Chapter 2: A Global Roadmap for Security

TRUE/FALSE

1. Most governmental organizations are unlike the structure of large business organizations in terms of bureaucracy and hierarchy.

   ANS: F PTS: 1 REF: 20

2. In effect, there is nothing special about the management structure of a government organization.

   ANS: T PTS: 1 REF: 20

3. The larger and more complex the organization, the easier it is to identify and inter-relate all of the required elements of the EBK into a proper security system.

   ANS: F PTS: 1 REF: 21

4. The structure of the EBK makes it easy to add that standard role to the 10 basic roles that are presently contained in the model.

   ANS: T PTS: 1 REF: 34

5. EBK roles are generic in nature and by design are broadly defined in order to cover several job titles in different industries.

   ANS: T PTS: 1 REF: 35

MULTIPLE CHOICE

1. Like most strategic practice standards, the EBK was created by ____ from the expert community.
   a. examining output
   b. studying plans
   c. facilitating input
   d. defining input

   ANS: C PTS: 1 REF: 20

2. The EBK contains what is recognized to be a coherent and correct set of behaviors based on ____.
   a. expert opinion
   b. expert information
   c. expert consensus
   d. expert discussion

   ANS: A PTS: 1 REF: 20

3. The aim of a high-level model like the EBK is to provide a strategic ____ that specifies all of the commonly accepted activities and inter-relationships associated with good security.
   a. toolkit
   b. plan
   c. roadmap
   d. framework

   ANS: D PTS: 1 REF: 21

4. The intent of the EBK is to present the most comprehensive possible listing of the ____ that could potentially help an organization become more secure.
   a. areas
   b. competencies
   c. foundations
   d. skills

ANS: B PTS: 1 REF: 21

5. All of the behaviors that the creators of the EBK deemed necessary to ensure fundamentally proper security were categorized into ____ competency areas.

a. 10	c. 14
b. 12	d. 16

ANS: C PTS: 1 REF: 22

6. The work of actually vetting and compiling the competencies in the EBK was done by a group of ____.

a. experts	c. field personnel
b. subject matter experts	d. researchers

ANS: B PTS: 1 REF: 22

7. Analysis of the EBK standards produced ____ critical work functions.

a. 14	c. 41
b. 35	d. 53

ANS: D PTS: 1 REF: 22

8. The definitions for the functional areas are listed in ____ of the EBK.

a. Section 4.0	c. Section 4.2
b. Section 4.1	d. Section 4.3

ANS: A PTS: 1 REF: 22

9. Information security work involves a very wide range of ____.

a. required activities	c. potential activities
b. required competencies	d. potential competencies

ANS: C PTS: 1 REF: 24

10. The 10 roles in the EBK represent job ____.

a. titles	c. possibilities
b. functions	d. growth

ANS: B PTS: 1 REF: 25

11. The first step in the ____ process is to equate the EBK role definitions with whatever the organization presently calls that role.

a. mapping	c. implementation
b. discovery	d. evaluation

ANS: A PTS: 1 REF: 25

12. ____ functions are those that relate to the conceptualization and development of security-related functionality.

a. Manage	c. Design
b. Implement	d. Evaluate

ANS: C PTS: 1 REF: 29

13. ____ functions are those that involve tasks associated with the establishment of the operational security measures, including programs, policies, and procedures.

a. Manage
b. Implement
c. Design
d. Evaluate

ANS: B PTS: 1 REF: 29

14. The CIO’s role in enterprise continuity is classified in the EBK as a(n) ____ function.
a. evaluate
b. implement
c. design
d. manage

ANS: D PTS: 1 REF: 30

15. The ____ system integrates all necessary controls for all relevant recommendations into a single comprehensive solution.
a. department information security
b. company-wide information security
c. unit information security
d. personal information security

ANS: B PTS: 1 REF: 32

16. Ensuring ____ validates the purpose of each of the controls in an action plan.
a. accountability
b. authentication
c. traceability
d. attainability

ANS: C PTS: 1 REF: 33

17. The management plan specifies the ____ required to satisfy each function.
a. behaviors
b. jobs
c. competencies
d. roles

ANS: A PTS: 1 REF: 33

18. The ____ plan lays out the planned behaviors that the organization feels will satisfy the intent of the management functions described in the EBK.
a. design and implementation
b. evaluation
c. assessment
d. management

ANS: D PTS: 1 REF: 33

19. The ____ plan defines the behaviors that the organization thinks will satisfy the EBK’s recommendations regarding the design and implementation of common functions that are a part of each competency area.
a. design and implementation
b. evaluation
c. assessment
d. management

ANS: A PTS: 1 REF: 33

20. The evaluation plan has to specify the provisions to assure the continuing ____ of the overall security process.
a. compliance
b. renewal
c. trustworthiness
d. revision

ANS: C PTS: 1 REF: 33

21. The ____ plan is written to ensure the consistent execution of the behaviors that are specified in the management and the design and implementation plans.
a. design and implementation
b. evaluation
c. assessment
d. management

ANS: B PTS: 1 REF: 33

COMPLETION

1. A(n) ____________________ is recognized to be a coherent and correct set of behaviors based on expert opinion.

   ANS: best practice

   PTS: 1 REF: 20

2. The EBK specifies a detailed and commonly accepted set of required security ____________________.

   ANS: competencies

   PTS: 1 REF: 21

3. The EBK can be considered to contain the most authoritative possible representation of security practices and their clarifying ____________________.

   ANS: terminology

   PTS: 1 REF: 23

4. The ____________________ plan defines a set of explicit actions that the organization plans to take, to ensure that each EBK role properly executes its requisite management functions.

