PassQueen
a.k.a dumpsqueen.com

Google Cloud Certified - Professional Google Workspace Administrator

Google Google-Workspace-Administrator

Version Demo

Total Demo Questions: 25

Total Premium Questions: 253

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Managing user accounts, domains, and groups	48
Topic 2, Managing Google Workspace services	62
Topic 3, Managing devices and endpoints	23
Topic 4, Managing security and compliance	100
Topic 5, Troubleshooting common issues	20
Total	253

QUESTION NO: 1

User A is a Basic License holder. User B is a Business License holder. These two users, along with many additional users, are in the same organizational unit at the same company. When User A attempts to access Drive, they receive the following error: “We are sorry, but you do not have access to Google Docs Editors. Please contact your Organization Administrator for access.” User B is not presented with the same error and accesses the service without issues.

How do you provide access to Drive for User A?

A. Select User A in the Directory, and under the Apps section, check whether Drive and Docs is disabled. If so, enable it in the User record.

B. In Apps > Google Workspace > Drive and Docs, select the organizational unit the users are in and enable Drive for the organizational unit.

C. In Apps > Google Workspace, determine the Group that has Drive and Docs enabled as a service. Add User A to this group.

D. Select User A in the Directory, and under the Licenses section, change their license from Basic to Business to add the Drive and Docs service.

ANSWER: C

Explanation:

In Apps > Google Workspace, determine the Group that has Drive and Docs enabled as a service. Add User A to this group. Google Workspace administrators can control access to Google Workspace services, including Drive and Docs, for groups as well as organizational units. Group-based service configuration is useful when users within the same organizational unit require different service access. In this scenario, the shared organizational unit is already compatible with Drive access because another user in it can use the service. The relevant distinction is therefore the group-based access assignment that grants Drive and Docs to the users who are members of the enabled group. Adding User A to that group applies the group’s service setting and allows the user to open Drive and use Google Docs Editors. A Basic license includes the Google Drive and Docs service; the license name itself does not inherently prevent this user from accessing it. After membership is added, allow time for the group and service-setting change to propagate before testing access again. Google documents group-based service controls in its Turn a service on or off for Google Workspace users guidance, and explains how administrators can manage membership in the Groups Admin help documentation.

QUESTION NO: 2

A company-issued ChromeOS device is reported lost. The device contains locally available files and users can sign in to it with managed Google accounts. You need to prevent further use of the device and remove local organizational data if the device connects to the internet.

What two actions should you take? (Choose two.)

A. Disable the ChromeOS device in the Admin console.

B. Wipe the ChromeOS device from the Admin console.

C. Remove the device from its organizational unit.

D. Delete the employee’s Google Workspace account.

E. Turn off ChromeOS automatic updates for the device.

ANSWER: A B

Explanation:

Disable the ChromeOS device in the Admin console prevents users from signing in to the managed device. This provides immediate containment for a lost endpoint while the organization investigates the incident or attempts to recover the hardware.

Wipe the ChromeOS device from the Admin console sends a remote command that resets the device and removes locally stored user data when the device next connects to the internet. Wiping is appropriate when the organization must protect data that might be available on the lost device. Administrators can manage these actions from the ChromeOS devices section of the Admin console.

QUESTION NO: 3

Your organization is replacing its external identity provider with a new SAML identity provider. The existing provider currently controls sign-in to Google Workspace. You need to prevent an administrator lockout while validating the new configuration.

What two actions should you take? (Choose two.)

A. Maintain at least two super administrator accounts that can sign in using Google credentials.

B. Test the new SAML configuration with a non-administrator test user before enforcing it broadly.

C. Delete the existing identity provider configuration before creating the new configuration.

D. Assign the Super Admin role to all members of the IT department.

E. Disable 2-Step Verification until the new identity provider is operational.

ANSWER: A B

Explanation:

Maintain at least two super administrator accounts that can sign in using Google credentials provides a recovery path if the new SAML configuration is incomplete, the identity provider becomes unavailable, or an assertion configuration error prevents normal users from signing in. Super administrator access should be tightly controlled and protected with strong 2-Step Verification.

Test the new SAML configuration with a non-administrator test user before enforcing it broadly allows the organization to validate the identity provider metadata, certificate, NameID format, and expected sign-in flow without risking the administrative accounts required to reverse a configuration problem. After successful validation, the organization can transition the wider user population. See Set up single sign-on for managed Google Accounts.

QUESTION NO: 4

Your organization wants to prevent a group of users from logging into their Google Drive when they are traveling internationally for business.

You have added these users to an organizational unit (OU). You need to secure the usersâ€™ access to the Google Drive app to meet this requirement.

