ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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:
Creating a matter and placing a hold on the relevant data sources ensures that all communications related to the specific project are preserved, even if users try to delete them. This will help in maintaining compliance with legal or regulatory requirements for e-discovery, and it ensures that data cannot be modified or deleted during the audit process.

Question: 2

Several employees from your finance department are collaborating on a long-term, multi-phase project. You need to create a confidential group for this project as quickly as possible. You also want to minimize management overhead. What should you do?

A. Create a Google Group by using Google Cloud Directory Sync (GCDS) to automatically sync the members.

B. Create a dynamic group and define the Department user attribute as a condition for membership with the value as the finance department.

C. Create a Google Group and update the settings to allow anyone in the organization to join the group.

D. Create a Google Group and appoint a group admin to manage the membership of this group.

Answer: B

Explanation:

A dynamic group automatically updates membership based on user attributes, such as department, ensuring that only relevant employees (e.g., those in the finance department) are added to the group. This minimizes management overhead because the membership is updated automatically, without the need for manual intervention. It also ensures that the group remains up to date as employees join or leave the department.

Question: 3

Today your company signed up for Google Workspace Business Starter with an existing domain name. You want to add team members and manage their access to email and other services. However, you are unable to create new user accounts or change user settings. You need to fix this problem. What should you do?

A. Run the Transfer tool to bring unmanaged users to your Workspace account.

B. Check domain ownership in the DNS settings.

C. Wait 24 hours after signing up for the features to become active.

D. Upgrade to a Google Workspace Enterprise edition.

Answer: B

Explanation:

To manage users and settings in Google Workspace, you must verify domain ownership. If the domain is not verified, you won't be able to create new user accounts or modify user settings. Checking the DNS settings and completing the domain verification process will resolve the issue and allow you to manage users and services in Google Workspace.

Question: 4

A team of temporary employees left your organization after completing a shared project. Per company policy, you need to disable their Google Workspace accounts while preserving all project data and related communications in Google Vault for a minimum of two years. You want to comply with this policy while minimizing cost. What should you do?

A. Purchase and assign Archived User licenses to the former employees.

B. Transfer the former employees' files and data to active user accounts. Delete the former employees' Workspace accounts.

C. Purchase additional user licenses and suspend the former employees' accounts.

D. Move the former employees to their own organizational unit (OU) and disable access to Google services for that OU.

Answer: A

Explanation:

Google Workspace offers Archived User licenses, which allow you to retain access to the data and communications of former employees without paying for a full user license. This option ensures compliance with the policy of retaining project data and communications in Google Vault while minimizing costs by avoiding unnecessary full user licenses.

Question: 5

The legal department at your organization is working on a time-critical merger and acquisition (M&A) deal. They urgently require access to specific email communications from an employee who is currently on leave. The organization's current retention policy is set to indefinite. You need to retrieve the required emails for the legal department in a manner that ensures data privacy. What should you do?

A. Instruct the IT department to directly access and forward the relevant emails to the legal department.

B. Temporarily grant the legal department access to the employee's email account with a restricted scope that is limited to the M&A-related emails.

C. Ask a colleague with delegate access to the employee's mailbox to identify and forward the relevant emails to the legal department.

D. Use Google Vault to create a matter specific to the M&A deal. Search for relevant emails within the employee's mailbox. Export and share relevant emails with your legal department.

Answer: D

Explanation:

Using Google Vault to create a matter specific to the M&A deal allows for legal, secure, and privacy- compliant retrieval of emails. You can search for the specific emails related to the merger and acquisition, export them, and share them with the legal department without granting direct access to the employee's mailbox. This approach ensures both data privacy and compliance with organizational policies.

Question: 6

Your company distributes an internal newsletter that contains sensitive information to all employees by email. You've noticed unauthorized forwarding of this newsletter to external addresses, potentially leading to data leaks. To prevent this, you need to implement a solution that automatically detects and blocks such forwarding while allowing legitimate internal sharing. What should you do?

A. Add a banner to the newsletter that warns users that external sharing is prohibited.

B. Create a Gmail content compliance rule that targets the internal newsletter, identifying instances of external forwarding. Configure the rule to reject the message when such forwarding is detected

C. Develop an Apps Script project by using the Gmail API to scan sent emails for the newsletter content and external recipients. Automatically revoke access for violating users.

D. Create a content compliance rule to modify the newsletter subject line, adding a warning against external forwarding.

Answer: B

Explanation:

A Gmail content compliance rule allows you to specifically target the internal newsletter and automatically detect when it is forwarded to external addresses. By rejecting such messages, you can prevent unauthorized sharing of sensitive information while still permitting internal sharing. This solution is effective for enforcing data security policies without manual intervention.

Question: 7

Your organization has hired temporary employees to work on a sensitive internal project. You need to ensure that the sensitive project data in Google Drive is limited to only internal domain sharing. You do not want to be overly restrictive. What should you do?

A. Configure the Drive sharing options for the domain to internal only.

B. Restrict the Drive sharing options for the domain to allowlisted domains.

C. Create a Drive DLP rule, and use the sensitive internal Project name as the detector.

D. Turn off the Drive sharing setting from the Team dashboard.

Answer: A

Explanation:

By configuring the Drive sharing options for your domain to "internal only," you ensure that sensitive project data is restricted to your organization's internal users. This prevents any external sharing while allowing your team members to collaborate freely within the organization. It strikes the right balance between maintaining security and avoiding unnecessary restrictions on collaboration.

Question: 8

Several employees at your company received messages with links to malicious websites. The messages appear to have been sent by your company's human resources department. You need to identify which users received the emails and prevent a recurrence of similar incidents in the future. What should you do?

A. Search the sender's email address by using Email Log Search. Identify the users that received the messages. Instruct them to mark them as spam in Gmail, delete the messages, and empty the trash.

B. Search for the sender's email address by using the security investigation tool. Mark the messages as phishing. Add the sender's email address to the Blocked senders list in the Spam, Phishing and Malware setting in Gmail to automatically reject future messages.

C. Collect a list of users who received the messages. Search the recipients' email addresses in Google Vault. Export and download the malicious emails in PST file format. Add the sender's email address to a quarantine list setting in Gmail to quarantine any future emails from the sender.

D. Search for the sender's email address by using the security investigation tool. Delete the messages. Turn on the safety options for spoofing and authentication protection in Gmail settings.

Answer: B

Explanation:

The security investigation tool in Google Workspace allows you to identify the impacted users and messages. By marking the messages as phishing, you acknowledge their malicious nature, helping to protect the users. Adding the sender's email address to the Blocked senders list ensures that future messages from this sender will be automatically blocked, preventing recurrence of similar incidents.

Question: 9

Your organization's users are reporting that a large volume of legitimate emails are being misidentified as spam in Gmail. You want to troubleshoot this problem while following Google- recommended practices. What should you do?

A. Adjust the organization's mail content compliance settings in the Admin console.

B. Advise users to individually allowlist senders.

C. Disable spam filtering for all users.

D. Contact Google Workspace support and report a suspected system-wide spam filter malfunction.

Answer: D

Explanation:

If legitimate emails are being misidentified as spam across the organization, it suggests that there may be a broader issue with the spam filtering system. Contacting Google Workspace support to investigate and resolve the problem is the recommended approach. Disabling spam filtering or adjusting individual settings may not resolve the root cause and could potentially lead to further issues.

Question: 10

Your organization's security team has published a list of vetted third-party apps and extensions that can be used by employees. All other apps are prohibited unless a business case is presented and approved. The Chrome Web Store policy applied at the top-level organization allows all apps and extensions with an admin blocklist. You need to disable any unapproved apps that have already been installed and prevent employees from installing unapproved apps. What should you do?

A. Change the Chrome Web Store allow/block mode setting to allow all apps, admin manages blocklist, In the App access control card, block any existing web app that is not on the security team's vetted list.

B. Change the Chrome Web Store allow/block mode setting to block all apps, admin manages allowlist. Add the apps on the security team's vetted list to the allowlist.

C. Disable Extensions and Chrome packaged apps as Allowed types of apps and extensions for the top-level organizational unit. Selectively enable the appropriate extension types for each suborganization

D. Disable the Chrome Web Store service for the top-level organizational unit. Enable the Chrome Web Store service for organizations that require Chrome apps and extensions.

Answer: B

Explanation:

Changing the Chrome Web Store policy to block all apps and managing an allowlist ensures that only vetted, approved apps are allowed for installation. This approach enforces the security team's policy by restricting access to unapproved apps while enabling the installation of only those apps that have
been explicitly approved. This method provides control over what can be installed, aligning with the organization's security requirements.

Question: 11

Your company handles sensitive client data and needs to maintain a high level of security to comply with strict industry regulations. You need to allow your company's security team to investigate potential security breaches by using the security investigation tool in the Google Admin console.

What should you do?

A. Create an activity rule that triggers email notifications to the security team whenever a high-risk security event occurs.

B. Assign the User Management Admin role to the security team.

C. Assign the super admin role to the security team

D. Create an administrator role with Security Center access. Assign the role to the security team.

Answer: D

Explanation:

To allow the security team to investigate potential security breaches using the security investigation tool, you should create a custom administrator role with Security Center access. This role will provide the security team with the necessary permissions to access and use the security investigation tool without granting them unnecessary permissions, such as those associated with User Management or Super Admin roles. This approach ensures both security and compliance with industry regulations.

Question: 12

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:

Transport Layer Security (TLS) ensures that emails are encrypted in transit between your organization and the banks, thereby enhancing privacy and security. By setting up TLS compliance and validating TLS connections for the banks' email domains, you ensure that the communication is secure and protected from interception, even if the banks use various email providers. This approach provides the highest level of privacy for sensitive financial communications.

Question: 13

An end user has thousands of files stored in Google Drive. Their files are well organized with Drive labels. You need to advise the end user on how to quickly identify all files that are contracts. What should you do?

A. Advise the user to use the Google Drive API to search for files with the keyword "contracts'

B. Advise the user to search in Drive for files with the keyword "contracts', and use the "modified by me' filter.

C. Advise the user to search for files that are labeled as "contracts'.

D. Advise the user to use the Investigation tool to search for files with the keyword "contracts' and updated by you.

Answer: C

Explanation:

Since the files are already organized with labels in Google Drive, the most efficient way for the user to quickly identify all files that are contracts is to search for files with the "contracts" label. This will filter and display only the files labeled as contracts, making it the quickest and most straightforward method for locating the required files.

Question: 14

You've received multiple reports about a suspicious email from someone who is pretending to be from your organization's human resources department. The email is prompting employees to click a link for a password update. You want to remediate this sender's emails. What should you do?

A. Use the security investigation tool to search for users who received the suspicious email, and select Mark message as phishing.

B. Use the security investigation tool to action the suspicious email and select Mark message as spam.

C. Create an activity rule to alert administrators to similar emails from that sender.

D. Notify all employees and request that they report this email as spam.

Answer: A

Explanation:

The security investigation tool allows you to search for and take action on suspicious emails within your organization. Marking the email as phishing helps to flag the email as malicious and prevents further emails from the same sender from being delivered to users' inboxes. This also ensures that the email is properly categorized for review and investigation by your security team.

Question: 15

Your company's security team has requested two requirements to secure employees' mobile devices-enforcement of a passcode and remote account wipe functionality. The security team does not want an agent to be installed on the mobile devices or to purchase additional licenses.

Employees have a mix of iOS and Android devices. You need to ensure that these requirements are met. What should you do?

A. Implement a third-party enterprise mobility management (EMM) provider.

B. Set up advanced mobile management for iOS devices and basic mobile management for Android devices.

C. Set up basic management for both iOS and Android devices.

D. Set up advanced management for both iOS and Android devices.

Answer: D

Explanation:

Advanced mobile management in Google Workspace provides the necessary features for securing mobile devices without the need for third-party apps or additional licenses. This includes enforcing passcodes and enabling remote account wipe functionality for both iOS and Android devices. Advanced management ensures that both security requirements are met while keeping the setup efficient and within the organization's existing licenses.

Question: 16

Your organization needs an approval application for purchases where a user can enter information on the purchase required and then submit it for management approval. You need to suggest a solution to create the application that must be available on both the web and mobile devices. Your organization does not have software developers or the budget to hire a third party. What should you do?

A. Suggest that the organization develop an application internally with a database, a backend service for data retrieval, and a frontend service for the application's user interface.

B. Suggest that the organization continue to approve requests manually until budget is available to use a third-party application provider.

C. Suggest the organization use AppSheet to create the application.

D. Suggest that the organization use AppScript to create forms linked to a Google Sheet to store the purchase data.

Answer: C

Explanation:

AppSheet is a no-code platform that allows users to create custom applications without the need for software development skills. It is capable of building applications that can be used both on the web and mobile devices. AppSheet would allow the organization to create the approval application efficiently, meeting the requirements of the purchase process, and would be a cost-effective solution that does not require hiring developers or using a third-party application provider.

Question: 17

Your organization is concerned about unauthorized access attempts. You want to implement a security measure that makes users change their password if there are twenty or more failed login attempts within one hour. You want to use the most effective and efficient approach. What should you do?

A. Set up a Chrome action rule to restrict users from defined ChromeOS actions after twenty failed password attempts.

B. Create an activity rule for user log events, define a time period and threshold, and select an Action for the rule to force a password change.

C. Create an activity rule for live-state data sources that meets the required time period and threshold to identify users who need to change their password.

D. Enable email alerts to notify users that they need to change their password.

Answer: B

Explanation:

Creating an activity rule for user log events allows you to monitor failed login attempts within a specific time period (such as one hour) and set a threshold (like twenty attempts). This rule can automatically trigger an action, such as forcing a password change, when the defined threshold is met. This is the most effective and efficient approach to addressing unauthorized access attempts while ensuring that security measures are enforced without manual

intervention.

Question: 18

An employee using a Workspace Enterprise Standard license was terminated from your organization. You need to ensure that the former employee no longer has access to their Workspace account and preserve access to the former employee's documents for the manager and the team.

You want to minimize license cost. What should you do?

A. Delete the former employee's Workspace account.

B. Suspend former employee's Workspace account.

C. Reset the password of the former employee and keep their Workspace license active.

D. Switch the license type of the former employee's Workspace account to an Archived User license.

Answer: D

Explanation:
Switching the former employee's account to an Archived User license ensures that their data and documents are preserved, and access is retained for the manager and team without incurring the full cost of an active Workspace license. Archived User licenses are a cost-effective way to maintain access to documents while preventing unauthorized access to the account.

Question: 19

Your organization's employees frequently collaborate with external clients and vendors by using Google Meet. There are active instances of unsupervised meetings within your organization that do not have a host, and unsupervised meetings that continue after an event has completed. You want to end all meetings that are being used inappropriately as quickly as possible. What should you do?

A. End all unsupervised meetings by using the Google Meet APIs.

B. Enable Host Management for Google Meet, and train internal host employees how to end meetings for everyone.

C. Turn off Google Meet in the Admin console for your organization. Turn Google Meet back on after two minutes.

D. Identify and end all unsupervised meetings by using the security investigation tool.

Answer: A

Explanation:

Using the Google Meet APIs allows you to programmatically end all unsupervised meetings quickly. This approach is the most effective for managing unsupervised meetings in real-time, especially if there are multiple such meetings happening across the organization. It provides a centralized method to monitor and take action on these meetings, ensuring security and preventing misuse.

Question: 20

Your organization uses live-streaming to host large Google Meet meetings. You need to limit the participation to affiliated Google Workspace domains by using the Admin console. What should you do?

A. Add the Trusted Workspace domain names in the Stream dialog box.

B. Turn off live streaming to Youtube.

C. Add participants to an organizational unit (OU). Turn on live streaming.

D. Turn on in-house live streaming. Invite users from affiliated domains.

Answer: C

Explanation:

By organizing participants into an organizational unit (OU) in the Admin console, you can control access to live streaming and ensure that only users from affiliated Google Workspace domains are allowed to participate in the live-streamed meetings. Turning on live streaming within this context will ensure that the meeting is restricted to the appropriate participants from the specified domains.

Question: 21

You are configuring email for your company's Google Workspace account. The company wants to prevent certain types of files from being sent or received as email attachments in the simplest and most cost-effective way. What should you do?

A. Adjust the maximum message size limit to prevent large files from being sent or received.

B. Enable the Security Sandbox in Gmail to automatically quarantine emails with suspicious attachments.

C. Scan all incoming and outgoing emails for malicious attachments by using an industry standard third-party email security solution.

D. Configure an attachment compliance rule in Gmail settings to block specific file types.

Answer: B

Explanation:

Configuring an attachment compliance rule in Gmail allows you to specifically block certain types of files from being sent or received as email attachments. This approach is simple and cost-effective because it leverages Google Workspace's built-in functionality without requiring third-party solutions or advanced configurations. You can easily specify which file types to block, ensuring that your organization is protected from undesirable attachments.

Question: 22

Your organization has a Shared Drive with 150 users organized as a group. All users of the group need to be able to add and edit files, but the ability to move, delete, and share content must be limited to a single user. You need to configure the shared drive to meet these requirements efficiently.

What should you do?

Your organization has a Shared Drive with 150 users organized as a group. All users of the group need to be able to add and edit files, but the ability to move, delete, and share content must be limited to a single user. You need to configure the shared drive to meet these requirements efficiently.

What should you do?

A. Create a folder inside the shared drive. Share the files with the group by using the share function.

B. Create a folder inside the shared drive. Share the folder link with the group.

C. In the Admin console, assign Contributor access for the shared drive to each user. Assign Content Manager access for the shared drive to the single user.

D. In the Admin console, assign Contributor access for the shared drive to the group. Assign Content Manager access for the shared drive to the single user.

Answer: D

Explanation:

By assigning Contributor access to the group, all 150 users will be able to add and edit files in the shared drive. Assigning Content Manager access to the single user ensures that only that person has the ability to move, delete, and share content within the shared drive. This approach efficiently meets the requirement of limiting certain administrative privileges while allowing the group to collaborate on content.

Question: 23

Your company wants to minimize distractions and inappropriate content in their Google Chat spaces. You need to give trusted employees the ability to remove messages and ban users from specific Chat spaces. What should you do?