   ANS: management

   PTS: 1 REF: 33

5. The ____________________ plan documents how the company will assure performance.

   ANS: evaluation

   PTS: 1 REF: 33

MATCHING

Match each term with the correct statement below.

a. IT Security Training and Awareness
b. Strategic Security Management
c. Enterprise Continuity
d. Date Security
e. Personnel Security
f. System and Application Security
g. Digital Forensics
h. Regulatory and Standards Compliance
i. IT Systems Operations and Maintenance

1. Techniques aimed at ensuring electronic data
2. Techniques aimed at evidence collection after an adverse event
3. Techniques aimed at ensuring the competency of the members of the organization
4. Techniques aimed at ensuring the continuing functioning of the enterprise after an adverse event
5. Techniques aimed at ensuring continuous secure functioning of the enterprise

6. Techniques aimed at ensuring secure practice by the employees of the organization
7. Techniques aimed at ensuring that the enterprise does not violate a regulation, standard, or law related to security
8. Strategic methods for ensuring that the organization maintains a secure infrastructure
9. Techniques for ensuring that the operating environment of the machine and all of its associated applications remains secure

1. ANS: D PTS: 1 REF: 23
2. ANS: G PTS: 1 REF: 23
3. ANS: A PTS: 1 REF: 23
4. ANS: C PTS: 1 REF: 23
5. ANS: I PTS: 1 REF: 23
6. ANS: E PTS: 1 REF: 23
7. ANS: H PTS: 1 REF: 23
8. ANS: B PTS: 1 REF: 23
9. ANS: F PTS: 1 REF: 23

SHORT ANSWER

1. What three things must the EBK do to ensure that it is the right model to ensure that it can protect a company's information from the sort of criminal activities?

   ANS:
   First, there has to be recommendations in the EBK that would allow the company to identify and then formulate a substantive and effective set of measures to ensure that the company's information was adequately protected. Second, the EBK would have to provide a means to identify all relevant threats. Finally, the EBK must make it possible to generate explicit policies, procedures, and work instructions from the EBK that would ensure the most comprehensive governance solution possible.

   PTS: 1 REF: 21

2. Explain what the 10 roles in the EBK represent.

   ANS:
   The 10 roles in the EBK represent job functions rather than job titles. These functions range across the IT security workforce. In order to avoid getting caught up in the myriad job titles that actually exist for equivalent jobs, the EBK takes a role-based approach to the definition of the work to be done. It is up to the individual organization then, to assign a job title that is equivalent to the functions specified by a given EBK security role. The title is likely to vary across organizations, but the required competencies and accountabilities will essentially remain the same.

   PTS: 1 REF: 25

3. Discuss the purpose of mapping.

   ANS:
   The aim of mapping is to understand how each of the existing job titles fits within the standard role definitions provided by the EBK. That is because the role definitions contribute specific competencies. And it is those competencies that form the ultimate basis for the duties required in every practical implementation.

   PTS: 1 REF: 26

4. Why is it important to document controls?

   ANS:
   Each control has to be documented individually in order to put it into practice. The documentation of all controls then serves as the practical handbook for the day-to-day execution of the information security process.

   PTS: 1 REF: 33

5. Discuss the purpose of the management plan.

   ANS:
   The management plan lays out the planned behaviors that the organization feels will satisfy the intent of the management functions described in the EBK. In other words, the management plan defines a set of explicit actions that the organization plans to take, to ensure that each EBK role properly executes its requisite management functions. The plan specifies the behaviors required to satisfy each function, as well as how each of those behaviors will be performed, monitored, and assessed.

   PTS: 1 REF: 33

6. Explain the purpose of the design and implementation plan.

   ANS:
   The design and implementation plan defines the behaviors that the organization thinks will satisfy the EBK's recommendations regarding the design and implementation of common functions that are a part of each competency area. Because the design and implementation common functions itemize the activities that will constitute the day-to-day security activities of the organization, the design and implementation plan is really the practical operations manual for the organization's security system.

   PTS: 1 REF: 33

7. Describe the evaluation plan.

   ANS:
   The evaluation plan documents how the company will assure performance. The evaluation plan is written to ensure the consistent execution of the behaviors that are specified in the management and the design and implementation plans. The evaluation plan also has to specify the provisions to assure the continuing trustworthiness of the overall security process. Because that involves assessment, those plans have to specify who will be responsible for doing the actual evaluation and when the evaluation will be done, as well as the specific measures that will be used to assess performance.

   PTS: 1 REF: 33

8. Discuss why a company might need to add roles and competencies to the EBK basic model.

   ANS:
   Once a company has surveyed its operation, it is more than likely to discover that in order to satisfy obvious security needs, it will need to add roles and competencies that do not exist in the basic model. Examples of such a need might be the addition of a biometric specialist role for high-tech access control, or a physical network infrastructure specialist, or even a strategic supply chain manager. Since the original assumption was that the changing nature of any security situation will require adaptation of the basic model, the EBK framework was purposely designed to be easy to expand.

PTS: 1 REF: 34

9. Explain the assumption behind the core framework of roles and competencies of EBK.

ANS:
The assumption behind the EBK is that its core framework of roles and competencies are a valid and coherent baseline representation of fundamental security requirements.

PTS: 1 REF: 34

10. What are the two logical dimensions in which the EBK expands?

ANS:
The EBK expands in two logical dimensions. First, additional roles that could be added as new security requirements are identified. Also, additional competencies can be added to a role, or even defined as an entirely separate competency category.

PTS: 1 REF: 34-35