What should you do?

A. Disable Google Drive for users in the OU.

B. Define location-based access levels. Assign the levels to the Google Drive app for the OU.

C. Require 2-step verification (2SV) when users in the OU sign in.

D. Define user-based access levels. Assign the levels to the Google Drive app for the OU.

ANSWER: B

Explanation:

Define location-based access levels. Assign the levels to the Google Drive app for the OU. Context-Aware Access lets an administrator apply access controls to Google Workspace applications, including Drive, according to contextual conditions evaluated at sign-in or access time. A location-based access level can use the user's geographic location, derived from their

IP address, to establish where access is permitted. The administrator can configure the access level to allow the organization's approved country or regions and then assign that access level to Google Drive for the organizational unit containing the affected users. Consequently, members of that OU can use Drive while they are in approved locations, but access is denied when their connection is identified as originating outside those permitted locations. This approach meets the requirement without removing Drive as a service for the users; it specifically enforces the organization's travel-related location policy. Google documents the setup and assignment of Context-Aware Access policies to organizational units and supported Workspace apps in its Context-Aware Access overview. Details about defining conditions, including geographic location criteria, are available in the Create access levels documentation.

QUESTION NO: 5

A company wants to distribute iOS devices to only the employees in the Sales OU. They want to be able to do the following on these devices:

What two steps are required before configuring the device policies? (Choose two.)

A. Turn on Advanced Mobile Management for the domain.

B. Turn on Advanced Mobile Management for Sales OU

C. Set up Device Approvals.

D. Set up an Apple Push Certificate.

E. Deploy Apple Certificate to every device.

ANSWER: A D

Explanation:

Turning on Advanced Mobile Management for the domain is required because it enables the Google Admin console's advanced endpoint-management capabilities for the organization. After advanced management is enabled, administrators can scope iOS management settings and policies to the Sales organizational unit, allowing only users in that OU to receive the intended device-management configuration. Advanced mobile management is enabled at the organization level rather than being initially enabled separately for an individual OU; organizational units are then used to target the applicable policies.

Setting up an Apple Push Certificate is also required before Google Workspace can manage iOS and iPadOS devices through Apple's Push Notification service (APNs). The APNs certificate establishes the connection that allows Google endpoint management to send management commands, policy updates, and other device actions to enrolled Apple devices. It must be created and uploaded in the Admin console before configuring and using iOS device-management policies. Google documents both the organization-level setup for advanced mobile management and the requirement to configure an Apple push certificate for Apple device management in Set up advanced mobile management and Set up Apple device management.

QUESTION NO: 6

Your corporate LDAP contains the email addresses of several hundred non-employee business partners. You want to sync these contacts to Google Workspace so they appear in Gmail's address autocomplete for all users in the domain.

What are two options to meet this requirement? (Choose two.)

A. Use the Directory API to upload a .csv file containing the contacts.

B. Configure GCDS to populate a Group with external members.

C. Use the People API to upload a .csv file containing the contacts.

D. Develop a custom application to call the Domain Shared Contacts API.

E. Configure GCDS to synchronize shared contacts.

ANSWER: D E

Explanation:

Develop a custom application to call the Domain Shared Contacts API. is a valid programmatic approach for publishing contacts that are shared throughout a Google Workspace domain. Domain shared contacts are centrally managed contacts, rather than personal contacts belonging to one user. After the external partners' names and email addresses are created as domain shared contacts, they are available to users for address lookup and autocomplete in Google services such as Gmail. A custom application can read the corporate LDAP data, transform it as needed, and create, update, or delete the corresponding shared-contact records through the API.

Configure GCDS to synchronize shared contacts. directly matches the requirement to synchronize an LDAP directory into Google Workspace. Google Cloud Directory Sync supports synchronizing shared contacts from an LDAP server, including creating and updating the centrally available contact information. This is especially suitable for several hundred contacts because it provides scheduled, repeatable synchronization and maintains alignment as the LDAP directory changes. Google's GCDS documentation describes shared-contact synchronization and its required LDAP mapping configuration, while the Domain Shared Contacts API documentation describes the API resource for domain-wide contacts. See Synchronize shared contacts with GCDS and Domain Shared Contacts API.

QUESTION NO: 7

A user in your organization reported that their internal event recipient is not receiving the Calendar event invites. You need to identify the source of this problem. What should you do?