A. Assign the trusted employees as moderators for the relevant Chat spaces.

B. Create a data loss prevention (DLP) rule that blocks inappropriate content from being shared

C. Use the security investigation tool to audit and monitor Chat messages.

D. Disable all Chat spaces except those specifically approved by management.

Answer: A

Explanation:

Assigning trusted employees as moderators for the relevant Chat spaces will give them the necessary privileges to

remove messages and ban users when needed. This is the most efficient way to control inappropriate content and maintain a positive and productive environment within the spaces. Moderators can take action to address issues directly without requiring more complex or restrictive solutions.

Question: 24

Your organization acquired a small agency. You need to create user accounts for these new employees. The new users must be able to use their new organization's email address and their email address with the sub-agency domain name. What should you do?

Your organization acquired a small agency. You need to create user accounts for these new employees. The new users must be able to use their new organization's email address and their email address with the sub-agency domain name. What should you do?

A. Redirect the acquired domain to Google's MX records and add the account as a "send as" address.

B. Set up the acquired agency as a secondary domain from the Manage domains page.

C. Set up the acquired agency as a user alias domain from the Manage domains page.

D. Set up the acquired agency as a secondary domain and swap it to the primary domain.

Answer: C

Explanation:

Setting up the acquired agency as a user alias domain allows users to have their new organization's email address while still being able to send and receive emails using their previous email address with the sub-agency domain. This approach efficiently ensures they can use both email addresses without requiring additional configuration for separate accounts.

Question: 25

The current data storage limit for the sales organizational unit (OU) at your company is set at 10GB per user. A subset of sales representatives in that OU need 100GB of storage across shared services. You need to increase the storage for only the subset of sales representatives by using the least disruptive approach and the fewest configuration steps. What

should you do?

A. Move the subset of users to a sub-OU, and assign a 100GB storage limit to that sub-OU.

B. Instruct the subset of users to store their documents in a Shared Drive with a 100GB limit.

C. Change the storage limit of the sales OU to 100GB.

D. Create a configuration group, and add the subset of users to that group. Set the group storage limit to 100GB.

Answer: A

Explanation:

By moving the subset of sales representatives to a sub-organizational unit (OU) and assigning a 100GB storage limit to that sub-OU, you can efficiently increase the storage for those users without affecting the rest of the sales team. This approach allows you to target the specific users that require more storage, maintaining minimal disruption and configuration steps.

Question: 26

Your company's security team should be able to investigate unauthorized external file sharing. You need to ensure that the security team can use the security investigation tool and you must follow the principle of least privilege.
What should you do?

A. Grant the super admin role to a delegate from the security team.

B. Create a pre-built reporting role. Assign the role to the security team alias.

C. Share the Drive audit log with the security team.

D. Create a custom admin role with security center privileges. Assign the role to the individual security team members.

Answer: D

Explanation:

By creating a custom admin role with security center privileges, you can ensure that the security team has the necessary access to investigate unauthorized external file sharing while adhering to the principle of least privilege. This approach provides the security team with the specific permissions they need without granting unnecessary broader privileges, such as those associated with the super admin role.

Question: 27

Users at your company are reporting that they are not receiving some emails in their corporate Gmail account. You have checked the Google Workspace Status Dashboard and you found no service disruptions. You need to identify the root cause of the problem and resolve the mail delivery issues. What should you do? (Choose two.)

A. Use Email Log Search (ELS) to identify specific delivery failures.

B. Verify whether the organization's Mail Exchange (MX) records are correctly configured.

C. Check the users' spam folders to determine whether emails are being misdirected.

D. Investigate the Gmail log events for error messages or unusual patterns.

E. Check the senders' IP addresses in the inbound mail gateway.

Answer: A, B

Explanation:

Use Email Log Search (ELS): ELS allows you to trace email delivery and identify issues, such as undelivered or bounced messages. This is an essential tool for identifying the root cause of mail delivery issues.

Verify whether the organization's Mail Exchange (MX) records are correctly configured: Incorrect MX records could prevent emails from being delivered to the organization's Gmail accounts. It's important to verify that these records are set up properly to ensure smooth email delivery.

Question: 28

You are designing a group structure for your company that will be used to grant access to a specific shared drive. You

need this solution to automatically add and remove employees based on their job role. What should you do?

A. Create a security group. Add all employees with the desired job role. Grant the security group access to the shared drive.

B. Create a distribution list. Add all employees with the desired job role. Grant the distribution list access to the shared drive.

C. Create a dynamic group. Set the membership criteria to the desired job role. Grant the dynamic group access to the shared drive.

D. Create a configuration group. Add users on an exception basis. Grant the configuration group access to the shared drive.

Answer: C

Explanation:

A dynamic group automatically manages its membership based on user attributes, such as job role. This approach ensures that employees are automatically added or removed from the group based on their role, minimizing manual effort and ensuring that the group always reflects the current team composition. Granting this dynamic group access to the shared drive ensures that the right users have the appropriate permissions without requiring constant manual updates.

Question: 29

An executive at your organization asked you to give their executive administrator access to their Workspace account. You need to ensure that this executive administrator can manage emails in the executive's account. You need to maintain security and privacy of the executive's account. What should you do?

A. Assist the executive in setting up email forwarding to their executive administrator.

B. Instruct the executive to share their password with their executive administrator.

C. Create a Google Group, and add all executive administrators. Enable delegated access to the Group.

D. Grant delegated access to the executive's Gmail account, and assign access to their executive administrator in Gmail settings.

Answer: D

Explanation:

Granting delegated access allows the executive administrator to manage the executive's emails without requiring access to the executive's password. This solution ensures security and privacy by limiting the permissions to email management only, while keeping the executive's account secure. The executive administrator will be able to send, read, and delete emails on behalf of the executive, but they won't have access to other aspects of the account.

Question: 30

The innovation team at your organization has a dedicated room with prototype equipment. You need to make the room bookable, add the equipment, and ensure that there are no booking conflicts. Only the innovation team and the sales directors can access this room. What should you do?

A. Create a separate Google Calendar resource for the room. Manually manage booking requests from both teams.

B. Create a Google Group for the innovation team and another Google Group for sales directors. Share the room's calendar with both groups.

C. Create a Google Calendar event for the room. Share the event with the innovation team and sales directors.

D. Edit the Google Calendar settings for the room resource. Adjust the permission settings so only the innovation team and sales director group can view and book time on this calendar.

Answer: D

Explanation:

By creating a dedicated Google Calendar resource for the room and adjusting its permission settings, you can ensure that only the innovation team and sales directors have access to book the room. This approach allows for centralized management of room bookings while preventing conflicts, as Google Calendar will automatically handle scheduling and prevent double-bookings.

Question: 31

You work for a healthcare provider that uses an external medical billing company to manage patient records and invoices. Your organization's employees need to share patient documents with the billing company's employees for processing. You need to configure access so the medical billing company's employees can view and edit the documents, but they cannot delete the documents. What should you do?

A. Create a shared drive that is managed by your organization's employees. Grant Contributor access to the billing company's staff.

B. Create a shared drive. Grant Content Manager access to your organization's employees and the billing company.

C. Create a group, and add the employees from your organization and the billing company. Create a shared folder on Google Drive. Grant Editor access to the group

D. Restrict access for the medical billing company's employees by using Data Loss Prevention (DLP) policies.

Answer: A

Explanation:
Creating a shared drive and granting Contributor access to the billing company's staff allows them to view and edit documents, but not delete them. This is the most suitable approach because it ensures that only your organization's employees manage the overall shared drive, while still allowing external users to collaborate on documents without compromising their integrity by preventing deletion. The shared drive structure also offers better control over document permissions compared to shared folders.

Question: 32

You are migrating your organization's email to Google Workspace. Your organization uses the terramearth.com email domain. You need to configure Google Workspace to receive emails sent to terramearth.com. What should you do?

A. Add terramearth.com as a primary, secondary, or alias domain in Google Workspace. Update the Mail Exchange (MX) records with your domain registrar to direct mail flow to Google's mail servers.

B. Establish a Transport Layer Security (TLS) connection between your company's existing mail servers and

Google's mail servers

C. Configure an email address in Google Workspace to capture emails sent to unverified domains, including terramearth.com.

D. Create a domain alias for terramearth.com in Google Workspace. Configure email forwarding to redirect emails to the new Google Workspace accounts.

Answer: A

Explanation:

To receive emails for your domain (terramearth.com) in Google Workspace, you need to add the domain to Google Workspace as either a primary, secondary, or alias domain, depending on your organization's requirements. After adding the domain, you must update the Mail Exchange (MX) records at your domain registrar to point to Google's mail servers. This step is essential to ensure that emails are correctly routed to Google Workspace.

Question: 33

Your organization is migrating their current on-premises email solution to Google Workspace. You need to ensure that emails sent to your domain are correctly routed to Gmail. What should you do?

A. Change the Mail Exchange (MX) records in your current email domain's DNS settings to point to Google's mail servers.

B. Set up email forwarding from your on-premises email provider to Gmail.

C. Create a content compliance rule to filter and route incoming emails.

D. Configure SPF, DKIM, and DMARC records in your current email domain's DNS settings.

Answer: A

Explanation:

To ensure that emails sent to your domain are correctly routed to Gmail, you need to update the Mail Exchange (MX) records in your domain's DNS settings to point to Google's mail servers. This is a critical step in the migration process, as

it ensures that all incoming email traffic is directed to Google Workspace after the switch.

Question: 34

Your compliance team has observed that employees at your organization are frequently resetting their passwords and is concerned about account hijacking. You need to create a solution to notify the compliance team whenever a user updates or resets their password. What should you do?

A. Create and enforce a new password policy for all users in your organization.

B. Move all compliance team members into a separate organizational unit (OU). Create and enforce a new password policy for the members of this OU.

C. Create an activity rule that is triggered by the User's password changed event. Add compliance team members as email recipients.

D. Create a new alert by using user log events. Check that the challenge type is "Password", and add the compliance team as email recipients.

Answer: C

Explanation:

Creating an activity rule that triggers on the "User's password changed" event allows you to automatically notify the compliance team whenever a user updates or resets their password. This approach is efficient because it directly ties the event to the rule and sends alerts without requiring manual monitoring or additional steps. By adding the compliance team as email recipients, you ensure they are promptly notified of any changes.

Question: 35

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 sender'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 users' Calendar settings to confirm whether they have accidentally blocked invitations from the specific department.

Answer: A

Explanation:
Using the Google Admin Toolbox to analyze the message headers of the sent invitations helps you identify if there are any issues with the delivery of the invitations, such as misrouted messages or issues with email delivery to the affected users. This approach will give you detailed information on what might be causing the issue, even if no error messages appear in the sender's logs.

Question: 36

The names and capacities of several conference rooms have been updated. You need to use the most efficient way to update these details.

What should you do?

A. Export the resource list to a CSV file, make the changes, and re-import the updated file.

B. Edit each resource in the Google Admin console.

C. Add the modified rooms as new resources. Tell employees not to use old rooms.

D. Delete the existing resources and recreate the resources with the updated information.

Answer: A

Explanation:

Exporting the resource list to a CSV file, making the necessary updates, and then re-importing the file is the most efficient method for updating multiple conference rooms at once. This approach allows you to make bulk updates quickly without needing to edit each resource individually or delete and recreate rooms. It also ensures that the updated information is applied to all affected rooms at once.

Question: 37

You are configuring Chrome browser security policies for your organization. These policies must restrict certain Chrome apps and extensions.

You need to ensure that these policies are applied on the devices regardless of which user logs into the device. What should you do?

A. Configure the allowed list of apps in the Devices page in the apps and extensions settings.

B. Configure the Chrome user setting to require users to sign in to use Chrome apps and extensions.

C. Configure the Policy Precedence to override the domain-wide policy applied for apps and extensions.

D. Require 2SV for user logins.

Answer: A

Explanation:

To ensure that Chrome apps and extension policies are applied regardless of which user logs into the device, you should configure the allowed list of apps in the Devices section of the apps and extensions settings. This policy applies at the device level, ensuring that the restrictions are enforced for any user who logs into that device, providing consistent security across the organization.

Question: 38

Your company's help desk is receiving technical support tickets from employees who report that messages from known external contacts are being sent to the spam label in Gmail. You need to correct the issue and ensure delivery of legitimate emails without introducing additional risk as soon as possible. What should you do?

A. Ask employees to select the messages in Gmail that are being delivered to spam and mark them as Not spam.

B. Contact the external senders, and tell them to authenticate their sent mail by using domain-based message authentication, reporting, and conformance (DMARC).

C. Turn off more aggressive spam filtering in spam policies that are applied to the users' organizational unit and add the senders' mail system IP addresses to the email allowlist.

D. Create an address list of approved senders so messages from these users bypass Gmail's spam filters and recipients can decide whether they are spam or not.

Answer: A

Explanation:

Asking employees to mark legitimate emails as "Not spam" helps train Gmail's spam filter to correctly identify these senders as trusted. This is a quick and effective way to correct the issue without introducing any additional risk or changes to the email filtering settings. Over time, Gmail will learn to recognize these senders as legitimate, reducing the likelihood of their messages being misclassified as spam in the future.

Question: 39

A user in your organization received a spam email that they reported for further investigation. You need to find out more details and the scope of this incident as quickly as possible. What should you do?

A. Conduct a Vault search to find this email and identify if additional users were affected.

B. Conduct a search to find all emails sent by the sender by using the Gmail API.

C. Conduct an Email reports search to find this email and all of the email's recipients.

D. Conduct a search in the security investigation tool to find this email, and identify whether additional users were affected.

Answer: D

Explanation:

The security investigation tool is specifically designed for investigating security incidents like spam and phishing emails. It allows you to search for emails, review their details, and determine the scope of the incident, including identifying whether other users were affected. This tool is the most appropriate and efficient way to respond to the incident.

Question: 40

You work at a large organization that prohibits employees from using Google Sites. However, a task force comprised of three people from five different departments has recently been formed to work on a project assigned by the Office of the CIO. You need to allow the users in this task force to temporarily use Google Sites. You want to use the least disruptive and most efficient approach. What should you do?

A. Turn Google Sites access on for each of the 15 users in the task force.

B. Create a configuration group for the task force's 15 users. Grant Google Sites access to the group.

C. Place the 15 task force users into a new organizational unit (OU). Turn on Google Sites access for the OU.

D. Create an access group for the task force's 15 users. Grant Google Sites access to the group.

Answer: C

Explanation:

Creating a new organizational unit (OU) for the task force members and turning on Google Sites access for that OU is the least disruptive and most efficient approach. It allows you to target only the users in the task force, granting them temporary access to Google Sites without impacting the rest of the organization. This solution also provides clear control over the access, which can be easily modified when the task force's work is completed.

Question: 41

Your organization collects credit card information in customer files. You need to implement a policy for your organization's Google Drive data that prevents the accidental sharing of files that contain credit card numbers with external users. You also need to record any sharing incidents for reporting.

What should you do?

A. Create a data loss prevention (DLP) rule that uses the predefined credit card number detector, sets the action to "block external sharing", and enables the "Log event" option.

B. Enable Gmail content compliance, and create a rule to block email attachments containing credit card numbers from being sent to external recipients.

C. Implement a third-party data loss prevention solution to integrate with Drive and provide advanced content detection capabilities.

D. Configure a data retention policy to automatically delete files containing credit card numbers after a specified period.

Answer: A

Explanation:

A data loss prevention (DLP) rule with the predefined credit card number detector will help you identify and prevent the accidental sharing of files that contain sensitive credit card information. Setting the action to "block external sharing" ensures that such files cannot be shared externally. Enabling the "Log event" option will record any incidents of external sharing for auditing and reporting purposes, fulfilling both the security and reporting requirements.

Question: 42

You are investigating a potential data breach. You need to see which devices are accessing corporate data and the applications used. What should you do?

A. Analyze the audit log in the Admin console for device and application activity.

B. Analyze the security investigation tool to access device log data.

C. Analyze the Google Workspace reporting section of the Admin console.

D. Analyze the User Accounts section in the Google Admin console.

Answer: A

Explanation:

The audit log in the Google Admin console provides detailed information about device and application activity, which is crucial for investigating a potential data breach. You can see which devices have accessed corporate data, as well as which applications were used, giving you a comprehensive view of any unauthorized or suspicious activities. This is the most appropriate and efficient tool for this investigation.

Question: 43

Your organization is implementing a new customer support process that uses Gmail. You need to create a cost-effective solution that allows external customers to send support request emails to the customer support team. The requests must be evenly distributed among the customer support agents. What should you do?

A. Create a Google Group, enable collaborative inbox settings, set posting permissions to "Anyone on the web", and add the customer support agents as group members.

B. Use delegated access for a specific email address that represents the customer support group, and add the customer support team as delegates for that email address.

C. Create a Google Group, add the support agents to the group, and set the posting permissions to "Public."

D. Set up an inbox for the customer support team. Provide the login credentials to the customer support team.

Answer: A

Explanation:
A Google Group with collaborative inbox settings allows you to evenly distribute support request emails among the team. By setting the posting permissions to "Anyone on the web," external customers can send emails directly to the group, and the emails will be distributed to the support agents as tasks. This is a cost-effective solution that also provides an organized way to manage and track customer support requests.

Question: 44

Your organization has enabled Google Groups for Business to let employees create and manage their own email distribution lists and web forums. You need to ensure that users cannot join external Google Groups with their Google

Workspace accounts without interrupting internal group usage. What should you do?

A. Set the setting for Google Groups for Business called Accessing groups from outside this organization to Private.

B. In Additional Google Services, turn Google Groups OFF at the root organizational unit.

C. Use the Directory API to change the settings of user-created groups to disable features that allow external users to access, view, or post on groups.

D. Set the setting for Google Groups for Business called Default for permission to view conversations to All organization users.

Answer: A

Explanation:

By setting the Accessing groups from outside this organization to Private, you prevent users from joining external Google Groups while still allowing internal users to use Google Groups within the organization. This setting ensures that only members of your organization can join and interact with internal groups, effectively stopping external access without affecting internal group usage.

Question: 45

You manage Chrome Enterprise browsers for your large organization. You want to ensure that specific extensions are automatically installed on all managed Chrome Enterprise browsers. What should you do?

A. Allowlist the specific Chrome browser extensions.

B. Configure a script to deploy the extensions upon user login.

C. Publish the extensions in the Chrome Web Store.

D. Force-install the extensions through Chrome browser policies.

Answer: D

Explanation:

Using Chrome browser policies, you can force-install specific extensions on all managed Chrome Enterprise browsers. This ensures that the desired extensions are automatically installed on users' browsers without requiring manual installation. This approach is the most efficient and scalable solution for managing extensions across a large organization.

