Question: 1

Pass-through Authentication
Give this one a try later!

A. The highest level role, which allows for complete control over the IdentityNow tenant.
B. Separation of Duties Policy
C. Any system of interest where you want to manage user access.
D. For authentication that uses another system like AD or LDAP to manage authentication.

Answer: D

Question: 2

All tenants have access to a set of shared services.
Give this one a try later!

A. True
B. False

Answer: A

Question: 3

Which of the following is not an option for handling the provisioning of passwords for new accounts?
Give this one a try later!

A. Using a static password for everyone.
B. Emailing a generated password to the user.
C. Setting an initial password based on identity data the user will know.
D. Setting a random password and having the user reset it before logging in.

Answer: B

Question: 4

All non-authoritative sources need a separate source of entitlement (group) data that can be aggregated to provide information like display names and descriptions.
Give this one a try later!

A. True
B. False

Answer: B

Question: 5

What is the Certification Email?
Give this one a try later!

A. 1. Entitlement Matching
2. Attribute Matching
3. Identity List
B. Sent to certifiers at the beginning of a campaign.
C. A create profile is applied anytime IdentityNow creates an account for a user on a source.
D. 1. Source Metadata
2. Account Schema
3. Manager Correlation

Answer: B

Question: 6

Can any attribute from a source create profile be used for attribute syncing?
Give this one a try later!

A. Yes
B. No

Answer: B

Question: 7

What does the Identity Profile encompass?
Give this one a try later!

A. 1. Authoritative Settings
2. Identity Attribute Mappings

3. Lifecycle States (optional)
B. 1. With every aggregation/identity refresh
2. In a daily refresh job
3. On manual update
C. 1. Static Passwords
2. Dynamic Known Passwords
3. Dynamic Unknown Passwords
D. 1. Data-driven/automated
2. Request-driven/user-initiated

Answer: A

Question: 8

Governance groups require that all members sign off on an access request before it can be approved.
Give this one a try later!

A. True
B. False

Answer: B

Question: 9

Every identity is required to login to IdentityNow.
Give this one a try later!

A. True
B. False

Answer: B

Question: 10

All entitlements that are aggregated into IdentityNow are automatically visible and requestable in the Request Center.
Give this one a try later!

A. True
B. False

Answer: B

Question: 11

Access will be removed from an identity if the access was previously granted by a role and the identity no longer meets the role membership criteria.
Give this one a try later!

A. True
B. False

Answer: A

Question: 12

Which of the following user levels in IdentityNow are in the default? (select all that apply)
1. User
2. Admin
3. Helpdesk User
4. Accountant Admin
5. Provisioning Admin
Give this one a try later!

A. 1. User ID
2. Last Name
3. First Name
4. Email
B. Source Type
C. The access to the role is revoked.
D. 1. User
2. Admin
3. Helpdesk User

Answer: D

Question: 13

What happens when a user gets assigned a role in which they have a subset of the access profiles/entitlements?
Give this one a try later!

A. The process of granting, changing, or removing user access to systems, application, and databases based on unique user identity.
B. The access they do not have is assigned to them and the access they have gets rolled up into the role.
C. Specifies the type of access or permissions a user has when logging into an application.
D. Layer certification processes.
Use search and filters to focus campaigns on specific areas of business.
Avoid overwhelming certifiers with certification fatigue.

Answer: B

Question: 14

What are the four certification reports?
Give this one a try later!

A. IdentityNow will confirm the new password value meets all criteria before submitting the request.
B. 1. Campaign Composition Report
2. Campaign Status Report
3. Certification Signoff Report
4. Campaign Remediation Status Report
C. 1. Automated evaluation occurs with every aggregation.
2. You can manually execute individual role evaluation from the role configuration screen.
3. You can programmatically trigger an evaluation through the REST API.
D. To push any changes made to identity attributes out to source attributes that need to share the same values.

Answer: B

Question: 15

Native Authentication
Give this one a try later!

A. The highest level role, which allows for complete control over the IdentityNow tenant.
B. For users invited through IdentityNow and their information is stored in IdentityNow.
C. 1. Identities
2. Roles
3. Access Profiles
4. Entitlements
5. Events
6. Account Activity
D. An administrator can confirm the accuracy of the campaign parameters, cancel, start, or reassign.

Answer: B