A. Check whether the business hours are set up in the event recipient ' s Calendar settings.

B. Check if Calendar service is turned off for the event creator.

C. Check whether the Calendar event has more than 50 guests.

D. Check whether the event recipient has turned off their email notifications for new events in their Calendar settings.

ANSWER: D

Explanation:

Check whether the event recipient has turned off their email notifications for new events in their Calendar settings. Google Calendar lets each user control notification delivery for their calendars, including email notifications for newly added events. An invitation can be processed by Calendar and appear on the recipient's calendar while the recipient does not receive the expected invitation-related email message because their calendar notification preferences do not include email delivery for new events. This makes the recipient's Calendar notification configuration an appropriate first troubleshooting point when the reported symptom is specifically that an internal recipient is not receiving event invites by email. The administrator can ask the recipient to open Google Calendar settings, select the affected calendar, and review its event notification settings, or guide them to restore email notifications as appropriate for the organization's workflow. This investigation also distinguishes a notification-delivery expectation from an event-creation or scheduling issue: it focuses directly on the user-level setting that governs whether Calendar sends email notifications for events on that calendar. Google's Calendar Help describes how users manage notification settings for a calendar, including event-related email notifications: Change notification settings. For broader behavior concerning invitations and how they are added to a user's calendar, see Respond to event invitations.

QUESTION NO: 8

Your company uses a whitelisting approach to manage third-party apps and add-ons. The Senior VP of Sales

& Marketing has urgently requested access to a new Marketplace app that has not previously been vetted. The company's Information Security policy empowers you, as a Google Workspace admin, to grant provisional access immediately if all of the following conditions are met:

Which actions should you take first to ensure that you are compliant with Infosec policy?

A. Move the Senior VP to a sub-OU before enabling Marketplace Settings > "Allow Users to Install Any App from Google Workspace Marketplace."

B. Confirm that the Senior VP's OU has the following Gmail setting disabled before whitelisting the app: "Let users delegate access to their mailbox."

C. Review the Marketplace app's OAuth scopes in Security > Access and data control > API controls, then add it to the allowlist and limit access to an OU containing the Senior VP.

D. Search the Google Workspace support forum for feedback about the app to include in the risk analysis report.

ANSWER: C

Explanation:

Review the Marketplace app's OAuth scopes in the Admin console API controls, then add the app to the allowlist and limit its access to an organizational unit containing the Senior VP. This supports a whitelist-based security process because the administrator evaluates precisely what Google Workspace data and services the app requests before permitting the app to access organizational accounts. OAuth scopes are the relevant permissions for assessing whether an app needs access to sensitive data such as Gmail, Drive, Calendar, or contacts. After that review, the app can be designated as trusted or allowed under the organization's third-party app access controls and made available only to the intended organizational unit. Restricting deployment to a dedicated OU provides the requested provisional access without expanding availability across the company, and it gives the security team a contained configuration to monitor or revoke if later review identifies a concern. Google documents how administrators can review and control third-party OAuth app access, including the data scopes requested by apps, in Control which third-party and internal apps access Google Workspace data. It also documents administrative controls for installing and managing Marketplace apps in Manage Google Workspace Marketplace apps.

QUESTION NO: 9

A user does not follow their usual sign-in pattern and signs in from an unusual location.

What type of alert is triggered by this event?

A. Suspicious mobile activity alert.

B. Suspicious login activity alert.

C. Leaked password alert.

D. User sign-in alert.

ANSWER: B

Explanation:

Suspicious login activity alert. is the correct alert because Google Workspace monitors sign-in behavior and evaluates signals that can indicate a potentially unauthorized account access attempt. A sign-in that differs substantially from a user's established activity pattern, including one originating from an unusual geographic location, is a relevant risk signal. When Google identifies such a sign-in as suspicious, it generates a suspicious login activity alert in the Alert Center so that administrators can investigate the event, review affected-user and sign-in details, and take appropriate account-security actions if necessary.

This alert supports early detection of account compromise without requiring an administrator to manually review every authentication event. The investigation can be supplemented with audit information, including the time of the login, source IP address, and location-related details, where available. Administrators should assess whether the user recognizes the sign-in and can secure the account through actions such as resetting the password or ending active sessions when compromise is suspected. Google documents suspicious login activity as an Alert Center alert type and describes the available investigation workflow in its administrator guidance. See Google Workspace Alert Center documentation and Google Workspace administrator security guidance.

QUESTION NO: 10

You've noticed an increase in phishing emails that contain links to malicious files hosted on external Google Drives. These files often mimic legitimate documents and trick users into granting access to their accounts. You need to prevent users from accessing these malicious external Drive files, but allow them to access legitimate external files. What should you do? (Choose two.)