Question: 46

You need to grant a specific set of users in your company access to YouTube, and you want to restrict their access to Merchant Center. What should you do?

A. Enable YouTube for all users in the company. Individually restrict access to Merchant Center for specific Groups or organizational units (OUs).

B. Create YouTube and Merchant Center as custom web apps. Apply access policies at the Group or organizational unit (OU) level.

C. Contact Google Support and request that they enable YouTube access for the specific set of users and restrict their access to Merchant Center.

D. Enable access to YouTube at the Group or organizational unit (OU) level for the subset of users. Disable access to Merchant Center.

Answer: D

Explanation:

By enabling YouTube access at the Group or organizational unit (OU) level, you can target a specific set of users, allowing them to access YouTube. Simultaneously, you can disable access to Merchant Center for those same users, ensuring they can access YouTube but not Merchant Center. This approach uses Google Workspace's built-in capabilities to manage access based on user groups or organizational units.

Question: 47

Your organization is about to conduct its biannual risk assessment. You need to help identify security risks by quickly reviewing all security settings for Gmail, Drive, and Calendar. What should you do?

A. In the reporting section of the Admin console, review the Gmail, Drive, and Calendar reports.

B. In the alert center, review all of the alerts.

C. In each individual organizational unit (OU), review the security settings.

D. In the Google Admin console, review the security health page.

Answer: D

Explanation:

The security health page in the Google Admin console provides an overview of security settings and highlights potential risks across various services, including Gmail, Drive, and Calendar. This page offers a consolidated view of the security posture of your organization, making it the most efficient option for quickly identifying security risks in preparation for a risk assessment.

Question: 48

You need to ensure that data owned by former employees remains available in Google Vault. You want to use the most cost-effective solution.

What should you do?

A. Migrate the former employees' Gmail to their manager(s) by using the data migration service during the deletion process. Transfer the former employees' Google Drive files to a new owner.

B. Change the Google account passwords of the former employees.

C. Suspend the former employees' Google accounts. Create an organizational unit (OU). Move the former employees into that OU.

D. Assign an Archived User license to the former employees' Google accounts.

Answer: C

Explanation:

Suspending the accounts of former employees while moving them to a dedicated organizational unit (OU) ensures that their data remains in Google Vault and accessible without the need for additional licenses. This is a cost-effective solution because suspending the account keeps the data intact but prevents the employees from accessing their accounts.

Question: 49

A user is experiencing intermittent issues accessing their Gmail inbox. Sometimes their Gmail loads slowly, and other times the user encounters error messages that haven't been documented. You need to effectively troubleshoot this recurring problem. What should you do?

A. Check the Google Workspace Status Dashboard for any reported service disruptions.

B. Instruct the user to generate a HAR file the next time they experience slowness or an error.

C. Instruct the user to try to access Gmail from another device or network to see if the issue persists.

D. Instruct the user to clear their browser cache and cookies.

Answer: B

Explanation:

A HAR file (HTTP Archive) records detailed information about the user's network activity, including HTTP requests and responses. This file can help diagnose issues with Gmail loading slowly or errors occurring, especially when they are intermittent. By generating a HAR file, you can provide valuable data for troubleshooting the issue and pinpoint any underlying network or browser-related issues.

Question: 50

You are managing the buildings and resources for your organization. You need to create several conference rooms with a capacity of 10 people each, equipped with a whiteboard and projector, and wheelchair accessible. You want to ensure the process is efficient. What should you do?

A. Automate room creation by using a third-party app from the Google Workspace Marketplace.

B. Create a CSV file and add all resources. Write a script using the Workspace API to reference the CSV file and

create all the resources.

C. Create each conference room individually in the Google Admin console. Add the features for each room.

D. Use the Google Admin console to bulk upload the rooms. Create a resource with the specified features and apply the features to that resource.

Answer: B

Explanation:

Using a CSV file to list all the conference rooms and a script to automate their creation via the Workspace API is the most efficient solution. This approach allows you to batch-create the rooms with the specified attributes (capacity, whiteboard, projector, wheelchair accessible) without manually inputting each room individually. It minimizes manual effort and ensures consistency across all room configurations.

Question: 51

Your organization allows employees to use their personal mobile devices to check their work emails.
You need to remove the employee's work email data from their phone when they leave the organization. What should you do?

A. Set up basic mobile management on the devices.

B. Set up advanced mobile management on the devices.

C. Set up data protection rules to prevent data sharing externally.

D. Set up 2SV authentication on the devices.

Answer: B

Explanation:

With advanced mobile management, you can remotely manage and wipe work-related data from personal devices when an employee leaves the organization. This includes the ability to enforce policies such as requiring a password to

access the device, remotely wiping corporate data, and managing access to work resources without affecting the personal data on the device. This solution provides the necessary tools to ensure data security and compliance.

Question: 52

External sharing at your company is only permitted for the sales and marketing department.

Engineering is not allowed to share externally. You need to configure the sharing settings to comply with this policy. What should you do?

A. Use a data loss prevention (DLP) solution to control external sharing based on user groups.

B. Create separate shared drives for each department with different external sharing settings.

C. Create organizational units (OUs) for each department. Configure different external sharing settings for each OU.

D. Configure Drive trust rules to restrict the engineering department from sharing externally.

Answer: C

Explanation:

By creating separate organizational units (OUs) for each department, you can apply different external sharing settings based on the department's requirements. For example, you can configure the sales and marketing department's OU to allow external sharing, while configuring the engineering department's OU to restrict external sharing. This approach allows you to enforce departmental policies efficiently without impacting other departments.

Question: 53

Your company has purchased Gemini licenses for a subset of employees. You need to ensure that only users in the marketing and sales departments have access to Gemini features by using the most efficient approach. What should you do?

A. Create a script to assign a Gemini license to new users if they are in marketing or sales. Run the script daily.

B. Create an organizational unit (OU) for marketing and sales. Assign the Gemini licenses to that OU, and enable Gemini for that OU only.

C. Assign Gemini licenses to each user in the marketing and sales departments.

D. Enable Gemini for the entire organization. Instruct users in other departments not to use Gemini.

Answer: B

Explanation:

Creating separate organizational units (OUs) for marketing and sales allows you to apply the Gemini licenses to only those departments. By enabling Gemini for just that OU, you ensure that only the employees in marketing and sales have access to Gemini features, ensuring an efficient and scalable solution. This avoids the need for manual assignment or unnecessary instructions to users in other departments.

Question: 54

Your company wants to enable single sign-on (SSO) for its employees to access a newly acquired cloud-based marketing platform. The marketing platform vendor has confirmed SAML 2.0 compatibility and provided the necessary metadat

a. You need to streamline user access and centralize authentication through Google Workspace. What should you do?

A. Request an API key from the marketing platform vendor for SAML integration.

B. Enable two-factor authentication for all users to enhance security before implementing SSO.

C. Instruct employees to log in to the marketing platform using the Sign In with Google functionality.

D. Create a new SAML application in the Google Admin console.

Answer: D

Explanation:

To enable single sign-on (SSO) through Google Workspace, you need to create a new SAML application in the Google

Admin console. This allows users to authenticate centrally through Google Workspace when accessing the marketing platform, leveraging SAML 2.0 compatibility. You can then upload the metadata provided by the marketing platform vendor to complete the integration. This approach ensures streamlined access and centralized authentication for your employees.

Question: 55

Your organization handles a significant amount of sensitive customer data and must follow strict industry regulations. To meet an upcoming compliance deadline, you need to quickly implement a solution that automatically classifies files stored in Google Drive based on the content of files.

What should you do?

A. Create data loss prevention (DLP) rules for Drive. Configure the rules to apply Drive labels based on content.

B. Apply Drive labels based on content. Use Google Vault to create retention rules based on Drive labels, ensuring that data is kept for the required duration.

C. Implement a third-party data governance tool that integrates with Drive and provides advanced classification capabilities.

D. Add users into organizational units (OUs). Configure default file classification in Drive for the desired OUs.

Answer: A

Explanation:

Data loss prevention (DLP) rules in Google Workspace allow you to automatically classify and label files in Google Drive based on their content, such as identifying sensitive customer data. This ensures compliance by applying the appropriate classification to files as they are stored, allowing you to quickly meet the compliance deadline while automating the classification process based on predefined criteria.

Question: 56

Your company provides shared Chromebook workstations for employees to access sensitive company dat

a. You must configure the devices to ensure no sensitive data is stored locally and that browsing data is cleared after each use. What should you do?

A. Force ephemeral mode in Chrome. Disable ofline access for sensitive Workspace apps like Docs, Sheets, and Drive.

B. Enable the Manage Guest Session functionality, and set the maximum user session length.

C. Force ephemeral mode in Chrome. Allow ofline access for all Workspace apps with strict expiration times.

D. Disable ofline access for all Workspace apps. Enable incognito mode for Chrome browsing sessions.

Answer: A

Explanation:

Enabling ephemeral mode in Chrome ensures that all browsing data is cleared after each session, and nothing is stored locally on the Chromebook. Disabling ofline access for sensitive Workspace apps, such as Docs, Sheets, and Drive, ensures that users cannot download or store sensitive data locally. This combination provides a secure environment, preventing the retention of any sensitive data on the device after use.

Question: 57

A new user at your organization is unable to access Google Meet. You have verified that the user's account is active and the correct licenses are assigned. You need to resolve the access issue. What should you do?

A. Check the user's browser settings to ensure that Meet is not blocked.

B. Instruct the user to clear their browser's cache and cookies.

C. Restart the user's computer to refresh their network connection.

D. Verify that Meet is enabled as a service for the user's account in the Admin console.

Answer: D

Explanation:

To resolve access issues with Google Meet, it's important to verify that Google Meet is enabled as a service for the user's account in the Admin console. Sometimes, individual services may be disabled for specific users or organizational units, even if the user has the correct license assigned. Ensuring that Google Meet is enabled for the user's account will grant them the necessary access to the service.

Question: 58

During a recent Google Meet video conference, several employees reported that they could not hear the presenters. The presenters confirmed that their laptops' microphones were working. The affected employees were all using company-issued laptops. You need to quickly diagnose the source of the issue. What should you do first?

A. Verify that the audio drivers on the affected laptops are up-to-date and functioning correctly.

B. Check the Admin console to determine whether there are recent Meet-related notifications or alerts.

C. Check if Context-Aware access rules were set to prevent Meet access from the user's network location.

D. Use the Meet quality tool for each affected user to analyze their microphone settings and configurations during the meeting.

Answer: A

Explanation:

Since the presenters' microphones are working, the issue likely lies with the affected employees' laptops. The first step in diagnosing the problem is to verify that the audio drivers on the affected laptops are up-to-date and functioning correctly. Outdated or malfunctioning audio drivers can cause issues with hearing sound during video conferences. Once the drivers are confirmed to be functional, further troubleshooting steps can be taken if necessary.

Question: 59

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 users' 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:
To restrict access to Google Drive for users when they are traveling internationally, you can define location-based access levels. By assigning these levels to the Google Drive app for the specific organizational unit (OU), you can control access based on the geographical location of the user. This ensures that users will only be able to access Google Drive from approved locations, effectively preventing access when they are traveling internationally for business.

Question: 60

Your company is transitioning to Google Workspace from legacy communication and collaboration applications. User accounts are managed in Active Directory and synced to Google Workspace by using Google Cloud Directory Sync (GCDS). Your company is implementing a new security policy for all accounts that requires complex passwords. Passwords must be at least 20 characters long, contain 3 symbols, 4 numbers, and 2 capital letters.

You need to enforce the new password policy in Google Workspace. What should you do?

A. Share the instructions for changing a Google account password with your users. Monitor password strength in the Google Admin console as users change their passwords.

B. Enable strong password enforcement and require a minimum length of 20 characters at the top level organizational unit.

C. Create a password policy in Active Directory. Install Password Sync on the global catalog servers for Active Directory and require a password change for your users.

D. Create a password policy in Active Directory. Enable password synchronization in GCDS.

Answer: D

Explanation:

Since user accounts are managed in Active Directory (AD) and synced to Google Workspace via Google Cloud Directory Sync (GCDS), the best approach to enforce the new password policy is to create the password policy within Active Directory and then enable password synchronization in GCDS. This ensures that the complex password requirements are enforced within AD, and when passwords are updated, they will be synchronized with Google Workspace, maintaining consistency across both systems.

Question: 61

Your company's legal department has issued a litigation hold that requires you to preserve all data related to a specific project. You need to ensure that all data for this project, including emails, documents, and chats, are preserved indefinitely and cannot be deleted by users. What should you do?

A. Create a hold in Google Vault that includes all users and data sources associated with the project.

B. Assign an Archived User license to all users involved in the project.

C. Set up a retention rule in Google Vault that retains all data from Gmail and Drive indefinitely.

D. Export all project related data from Google Workspace and store the data in a separate, secure location.

Answer: A

Explanation:

To preserve all data related to the project, including emails, documents, and chats, and to prevent it from being deleted by users, you should create a hold in Google Vault. A hold ensures that data is preserved indefinitely, regardless of user actions, and applies to the users and data sources (such as Gmail, Drive, and Chats) associated with the project. This is the most efficient and compliant way to meet the litigation hold requirements.

Question: 62

Your organization allows employees to use their personal devices for work purposes. You want to ensure these devices follow the company's security policies. You need to choose a mobile management solution that provides minimal passcode enforcement and allows for an admin to remotely wipe a user's account from the device. You also want to avoid having to install agents on employees' personal devices. What should you do?

A. Implement Google's advanced management on mobile devices.

B. Implement Google's basic management on mobile devices.

C. Enforce a strong password policy, and enforce the password policy at the next sign-in.

D. Deploy a third-party mobile device management (MDM) solution.

Answer: B

Explanation:

Google's basic management for mobile devices allows administrators to enforce minimal security policies, such as passcode enforcement, without requiring the installation of any agents on employees' personal devices. This solution also allows for remotely wiping a user's account from the device if needed, ensuring data security while maintaining a less intrusive management approach for personal devices.

Question: 63

An employee is leaving your company and has numerous files stored in My Drive. Their manager wants to retain access to these files. You need to offboard the departing employee's Google Workspace account while ensuring that the manager can still access the files while following Google- recommended practices. What should you do?

A. Use Google Vault to establish a retention policy for the organizational unit (OU) of the departing employee.

Assign the Google Archived User license.

B. Instruct the departing employee to share their My Drive folder with the manager before leaving. Delete the Google Workspace account on the departing employee's last day.

C. Download the departing employee's Drive data by using Google Takeout. Upload the data to the manager's Drive before deleting the departing employee's Google Workspace account.

D. Transfer ownership of the departing employee's files to the manager during the user deletion process.

Answer: D

Explanation:

Transferring ownership of the departing employee's files to the manager ensures that the manager retains access to all the files, including those stored in My Drive, without requiring additional steps like downloading or sharing files. This method follows Google-recommended practices and ensures that the files remain under proper management even after the employee's account is deleted. This process can be done efficiently during the offboarding process to ensure continuity of access.

Question: 64

You need to create an automated application or process that includes connectors to external data, leverages Google Sheets data, and is easily shared as a mobile application. What should you do?

A. Create an application by using App Engine. Connect the application to your Workspace environment

B. Copy the external data to BigQuery. Use a Connected Sheet to interact with the data.

C. Create an AppSheet application to connect the different data sources. Set up the mobile application.

D. Create an automation process by using Apps Script. Run the process through Google Sheets.

Answer: C

Explanation:

AppSheet is a no-code platform that allows you to easily create mobile applications that can connect to external data sources, including Google Sheets. It is ideal for quickly building automated apps that integrate data from various sources and can be easily shared with others on mobile devices.
AppSheet provides an efficient way to create, customize, and deploy mobile applications without the need for extensive development skills.

Question: 65

Your organization recently deployed Google Workspace. Over 3,000 external contacts were shared in public folders in Microsoft Exchange before the implementation. You need to ensure that these external contacts appear to domain users in Gmail. What should you do?

A. Export the external contacts to a CSV file, upload the file to Google Drive, and instruct users to import to their My Contacts.

B. Use Google Cloud Directory Sync to sync the external contacts from the public folders in Microsoft Exchange to the Directory.

C. Use the Domain Shared Contacts API to add the external contacts to the Directory.

D. Create a user account, add the external contacts, and delegate them to all users in the domain.

Answer: C

Explanation:

The Domain Shared Contacts API allows you to add external contacts to the Google Workspace directory, making them available to all users in the domain. This is the most effective and scalable solution for adding a large number of external contacts (like the 3,000 from Microsoft Exchange) to your Google Workspace environment. Once the contacts are added to the directory, they will be accessible to all users in Gmail and other Google Workspace apps.

Question: 66

Your organization has experienced a recent increase in unauthorized access attempts to your company's Google Workspace instance. You need to enhance the security of user accounts while following Google-recommended

practices. What should you do?

A. Disable password recovery options to prevent unauthorized individuals from accessing user accounts.

B. Implement a strong password policy and enable text messages as the 2-Step Verification (2SV) using text messages.

C. Enforce the use of physical security keys as the 2-Step Verification (2SV) method for all users.

D. Enforce a strong password policy that requires users to include special characters, numbers, and uppercase letters.

Answer: C

Explanation:

Enforcing the use of physical security keys for 2-Step Verification (2SV) provides a highly secure method of protecting user accounts from unauthorized access. Physical security keys are one of the most robust forms of two-factor authentication because they cannot be easily phished or stolen, even if an attacker knows the user's password. Google recommends using physical security keys as the 2SV method, as they provide strong protection against unauthorized access attempts.

Question: 67

Your company operates several primary care clinics where employees routinely work with protected health information (PHI). You are in the process of transitioning the organization to Google Workspace from a legacy communication and collaboration system. After you sign the Business Associate Agreement (BAA), you need to ensure that data is handled in compliance with regulations when using Google Workspace. What should you do?

A. Implement a third-party backup service that is also compliant with Google Workspace core services.

B. Create a label for Google Drive content to help employees identify sensitive data.

C. Instruct the staff to not store any PHI in Google Workspace core services, including Google Drive. Docs. Sheets, and Keep.

