CISA Q&As

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cisa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

QUESTION 1

To develop meaningful recommendations \\'or findings, which of the following is MOST important \\'or an IS auditor to determine and understand?

A. Root cause

B. Responsible party

C. impact

D. Criteria

Correct Answer: A

QUESTION 2

Which of the following is the MOST important consideration when incorporating data analytics into an audit?

A. Ability of the auditor to perform complex analysis

B. Availability and cost of the tools

C. Complexity of the data and related audit process

D. Availability and quality of data

Correct Answer: C

QUESTION 3

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a pattern of behaviors, effects, assumptions, attitude and ways of doing things?

A. Governing

B. Culture

C. Enabling and support

D. Emergence

Correct Answer: B

Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and

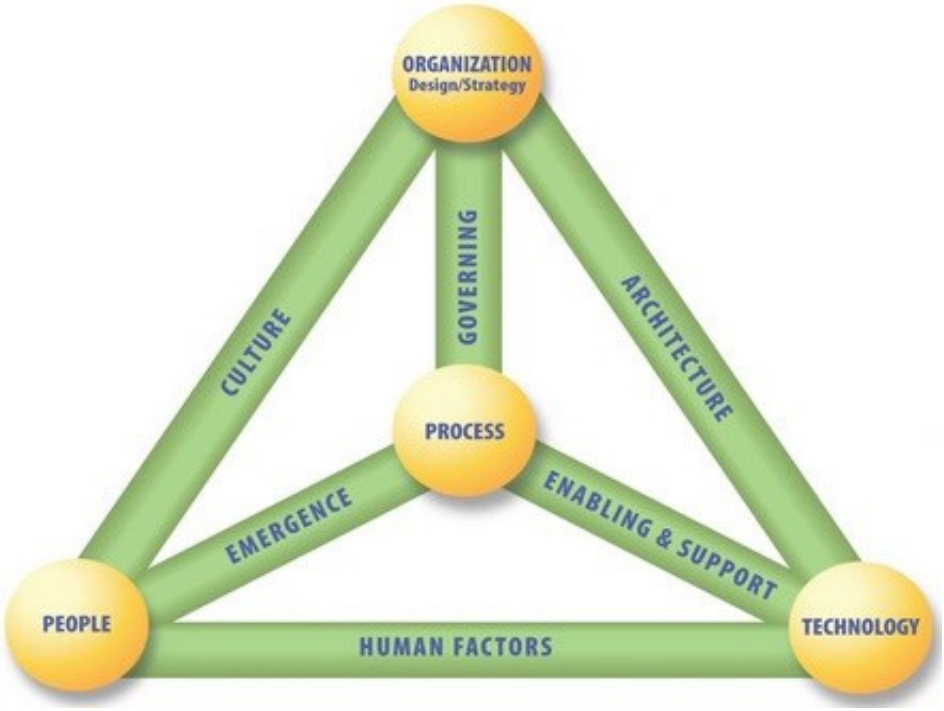
social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

For your exam you should know the information below.

Business Model for Information Security The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically ?not merely as a sum of its parts ?to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. "Systems thinking" is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why "the whole is more than the sum of its parts." Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections. All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

1.

Organization Design and Strategy ?An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal. An enterprise\\'s strategy specifies its business goals and the

objectives to be achieved as well as the values and missions to be pursued. It is the enterprise\\'s formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to

design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2.

People ?The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases.

Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:

Recruitment strategies (access, background checks, interviews, roles and responsibilities)

Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)

Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and

need to be considered within the security posture.

3.

Process ?Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections. Processes identify, measure, manage and control risk, availability,

integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4.

Technology ?Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise\\'s

dependence on technology, technology constitutes a core part of the enterprise\\'s infrastructure and a critical component in accomplishing its mission. Technology is often seen by the enterprise\\'s management team as a way to resolve

security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason, information security managers

must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1.

Governing ?Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise\\'s resources are used responsibly.

2.

Culture ?Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3.

Enabling and support ?The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4.

Emergence ?Emergence ?which connotes surfacing, developing, growing and evolving ?refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5.

Human factors ?The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise\\'s human resources on pertinent skills.

6.

Architecture ?A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise\\'s security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise\\'s resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Emergence ?Emergence ?which connotes surfacing, developing, growing and evolving ?refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

Reference:

CISA review manual 2014 page number 37 and 38 http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

QUESTION 4

Which of the following is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources?

A. Functional Point analysis

B. Gantt Chart

C. Critical path methodology

D. Time box management

Correct Answer: D

Time box management is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources. There is a need to balance software quality and meet the delivery requirements within the time box or timeframe. The project manager has some degree of flexibility and uses discretion is scoping the requirement. Timebox management can be used to accomplish prototyping or RAPID application development type in which key feature are to be delivered in a short period of time.

The following were incorrect answers:

Critical path Method -The critical path method (CPM) is an algorithm for scheduling a set of project activities Gantt Chart -A Gantt chart is a type of bar chart, developed by Henry Gantt in the 1910s, that illustrates a project schedule. Gantt charts illustrate the start and finish dates of the terminal elements and summary elements of a project. Terminal elements and summary elements comprise the work breakdown structure of the project. Modern Gantt charts also show the dependency (i.e. precedence network) relationships between activities. Gantt charts can be used to show current schedule status using percent-complete shadings and a vertical "TODAY" line as shown here.

Functional Point Analysis -Function Point Analysis (FPA) is an ISO recognized method to measure the functional size of an information system. The functional size reflects the amount of functionality that is relevant to and recognized by the user in the business. It is independent of the technology used to implement the system.

Reference:

CISA review manual 2014 Page number 154

QUESTION 5

Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

A. Availability of IS audit resources

B. Remediation dates included in management responses

C. Peak activity periods for the business

D. Complexity of business processes identified in the audit

Correct Answer: C