A. Enforce stricter password policies.

B. Conduct regular security awareness training to educate users.

C. Create a Drive trust rule that blocks all external domains except for a pre-approved list of trusted partners.

D. Deploy advanced malware detection software on all user devices to scan and block malicious files.E Implement two-factor authentication for all users

ANSWER: B C

Explanation:

Creating a Drive trust rule that blocks all external domains except for a pre-approved list of trusted partners provides the administrative control needed to restrict Drive interactions with untrusted external domains while preserving collaboration with known, legitimate partners. Trust rules can be scoped to Google Drive and configured with trusted organizations or domains, allowing the administrator to enforce a deliberate allowlist rather than relying on users to judge every external sharing invitation or file link. This directly reduces exposure to phishing campaigns that use externally hosted Drive content as their delivery mechanism. Google documents Drive trust rules and their use in controlling external sharing and collaboration at Google Workspace Admin Help: Trust rules.

Conducting regular security awareness training to educate users is also an essential preventive control. Users must be able to identify suspicious messages, misleading document names, unexpected permission prompts, and requests for OAuth access before opening a link or authorizing an application. Training reinforces safe verification practices, such as confirming the sender and expected context through a separate channel. Google's phishing guidance recommends educating users and reporting suspicious messages; see Protect your organization from phishing.

QUESTION NO: 11

Your company is using Google Workspace Enterprise Plus, and the Human Resources (HR) department is asking for access to Work Insights to analyze adoption of Google Workspace for all company employees. You assigned a custom role with the work Insights permission set as "view data for all teams" to the HR group, but it is reporting an error when accessing the application. What should you do?

A. Allocate the "view data for all teams" permission to all employees of the company.

B. Confirm that the Work Insights app is turned ON for all employees.

C. Confirm in Security > API controls > App Access Controls that Work Insights API is set to "unrestricted."

D. Confirm in Reports > BigQuery Export that the job is enabled.

ANSWER: C

Explanation:

Confirm in Security > API controls > App Access Controls that Work Insights API is set to "unrestricted." Assigning the "view data for all teams" administrative privilege authorizes the HR group to view organization-wide Work Insights information, but the service must also be permitted to access the Google Workspace data required to produce those insights. App access controls can restrict an application's access to Workspace services and data, including when the affected users otherwise have the appropriate administrator privileges. If the Work Insights API is restricted or blocked, Work Insights cannot retrieve the underlying adoption and collaboration signals and may display an access error. Setting the Work Insights API to unrestricted ensures that the application is allowed to make the required calls for the HR users who have been assigned the applicable custom role. This is an organization-level API access configuration and should be validated alongside the custom-role assignment when enabling access to a Workspace reporting service. Google documents how administrators manage application access through API controls in the App access control guidance. The underlying principle is also consistent with

Google's documentation on using administrator roles and privileges: a role grants administrative capability, while applicable service and access-control settings must still allow the service to operate.

QUESTION NO: 12

Your organization uses Google Vault for retention and eDiscovery. The legal department has received a new litigation request involving a project team. Legal needs to preserve the team's Google Chat messages and search the preserved data within an access-controlled case workspace.

What two actions should you take? (Choose two.)

A. Create a matter in Google Vault and grant the legal team access.

B. Create a Google Chat hold for the identified project-team accounts.

C. Export the project team's Chat messages to each team member's My Drive.

D. Reset the passwords for every member of the project team.

E. Move the project team into a new organizational unit with a longer Gmail retention rule.

ANSWER: A B

Explanation:

Create a matter in Google Vault and grant the legal team access establishes the access-controlled workspace for the case. Authorized legal users can use the matter to manage holds, search data, review results, and export evidence without receiving direct access to employee accounts.

Create a Google Chat hold for the identified project-team accounts preserves the relevant Chat messages while the hold remains in place. A hold takes precedence over applicable retention rules for covered data, helping ensure that messages required for the litigation are not permanently deleted during the investigation. Google documents Vault matters and placing Chat messages on hold.

QUESTION NO: 13

Your company is opening offices in several cities and wants employees to find and reserve meeting rooms in Google Calendar. Employees must be able to search rooms by office location and features such as video conferencing and wheelchair access.

What two actions should you take? (Choose two.)

A. Create buildings and define the relevant room features.

B. Create Calendar resources for the meeting rooms and assign the applicable building and features.

C. Create an organizational unit for each office location.

D. Create a Google Group for each meeting room.

E. Create a shared drive for each office and store room schedules in Sheets.

ANSWER: A B

Explanation:

Create buildings and define the relevant room features establishes the location and feature information that Calendar uses when users search for an appropriate room. Buildings can represent offices or sites, while features identify room capabilities and accessibility characteristics.