D. Disable integrations with third-party apps and turn off non-core Google services.

Answer: B

Explanation:

To ensure compliance with regulations when handling protected health information (PHI) in Google Workspace, creating labels for sensitive data, such as PHI, helps employees identify and manage this information properly. Labels can be used to mark files that contain sensitive data, providing an additional layer of organization and protection. This approach aligns with regulatory requirements by ensuring that employees can easily distinguish PHI from other data and apply the necessary policies and security measures.

Question: 68

You are onboarding a new employee who will use a company-provided Android device. Your company requires the ability to enforce strong security policies on mobile devices, including password complexity requirements and remote device wipe capabilities. You need to choose the appropriate Google Workspace mobile device management solution. What should you do?

A. Use a third-party mobile device management (MDM) solution to manage the device.

B. Allow the employee to use their personal device without enrolling it in any mobile device management (MDM) solution.

C. Implement Google's basic management solution for the mobile device.

D. Implement Google's advanced management solution for the mobile device.

Answer: D

Explanation:

Google's advanced management solution for mobile devices provides the ability to enforce strong security policies, including password complexity requirements and remote wipe capabilities. This solution allows administrators to manage and secure company-provided Android devices, ensuring compliance with company security policies. Advanced management offers greater control over device settings and security features compared to basic management, which is more limited in scope.

Question: 69

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:

By setting the default conversation history to "ON" at the top level, all employees will have chat history enabled by default. Allowing users to change their own history setting gives them the flexibility to turn off chat history if they choose to do so. This approach aligns with your goal of enabling chat history by default while still giving employees the option to turn it off.

Question: 70

Your company wants to start using Google Workspace for email. Your domain is verified through a third-party provider. You need to route the email to Google Workspace. What should you do?

A. Change your domain's A record to point to Google's mail servers.

B. Configure a forwarding rule in your current email system to redirect all messages to Gmail.

C. Update your domain's MX records to the Google Workspace MX records provided in the setup instructions.

D. Create a CNAME record that maps your domain to "gmail.com."

Answer: C

Explanation:

To route your email to Google Workspace, you need to update your domain's MX (Mail Exchange) records to point to Google's mail servers. This step ensures that emails sent to your domain are delivered to your Google Workspace Gmail accounts. The MX records are provided in the setup instructions during the Google Workspace configuration process.

Question: 71

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:

Conduct regular security awareness training to educate users: Educating users about phishing threats and safe online practices can help them recognize and avoid phishing attempts, reducing the chances of them falling for such scams.

Create a Drive trust rule that blocks all external domains except for a pre-approved list of trusted partners: By setting up a Drive trust rule to limit access to files from external domains, you can block links to malicious files hosted on untrusted external Google Drives while still allowing access to legitimate external files from trusted sources.

Question: 72

A user accessing sensitive data is experiencing repeated issues with accessing certain files in Google Drive from their laptop by using the Chrome browser. When you contact Google support, the support representative asks to review an HTTP archive file recording (HAR). You need to share logs with Google support without compromising data privacy. What should you do?

A. Open the HAR file in a text editor and delete sensitive information. Upload the HAR file to Google Drive and share the file only with the Google support representative

B. Ask the Google support representative for access to a Google Drive folder used by the Google support team. Upload the HAR file.

C. Share your screen with the Google support representative so they can view the file without having a copy of the file.

D. Upload the HAR file to Google Drive and share the file with the Google support representative.

Answer: A

Explanation:

The HAR (HTTP Archive) file can contain sensitive information, such as URLs, request headers, cookies, or other data that could expose personal or confidential information. To ensure privacy and security, you should review the HAR file, remove any sensitive information manually using a text editor, and then upload the file to Google Drive for sharing with the Google support representative. This approach allows you to provide the necessary logs for troubleshooting without compromising data privacy.

Question: 73

Per regulatory requirements, your company is required to keep the data of employees located in Germany within Europe and the data of employees located in the US within the US. The employees in Germany are in a separate organizational unit (OU) than employees in the US. You need to ensure that where employee data is stored is in compliance with the location regulations.

What should you do?

A. Instruct employees to use Drive for desktop to keep documents on their corporate computers.

B. Create two Groups. Assign employees into the Germany or US Group based on their location. Use Google Drive trust rules to prevent sharing between the Groups.

C. Navigate to the Data Regions function in the Admin console. Select the Europe region for employees in Germany, and select the US region for US employees.

D. Navigate to the Data Regions function in the Admin console. Select 'No preference.'

Answer: C

Explanation:
Using the Data Regions function in the Google Admin console, you can specify where data is stored for different organizational units (OUs) based on their geographical location. This ensures that employee data for those in Germany is stored within Europe, while data for US employees is stored within the US, meeting the regulatory requirements for data locality. This approach automates compliance and eliminates the need for manual tracking or additional configurations.

Okay, I will carefully review the question and provide a 100% verified answer based on the official Associate Google Workspace Administrator documentation, correct any typing errors, and present it in the requested format.

Question: 74

Your company has recently migrated from an on-premises email solution to Google Workspace. You have successfully added and verified the new primary domain. However, you also want to continue receiving emails sent to your former on-premises email server for a transitional period. You need to ensure that emails sent to your former domain are still delivered to your on-premises server, even though your primary email system is now Google Workspace. What should you do?

A. Configure MX records for the former domain to point to your on-premises email servers.

B. Add the former domain as a secondary domain in your Google Workspace settings and verify the domain.

C. Adjust the TTL (Time-to-Live) for the former domain to ensure a smooth transition.

D. Add the former domain as a domain alias for the primary domain.

Answer: A

Explanation:

To ensure that emails sent to your former domain are still delivered to your on-premises server during a transitional period after migrating your primary email to Google Workspace, you need to configure the MX (Mail Exchanger) records for the former domain to point to your on-premises email servers.

Here's why the other options are incorrect and why configuring MX records is the correct approach, based on the principles of email routing and domain management within Google Workspace:

A . Configure MX records for the former domain to point to your on-premises email servers.

MX records are DNS records that specify the mail servers responsible for accepting email messages on behalf of a domain. 1 By configuring the MX records for your former domain to point to the IP addresses or hostnames of your on-premises email servers, you are instructing the internet's DNS system that any email addressed to users on your former domain should be routed to those specific servers. This ensures that mail for the former domain bypasses Google Workspace and continues to be delivered to your existing infrastructure.

Associate Google Workspace Administrator topics guides or documents reference: While the exact phrasing might vary across different Google Workspace support articles and documentation, the core concept of MX records and their role in email routing is fundamental to domain setup and management. The official Google Workspace Admin Help documentation on "Set up MX records for Google Workspace" (or similar titles) explicitly explains how MX records control where email for a domain is delivered. In this scenario, you are essentially managing the MX records for a domain that is not the primary Google Workspace domain to direct its mail flow.

B . Add the former domain as a secondary domain in your Google Workspace settings and verify the domain.

Adding a domain as a secondary domain within Google Workspace allows you to create separate user accounts with email addresses on that domain, all managed within your Google Workspace organization. This would mean that Google Workspace would handle the email for the former domain, which is the opposite of what you need in this scenario (you want the emails to go to your on-premises server).

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Add a domain or domain alias" clearly distinguishes between secondary domains and domain aliases and their respective functionalities. Secondary domains are for managing separate sets of users, not for routing mail to external servers.

C . Adjust the TTL (Time-to-Live) for the former domain to ensure a smooth transition.

TTL is the amount of time a DNS record is cached by resolving name servers. While adjusting TTL can be important when making DNS changes (like switching MX records to Google Workspace), it doesn't directly control where email is delivered. Lowering the TTL before making MX changes to point to Google Workspace helps with a faster transition, but

in this case, you are not pointing the former domain's mail to Google Workspace. Therefore, adjusting the TTL alone will not achieve the desired outcome.

Associate Google Workspace Administrator topics guides or documents reference: Information on

TTL is typically found within the context of DNS management best practices in Google Workspace Admin Help, often related to domain verification or MX record changes to Google. It doesn't serve as a mechanism for routing mail to external, non-Google Workspace servers for a domain that isn't managed by Google Workspace for email.

D . Add the former domain as a domain alias for the primary domain.

Adding a domain as a domain alias means that emails sent to addresses on the alias domain will be delivered to the corresponding user accounts on your primary Google Workspace domain. This is useful when you want users to receive email at multiple domain names within your Google Workspace environment. It does not route email to an external, on-premises server.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Add a domain or domain alias" clearly explains the functionality of domain aliases. It emphasizes that email sent to a domain alias is received by the users on the primary domain, not an external system.

Therefore, the only way to ensure emails sent to your former domain are still delivered to your onpremises server is by configuring the MX records for that former domain to point to your onpremises mail server.

Question: 75

Your company's sales team writes many business proposals in Google Docs. They want to streamline the proposal process by using templates. You need to create a document template with prepopulated sections that the sales team can access. What should you do?

A. Create the templates in Google Drive. Grant edit access to the sales team.

B. Create the templates in Google Drive. Make a copy for each sales representative. Transfer ownership of each template to the sales representatives.

C. Enable organization branding in the Admin console. Create the templates in Google Drive. Add the templates to default themes and templates for the entire organization.

D. Create the templates in Google Drive and download the files as PDFs. Upload PDF files to a drive shared with your sales team.

Answer: C

Explanation:

To create document templates with pre-populated sections that the sales team can easily access and use to streamline their proposal process, the most efficient and centrally managed approach is to utilize the Google Workspace template gallery. This involves enabling organization branding (though not strictly required for basic templates, it's often associated with organizational templates) and then adding the created templates to the default themes and templates for the entire organization or specific groups.

Here's a breakdown of why option C is correct and why the others are not the ideal solutions:

C . Enable organization branding in the Admin console. Create the templates in Google Drive. Add the templates to default themes and templates for the entire organization.

This option leverages the built-in template gallery feature of Google Workspace. By creating the templates in Google Docs (which are stored in Google Drive) and then adding them to the organization's default themes and templates through the Google Admin console, you make these templates easily discoverable by all users (or a specific organizational unit) when they go to create a new document from the template gallery. Enabling organization branding can help customize the look and feel, but the crucial part is adding the templates to the gallery.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation provides detailed instructions on "Create and manage document templates for your organization." This documentation explains how to prepare a document as a template in Google Drive and then submit it through the Admin console to the template gallery, making it available to users within the organization. Topics covered include:Submitting templates to your organization's gallery: This process involves going to Apps > Google Workspace > Drive and Docs > Templates in the Admin console.

Setting up a custom template gallery: The documentation guides administrators on how to manage the templates that appear for their users.

Organizational units: Templates can often be made available to specific organizational units, allowing for tailored templates for different teams like the sales team.

A . Create the templates in Google Drive. Grant edit access to the sales team.

Granting edit access to the sales team on the master templates is problematic. It could lead to accidental or intentional modifications of the original templates, causing inconsistencies and requiring ongoing management to ensure the templates remain in their intended state. Users should ideally create copies of the template to work on, leaving the original template untouched.

Associate Google Workspace Administrator topics guides or documents reference: Best practices for file sharing and collaboration in Google Drive emphasize providing appropriate levels of access. For

templates, the goal is usually for users to use the template to create new documents, not to edit the original.

B . Create the templates in Google Drive. Make a copy for each sales representative. Transfer ownership of each template to the sales representatives.

This approach is inefficient and difficult to manage. Creating and transferring ownership of individual copies of the template to each sales representative would be time-consuming for the administrator. Furthermore, if the template needs to be updated, each individual copy would need to be modified, leading to version control issues and inconsistencies across the sales team.

Associate Google Workspace Administrator topics guides or documents reference: Google Drive's sharing and ownership features are designed for collaborative work on documents, not for distributing and managing templates in this manner. Centralized management through the template gallery is the recommended method.

D . Create the templates in Google Drive and download the files as PDFs. Upload PDF files to a drive shared with your sales team.

Saving the templates as PDFs defeats the purpose of having editable templates. The sales team would not be able to easily modify the pre-populated sections or add their specific proposal details to a PDF. Templates are meant to be starting points for new, editable documents.

Associate Google Workspace Administrator topics guides or documents reference: Google Docs is designed for creating and editing documents. Templates are a feature within this editable format, allowing users to start with a pre-structured document that they can then customize. PDFs are for final, non-editable versions.

Therefore, the correct approach is to leverage the Google Workspace template gallery to provide a streamlined and centrally managed way for the sales team to access and use the proposal templates. This is achieved by creating the templates in Google Drive and then adding them to the organizational templates through the Admin console. While enabling organization branding is mentioned in option C, the core functionality relies on the template gallery feature.

Question: 76

You are configuring data governance policies for your organization's Google Drive. You need to ensure that employees in the Research and Development department can share files with external users, while employees in the Finance department are blocked from sharing any files externally. What should you do?

A. Create a Drive trust rule that allows external sharing for the Research and Development organizational unit (OU) and another rule that blocks external sharing for the Finance OU.

B. Enable Vault for the Finance organizational unit (OU) to ensure that all files shared externally are retained and auditable.

C. Apply an organization-wide data loss prevention (DLP) rule that scans for sensitive information and prevents external sharing of those files. Apply that rule to the Finance organizational unit (OU).

D. Create a separate Google Workspace domain for the Finance organizational unit (OU) and disable external sharing for that domain.

Answer: A

Explanation:

To enforce different external sharing policies for different departments within the same Google Workspace domain, you should use Google Drive sharing policies configured at the organizational unit (OU) level. Drive trust rules are the mechanism within Google Workspace to control how users can share files inside and outside the organization.

Here's why option A is correct and why the others are not the most appropriate solutions:

A . Create a Drive trust rule that allows external sharing for the Research and Development organizational unit (OU) and another rule that blocks external sharing for the Finance OU.

Google Workspace allows administrators to set specific Drive sharing settings for different organizational units. By creating a Drive trust rule (or more accurately, configuring the external sharing options within Drive and Docs settings for each OU), you can enable external sharing for the Research and Development OU while simultaneously restricting or completely blocking external sharing for the Finance OU. This granular control at the OU level directly addresses the requirement of having different policies for the two departments.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "Control how users can share Drive files externally" (or similar titles) explains how to manage external sharing options at the organizational unit level. This includes:Setting sharing options by organizational unit: The documentation details how to navigate to Apps > Google Workspace > Drive and Docs > Sharing settings in the Admin

console and then select a specific organizational unit to customize its sharing permissions.

Controlling sharing outside your organization: This section explains the various settings available, including allowing sharing with anyone, only with specific domains, or completely preventing external sharing.

While the term "Drive trust rule" might be used in more advanced contexts related to trusted domains, the core functionality of controlling external sharing based on OUs is the key here. The settings within the Drive and Docs sharing configuration for each OU achieve the desired outcome.

B . Enable Vault for the Finance organizational unit (OU) to ensure that all files shared externally are retained and

auditable.

Google Vault is used for eDiscovery, legal holds, and retention of data. While it can retain and audit externally shared files (if sharing is allowed), it does not prevent external sharing. Enabling Vault for the Finance OU would not block them from sharing files externally; it would only ensure that if they do, those shared files are preserved and can be audited. This does not meet the requirement of blocking external sharing for the Finance department.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on Google Vault clearly outlines its purpose and functionalities, which are focused on data retention, legal holds, and search/export for compliance and legal reasons, not on preventing sharing.

C . Apply an organization-wide data loss prevention (DLP) rule that scans for sensitive information and prevents external sharing of those files. Apply that rule to the Finance organizational unit (OU).

While DLP rules can prevent the external sharing of files containing sensitive information, they are triggered by the content of the files, not by a blanket restriction on all external sharing for a specific OU. The requirement is to block all external sharing for the Finance department, regardless of the content. Applying a DLP rule only to the Finance OU might be complex to manage for a complete block and is not the most direct way to achieve the stated goal. OU-based sharing settings are more straightforward for this purpose.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on Data Loss Prevention (DLP) explains how to create rules based on content to prevent sensitive data leaks. While DLP can control sharing, it's not the primary mechanism for completely blocking all external sharing for an entire OU.

D . Create a separate Google Workspace domain for the Finance organizational unit (OU) and disable external sharing for that domain.

Creating a separate Google Workspace domain for the Finance department is an overly complex and administratively burdensome solution. It would involve managing two separate domains, user

accounts, billing, and potentially complicate internal collaboration between departments. Using organizational units within the same domain provides a much more efficient and manageable way to apply different policies.

Associate Google Workspace Administrator topics guides or documents reference: Google Workspace's organizational unit structure is specifically designed to allow administrators to apply different settings and policies to groups of users within a single domain, avoiding the need for separate domains for policy enforcement.

Therefore, the most direct and appropriate solution is to configure the Google Drive sharing settings at the organizational unit level, allowing external sharing for the Research and Development OU and blocking it for the Finance OU.

Question: 77

A department at your company wants access to the latest AI-powered features in Google Workspace.
You know that Gemini offers advanced capabilities and you need to provide the department with immediate access to Gemini's features while retaining control over its deployment to ensure that corporate data is not available for human review. What should you do?

A. Enable Gemini for the department's organizational unit and assign Gemini licenses to users in the department.

B. Monitor Gemini adoption through the administrator console and wait for wider user adoption before assigning licenses.

C. Enable Gemini for non-licensed users in that department so they have immediate access to the free service.

D. Enable Alpha features for the organization and assign Gemini licenses to all users.

Answer: A

Explanation:

To provide a specific department with immediate access to Gemini's features in Google Workspace while maintaining control and ensuring corporate data privacy, you need to enable Gemini for that department's organizational unit and assign the necessary licenses to the users within that OU. This approach allows for targeted deployment and ensures that the features are used within the governed Google Workspace environment.

Here's why option A is correct and why the others are not the appropriate solutions:

A . Enable Gemini for the department's organizational unit and assign Gemini licenses to users in the department.

Google Workspace allows administrators to manage services and features at the organizational unit (OU) level. By enabling Gemini specifically for the OU of the department that needs it, you grant access only to those users. Assigning Gemini licenses ensures that they have the required entitlements to use the advanced AI features. Importantly, when Gemini is enabled and used within a Google Workspace account with the appropriate controls, the data generated is governed by Google Workspace's data privacy and security commitments, ensuring corporate data is not available for

human review in a way that compromises privacy. Administrators have controls over how Gemini for Workspace interacts with organizational data.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Turn Gemini for Google Workspace on or off for users" (or similar titles) explains how to control access to Gemini features at the organizational unit or group level. It also details the licensing requirements for Gemini for Workspace and how to assign these licenses to specific users. Furthermore, documentation on "Data privacy and security in Gemini for Google Workspace" outlines how user data is handled and protected when using these features within a Google Workspace environment, emphasizing controls to prevent inappropriate human review of corporate data.

