☒ **C** is incorrect because the bottom-left quadrant contains low impact, low probability risks. This means that there is a low chance that specific threats will exploit specific vulnerabilities. These risks are commonly infrequent and their business impact is low. Out of the four quadrants, the risks that reside in this quadrant should be dealt with after the risks in all of the other three quadrants. An example of this type of risk would be a legacy file server that is hardly used failing and going offline. Since it is not commonly used by users, it would have a low business impact, and if the correct countermeasures are in place, there would be a low probability of this occurring.

23. What are the three types of policies that are missing from the following graphic?



A. Regulatory, Informative, Advisory

B. Regulatory, Mandatory, Advisory

C. Regulatory, Informative, Public

D. Regulatory, Informative, Internal Use

☑ **A.** A **Regulatory** type of policy ensures that the organization is following standards set by specific industry regulations. It is very detailed and specific to a type of industry. It is used in financial institutions, healthcare facilities, public utilities, and other government-regulated industries. An **Informative** type of policy informs employees of certain topics. It is not an enforceable policy, but rather one that teaches individuals about specific issues relevant to the company. It could explain how the company interacts with partners, indicate the company's goals and mission, and provide a general reporting structure in different situations. An **Advisory** type of policy strongly advises employees as to which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical information, financial transactions, or how to process confidential information.

☒ **B** is incorrect because Mandatory is not one of the categories of a type of policy; thus, this answer is a distracter.

☒ **C** is incorrect because Public is not one of the categories of a type of policy; thus, this answer is a distracter.

☒ **D** is incorrect because Internal Use is not one of the categories of a type of policy; thus, this answer is a distracter.

24. List in the proper order from the table that follows the learning objectives that are missing and their proper definitions.

	Awareness	**Training**	**Education**
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning objective:			
Example teaching method:	**Media** • Videos • Newsletters • Posters	**Practical instruction** • Lecture and/or demo • Case study • Hands-on practice	**Theoretical instruction** • Seminar and discussion • Reading and study • Research
Test measure:	True/False Mutiple choice (Identify learning)	Problem solving, i.e., recognition and resolution (Apply learning)	Essay (Interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

A. Understanding, recognition and retention, skill

B. Skill, recognition and retention, skill

C. Recognition and retention, skill, understanding

D. Skill, recognition and retention, understanding

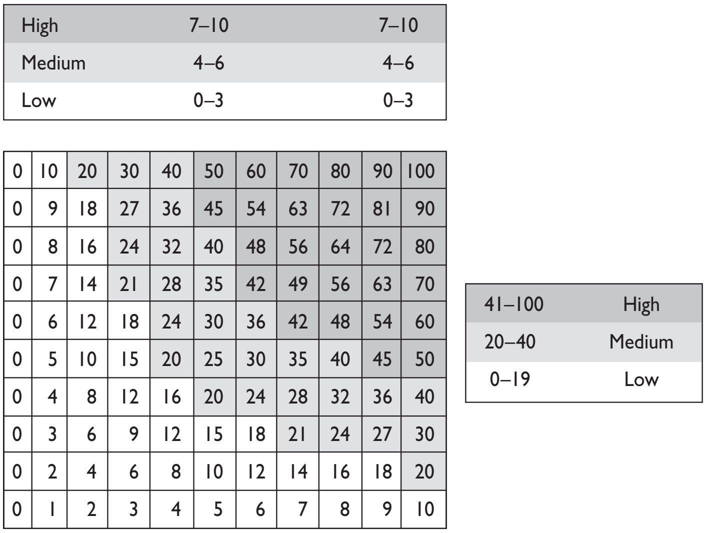
☑ **C.** Awareness training and materials remind employees of their responsibilities pertaining to protecting company assets. Training provides skills needed to carry out specific tasks and functions. Education provides management skills and decision-making capabilities.

☒ **A** is incorrect because the different types of training and education do not map to the listed results. Companies today spend a lot of money on security devices and technologies, but they commonly overlook the fact that individuals must be trained to use these devices and technologies. Without such training, the money invested toward reducing threats can be wasted, and the company is still insecure.

☒ **B** is incorrect because the different types of training and education do not map to the listed results. Different roles require different types of training or education. A skilled staff is one of the most critical components to the security of a company.

☒ **D** is incorrect because the different types of training and education do not map to the listed results. A security-awareness program is typically created for at least three types of audiences: management, staff, and technical employees. Each type of awareness training must be geared toward the individual audience to ensure each group understands its particular responsibilities, liabilities, and expectations.

25. What type of risk analysis approach does the following graphic provide?



High	7–10	7–10
Medium	4–6	4–6
Low	0–3	0–3

0	10	20	30	40	50	60	70	80	90	100
0	9	18	27	36	45	54	63	72	81	90
0	8	16	24	32	40	48	56	64	72	80
0	7	14	21	28	35	42	49	56	63	70
0	6	12	18	24	30	36	42	48	54	60
0	5	10	15	20	25	30	35	40	45	50
0	4	8	12	16	20	24	28	32	36	40
0	3	6	9	12	15	18	21	24	27	30
0	2	4	6	8	10	12	14	16	18	20
0	1	2	3	4	5	6	7	8	9	10

41–100	High
20–40	Medium
0–19	Low

A. Quantitative

B. Qualitative

C. Operationally Correct

D. Operationally Critical

☑ **B.** A qualitative risk analysis approach does not assign monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions. Qualitative analysis techniques include judgment, best practices, intuition, and experience. This graphic shows a rating system, which qualitative risk analysis uses instead of percentages and monetary numbers.

☒ **A** is incorrect because a quantitative risk analysis attempts to assign percentages and monetary values to all elements of the risk analysis process. These elements may include safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, and so on. When all of these are quantified, the process is said to be quantitative. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

☒ **C** is incorrect because there is no Operationally Correct formal risk analysis approach. This is a distracter answer.

☒ **D** is incorrect because there is no formal Operationally Critical risk analysis approach. This is a distracted answer.