Create Calendar resources for the meeting rooms and assign the applicable building and features makes each room available as a reservable Calendar resource. When users create an event, they can search for available rooms using the configured building and feature details, then add the selected resource to the event.

Creating user organizational units or Google Groups does not create reservable room inventory in Calendar. See Create buildings, features, and Calendar resources.

QUESTION NO: 14

You are configuring Google Chat for your organization. Using the Adin console, you want to enable employees to view their chat history by default and allow employees to turn off chat history. What should you do?

A. Configure Google Vault to retain all Chat messages, and exclude organizational units (OUs) with users who want to turn Chat history off.

B. Set the space history setting to OFF and chat history to ON.

C. Set the top-level default conversation history setting to ON and allow users to change their history setting.

D. Set the top-level default conversation history settings to OFF and allow users in each organizational unit (OU) to change their history setting.

ANSWER: C

Explanation:

Set the top-level default conversation history setting to ON and allow users to change their history setting. This directly establishes the organization-wide behavior required: new direct-message conversations have history enabled by default, so employees can view prior messages in those conversations. Enabling the user setting for conversation history also preserves employee choice, allowing an individual to turn history off for their direct-message conversations when appropriate. Google Chat administrators configure this in the Admin console under Google Chat history settings, where they can select the default history state and determine whether users can change it. The top-level organizational unit is the appropriate place to apply this baseline when the desired policy applies to all employees. Conversation-history settings affect whether messages remain available in the conversation; they are separate from retention and preservation controls that an organization might configure in Google Vault. For the applicable Admin console procedure and the history behavior for Google Chat conversations, see Turn chat history on or off for your organization. For additional details on how Google Chat history works for direct messages and spaces, consult Learn about conversation history in Google Chat.

QUESTION NO: 15

Your organization stores product-design documents in Google Drive. Security requires users to classify documents containing unreleased product information and prevent those classified documents from being shared externally.

What two actions should you take? (Choose two.)

A. Create and publish a classification label for unreleased product information.

B. Create a Drive DLP rule that blocks external sharing for files with the classification label.

C. Require users to include the word Confidential in the file name.

D. Disable Google Drive for all users who work on product designs.

E. Configure a Gmail content compliance rule to reject messages containing product names.

ANSWER: A B

Explanation:

Create and publish a classification label for unreleased product information gives users a consistent, administrator-defined method to identify sensitive documents. Publishing the label to the applicable users makes it available in Drive for the intended population.

Create a Drive DLP rule that blocks external sharing for files with the classification label enforces the required control after the file is classified. The DLP rule can take action when users attempt to share labeled content outside the organization, reducing the chance that sensitive product information is exposed through Drive sharing. Classification labels and DLP rules provide both user-visible classification and centrally enforced protection.

QUESTION NO: 16

Your organization requires enhanced privacy and security when sending messages to banks and other financial institutions. Your organization uses Gmail, but the banks use various other email providers. You need to maximize privacy and limit access to messages sent and received between your organization and the banks. What should you do?

A. Set up Transport Layer Security (TLS) compliance for inbound and outbound messages with a list of the banks' email domains. Validate the TLS connections.

B. Configure Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) authentication for your email domains.

C. Enable Protect against unauthenticated emails in Gmail Safety.

D. Enable confidential mode for Gmail. Instruct employees to use confidential mode when sending messages to the banks.

ANSWER: A

Explanation:

Set up Transport Layer Security (TLS) compliance for inbound and outbound messages with a list of the banks' email domains. Validate the TLS connections. This is the appropriate control because it protects email while it travels between Google's mail servers and the banks' external mail systems, regardless of which email providers those institutions use. A Gmail TLS compliance setting can be scoped to the specified partner domains and configured to require secure SMTP delivery. Requiring TLS means Gmail does not fall back to an unencrypted connection when communicating with those domains; delivery is deferred if a compliant secure connection cannot be established. Certificate validation further helps confirm that Gmail is connecting to the intended receiving mail server and not an untrusted endpoint. Applying the rule to both inbound and outbound traffic establishes a protected transport requirement for the full exchange of sensitive financial correspondence, rather than only for messages sent by employees. Google Workspace administrators can configure secure transport requirements in Gmail routing settings and identify the partner domains covered by the policy. This provides the strongest available Gmail transport-level safeguard for communications with external banking organizations. See Google's instructions for requiring a secure connection for email and its overview of TLS compliance settings.

QUESTION NO: 17

HR informs you that a user has been terminated and their account has been suspended. The user is part of a current legal investigation, and HR requires the user's email data to remain on hold. The terminated user's team is actively working on a critical project with files owned by the user. You need to ensure that the terminated user's content is appropriately kept before provisioning their license to a new user.