B . Monitor Gemini adoption through the administrator console and wait for wider user adoption before assigning licenses.

This approach delays providing the requested access to the department that needs Gemini immediately. Monitoring adoption might be useful for broader rollouts, but it doesn't address the immediate need of the specific department.

Associate Google Workspace Administrator topics guides or documents reference: While the Admin console provides insights into usage and adoption of various Google Workspace services, it doesn't serve as the primary mechanism for granting initial access to new features like Gemini for specific teams.

C . Enable Gemini for non-licensed users in that department so they have immediate access to the free service.

There isn't a "free service" of Gemini directly integrated within Google Workspace that bypasses licensing and organizational controls in the way this option suggests. Gemini for Google Workspace is a licensed feature that needs to be enabled and assigned by the administrator. Enabling features for "non-licensed users" in a corporate environment without proper governance is not a standard or secure practice. It would likely mean users are accessing a consumer version of Gemini, which would not be subject to the same data privacy and security controls as the licensed Google Workspace version, potentially exposing corporate data to human review outside of the organization's policies.

Associate Google Workspace Administrator topics guides or documents reference: Google's documentation on Gemini for Workspace clearly outlines the licensing requirements and the integration within the Google Workspace environment, emphasizing administrative control over its deployment and usage.

D . Enable Alpha features for the organization and assign Gemini licenses to all users.

Enabling Alpha features for the entire organization carries significant risks as these features are still under development and may not be stable or fully secure. Assigning Gemini licenses to all users when only one department needs it is an unnecessary cost and expands the deployment before proper evaluation and targeted rollout. It also doesn't specifically address the need to limit access to the requesting department initially.

Associate Google Workspace Administrator topics guides or documents reference: Google's guidelines on release channels (Rapid, Scheduled, Alpha/Beta) strongly advise against enabling prerelease features like Alpha for production environments due to potential instability and lack of full support. Controlled rollouts to specific OUs are recommended for new features.

Therefore, the most appropriate action is to enable Gemini for the specific organizational unit of the requesting department and assign Gemini licenses to the users within that OU. This provides immediate access while maintaining administrative control and ensuring that the usage of AI features within the Google Workspace environment adheres to the organization's data privacy policies.

Question: 78

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:

When an internal user reports not receiving Google Calendar event invites, the most likely immediate cause to investigate on the recipient's end is their notification settings within Google Calendar. Users can customize their notification preferences, and it's possible they have turned off email notifications for new events.

Here's why option D is the most relevant first step and why the other options are less likely to be the primary cause of this specific issue:

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

Google Calendar allows users to configure various notification settings, including whether they receive email

notifications for new events, changes to events, reminders, etc. If the recipient has disabled email notifications for new events, they would not receive the invites in their inbox, even though the event might be correctly added to their Calendar.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Calendar Help documentation for users, such as "Change notification settings," explains how users can customize their event notifications. This includes options to turn off email notifications for new events. While administrators don't directly manage individual user's notification settings, understanding these user-level controls is crucial for troubleshooting. An administrator might guide the user to check these settings.

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

Business hours in Google Calendar primarily affect meeting scheduling suggestions and how a user's availability is displayed to others. They do not directly prevent a user from receiving event

invitations. Whether or not a recipient has configured their business hours will not stop the email notification for a new event from being sent (unless perhaps in very specific and unusual edge cases related to resource scheduling, which isn't indicated here).

Associate Google Workspace Administrator topics guides or documents reference: The Google Calendar Help documentation on "Set your working hours and location" explains the purpose of business hours, which is related to availability and scheduling, not the receipt of invitations.

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

If the Calendar service is turned off for the event creator, they would not be able to create or send any Calendar events in the first place. Since the user created and sent the invite (as mentioned by the recipient not receiving it), the Calendar service must be active for the creator.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Turn Google Calendar on or off for users" explains how administrators can control access to the Calendar service. If the service is off for a user, they would not have Calendar functionality.

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

While there might be limitations on the number of guests that can be added to a single Calendar event, exceeding this limit typically results in an error message for the event creator during the invitation process, not a failure of the recipient to receive the invite. Even if there were such a limit affecting receipt (which is not a common documented issue for internal users within reasonable limits), it wouldn't be the first thing to check.

Associate Google Workspace Administrator topics guides or documents reference: Google Calendar Help documentation might mention limits on the number of guests, but these limits usually pertain to the ability to add guests, send updates, or view responses, not a complete failure of delivery to some recipients within the organization.

Therefore, the most logical first step in troubleshooting why an internal recipient isn't receiving Calendar event invites is to have the recipient check their own Calendar notification settings to ensure that email notifications for new

events are enabled.

Question: 79

Your company has recently purchased a new domain name to use for the corporate email addresses. However, you are unable to access certain features in Google Workspace because the domain is not verified. You need to verify the domain. What should you do?

A. Contact Google support and request manual verification.

B. Add an MX record to your DNS zone that points to Google Workspace.

C. Request a TXT record be added to the DNS zone by your domain registrar.

D. Purchase a SSL certificate for your domain.

Answer: C

Explanation:

To verify a domain name with Google Workspace and gain access to all its features, you typically need to prove that you own the domain. One of the most common methods for doing this is by adding a specific TXT record to your domain's DNS (Domain Name System) zone. Google provides this unique TXT record, and once it's published in your DNS, Google can verify your ownership.

Here's why option C is the correct approach and why the others are not the standard methods for domain verification in Google Workspace:

C . Request a TXT record be added to the DNS zone by your domain registrar.

Google Workspace provides a unique TXT record that you need to add to your domain's DNS settings. This record contains a specific code that Google's systems check for. By finding this record in your domain's public DNS, Google can confirm that you have control over the domain and are authorized to use it with Google Workspace. You usually manage DNS records through the interface provided by your domain registrar or your DNS hosting provider.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "Verify your domain for Google Workspace" (or similar titles) explicitly outlines the different methods for domain verification. Adding a TXT record is consistently presented as a primary and recommended method. The documentation provides the exact steps:Sign in to your domain host (domain registrar).

Go to your domain's DNS records.

Add a TXT record with the value provided by Google.

Save the TXT record.

In the Google Admin console, start the verification process. Google will then check for the TXT record.

A . Contact Google support and request manual verification.

While Google support can assist with domain verification issues, it's not the standard first step. Manual verification is usually reserved for situations where the standard methods (like TXT or CNAME records) cannot be used or have failed. You should first attempt one of the standard DNSbased verification methods.

Associate Google Workspace Administrator topics guides or documents reference: The standard domain verification process, as documented in Google Workspace Admin Help, primarily involves DNS record modifications. Contacting support is usually a step taken if there are problems with these standard methods.

B . Add an MX record to your DNS zone that points to Google Workspace.

MX records are for directing email to the correct mail servers. While you will eventually need to configure MX records to use Gmail with your domain, adding them is not the primary step for verifying the domain's ownership. Domain verification needs to be completed before you can fully set up email and have Google manage your domain's email flow.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation clearly separates the steps for domain verification from setting up MX records for email. Verification comes first to prove ownership.

D . Purchase an SSL certificate for your domain.

An SSL (Secure Sockets Layer) certificate is used to secure communication between a web server and a browser, typically for websites. It is not related to verifying domain ownership for Google Workspace services. While having an SSL certificate is important for website security, it does not serve as a method for Google to confirm that you own the domain for Google Workspace setup.

Associate Google Workspace Administrator topics guides or documents reference: Google Workspace domain verification methods are specifically focused on demonstrating control over the domain's DNS records. SSL certificates are a separate aspect of web security.

Therefore, the correct action to verify your domain for Google Workspace is to request a TXT record from Google and add it to your domain's DNS zone through your domain registrar's management interface.

Question: 80

You notice an increase in support cases related to Chrome browser within your organization. You suspect a potential outage or service disruption with Chrome browser. You need to determine whether any information has been released about the issue and if there are any projected timelines for its resolution. What should you do first?

A. Use the Help Assistant within the Google Admin console to identify if there was a recent outage.

B. Collect a HAR file, and use the Google Admin Toolbox to identify potential failures.

C. Review the Google Workspace Status Dashboard.

D. Log a case with Chrome Enterprise support.

Answer: C

Explanation:

When experiencing a potential service disruption with a Google product like Chrome browser that is impacting your organization, the first and most efficient step to check for known outages and their resolution timelines is to review the Google Workspace Status Dashboard. This dashboard provides real-time information about the status of various Google Workspace services, including Chrome Enterprise.

Here's why option C is the correct first step and why the others are less immediate or less likely to provide the initial information you need:

C . Review the Google Workspace Status Dashboard.

The Google Workspace Status Dashboard is the official source for information about outages, service disruptions, and maintenance affecting Google Workspace services. It provides the current status of each service, any reported issues, and often includes updates on investigations and estimated times for resolution if an outage is confirmed. Checking this dashboard first will quickly tell you if Google is aware of a widespread issue with Chrome and if there's any information available.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation explicitly directs administrators to use the Status Dashboard for checking service outages. Articles like "Check the Google Workspace status" or similar titles explain how to access and interpret

the information on the dashboard. It is the primary communication channel from Google regarding service health.

A . Use the Help Assistant within the Google Admin console to identify if there was a recent outage.

The Help Assistant in the Google Admin console is a useful tool for general troubleshooting and finding help articles. While it might eventually point you to the Status Dashboard or provide information based on known issues, it is not the most direct and real-time source for immediate outage information. Checking the Status Dashboard directly is faster and more reliable for immediate outage identification.

Associate Google Workspace Administrator topics guides or documents reference: The Help Assistant is primarily designed for guiding administrators through tasks and providing access to support documentation, not as a real-time status indicator for service outages.

B . Collect a HAR file, and use the Google Admin Toolbox to identify potential failures.

Collecting a HAR (HTTP Archive) file and using the Google Admin Toolbox are more relevant for diagnosing specific technical issues at the user or network level. While these tools can be helpful for troubleshooting individual problems or investigating the root cause of an issue after confirming it's not a known outage, they are not the first step to take when suspecting a widespread service disruption. They are more for in-depth technical analysis.

Associate Google Workspace Administrator topics guides or documents reference: Documentation on the Google Admin Toolbox describes its various utilities for diagnosing and troubleshooting specific issues, often requiring technical expertise and focusing on local or account-specific problems rather than broad service outages.

D . Log a case with Chrome Enterprise support.

Logging a support case is appropriate when you have investigated and cannot find information about a known outage, or when you need assistance with a specific issue that is not related to a general service disruption. It takes time to receive a response from support, so it's not the quickest way to check for a known outage and its timeline. You should first check the official status dashboard.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help provides guidance on when and how to contact support. Checking the Status Dashboard is typically recommended as the first step for service-related issues.

Therefore, the most efficient first step to determine if there's a known outage or service disruption with Chrome browser and to find any projected timelines for resolution is to review the Google Workspace Status Dashboard.

Question: 81

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:

To quickly determine if an employee has shared confidential documents externally, you should utilize the security investigation tool in the Google Admin console and specifically review the Drive log events associated with that employee's account. This tool provides a centralized place to audit user activity related to Google Drive, including sharing actions.

Here's why option A is the most direct and efficient first step:

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

The security investigation tool allows administrators to examine various logs related to user activity and potential security incidents. By focusing on the Drive log events for the specific employee in question, you can quickly filter and review actions such as file sharing, permission changes, and external access. This will provide a direct view of whether the employee has indeed shared documents externally and to whom.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on the "Security investigation tool" (or similar titles) explains its capabilities. Specifically, the section on "Investigating Drive log events" details how administrators can use filters to view file sharing activities, including external sharing, by specific users and timeframes. This tool is designed for precisely such scenarios where you need to quickly

audit user actions related to data access and sharing.

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

While the Admin SDK Reports API can provide detailed information about Drive activity, using it requires programming skills and setting up custom scripts or applications. This is not the quickest way to investigate a potential immediate security concern. The security investigation tool offers a userfriendly interface for administrators to perform such investigations without needing to code.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin SDK documentation describes the Reports API and its capabilities. While powerful for custom reporting and automation, it's not the fastest method for a quick, ad-hoc security investigation compared to the built-in security

investigation tool.

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

The user log events in the security investigation tool cover a broader range of activities beyond just Google Drive, such as login attempts, password changes, and device management actions. While this might provide some context, it is less focused on file sharing activities compared to the Drive log events. To quickly determine if confidential documents were shared, filtering directly for Drive- related actions is more efficient.

Associate Google Workspace Administrator topics guides or documents reference: The documentation on the security investigation tool outlines the different log sources available, including user logs and Drive logs. For investigating file sharing, the Drive logs provide more specific and relevant information.

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

The security dashboard provides an overview of your organization's security posture and includes pre-built reports and insights. While you can create custom reports, this process might take longer than directly investigating the Drive log events for the specific employee in the security investigation tool. The investigation tool is designed for targeted and immediate analysis of potential security incidents related to user actions.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on the "Security dashboard" explains its features, which focus on overall security trends and insights. While it can be useful for identifying patterns, the security investigation tool is more suited for investigating specific user actions and potential data leaks on demand.

Therefore, the most efficient and direct way to quickly determine if the employee has shared confidential documents externally is to review the employee's Drive log events in the security investigation tool.

Question: 82

You are employed at a multinational organization with offices around the world. You want to ensure that employees in each region receive region-specific emails in a timely manner with minimal administrative burden. When new employees are hired in each region, you want to automate the email distribution process so that staff changes are reflected quickly. What should you do?

A. Create a Google Group for each region and add the respective employees to the appropriate group.

B. Create a dynamic group for each region by setting the location as a condition.

C. Create a Google Group for each region and set permissions that allow employees to discover and join the groups.

D. Create a security group for each region, and apply the location label to allow employees to join based on their region.

Answer: B

Explanation:

To automate email distribution to employees based on their region with minimal administrative overhead and ensure that staff changes are reflected quickly, the most efficient solution is to use dynamic groups in Google Workspace. You can create a dynamic group for each region and set membership rules based on a user attribute, such as their location. When a new employee is added and their location is correctly set in their user profile, they will automatically be added to the corresponding dynamic group.

Here's why option B is the best choice and why the others are less suitable for automation:

B . Create a dynamic group for each region by setting the location as a condition.

Dynamic groups automatically manage their membership based on criteria you define using user attributes in the Google Workspace directory (e.g., department, location). By creating a dynamic group for each region and setting the condition to match the employees' location as specified in their user profiles, new hires will be automatically added to the correct regional email distribution list
when their account is created with the appropriate location. Similarly, if an employee's location changes in their profile, their group membership will be updated automatically. This minimizes manual administrative work and ensures timely updates to the email lists.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "About dynamic groups" (or similar titles) explains the benefits and functionality of dynamic groups. It highlights their ability to automatically manage membership based on user attributes, reducing the need for manual additions and removals. The documentation also details how to create dynamic groups and set up membership rules based on various user profile fields, including location.

A . Create a Google Group for each region and add the respective employees to the appropriate group.

While standard Google Groups can be used for email distribution, they require manual addition and removal of members. This approach does not automate the process when new employees are hired or when employees move between regions, leading to administrative overhead and potential delays in updating the email lists.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Create a group" explains how to create and manage standard Google Groups. It emphasizes manual member management unless used in conjunction with other tools or processes.

C . Create a Google Group for each region and set permissions that allow employees to discover and join the groups.

Allowing employees to discover and join groups can reduce some administrative burden, but it relies on employees to actively find and join the correct regional group. This is not as reliable or immediate as automatic membership based on a defined attribute. Additionally, it might lead to employees joining incorrect groups.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Choose who can join your group" outlines the different join settings for Google Groups. While self-joining can be useful for certain types of groups, it doesn't guarantee that all relevant employees will join the correct regional distribution lists automatically upon hiring.

D . Create a security group for each region, and apply the location label to allow employees to join based on their region.

Security groups in Google Workspace are primarily used for managing access to resources and services, not typically for email distribution lists in the same way as Google Groups. While you can add security groups to email lists, the mechanism for employees to join based on a "location label" isn't a standard automated feature of security groups. Dynamic groups are specifically designed for automatic membership based on user attributes.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "About security groups" explains their purpose in managing access and permissions. While they can contain users based on attributes, the automatic, attribute-based membership management for email distribution is the core functionality of dynamic groups.

Therefore, the most effective and automated solution to ensure region-specific email distribution with minimal administrative burden is to create a dynamic group for each region by setting the location as a condition. This ensures that new employees are automatically added to the correct regional email list based on their user profile information.

Question: 83

You are applying device and user policies for employees in your organization who are in different departments. You need each department to have a different set of policies. You want to follow Google-recommended practices. What should you do?

A. Create separate top-level organizational units for each department.

B. Create an Access group for each department. Configure the applicable policies.

C. Add all managed users and devices in the top-level organizational unit.

D. Create a child organizational unit for each department.

Answer: D

Explanation:

Google recommends using the organizational unit (OU) structure for applying different settings and policies to different groups of users and devices within your Google Workspace domain. To apply a unique set of policies to each department, you should create a child organizational unit for each department under your main domain structure.

Here's why option D aligns with Google's best practices and why the others are less suitable:

D . Create a child organizational unit for each department.

Organizational units provide a hierarchical structure for managing users and devices. By creating a child OU for each department, you can then apply specific device and user policies to that OU. Users and devices within a child OU inherit policies from parent OUs but can also have OU-specific policies that override or supplement the inherited ones. This allows for granular control and ensures that each department can have the policies tailored to its needs. This is the recommended method by Google for managing policies based on departments or other logical groupings within an organization.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "How the organizational structure works" and "Apply settings for specific groups of users or devices" (or similar titles) clearly explains the purpose and benefits of using OUs for policy management. It emphasizes the hierarchical nature and how policies are applied and inherited through the OU structure. Creating child OUs for departments is a direct application of this recommended practice.

A . Create separate top-level organizational units for each department.

Creating separate top-level OUs for each department is generally not recommended for managing policies within the same organization. Top-level OUs are meant to represent distinct functional or administrative units that might have their own domain settings and administrators. Managing all departments under a single domain but in separate top-level OUs can complicate overall administration, sharing, and user management across the organization. Child OUs within a single domain provide the necessary separation for policy application while maintaining a unified organizational structure.

