Exam Code: 000-013

Exam Name: Applying Fundamentals of Enterprise Solutions Using IBM

Vendor: IBM

Version: DEMO

Part: A

1: A good user management process includes the following tasks:

- receive new user identity requests

- receive requests for changes to user identities

- use access policies to evaluate requests

- gather approvals

- place users in groups

- update accounts

- synchronize passwords

Which additional step is essential in a good user management process?

A.back up directory information

B.check that existing accounts are valid

C.verify user management process ownership

D.grant or block access to programs, based on access policy

Correct Answers: B

2: What is considered the lowest maturity level in Identity Management maturity?

A.password management

B.access rights accountability

C.provisioning approval and process automation

D.connectors to access controlled systems (one tool managing multiple systems)

Correct Answers: D

3: After a number of interviews with various customer personnel, the term "user productivity logon and transaction experience" comes up as a business process. Other than the word "logon", the description does not provide much insight into how this process relates to security. Which list of security (and related) elements relate most strongly to this customer business process?

A.firewall, filtering router, intrusion detection

B.SSL acceleration, content filtering, pop-up blockers

C.single sign-on, personalization, scalability, availability

D.identification, public-key infrastructure, multi-factor authentication

Correct Answers: C

4: What information should a customer baseline document include?

A.proof that there are no existing orphan accounts

B.the naming convention in place for all current users

C.the customer key business processes related to security

D.a list of all authentication mechanisms used by the customer

Correct Answers: C

5: A customer has resources being managed in different facilities. When configuring a security solution, what is the most important element to consider in the design of the system?

A.use of a fiber optic backbone

B.the encryption protocol to be used

C.location of firewalls in the internal network

D.the time zone in which each facility is located

Correct Answers: C

6: What is the objective of documenting the business and IT organizational structure of a company?

A.It helps the solution advisor identify the number of products that need to be deployed.

B.This step is essential to identify key areas of the business processes that relate to security.

C.It indicates the approximate number of licenses required for each product the company purchases.

D.The business organizational structure must match certain specifications for the product to be usable.

Correct Answers: B

7: What needs to be defined for the Identity Management aspect of a Security Solution?

A.processes

B.driver's licenses

C.password selection

D.employee pay bands

Correct Answers: A

8: Good workflow capability is a sign of maturity related to which aspect of security?

A.provisioning

B.authorization

C.authentication

D.new initiative deployment

Correct Answers: A

9: Who must approve a requirements specification?

A.the customer and the sales team

B.the customer and the implementation team

C.the implementation team and the sales team

D.the implementation team and the product support team

Correct Answers: B

10: What is the purpose of the context diagram for a security solution?

A.It provides a detailed listing of the software used in the solution and how the software is connected.

B.It provides a detailed listing of the hardware used in the solution and how the hardware is connected.

C.It scopes the security system's responsibilities and provides a black box view of the system interface.

D.It provides a listing of the hardware and software used in the system and how they are

interconnected.
Correct Answers: C

11: What information is needed when creating a document concerning a customer's IT and business organizational structure? (Choose two.)

A.number of business units

B.annual expenditure on IT assets

C.number of employees in IT organization

D.list of divisions within the IT department

E.total number of systems used by the company

Correct Answers: A D

12: In describing their business processes, the customer provides the following aspects of "audit/compliance":

1. Physical building access security

2. Security of servers

3. Security of desktops

4. Audit of user identities/accounts

5. Audit of access control (policy and actuals)

6. Audit of security of business partners

7. Revoke compromised certificates

From this list, what can be addressed by IBM Tivoli security solutions?

A.2, 3, 5, 7

B.2, 3, 4, 5

C.2, 3, 4, 6

D.4, 5, 6, 7

Correct Answers: B

13: Based on IBM best practices, what are three IBM Tivoli Access Manager for e-business authentication capabilities that indicate a higher level of authentication maturity? (Choose three.)

A.Basic authentication

B.Shared authentication

C.Step-up authentication

D.Forced re-authentication

E.Multi-factor authentication

F.Forms-based authentication

Correct Answers: C D E

14: Which programming languages need to be available to manage an unsupported operating system with an IBM Tivoli Identity Manager adapter?

A.Java and C

B.Cobol and REXX

C.C++ and Javascript

D.Visual Basic and C#

Correct Answers: A

15: Which tasks need to be accomplished during an initial meeting with the customer when reviewing a company organizational chart?

A.determine the products to be used and provide Proof of Concept of the products in the solution

B.document the key players and their roles and provide Proof of Concept of the products in the solution

C.identify key decision makers and determine the products to be used

D.identify key decision makers and document the key players and their roles

Correct Answers: D

16: Which is an accurate description of a highly mature company, in the area of authorization?

A.They are highly mature, because they use a single authorization engine, shared by many applications.

B.Their approach to authorization is in a leadership position, because they address WS-Provisioning, SAML and Liberty.

C.They are addressing authorization optimally because they are handling authorization within the application, and it best to address authorization decisions close to the decision point.

D.Their approach to authorization is highly secure and therefore highly mature, because their infrastructure uses many different authorization standards and thus is least likely to be penetrated.

Correct Answers: A

17: While reviewing the current security policies for a company, you find that a standard exists, which dictates that information access must conform to HIPAA. Currently the customer has no automated method to verify adherence to this policy. Which IBM Tivoli security solution should you recommend to provide the customer with the ability to report on exceptions to this policy?

A.IBM Tivoli Identity Manager

B.IBM Tivoli Security Compliance Manager

C.IBM Tivoli Access Manager for e-business

D.IBM Tivoli Access Manager for Enterprise Single Sign-On

Correct Answers: B

18: A current IBM Tivoli security customer is very satisfied with their current IBM Tivoli Identity Manager (ITIM) and IBM Tivoli Access Manager (ITAM) implementations. The customer has benefited greatly from the user management and provisioning, authentication, authorization and Web single sign-on processes now in place.

The customer sees the value of Web services and wants to leverage their business partnerships to greatly expand their online services, for a relatively small investment. They are expecting that their existing ITIM and ITAM investments can simply be stretched to include these business-to-business (B2B) flows.

IBM Tivoli Federated Identity Manager should be added to this scenario to address which security requirement?

A.the blocking of threats that might otherwise cross enterprise boundaries

B.the handling of potentially millions of users, which neither ITIM nor ITAM was built to address

C.the integration with firewalls that control security between any two businesses involved in these B2B flows

D.the handling of multiple types of standards-based protocols and user tokens that need to be passed between participating businesses

Correct Answers: D

19: What is an important guideline to follow when considering security audit and security compliance scenarios?

A.avoid consolidating audit information, as that can dilute the value of the collected information and possibly render it useless

B.align the scope with the capabilities of Tivoli Security Compliance Manager, compliance of servers and desktops to stated security policies

C.avoid considering all rules, regulations, laws and internal customer requirements, as this can consume a lot of time while not yielding much useful information

D.consider compliance from multiple points of view, including desktop security, server security, access control policy, provisioning policy, authentication policy and risk management policy

Correct Answers: D

20: Which three actions provide relevant input to customer authentication scenarios? (Choose three.)

A.The customer wants to digitally sign all messages.

B.The customer runs a successful PKI project and now wants to more fully adopt PKI.

C.The customer partially implements single sign-on, and wants to more fully implement it.

D.The customer feels they have too many places where audit data is kept, and they want to consolidate it.

E.The customer needs to issue identification tokens to people holding certain special job categories, for use in Web transactions.

F.The customer wants to cipher (encrypt) sensitive data while it is stored on servers, on desktops and while in transit in message flows and Web transactions.

Correct Answers: B C E