What two actions should you take? (Choose two.)

A. Extend the legal hold on the user's email data.

B. Move project files to a Team Drive or transfer ownership.

C. Rename the account to the new user starting next week.

D. Delete the account, freeing up a Google Workspace License.

E. Assign the terminated user account an Archive User license.

ANSWER: B E

Explanation:

Move project files to a Team Drive or transfer ownership. ensures that the team retains access to the critical project content independently of the terminated employee's active account. An administrator can transfer ownership of eligible Google Drive files to another user, or move appropriate shared content into a shared drive, where files are owned by the organization rather than an individual. This protects operational continuity before the former user's standard Workspace license is reassigned.

Assign the terminated user account an Archive User license. is the appropriate way to retain a departed employee's Workspace data without consuming a standard user license. Archived User licensing preserves data such as Gmail and Drive content and supports retention requirements, including use with Google Vault. Because the account already has a legal hold, the held email remains preserved until the hold is released; a legal hold does not need to be "extended" as part of license reassignment. This combination preserves investigation-relevant data while making the regular license available for the incoming user.

See Google's guidance on Archived User licenses and transferring Drive file ownership.

QUESTION NO: 18

You've noticed an increase in phishing emails that contain links to malicious files hosted on external Google Drives. These files often mimic legitimate documents and trick users into granting access to their accounts. You need to prevent users from accessing these malicious external Drive files, but allow them to access legitimate external files. What should you do? (Choose two.)

A. Enforce stricter password policies.

B. Conduct regular security awareness training to educate users.

C. Create a Drive trust rule that blocks all external domains except for a pre-approved list of trusted partners.

D. Implement two-factor authentication for all users.

ANSWER: B C

Explanation:

Conduct regular security awareness training to educate users is appropriate because phishing resistance depends substantially on users recognizing suspicious messages, deceptive document links, unexpected access-consent prompts, and impersonated sharing notifications. Training should give users practical guidance for verifying the sender, destination domain, requested permissions, and legitimacy of an external file before opening it or granting access. Google's phishing guidance recommends educating users and encouraging prompt reporting of suspicious content, allowing administrators to investigate and respond quickly.

Create a Drive trust rule that blocks all external domains except for a pre-approved list of trusted partners provides the necessary preventive control for external Drive collaboration. Drive trust rules let administrators establish trusted external organizations and apply rules governing inbound and outbound sharing. A restrictive inbound-sharing policy, with explicit allowances for approved partner domains, limits users' ability to receive or access shared content from unapproved external domains while preserving collaboration with known legitimate partners. This layered approach combines a policy-based boundary for external sharing with informed user decision-making for the legitimate content that remains available. See Google's Manage trust rules for Drive and Protect users from phishing and malware.

QUESTION NO: 19

Your cyber security team has requested that all email destined for external domains be scanned for credit card numbers, and if found, the email must be encrypted using your cloud-based third-party encryption provider. You are responsible for configuring to meet this request.

What should you do?

A. Create a content compliance rule on outbound mail and internal-sending mail using the predefined rule for credit card numbers, and add a custom header that your third-party encryption provider can scan for and encrypt.

B. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check “Encrypt message if not encrypted”.

C. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and add a custom header that your third-party encryption provider can scan for and encrypt.

D. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check “Change route” to send to your third-party encryption provider to encrypt.

ANSWER: D

Explanation:

Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check “Change route” to send to your third-party encryption provider to encrypt. This targets mail leaving the organization, which is the required scope for messages addressed to external domains. Gmail content compliance rules can inspect outbound messages using predefined content detectors, including the detector for credit card numbers. When the detector finds matching content, the rule can apply a routing action only to those messages.

“Change route” sends the matching message through a mail route configured for the organization’s third-party encryption service. The provider can then process and encrypt the message before final delivery. This approach preserves normal direct delivery for outbound mail that does not contain a detected card number, while ensuring that sensitive matching content is routed through the encryption workflow. Configure the third-party provider’s SMTP host as the destination mail route first, then select that route as the action in the content compliance setting. Google documents content compliance matching and actions at Set up content compliance rules and explains the mail-routing configuration used by routing actions at Set up mail routing.

QUESTION NO: 20

Your organization has just completed migrating users to Workspace. Many employees are concerned about their legacy Microsoft Office documents, including issues of access, editing, and viewing. Which two practices should you use to alleviate user concerns without limiting Workspace collaboration features? (Choose two.)