Associate Google Workspace Administrator topics guides or documents reference: Google's documentation on organizational structure usually advises on creating a logical hierarchy of child OUs under a single top-level OU representing the organization. Separating departments into toplevel OUs is not a standard or recommended practice for policy management within a single domain.

B . Create an Access group for each department. Configure the applicable policies.

Access groups are primarily used for controlling access to specific resources or services. While you can manage group membership based on departments, policies for users and devices are typically applied at the organizational unit level, not directly to access groups. While some settings might be influenced by group membership, OUs are the primary mechanism for policy enforcement.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help distinguishes between organizational units and groups (including access groups). Policies are consistently described as being applied to OUs. Groups are for managing access and collaboration.

C . Add all managed users and devices in the top-level organizational unit.

Applying all policies at the top-level OU would mean that all users and devices inherit the same set of policies. This contradicts the requirement of having different policies for each department. To

achieve department-specific policies, you need to organize users and devices into separate OUs.

Associate Google Workspace Administrator topics guides or documents reference: Google's documentation emphasizes the flexibility of the OU structure to apply different policies to different subsets of users and devices. Placing everyone in the top-level OU negates this flexibility.

Therefore, the Google-recommended practice for applying different device and user policies to employees in different departments is to create a child organizational unit for each department. This allows for targeted policy application and management within the overall organizational structure.

Question: 84

You are configuring Gmail for your company and want to implement a layered security approach. You decide to implement industry-standard email authentication protocols. What should you do?

Choose 2 answers

A. Enable a default email quarantine for all users to isolate suspicious emails and determine if the messages haven't been authenticated.

B. Configure a blocked senders rule to block all emails from unknown senders.

C. Configure DKIM to digitally sign outbound emails and verify their origin.

D. Disable IMAP for your organization to prevent external clients from accessing Gmail.

E. Set up SPF records to specify authorized mail servers for your domain.

Answer: CE

Explanation:

To implement industry-standard email authentication protocols as part of a layered security approach for Gmail, you should configure DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) records for your domain. These protocols are crucial for verifying the sender's identity and ensuring the integrity of email messages.

Here's a breakdown of why options C and E are correct and why the others are not primarily email authentication protocols or best practices in this context:

C . Configure DKIM to digitally sign outbound emails and verify their origin.

DKIM adds a digital signature to the headers of outbound emails. This signature is verified by receiving mail servers using a public key published in your domain's DNS records. DKIM helps to confirm that the email was indeed sent from your domain and that its content has not been altered in transit. It is a key email authentication protocol that enhances deliverability and protects against email spoofing.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "Help prevent email spoofing with DKIM" (or similar titles) explains how to set up DKIM for your domain. It details the process of generating a DKIM key, adding the public key as a TXT record in your DNS, and enabling DKIM signing in the Google Admin console. The documentation emphasizes DKIM's role in authenticating outbound mail and improving email security.

E . Set up SPF records to specify authorized mail servers for your domain.

SPF is a DNS-based email authentication protocol that allows you to specify which mail servers are authorized to send emails on behalf of your domain. Receiving mail servers check the SPF record in the sender's domain's DNS to verify if the sending server's IP address is listed as authorized. This helps to prevent spammers from forging the "From" address of your domain.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Help prevent spoofing with SPF" (or similar titles) guides administrators on creating and publishing SPF records in their domain's DNS. It explains the syntax of SPF records and how they help receiving servers validate the sender's origin, thus reducing spoofing and improving deliverability.

Now, let's look at why the other options are not the primary choices for implementing industrystandard email authentication protocols:

A . Enable a default email quarantine for all users to isolate suspicious emails and determine if the messages haven't been authenticated.

Email quarantine is a security feature that holds potentially harmful or suspicious emails for review. While it can help manage unauthenticated emails, it is a response to potential authentication failures or suspicious content, not an authentication protocol itself. Quarantine helps in handling emails that fail authentication checks (like SPF or DKIM) or are flagged by other security measures.

Associate Google Workspace Administrator topics guides or documents reference: Documentation on Gmail quarantine settings explains how to configure them to manage suspicious emails, including those that may not be properly authenticated. It's a post-authentication handling mechanism.

B . Configure a blocked senders rule to block all emails from unknown senders.

Blocking all emails from "unknown senders" is an overly aggressive and impractical approach for most organizations, as you will likely receive legitimate emails from new contacts or domains. While you can create blocklists, it's not a standard email authentication protocol and can lead to significant disruption of email flow.

Associate Google Workspace Administrator topics guides or documents reference: Gmail's blocking features allow users and administrators to block specific addresses or domains, but blocking all unknown senders is not a recommended security practice.

D . Disable IMAP for your organization to prevent external clients from accessing Gmail.

Disabling IMAP can enhance security by limiting how users access their email, potentially reducing the risk of compromised third-party applications. However, it is not an email authentication protocol that verifies the sender of an email. It controls access to the mailbox, not the authentication of emails received or sent.

Associate Google Workspace Administrator topics guides or documents reference: Documentation on managing IMAP and POP access explains how to enable or disable these protocols for users, focusing on access methods rather than email sender authentication.

Therefore, the two correct answers for implementing industry-standard email authentication protocols are configuring DKIM to sign outbound emails and setting up SPF records to specify authorized sending servers.

Question: 85

Your company has just started using Search Ads 360. You need to limit access to Additional Google services for your entire organization by using the Admin console. Only the marketing team and a specific group of users from the web design team should have access. What should you do?

A. Enable Search Ads 360 for both the marketing and web design team organizational units (OUs). Create a group to explicitly deny access to Search Ads 360. Assign the group to the web design users who should not have access.

B. Enable Search Ads 360 at the top level of your organizational structure.

C. Enable Search Ads 360 for the marketing organizational unit (OU). Create a sub-OU under the marketing OU. and move the web design team users who need access into this sub-OU.

D. Enable Search Ads 360 for the marketing organizational unit (OU). Create a new group in the Admin console that includes the web design team users who need access. Enable Search Ads 360 for that group.

Answer: D

Explanation:

To limit access to Search Ads 360 to only the marketing team and a specific group of users from the web design team, the most effective and Google-recommended approach is to enable the service for the marketing organizational unit (OU) and then create a separate group containing the specific web design users who need access, enabling the service for that group as well. This allows for granular control and avoids granting access to the entire web design OU.

Here's why option D is the correct solution and why the others are less ideal:

E. Enable Search Ads 360 for the marketing organizational unit (OU). Create a new group in the Admin console that includes the web design team users who need access. Enable Search Ads 360 for that group.

This approach leverages both organizational units and groups for access control. By enabling Search Ads 360 for the marketing OU, you grant access to all users within that department. Then, by creating a separate group containing the specific web design users who require access and enabling Search Ads 360 for that group, you provide them with the necessary permissions without granting access to the entire web design OU. This method allows for targeted access based on both departmental affiliation and specific user needs, aligning with the principle of least privilege.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Turn services on or off for users" explains how to control access to Google services at both the organizational unit and group levels. It highlights the flexibility of using a combination of OUs and groups to achieve granular access control. Enabling a service for an OU applies it to all members of that OU, while enabling it for a group applies it only to the members of that specific group, regardless of their OU.

A . Enable Search Ads 360 for both the marketing and web design team organizational units (OUs). Create a group to explicitly deny access to Search Ads 360. Assign the group to the web design users who should not have access.

While you can deny service access using groups, it's generally more straightforward and less prone

to errors to explicitly grant access only to those who need it. Enabling the service for the entire web design OU and then trying to revoke access for some users within it adds unnecessary complexity and potential for misconfiguration. Deny rules can also sometimes interact in unexpected ways with allow rules.

Associate Google Workspace Administrator topics guides or documents reference: While the Admin console allows for denying service access through groups, the documentation often emphasizes granting access to specific OUs or groups that require it as a more manageable and transparent approach.

B . Enable Search Ads 360 at the top level of your organizational structure.

Enabling Search Ads 360 at the top level would grant access to the service to every user in your organization. This

directly contradicts the requirement to limit access to only the marketing team and a specific group within the web design team. This option provides the least control and violates the principle of least privilege.

Associate Google Workspace Administrator topics guides or documents reference: Google's best practices for service control emphasize granting access only to those who need it, typically by applying settings at the OU or group level, not organization-wide unless the service is intended for everyone.

C . Enable Search Ads 360 for the marketing organizational unit (OU). Create a sub-OU under the marketing OU. and move the web design team users who need access into this sub-OU.

Creating a sub-OU under the marketing OU for users from the web design team who need access is a less logical organizational structure. It mixes users from different departments within the same branch of the OU hierarchy, which can complicate future policy management and reporting. It's generally better to keep users within their respective departmental OUs and use groups for crossdepartmental service access.

Associate Google Workspace Administrator topics guides or documents reference: Google's guidance on OU structure recommends organizing users based on their functional role or department within the organization for logical policy management and reporting. Creating sub-OUs based on service access needs rather than organizational structure is not a typical recommendation.

Therefore, the most appropriate and manageable solution is to enable Search Ads 360 for the marketing OU and create a separate group containing the specific web design users who need access, then enable the service for that group as well.

Question: 86

Your company has a globally distributed remote work team. You want to ensure all team members adhere to the company's data security policies and only access authorized systems based on their location and role. What should you do?

A. Create and enforce data loss prevention (DLP) rules to control data sharing.

B. Set up and mandate the use of a company-wide VPN for all remote access.

C. Implement two-factor authentication for all remote team members.

D. Configure access control policies with conditional access.

Answer: D

Explanation:

To ensure that a globally distributed remote work team adheres to data security policies and only accesses authorized systems based on their location and role, you should configure access control policies with conditional access. Conditional access allows you to define rules that grant or block access to resources based on various factors, including the user's location, the device they are using, their role, and the application they are trying to access.

Here's why option D is the most comprehensive solution for the stated requirements and why the others address only parts of the problem:

D . Configure access control policies with conditional access.

Conditional access is a security framework that evaluates multiple signals before granting access to resources. By implementing conditional access policies, you can:Control access based on location: Restrict access to certain systems or data based on the geographic location of the user.

Control access based on role: Ensure that only users with specific roles have access to certain applications or data.

Enforce device compliance: Require users to access resources only from company-managed or compliant devices.

Implement multi-factor authentication (MFA): Require additional verification steps based on the context of the access attempt.

Conditional access provides a granular and dynamic way to enforce security policies based on the specific context of each access request, aligning with the goal of allowing access only to authorized systems based on location and role while maintaining data security.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Context-Aware Access" (which is Google's implementation of conditional access) explains how to set up policies based on user attributes (like group membership/role), device security status, and network location. This documentation details how to create access levels and assign them to applications based on specific conditions, ensuring that access is granted only when the requirements are met.

A . Create and enforce data loss prevention (DLP) rules to control data sharing.

DLP rules are crucial for preventing sensitive data from being shared inappropriately. However, they primarily focus on controlling what users can do with data after they have gained access. DLP does not, by itself, control who can access which systems based on their location and role. It's a complementary security layer but not the primary solution for access control based on these factors.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on Data Loss Prevention (DLP) explains how to create rules to prevent the sharing of sensitive information. It focuses on the content of the data and user actions related to sharing, not on controlling initial access based on location and role.

B . Set up and mandate the use of a company-wide VPN for all remote access.

A VPN (Virtual Private Network) can secure the connection between remote users and the company network by encrypting traffic and potentially routing it through company-controlled servers. While it can enhance security and provide a consistent network origin, it does not inherently control access based on the user's role or their geographic location (unless the VPN infrastructure is configured to enforce such restrictions, which would be part of a broader access control strategy). Mandating a VPN is a good security practice but doesn't fully address the need for role-based and location-aware access control.

Associate Google Workspace Administrator topics guides or documents reference: Documentation on VPNs and remote access might be mentioned in the context of securing connections, but it's not the primary mechanism for implementing granular access control based on user attributes and location within Google Workspace's administrative framework.

C . Implement two-factor authentication for all remote team members.

Two-factor authentication (2FA) adds an extra layer of security by requiring users to provide two forms of identification 1 before gaining access. This significantly reduces the risk of unauthorized access 2 due to compromised passwords. While 2FA is a critical security measure for remote teams, it doesn't, by itself, control which systems users can access based on their location and role. It verifies the user's identity but not the context of their access attempt in terms of location or rolebased authorization.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help strongly recommends enabling 2-Step Verification (Google's implementation of 2FA) for enhanced security. However, it is primarily focused on user authentication, not on contextual access control based on location and role.

Therefore, the most comprehensive solution to ensure adherence to data security policies and control access based on location and role for a globally distributed remote work team is to configure access control policies with conditional access. This framework allows for the creation of context- aware rules that take into account various factors to determine whether to grant or block access to resources.

Question: 87

Your organization wants to provide access to YouTube to a select group of users for educational purposes, while restricting YouTube access for all other users. You need to implement a solution that allows for granular control over YouTube access based on user roles or groups. What should you do?

A. Deploy a Chrome extension from the Google Workspace Marketplace that blocks YouTube for users who are not in the select user group.

B. Configure a SAML application to manage YouTube access for different user groups.

C. Instruct the select group of users to switch to their personal Google account when accessing YouTube.

D. Use organizational units (OUs) to apply a policy that restricts YouTube access, and create an exception for the select group of users.

Answer: D

Explanation:

To achieve granular control over YouTube access within your Google Workspace organization, allowing access to a select group while restricting it for others, the recommended approach is to use organizational units (OUs) in conjunction with service settings exceptions. You would apply a policy to restrict YouTube access at a higher-level OU (encompassing most users) and then create a child OU containing the select group, where you override the inherited policy to allow YouTube access.

Here's why option D is the most appropriate solution and why the others are less suitable for centrally managed, granular control within Google Workspace:

D . Use organizational units (OUs) to apply a policy that restricts YouTube access, and create an exception for the select group of users.

Google Workspace allows administrators to configure settings for various Google services, including YouTube, at the organizational unit level. You can set a policy to block YouTube access for the toplevel OU or a parent OU containing most of your users. Then, you can create a child OU specifically for the select group of users who need access and, within the settings for this child OU, override the inherited policy to allow YouTube access. This provides centralized management and ensures that the restrictions and exceptions are applied consistently based on the organizational structure.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "Control access to YouTube" (or similar titles) explains how to manage YouTube settings

at the OU level. It details the different access options available (e.g., unrestricted, restricted, signed-in users in your organization, off) and how these settings can be applied to specific OUs. The concept of OU inheritance and overriding settings in child OUs is fundamental to Google Workspace policy management, allowing for exceptions to be created for specific groups of users.

A . Deploy a Chrome extension from the Google Workspace Marketplace that blocks YouTube for users who are not in the select user group.

Relying on a Chrome extension for blocking and allowing access can be less reliable and harder to manage centrally compared to server-side policies enforced through the Admin console. Extensions can sometimes be bypassed or uninstalled by users. Additionally, managing access based on group membership via a third-party extension might not integrate seamlessly with your Google Workspace user and group structure.

Associate Google Workspace Administrator topics guides or documents reference: While Chrome extensions can extend browser functionality, they are not the primary mechanism for enforcing organizational-wide service access policies managed by Google. The Admin console provides more robust and centrally controlled settings for Google services.

B . Configure a SAML application to manage YouTube access for different user groups.

SAML (Security Assertion Markup Language) is typically used for single sign-on (SSO) to third-party applications. YouTube is a core Google service, and its access within a Google Workspace organization is managed directly through the Admin console's service settings, not via SAML application configuration. Configuring a SAML app for YouTube access within the same Google Workspace domain would be an unnecessary and likely unsupported complexity.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on SAML focuses on integrating external applications for SSO. Managing access to core Google services like YouTube is handled through the service settings within the Admin console.

C . Instruct the select group of users to switch to their personal Google account when accessing YouTube.

This approach is not a centrally managed solution and introduces several problems. It requires users to manually switch accounts, which can be inconvenient and lead to errors. More importantly, it means their YouTube activity would be associated with their personal accounts, not their organizational accounts, which might not align with the educational purpose and could bypass any organizational oversight or policies you might want to apply (e.g., content restrictions). It also doesn't effectively restrict access for other users within their organizational accounts.

Associate Google Workspace Administrator topics guides or documents reference: Google Workspace is designed to manage access to services within the organizational context. Instructing users to use personal accounts for organizational purposes bypasses this management and is generally not a recommended practice for maintaining control and security.

Therefore, the best practice for providing access to YouTube to a select group of users while restricting it for others is to use organizational units (OUs) to apply a policy that restricts YouTube access and create an exception (by overriding the policy) for the OU containing the select group of users.

Question: 88

Your company has offices in several different countries and is deploying Google Workspace. You're setting up Google Calendar and need to ensure that, when a user is creating a Google Calendar event, rooms are suggested in a nearby office. What should you do?

A. Assign building ID, floor name, and floor section to define users' work locations based on defined buildings and rooms.

B. Add your users to Google Groups by location. Add room resources to the corresponding groups.

C. Add your users to organizational units (OUs) by location. Add room resources to the corresponding OUs.

D. Restrict room sharing to a dynamic group based on user location.

Answer: C

Explanation:

To ensure that Google Calendar suggests nearby office rooms when a user creates an event, you need to associate both the users and the room resources with their respective locations within the Google Workspace organizational structure. The most effective way to do this is by organizing users into organizational units (OUs) based on their location and then associating the room resources with the corresponding OUs.

Here's why option C is the correct approach and why the others are less suitable for this specific requirement:

C . Add your users to organizational units (OUs) by location. Add room resources to the corresponding OUs.

Google Calendar uses the organizational unit (OU) structure to determine the proximity of resources to users. By placing users within OUs that correspond to their office locations and then assigning the room resources of each office to the same or relevant child OUs, Google Calendar can suggest nearby rooms to users when they schedule meetings. This method directly links users and resources based on their organizational location.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "Set up rooms and shared resources" (or similar titles) explains how to create and manage room resources. It also details how to associate these resources with specific buildings, floors, and, importantly, organizational units. While the documentation might not explicitly state that nearby suggestions solely rely on OUs, the OU structure is the primary way Google Workspace understands the organizational hierarchy and location

of users and resources. By aligning user and resource OUs, you provide the context for "nearby" suggestions.