A. Configure Context-Aware Access policies to block access to Microsoft Office applications.

B. Demonstrate the ability to convert Office documents to native Google file format from Drive.

C. Demonstrate and train users to use the Workspace Migrate tool.

D. Deliver training sessions that show the methods to access and edit native Office files in Drive, the Workspace file editors, and Drive for Desktop.

E. Continue to use installed Office applications along with Google Drive for Desktop.

ANSWER: B D

Explanation:

Demonstrating the ability to convert Office documents to native Google file format from Drive directly addresses users’ concerns about whether important Word, Excel, and PowerPoint content remains usable after migration. Drive supports converting compatible Office files into Google Docs, Sheets, or Slides, allowing users to use Workspace-native commenting, real-time co-editing, sharing controls, version history, and other collaboration capabilities. Conversion can be performed from Drive when appropriate, giving employees a practical migration path for documents that will be actively maintained in Workspace.

Delivering training sessions that show the methods to access and edit native Office files in Drive, the Workspace file editors, and Drive for Desktop is also essential. Users can open and edit Office files in Google Docs, Sheets, and Slides without necessarily converting them, while Drive for desktop provides familiar file-system access and supports workflows involving locally installed applications. Training on these choices reassures employees that they can select the appropriate workflow

for each document while continuing to collaborate through Drive. Google documents these Office-file editing capabilities at Edit Office files in Google Docs, Sheets, and Slides and conversion guidance at Convert Microsoft Office files to Google files.

QUESTION NO: 21

Your organization has noticed several incidents of accidental oversharing inside the organization. Specifically, several users have shared sensitive Google Drive items with the entire organization by clicking 'anyone in this group with this link can view'. You have been asked by senior management to help users share more appropriately and also to prevent accidental oversharing to the entire organization. How would you best accomplish this?

A. Create groups, add users accordingly, and educate users on how to share to specific groups of people.

B. Disable sharing to the entire organization so that users must consciously add every person who needs access.

C. Determine sharing boundaries for users that work with sensitive information, and then implement target audiences.

D. Temporarily disable the Google Drive service for individuals who continually overshare.

ANSWER: C

Explanation:

Determine sharing boundaries for users that work with sensitive information, and then implement target audiences. Target audiences are designed specifically to guide users toward appropriate internal sharing choices in Google Drive. An administrator can define audiences that represent approved groups of people, such as a department, project team, or staff who are authorized to handle sensitive information. When users share a file, Drive presents these audiences as recommended sharing targets, making the intended limited audience easier to select than a broad organization-wide link setting.

Sharing boundaries complement target audiences by controlling which internal sharing choices are available to users in particular organizational units or groups. This lets the organization apply more restrictive sharing behavior to users who work with sensitive data while still allowing collaboration patterns appropriate for other teams. Together, these controls address both parts of the requirement: they provide a simple, recognizable sharing destination for legitimate collaboration and reduce the likelihood that a sensitive item is shared to everyone in the organization by mistake. Administrators should align audience membership and boundary policies with the organization's data-classification and access-control requirements, then communicate the approved audiences to users. Google documents target audiences and their Drive sharing behavior in the Target audiences admin guide and describes internal Drive sharing controls in the Drive sharing settings guide.

QUESTION NO: 22

An employee at your organization may be sharing confidential documents with unauthorized external parties. You must quickly determine if any sensitive information has been leaked. What should you do?

A. Review the employee's Drive log events in the security investigation tool.

B. Audit Drive access by using the Admin SDK Reports API.

C. Review the employee's user log events within the security investigation tool.

D. Create a custom report of the user's external sharing by using the security dashboard.

ANSWER: A

Explanation:

Review the employee's Drive log events in the security investigation tool. Drive log events provide the focused audit trail needed to rapidly investigate possible external disclosure of files stored in Google Drive. An administrator can search and filter activity for the particular employee and relevant time period, then examine events associated with sharing and file access. This enables the investigation to identify affected files, determine whether sharing was changed to allow external access, and establish details about the sharing activity and recipients where those details are recorded. The security

investigation tool is designed for this kind of incident response because it supports interactive filtering, examination of event details, and follow-up actions from the investigation workflow. Using the Drive-specific event data keeps the review centered on the service in which the suspected disclosure occurred and provides the most direct evidence for assessing the scope of a potential leak. Google documents the available Drive audit events, including sharing-related activity, in its Drive log events reference. For guidance on querying event data and responding to security issues, see Google's security investigation tool documentation.

QUESTION NO: 23

Your company is undergoing a regulatory compliance audit. As part of the audit, you are required to demonstrate that you can preserve all electronic communications related to a specific project for a potential legal discovery process. You need to configure Google Vault to accomplish this goal. What should you do?