A . Assign building ID, floor name, and floor section to define users' work locations based on defined buildings and rooms.

While assigning building IDs, floor names, and sections is crucial for defining the physical location of room resources, it doesn't directly define the user's work location in a way that Google Calendar inherently uses for proximity-based suggestions. These attributes are primarily for the room resources themselves. To establish the "nearby" context, you need to link users to their locations within the organizational structure (i.e., through OUs).

Associate Google Workspace Administrator topics guides or documents reference: The documentation on setting up room resources will guide you through adding details like building, floor, and capacity to the resource. However, it's the OU assignment of both users and resources that provides the relational context for proximity.

B . Add your users to Google Groups by location. Add room resources to the corresponding groups.

Google Groups are primarily for communication and collaboration among users. While you can group users by location, Google Calendar's room suggestion logic is not primarily based on Google Group membership. Associating room resources with groups does not provide the necessary organizational context for suggesting nearby rooms to users when they create events.

Associate Google Workspace Administrator topics guides or documents reference: Google Groups functionality is focused on user communication and access management for group-related resources, not on the spatial or organizational relationships between users and physical meeting rooms for Calendar scheduling.

D . Restrict room sharing to a dynamic group based on user location.

Restricting room sharing to a dynamic group based on user location controls who can book the room, not necessarily whose nearby rooms are suggested when creating an event. Dynamic groups manage membership based on user attributes, but they don't inherently define a user's "nearby" location for Calendar suggestions in the same way that OU-based organizational structure does.

Associate Google Workspace Administrator topics guides or documents reference: Dynamic groups are useful for managing user membership based on attributes, but they are not the primary mechanism for defining the spatial relationship between users and resources for Google Calendar's room suggestions.

Therefore, the most effective method to ensure Google Calendar suggests nearby office rooms to users based on their location is to add your users to organizational units (OUs) by location and add room resources to the corresponding OUs. This aligns the organizational structure with the physical locations, allowing Google Calendar to understand proximity for room suggestions.

Question: 89

Your organization is increasingly concerned about its environmental impact. You want to assess the

environmental impact of using Google Workspace services. Which report should you use?

A. Carbon footprint report

B. Google Environmental Report

C. Apps Monthly Uptime report

D. Accounts report

Answer: A

Explanation:

To assess the environmental impact of using Google Workspace services, you should refer to the Google Environmental Report. Google publishes comprehensive reports detailing its environmental efforts, including the energy efficiency of its data centers, its use of renewable energy, and its overall carbon footprint, which includes the impact of services like Google Workspace.

Here's why option B is the correct choice and why the others are not relevant to assessing the overall environmental impact of using Google Workspace:

B . Google Environmental Report

Google regularly publishes detailed environmental reports that cover various aspects of its sustainability initiatives, including its progress towards using renewable energy, its efforts to improve energy efficiency in its operations (which power Google Workspace), and its overall carbon footprint. These reports provide insights into the environmental impact associated with using Google services.

Associate Google Workspace Administrator topics guides or documents reference: While there might not be a specific "Google Workspace Environmental Impact Report" as a standalone document within the Admin console, Google's overarching "Environmental Report" (often found on Google's sustainability or environmental responsibility websites) encompasses the infrastructure and practices that support all Google services, including Google Workspace. Administrators looking for this information would be directed to these publicly available Google reports.

A . Carbon footprint report

While the concept of a "carbon footprint report" is relevant to environmental impact, Google

typically includes this information within its broader "Environmental Report" rather than providing a separate report specifically for Google Workspace usage within an organization's Admin console. You would likely find data related to

the carbon efficiency of Google's infrastructure in their main environmental disclosures.

Associate Google Workspace Administrator topics guides or documents reference: Google's communication about its carbon footprint and environmental efforts is usually consolidated in their public sustainability reports.

C . Apps Monthly Uptime report

The Apps Monthly Uptime report provides information about the reliability and availability of Google Workspace services. It focuses on service performance and uptime metrics, not on environmental impact or sustainability.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on service-level agreements (SLAs) and service status provides information about uptime guarantees and how to monitor service availability, which is the focus of the Apps Monthly Uptime report.

D . Accounts report

The Accounts report in the Google Admin console provides details about user accounts within your organization, such as the number of active users, account status, and other user-related information. It does not contain any data or analysis related to the environmental impact of using Google Workspace services.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on reporting and user accounts describes the information available in the Accounts report, which is focused on user management and activity metrics.

Therefore, to assess the environmental impact of using Google Workspace services, your organization should refer to the publicly available Google Environmental Report, which details Google's sustainability efforts and overall environmental performance.

Question: 90

An employee with a Workspace Business Plus license at your company is going on a long leave soon. The employee will not need access to their Google Workspace data, but their teammates will need access to the employee’s dat

a. When the employee returns from leave, you will need to restore access to their account, data, emails, and shared documents. You need to preserve the employee’s Workspace data while also

minimizing cost while they are on leave. What should you do?

A. Suspend their account in the Admin console.

B. Purchase an Archived User license and assign the license to the employee.

C. Export the account data by using Takeout, and remove the user license in the Admin console.

D. Copy the employee’s emails, and transfer their file ownership to a teammate. Delete the user account.

Answer: B

Explanation:

To preserve an employee's Google Workspace data while they are on long leave, allow teammates access to that data, and minimize costs with the intention of fully restoring the account upon their return, the best course of action is to purchase an Archived User license and assign it to the employee.

Here's why option B is the most suitable and cost-effective solution that meets all the requirements:

B . Purchase an Archived User license and assign the license to the employee.

Google Workspace offers Archived User licenses at a significantly lower cost than a full user license. When you assign an Archived User license to an account, the data (including Gmail, Drive, and other Workspace services) is retained and can be accessed by other authorized users (e.g., administrators or delegated teammates). The user themselves cannot log in or use the services, thus minimizing cost. Upon the employee's return, you can easily reassign a full Business Plus license to their account, restoring their full access without any data loss or complex restoration processes.

Associate Google Workspace Administrator topics guides or documents reference: The official Google Workspace Admin Help documentation on "About Archived User licenses" (or similar titles) explicitly describes this scenario as the intended use case for Archived User licenses. It outlines the reduced cost, the preservation of data, the ability for administrators to access the data (and delegate access), and the seamless transition back to a full license when the user returns.

A . Suspend their account in the Admin console.

Suspending an account prevents the user from accessing it, but it typically retains the full license cost. While an administrator might be able to access some data in a suspended account, it doesn't offer the cost savings of an Archived User license. Additionally, depending on the suspension duration and Google's policies, there might be implications for long-term data retention without an active or archived license.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Suspend or restore users" explains the functionality of account suspension. It primarily focuses on temporarily revoking access, not on long-term, costeffective data preservation with potential for delegated access.

C . Export the account data by using Takeout, and remove the user license in the Admin console.

While Google Takeout allows you to export user data, this creates a separate archive that is not directly integrated with Google Workspace. Providing teammates access to this exported data would be cumbersome and not as seamless as accessing it within the original Workspace environment.

Removing the user license would stop data retention in Google Workspace, and restoring the account fully upon the employee's return would involve re-importing the data, which can be complex, time-consuming, and potentially lead to data loss or inconsistencies. This option does minimize cost by removing the license but at the expense of easy access and seamless restoration.

Associate Google Workspace Administrator topics guides or documents reference: Documentation on Google Takeout describes its purpose for exporting data out of Google services, primarily for personal use or data migration, not for temporary data preservation and collaborative access within the Workspace environment. Removing a license typically leads to data deletion after a certain period unless an alternative (like an Archived User license) is in place.

D . Copy the employee's emails, and transfer their file ownership to a teammate. Delete the user account.

This approach involves significant data manipulation and potential loss of context. Copying emails might not preserve the entire mailbox structure and could miss important information. Transferring file ownership can be complex and might not cover all types of data or shared items. Deleting the user account would permanently remove the data, making full restoration upon the employee's return impossible. This option is not suitable for preserving the employee's Workspace data and restoring their account later.

Associate Google Workspace Administrator topics guides or documents reference: Google Workspace's account management best practices emphasize preserving user accounts and data for returning employees. Deleting accounts with the intention of temporary leave is strongly discouraged due to the difficulty and risks associated with data recovery and account recreation.

Therefore, the most appropriate action that meets all the requirements of preserving data, providing access to teammates, minimizing cost during the leave, and allowing for full restoration upon return is to purchase an Archived User license and assign it to the employee.

Question: 91

Your company recently installed a free email marketing platform from the Google Workspace Marketplace. The marketing team is unable to access customer contact information or send emails through the platform. You need to identify the cause of the problem. What should you do first?

A. Verify that the email marketing platform's subscription is active and up-to-date.

B. Check the OAuth scopes that are granted to the email marketing platform and ensure the platform has access to Contacts and Gmail.

C. Confirm that the "Manage Third-Party App Access" setting in the Admin console is enabled.

D. Use the security investigation tool to review Gmail logs.

Answer: B

Explanation:

When a third-party application from the Google Workspace Marketplace is installed, it requests specific permissions (OAuth scopes) to access Google Workspace data and services. If the marketing team is unable to access customer contact information or send emails, the most likely cause is that the installed email marketing platform was not granted the necessary OAuth scopes for Contacts and Gmail during the installation or approval process.

Here's why other options are less likely to be the first step:

A . Verify that the email marketing platform's subscription is active and up-to-date. While important for continued use, a "free" platform from the Marketplace generally doesn't have a subscription that would prevent initial access to basic functions like contacts and sending emails unless it's a trial that expired, which isn't indicated as the primary problem. This would be a later troubleshooting step if scope issues are ruled out.

C . Confirm that the "Manage Third-Party App Access" setting in the Admin console is enabled. This setting controls whether users can install any third-party apps from the Marketplace. If it were disabled, the app likely wouldn't have been installed in the first place. If it was enabled and then disabled, the app would stop working, but the specific problem points to data access, not app

disablement.

D . Use the security investigation tool to review Gmail logs. The security investigation tool is excellent for reviewing security events, but it's more for post-incident analysis or suspicious activity. In this scenario, the problem is a lack of functionality for a newly installed app, not a security breach or misconfiguration that would necessarily show up in Gmail logs immediately as an access issue for the app itself. The OAuth scopes are the more direct and initial point of failure.

Reference from Google Workspace Administrator:

Manage third-party app access to data: Google Workspace administrators can control which third- party apps can access their organization's data. This includes reviewing and managing OAuth API access for configured apps.

Reference: Google Workspace Admin Help: Manage third-party app access to data

Understanding OAuth scopes: When an application requests access to Google data, it does so by requesting specific "scopes." These scopes define the particular resources and operations that the application is allowed to perform. For an email marketing platform, scopes for https://www.googleapis.com/auth/contacts (or a more specific contact scope) and https://www.googleapis.com/auth/gmail.send (or a broader Gmail scope) would be crucial.

Reference: Google Developers documentation on OAuth 2.0 Scopes for Google APIs (while not directly an "Admin Help" link, it's fundamental to understanding how Google Workspace apps get permissions). You would typically find this information linked or explained within the context of managing API client access in the Admin console.

Controlling which third-party & internal apps can access Google Workspace data: This section in the Admin console specifically allows administrators to review "Configured apps" and check their "OAuth API access." This is where you would see the scopes granted to the email marketing platform.

Reference: Google Workspace Admin Help: Control which third-party & internal apps can access Google Workspace data

Question: 92

You recently noticed a suspicious trend in your organization's Google Drive usage. Several users have shared sensitive documents outside the organization, potentially violating your company's data security policy. You need to identify the responsible users and the extent of the unauthorized sharing. What should you do?

A. Review the organization's sharing policies in the Admin console, and update the policies to prevent external sharing.

B. Use the security health page to identify misconfigured sharing settings in Drive.

C. Use the security investigation tool to analyze Drive logs and identify the users.

D. Create an activity rule in the Security Center to alert you of future external sharing events.

Answer: C

Explanation:

The core of the problem is to identify the responsible users and the extent of past unauthorized sharing. The Security Investigation Tool is designed precisely for this purpose. It allows administrators to search and analyze various audit logs, including Drive logs, to pinpoint specific events, users, and data.

Here's why the other options are less appropriate as the first or most direct action for this specific problem:

A . Review the organization's sharing policies in the Admin console, and update the policies to prevent external sharing. This is a crucial preventative measure for the future, and a necessary step after identifying the scope of the problem. However, it won't help you identify who shared what in the past.

B . Use the security health page to identify misconfigured sharing settings in Drive. The security health page provides an overview of your security posture and can highlight general misconfigurations. While useful for identifying potential vulnerabilities, it won't give you the granular details of specific users and shared documents that have already occurred, which is what the question asks for.

D . Create an activity rule in the Security Center to alert you of future external sharing events. Similar to option A, this is a future-oriented preventative and monitoring measure. It will help catch future violations but won't provide information about the past unauthorized sharing that has already happened.

Reference from Google Workspace Administrator:

Security investigation tool: This tool is explicitly designed for identifying, triaging, and taking action on security issues. It allows administrators to search and analyze logs from various Google Workspace services, including Drive, to investigate specific events like external sharing.

Reference: Google Workspace Admin Help: About the security investigation tool

Reference: Google Workspace Admin Help: Investigate security issues using the investigation tool (Specifically mentions investigating Drive sharing events).

Drive audit log events: The security investigation tool leverages audit logs. Drive audit logs capture events such as document sharing, changes in sharing permissions, and access.

Reference: Google Workspace Admin Help: Drive audit log events

Question: 93

The human resources department notified you of a legal investigation that was started for an employee in the finance department. You need to ensure that this employee's Google Drive data is preserved for at least one year and does not get deleted by the user or by other means. The Google Vault default retention rules for Drive are set for five years. What should you do?

A. Change the Vault default retention rule to one year instead of five.

B. Place the employee into a separate organizational unit (OU). Create a custom one-year retention rule for this OU.

C. Create a hold in Vault for the employee's Drive.

D. Confirm that the Vault default retention rule is set for five years.

Answer: C

Explanation:

When there's a legal investigation, the priority is to ensure that relevant data is preserved and not deleted, regardless of retention policies or user actions. A "hold" (also known as a litigation hold or legal hold) in Google Vault is specifically designed for this purpose. It overrides all retention rules (both default and custom) and prevents any data covered by the hold from being purged, even if a user attempts to delete it.

Here's why the other options are not the correct or best solution:

A . Change the Vault default retention rule to one year instead of five. Changing the default retention rule would affect all Drive data in your organization, not just this specific employee's. It's a broad

change and not suitable for a targeted legal hold. Moreover, it wouldn't guarantee preservation against user deletions.

B . Place the employee into a separate organizational unit (OU). Create a custom one-year retention rule for this OU. While creating custom retention rules for OUs is possible, it's not the primary mechanism for a legal hold. Retention rules define when data can be deleted, but a hold prevents deletion irrespective of the retention period. If the employee deletes the data, a retention rule won't stop it from moving to trash (and eventually being purged) unless a hold is in place. Furthermore, a one-year retention rule isn't the goal; the goal is to preserve for "at least one year" (meaning indefinitely until the hold is released). The default five-year rule is already longer than one year, but doesn't override user deletion.

D . Confirm that the Vault default retention rule is set for five years. The question states that the default retention rule for Drive is already set for five years. While this is good for general data retention, it does not prevent a user from deleting their own files from Drive, nor does it specifically address the need for a legal hold where data must be absolutely preserved. A default retention rule does not override user deletion or ensure data preservation for legal purposes.

Reference from Google Workspace Administrator:

Holds in Google Vault: This is the core concept. Holds prevent data from being purged from Google systems, regardless of retention rules or user actions, until the hold is released. They are specifically used for legal discovery or investigation purposes.

Reference: Google Workspace Admin Help: Place holds on user accounts

Reference: Google Workspace Admin Help: Holds prevent data from being purged (This page explicitly states that "Holds override retention rules—even if the retention period expires, data on hold is preserved.")

Retention rules in Google Vault: While relevant to data management, retention rules define when data can be deleted if no hold applies. They do not prevent users from deleting data or ensure preservation for legal holds.

Reference: Google Workspace Admin Help: How retention works with Google services

Question: 94

You work for a global organization that has offices in the United States and the European Union (EU). There is an organizational unit (OU) for employees in the United States and a separate OU for employees in the EU. Your company regulations need you to ensure that your users data is located in the same region as their physical office. What should you do?

A. Set the OU data location to No preference.

B. Turn on advanced settings and select Enable features that may process data across multiple regions.

C. Turn on advanced settings and select Disable features that may process data across multiple regions.

D. Set a data region policy for each region's OU.

Answer: D

Explanation:

Google Workspace allows organizations to control the geographic location of their data for compliance and regulatory reasons, often referred to as "data regions" or "data locality." To ensure user data is located in the same region as their physical office, especially for compliance with regulations like those in the EU, you need to set a data region policy for the respective organizational units.

Here's why the other options are incorrect:

A . Set the OU data location to No preference. "No preference" means Google can store the data wherever it deems appropriate, which goes against the requirement of ensuring data is located in a specific region (e.g., EU for EU users, US for US users).

B . Turn on advanced settings and select Enable features that may process data across multiple regions. This option would allow data to be processed across multiple regions, which directly contradicts the company regulation that requires data to be located in the same region as their physical office.

C . Turn on advanced settings and select Disable features that may process data across multiple regions. While this might seem related to controlling data flow, the primary mechanism for specifying data residency for OUs is through data region policies, not simply disabling cross-region processing features. Disabling such features might limit functionality without directly setting the data storage region.

Reference from Google Workspace Administrator:

Choose a data region for your data: Google Workspace provides options for administrators to choose a data region for covered Google Workspace services, which applies to primary customer data at rest. This can be set at the organizational unit (OU) level.

Reference: Google Workspace Admin Help: Choose a data region for your data

Data regions FAQ: This resource provides more details on what data is covered, how data regions work, and the implications of setting them. It emphasizes that you can set the data region at the OU level.

Reference: Google Workspace Admin Help: Data regions FAQ

Question: 95

Your organization acquired a small agency with only five users. You need to create user accounts for these new employees. Agency users must have their original email address. You have added the agency's domain as a secondary domain. What should you do?

A. Use the Directory API to automatically create the user accounts.

B. Manually create users from the Admin console. When creating the user account, choose the agency domain to be used for the email address.