A. Use the security investigation report to show Vault log events.

B. Use the search and export functionality to identify all relevant communications within the project timeframe.

C. Create a matter and a hold on all project-related data sources such as Email, Chat, and Drive within Google Workspace.

D. Create a custom retention policy for the project data. Ensure that the policy covers the required retention period.

ANSWER: C

Explanation:

Create a matter and a hold on all project-related data sources such as Email, Chat, and Drive within Google Workspace. A Vault matter provides the dedicated case workspace for a legal, regulatory, or audit investigation. Within that matter, an administrator can create holds that preserve data belonging to the users, groups, or organizational units involved in the project, and select the applicable Google Workspace services, including Gmail, Google Chat, and Drive. Holds take precedence over normal retention and prevent covered data from being permanently removed while the hold remains in effect, including data that users delete. This provides the defensible preservation needed before or during potential e-discovery, while also allowing authorized investigators to search and export the preserved material from the matter when needed. The hold's scope should be carefully aligned to the project participants and communication repositories so that the organization preserves the relevant electronic communications for the audit. Google documents the matter-based workflow and explains that holds preserve data indefinitely until they are released. See Create matters in Google Vault and Create holds in Google Vault.

QUESTION NO: 24

The CFO just informed you that one of their team members wire-transferred money to the wrong account because they received an email that appeared to be from the CFO. The CFO has provided a list of all users that may be responsible for sending wire transfers. The CFO also provided a list of banks the company sends wire transfers to. There are no external users that should be requesting wire transfers. The CFO is working with the bank to resolve the issue and needs your help to ensure that this does not happen again.

What two actions should you take? (Choose two.)

A. Configure objectionable content to reject messages with the words "wire transfer."

B. Verify that DMARC, DKIM, and SPF records are configured correctly for your domain.

C. Create a rule requiring secure transport for all messages regarding wire transfers.

D. Add the sender of the wire transfer email to the blocked senders list.

E. Enable all admin settings in Gmail's safety > spoofing and authentication.

ANSWER: B E

Explanation:

Verify that DMARC, DKIM, and SPF records are configured correctly for your domain because these email-authentication controls establish whether a message claiming to be from the organization is authorized to use its domain. SPF identifies authorized sending mail servers, DKIM provides a cryptographic signature for sent mail, and DMARC tells receiving systems how to handle mail that fails alignment and authentication checks. Correct configuration substantially reduces successful impersonation of the CFO using the company's own domain and provides reporting to help identify abuse. Google's guidance for protecting domains from spoofing is available in the Gmail email authentication documentation.

Enable all admin settings in Gmail's safety > spoofing and authentication because the incident is a business-email-compromise scenario based on sender impersonation. Gmail Safety settings provide layered protections, including enhanced spoofing detection and protections for messages impersonating employees or domains. Applying these protections across the organization helps Gmail identify and quarantine or reject suspicious messages before a finance employee acts on a fraudulent payment request. The available controls and their scope are documented in Google Workspace Gmail Safety settings.

QUESTION NO: 25

Multiple users in your organization are reporting that Calendar invitations sent from a specific department are not being received. You verified that the invitations are being sent and there are no error messages in the senderâ€™s logs. You want to troubleshoot the issue. What should you do?

A. Analyze the message headers of the sent invitations by using the Google Admin Toolbox to identify any delivery issues.

B. Verify that the senders in the specific department have the necessary permissions to share their calendars externally and send invitations outside of the organization.

C. Disable and re-enable the Calendar service for the affected users to refresh their connection.

D. Check the affected usersâ€™ Calendar settings to confirm whether they have accidentally blocked invitations from the specific department.

ANSWER: A

Explanation:

Analyze the message headers of the sent invitations by using the Google Admin Toolbox to identify any delivery issues. Calendar invitations are delivered as email messages containing calendar data, so the message headers provide technical delivery and routing details that are not necessarily visible in a sender's Calendar activity or logs. The Google Admin Toolbox Messageheader tool parses copied headers into a readable format and can expose relevant fields such as sender and recipient addressing, message IDs, mail servers that handled the message, authentication results, and routing-related information. Reviewing this information helps an administrator establish how the invitation was addressed and processed, then identify evidence that supports further investigation of delivery behavior affecting the recipients. This is particularly useful when the sender successfully creates and sends the event but the affected users do not see the invitation, because the issue may occur during mail transport or subsequent message handling rather than during event creation. Google describes the Messageheader tool and its header analysis capabilities in the Google Admin Toolbox Messageheader. For broader delivery tracing after header review, administrators can also use Email Log Search in the Admin console to investigate message-delivery events.