C. Use Google Cloud Directory Sync (GCDS) to sync users from an existing directory.

D. Bulk upload all users using a CSV file.

Answer: B

Explanation:

The key information here is "only five users" and "Agency users must have their original email address. You have added the agency's domain as a secondary domain."

For a small number of users (five), manually creating them in the Admin console is the most straightforward and least complex method. When creating a new user, the Admin console allows you to select the domain for their primary email address from any secondary domains you have added to your Google Workspace account.

Here's why the other options are less suitable:

A . Use the Directory API to automatically create the user accounts. While the Directory API can be used for automation, it requires scripting or programming knowledge. For just five users, this is overkill and introduces unnecessary complexity.

C . Use Google Cloud Directory Sync (GCDS) to sync users from an existing directory. GCDS is designed for syncing large numbers of users and groups from an on-premise directory (like Active Directory) to Google Workspace. For only five users, and if there isn't an existing directory that needs ongoing synchronization, GCDS is far too complex and unnecessary.

D . Bulk upload all users using a CSV file. Bulk upload using a CSV file is efficient for a larger number of users (e.g., dozens, hundreds, or thousands). For only five users, preparing a CSV file might take as much or more time than simply creating them one by one through the graphical interface, especially if it's a one-time task.

Reference from Google Workspace Administrator:

Add users one by one: This method is explicitly recommended for adding a small number of users (e.g., 10 or fewer). During the user creation process, you have the option to choose the domain for the user's primary email address from your available domains.

Reference: Google Workspace Admin Help: Add users one by one

Add a domain or domain alias: This is the prerequisite step mentioned in the question ("You have added the agency's domain as a secondary domain.") which allows you to use that domain for user email addresses.

Reference: Google Workspace Admin Help: Add a domain or domain alias

Question: 96

You notice an increase in support tickets related to Gmail. Multiple users are reporting that their emails are not loading, and they are receiving error messages. You need to troubleshoot the issue and identify potential causes. What should you do?

A. Analyze the users' Gmail labels and filters to determine whether incoming emails are being inadvertently blocked.

B. Collect the users' browser versions and extensions to identify potential compatibility issues.

C. Review the users' email forwarding settings to ensure that emails are not being redirected to incorrect addresses.

D. Gather HAR files from affected users to capture network traffic and analyze request/response details.

Answer: D

Explanation:

When users report issues like "emails not loading" and "receiving error messages" in Gmail, especially if it's a new or widespread problem, it often points to network-related issues, client-side problems, or interactions between the browser and Google's servers. A HAR (HTTP Archive) file captures all the network requests and responses that occur in a web browser. This detailed log is invaluable for diagnosing web application issues, including:

Identifying specific error codes from the server.

Analyzing request and response headers.

Checking the timing of requests to see if there are performance bottlenecks.

Pinpointing blocked requests or failed resources.

Here's why the other options are less effective as the first troubleshooting step for this type of widespread issue:

A . Analyze the users' Gmail labels and filters to determine whether incoming emails are being inadvertently blocked. While labels and filters can affect email visibility, they typically wouldn't cause "emails not loading" or generic "error messages" for the Gmail interface itself. This would be more relevant if emails were simply missing, but the interface was functional.

B . Collect the users' browser versions and extensions to identify potential compatibility issues. This is a good secondary troubleshooting step. Browser versions, extensions, or even cached data can certainly cause issues. However, a HAR file can often reveal if the problem is at the browser level (e.g., an extension blocking a script) or deeper within the network interaction. If the HAR shows clean network traffic, then looking at browser specifics becomes more critical.

C . Review the users' email forwarding settings to ensure that emails are not being redirected to incorrect addresses. Email forwarding affects where emails go after they arrive in Gmail, not whether the Gmail interface itself loads or displays errors. This is irrelevant to the reported symptoms.

Reference from Google Workspace Administrator:

While there isn't a direct "Gmail troubleshooting with HAR files" page in the Google Workspace Admin Help, the concept of using HAR files for web application troubleshooting is a fundamental best practice, widely used by Google support themselves when diagnosing complex browser-related issues with Google Workspace services.

General Troubleshooting Steps for Google Workspace (Implicit HAR File Use): Google's support often requests HAR files when diagnosing browser or network-related issues with any of their web-based services. This is a common diagnostic tool.

How to Generate a HAR file: Instructions on how to generate a HAR file are commonly available from browser developers (Chrome, Firefox, Edge, etc.) and are often shared by support teams when troubleshooting web application problems.

Example (General Web Development/Troubleshooting Resource): Various online tutorials and browser developer documentation provide instructions on how to generate HAR files (e.g., Chrome DevTools, Firefox Network Monitor). These are standard tools for web troubleshooting.

By capturing a HAR file, you get a comprehensive picture of the communication between the user's browser and

Google's servers, which is critical for identifying the root cause of loading errors and general functionality issues in a web application like Gmail.

Question: 97

You work for a multinational organization. Employees in several office buildings are experiencing issues with Google Voice, including dropped calls and poor call quality. You need to quickly determine whether this is a localized issue or a broader Google Voice service disruption. What should you do?

A. Verify whether users in the affected buildings have been assigned Google Voice licenses.

B. Check the Google Workspace Status Dashboard for reported service outages or disruptions.

C. Check the Google Workspace Updates blog for announcements about Google Voice issues.

D. Use the security investigation tool to search user log events for "Call failed", and analyze packet loss data.

Answer: B

Explanation:

When multiple users across different office buildings experience issues with a Google Workspace service like Google Voice (dropped calls, poor call quality), the first and most efficient step to determine if it's a widespread service disruption or a localized issue is to check the official Google Workspace Status Dashboard. This dashboard provides real-time and historical information on the status of all Google Workspace services.

Here's why the other options are less effective as the first step:

A . Verify whether users in the affected buildings have been assigned Google Voice licenses. If users are experiencing issues like dropped calls, it implies they have licenses and can generally access the service. A licensing issue would likely prevent them from using Google Voice at all, not just lead to poor quality. This would be a troubleshooting step if the dashboard shows no outage and individual users can't use the service at all.

C . Check the Google Workspace Updates blog for announcements about Google Voice issues. The Updates blog is for new features, policy changes, and sometimes post-mortems of past major incidents, but it's not a real-time status indicator for current outages. The Status Dashboard is designed for this immediate check.

D . Use the security investigation tool to search user log events for "Call failed", and analyze packet loss data. The security investigation tool is excellent for detailed forensic analysis of specific user activities and security events. While it could eventually reveal packet loss or call failure events, it's a time-consuming investigative tool. Before diving into granular logs, you first need to rule out a broader service outage that would affect many users. If the Status Dashboard

shows no issues, then using the investigation tool to look at specific user logs is a valid next step for localized troubleshooting.

Reference from Google Workspace Administrator:

Google Workspace Status Dashboard: This is the primary and official source for real-time information on the status of Google Workspace services. It is designed precisely for checking widespread outages or disruptions.

Reference: Google Workspace Admin Help: Check the status of a Google Workspace service

Reference: Google Workspace Status Dashboard: https://www.www.google.com/appsstatus/dashboard/

Question: 98

Your security team is concerned about disgruntled employees downloading large amounts of intellectual property. You need to create an automatic notification if any user downloads more than 500 files from Google Drive within a one-hour period. What should you do?

A. Create an activity rule in the security investigation tool to monitor Drive download events. Set a threshold to trigger an alert.

B. Use the alert center to review Drive audit logs for instances where users download a large number of files.

C. Configure a Data Loss Prevention (DLP) rule for Drive.

D. Set up an alert within Google Cloud Monitoring to track the number of Drive API calls and trigger a notification when a user makes an excessive number of download requests.

Answer: A

Explanation:

To create an automatic notification for a specific event (downloading more than 500 files from Google Drive within a one-hour period), an "activity rule" in the Google Workspace Security Center (which leverages the security investigation tool's capabilities) is the most appropriate and direct solution. Activity rules allow you to define conditions based on log events (like Drive downloads) and set thresholds to trigger alerts and even automated actions.

Here's why the other options are less suitable for this specific requirement:

B . Use the alert center to review Drive audit logs for instances where users download a large number of files. The Alert Center displays alerts, but it doesn't create the custom alert for this specific threshold. You would review existing alerts

here. While Drive audit logs are the source of the data, the Alert Center isn't where you configure the rule to generate the alert based on a specific count of downloads within a time period.

C . Configure a Data Loss Prevention (DLP) rule for Drive. DLP rules are designed to prevent sensitive data from being shared or downloaded. They focus on the content of the files (e.g., credit card numbers, PII). While useful for data exfiltration, a DLP rule wouldn't specifically count the number of downloads to trigger an alert based on a volume threshold, regardless of content.

D . Set up an alert within Google Cloud Monitoring to track the number of Drive API calls and trigger a notification when a user makes an excessive number of download requests. While technically possible via Google Cloud's logging and monitoring infrastructure if you're forwarding Google Workspace logs there, this is a more complex and advanced solution requiring integration with Google Cloud Platform. The Google Workspace Admin console offers a direct, built-in feature (activity rules) for this specific use case, making it the more efficient and less expensive solution within the context of Google Workspace administration.

Reference from Google Workspace Administrator:

Create and manage activity rules: This documentation directly explains how to create activity rules, including setting conditions based on log events (like Drive downloads) and defining thresholds to trigger alerts.

Reference: Google Workspace Admin Help: Create and manage activity rules

Specifically, for Drive download events: The activity rule configuration allows you to select "Drive log events" as the data source and then filter by "Download" event type. You can then define the threshold (e.g., count > 500 within 1 hour).

Drive audit log events: These logs are the source data that activity rules analyze. They capture events like "Download."

Reference: Google Workspace Admin Help: Drive audit log events

About the security investigation tool: Activity rules are often created within or leverage the capabilities of the security investigation tool.

Reference: Google Workspace Admin Help: About the security investigation tool

Question: 99

Your organization has detected a significant rise in unauthorized access to applications from personal devices. This poses a critical security risk and could lead to data loss. To mitigate this risk, you must immediately restrict user access to these applications. What should you do?

A. Limit apps access to company-issued devices by using context-aware access.

B. Enable multi-factor authentication for application access.

C. Enable data loss prevention rules.

D. Configure apps data access to Limited to only allow access to unrestricted services.

Answer: A

Explanation:

The problem states a "significant rise in unauthorized access to applications from personal devices," posing a "critical security risk" and potential "data loss." The immediate goal is to "immediately restrict user access to these applications" from personal devices.

Context-Aware Access (CAA) is specifically designed to control access to Google Workspace applications based on the "context" of the user and their device. This includes whether the device is managed (company-issued) or unmanaged (personal), its security posture, IP address, and location. By configuring CAA policies, you can enforce that users can only access specific applications if they

are using a company-issued device.

Here's why the other options are less effective or not the primary solution for this immediate restriction:

B . Enable multi-factor authentication for application access. MFA is a crucial security layer, but it authenticates the user, not the device. A disgruntled employee could still use their personal device with MFA enabled to download data if no device-based restriction is in place. It prevents unauthorized users but not authorized users on unauthorized devices.

C . Enable data loss prevention rules. DLP rules are excellent for preventing sensitive data from leaving the organization (e.g., by blocking sharing of files containing credit card numbers). However, they don't restrict access to applications based on the device type. An employee could still access and potentially download non-DLP-sensitive data from a personal device if only DLP is enabled. The immediate risk is access from personal devices, not just content-based data loss.

D . Configure apps data access to Limited to only allow access to unrestricted services. This option typically refers to allowing specific APIs or services to be accessed by third-party apps, or perhaps limiting access within a highly restricted environment. It's not a direct control mechanism for user access from personal vs. company-issued devices to core Google Workspace applications.

Reference from Google Workspace Administrator:

Protect your business with Context-Aware Access: This is the primary documentation for Context- Aware Access, explicitly mentioning its use case for "Allow access to apps only from company-issued devices."

Reference: Google Workspace Admin Help: Protect your business with Context-Aware Access

About Context-Aware Access: Provides an overview of how CAA works and its capabilities, including controlling access based on device security status (e.g., managed vs. unmanaged).

Reference: Google Workspace Admin Help: About Context-Aware Access

Question: 100

Your organization wants to ensure that all employees who use Chrome browsers for work adhere to specific security and configuration settings. You need to manage and control the Chrome browsers used within the company while using the least expensive solution. What should you do?

A. Use a third-party software deployment solution to manage the Chrome browser.

B. Remotely wipe all employee devices to ensure that they are using the latest Chrome browser version.

C. Enroll the Chrome browsers in your organization's domain and apply Chrome browser policies.

D. Disable all extensions on employee Chrome browsers to prevent any potential security risks.

Answer: C

Explanation:

Google Workspace (specifically Chrome Enterprise Core, which is often included or available for free with Google Workspace editions) provides built-in capabilities to manage Chrome browsers across an organization. By enrolling Chrome browsers in your domain, you can apply policies centrally from the Google Admin console, controlling security settings, extensions, updates, and more. This is a first- party, cloud-based solution that doesn't require additional software or licensing costs beyond your existing Google Workspace subscription, making it the "least expensive solution."

Here's why the other options are less suitable for managing Chrome browsers with the least expense:

A . Use a third-party software deployment solution to manage the Chrome browser. While possible, this would incur additional costs for the third-party software, its licensing, and potentially its maintenance. Google Workspace offers native browser management, so a third-party solution is not the "least expensive."

B . Remotely wipe all employee devices to ensure that they are using the latest Chrome browser version. Remotely wiping devices is a drastic and disruptive measure, typically used for lost/stolen devices or offboarding. It's not a standard or appropriate method for managing browser versions or applying configuration settings. It would also be highly expensive in terms of lost productivity and IT effort.

D . Disable all extensions on employee Chrome browsers to prevent any potential security risks. While disabling extensions can mitigate some risks, it's an overly broad and potentially disruptive action that could hinder employee productivity if legitimate and necessary extensions are disabled. More importantly, it's just one potential policy you might apply, not the method for managing the browsers centrally and cost-effectively. Chrome browser policies allow for granular control, including allowing/blocking specific extensions.

Reference from Google Workspace Administrator:

Set Chrome policies for users or browsers: This is the key administrative function that allows you to manage Chrome browsers. It describes how to apply policies to Chrome browsers enrolled in your organization's domain.

Reference: Chrome Enterprise and Education Help: Set Chrome policies for users or browsers

Chrome Enterprise Core: This outlines the free cloud-based management features available for Chrome browsers, which are often integrated with Google Workspace. It explicitly states that "cloudbased management and reporting for $0" are available with Chrome Enterprise Core.

Reference: Chrome Enterprise website: Chrome Enterprise - The Trusted Enterprise Browser for your Business (Look for sections describing Chrome Enterprise Core capabilities and pricing).

Maximizing Google Chrome Management in Google Workspace: This article further emphasizes that "the basic policies for Google Chrome management are available for free with Google Workspace."

Reference: itGenius blog: Maximizing Google Chrome Management in Google Workspace

By leveraging the built-in Chrome browser management capabilities within the Google Workspace Admin console, organizations can centrally control Chrome settings and security with no additional software cost, fitting the "least expensive solution" requirement.

Question: 101

Your company is streamlining workflows by creating custom applications for tasks like filing expense reports or requesting time off. You need to identify a Google Workspace solution to develop these applications. Your development team has only basic coding knowledge. What should you do?

A. Enable Gemini for Workspace. Direct users to use generative AI across Gmail and Drive to simplify the submission of expense reports.

B. Direct employees to use Google Forms to collect data and create basic workflows.

C. Enable AppSheet for your organization.

D. Enable AppScript for your organization and allow employees to build add-ons to existing Workspace solutions.

Answer: C

Explanation:

The core requirement is to create custom applications for workflows like expense reports and time off, with a development team that has "only basic coding knowledge." This strongly points to a "no-code" or "low-code" platform.

AppSheet is Google's no-code development platform, designed specifically for users (often referred to as "citizen developers") with basic or no coding knowledge to build custom mobile and web applications directly from data sources like Google Sheets, Forms, or other databases. It's ideal for automating business processes and creating custom workflows without traditional programming.

Here's why the other options are less suitable:

A . Enable Gemini for Workspace. Direct users to use generative AI across Gmail and Drive to simplify the submission of expense reports. Gemini for Workspace (Google's AI assistant) can help with tasks like drafting emails, summarizing documents, and generating content within existing Workspace apps. While it can "simplify" aspects, it is not a platform for developing custom applications with structured workflows and data capture for tasks like full expense report submission or time-off requests. It enhances existing tools, it doesn't build new ones.

B . Direct employees to use Google Forms to collect data and create basic workflows. Google Forms is excellent for data collection and can be used for very simple workflows (e.g., collecting time-off requests). However, it lacks the robust functionality needed for complex custom applications, such as managing approvals, displaying data in different views, ofline access, or integrating with other systems, without significant manual effort or custom scripting. The term "custom applications" suggests something more sophisticated than just a form.

D . Enable AppScript for your organization and allow employees to build add-ons to existing Workspace solutions. Google Apps Script allows for powerful automation and the creation of custom add-ons for Google Workspace applications (Gmail, Sheets, Docs). However, Apps Script requires knowledge of JavaScript. While it's relatively "basic coding" compared to full-stack development, it's still coding. The question emphasizes "only basic coding knowledge" and the need for a solution to develop applications, implying a more visual or declarative approach than coding from scratch. AppSheet is generally considered easier for those with "basic coding knowledge" or even no coding knowledge, making it a better fit for rapid application development by non-developers.

Reference from Google Workspace Administrator:

AppSheet: No-code App Development | Google Cloud: This is the primary resource for AppSheet, explicitly stating its purpose for "no-code app development" and enabling "everyone in your organization to build and extend applications without coding." It highlights use cases for automating business processes like order approvals (similar to expense reports/time off).

Reference: https://cloud.google.com/appsheet

Google AppSheet | Build apps with no code: Further reiterates that AppSheet helps "build powerful applications and automations that boost productivity. No coding required." It also mentions integration with Google Workspace,

including Google Sheets and Forms as data sources.

Reference: https://about.appsheet.com/home/

Quick start: Build your first app and automation using Google Forms - AppSheet Help: This resource demonstrates how AppSheet can take data from Google Forms and build an app with automation (e.g., email notifications for approvals), showcasing its capability for workflows like expense reports.

Reference: https://support.google.com/appsheet/answer/14714804?hl=en