<u>W-4, D-3</u>

1. Message trace using SCC.

<table>
<tr><td>Initial Option Trace</td><td>✓ <b>Default Queries</b> - Queries provided by Office 365
✓ <b>Custom Queries</b> - Queries created and saved by admins in your organization
✓ <b>Autosaved Queries</b> - Last 10 queries that were run but not saved manually</td></tr>
<tr><td colspan="2">✓ Please navigate to – <b>SCC</b> > <b>Mail flow</b> > <b>Message trace</b> > <b>+Start a trace</b>
✓ Please fill up – Date range, Time range, Time zone (default 2 days), Message ID, Delivery Status, Recipient, Sender
✓ Choose report type
o <b>Summary:</b>
▪ If the time range is less than <b>10 days,</b>
▪ No additional filtering options
▪ Results are available almost immediately
▪ Report returns up to <b>20,000 results</b>
o <b>Enhanced summary:</b>
▪ Downloadable CSV files.
▪ Require By these people, To these people, or Message ID.
▪ Report returns up to <b>50,000 results.</b>
▪ Include Direction, Original client IP address & many more.
o <b>Extended summary:</b>
▪ Downloadable CSV files.
▪ Require By these people, To these people, or Message ID.
▪ The Extended report returns up to <b>1000 results.</b>
▪ Include message events & routing details with report (comprehensive)</td></tr>
</table>

W-4, D-3

2. What is Content Search? How to retrieve data by doing Content Search?

<table>
<tr><td>Content Search</td><td>✓ For in-place items such as <b>email</b>, <b>documents</b>, and <b>instant messaging conversations</b> in your organization.
✓ Possible to retrieve deleted email and other items of user mailbox as a PST file.</td></tr>
<tr><td colspan="2">✓ Go to https://protection.office.com
✓ Click <b>Search</b> &gt; <b>Content search.</b>
✓ On the Search page, click the arrow next to Add icon <b>New search.</b>
✓ After you've set up your search query, click <b>Save &amp; run.</b>
✓ On the Save search page, type a name for the search, and an optional description that helps identify the search. The name of the search has to be unique in your organization.
✓ Click <b>Save</b> to start the search.
✓ After you save and run the search, any results returned by the search are displayed in the results pane. Depending on how you have the preview setting configured, the search results are display or you have to click Preview results to view them. See the next section for details.
✓ To access this content search again or access other content searches listed on the Content search page, select the search and then click Open.
✓ To clear the results or create another search, click Add icon <b>New search.</b>
✓ You can <b>Export results</b> and <b>Export report</b></td></tr>
</table>

3. What is Audit log search? How to perform it?

Audit Log	✓ Same as EAC except EAC has 8 different options available ✓ **Track user and administrative activity** within the tenant. ✓ Examples include changes made to Exchange Online and SharePoint Online tenant configuration settings, and changes made by users to documents and other items. ✓ Effectively manage **user experience, mitigate risks**, and fulfill **compliance obligations.**
Permission	✓ EAC Organization Management or, ✓ EAC Compliance Management or, ✓ MS 365 Global Admin
Steps of - Audit log search	✓ Navigation – **SCC** > **Search** > **Audit log search** ✓ Step 1: **Run** an audit log search ✓ Step 2: **View** the search results ✓ Step 3: **Filter** the search results ✓ Step 4: **Export** the search results to a file

W-4, D-3

4. What is the limitation of Content Search & Audit log search?

Limitation of - Content Search	✓ The maximum number of mailboxes in a Content Search that can be deleted 50,000 ✓ The maximum number of user mailboxes in a Content Search that can be previewed 1,000 ✓ Minimum alpha characters keyword 3 ✓ Maximum number of items per user mailbox that are displayed 100 ✓ The maximum number of items found in all user mailboxes that are displayed 1,000
Limitation of - Audit Log Search	✓ Download a maximum of **50,000** entries to a CSV file from a single audit log search. ✓ **Audit records** are retained for **90 days.** ✓ Take up to **30 minutes** or up to **24 hours** after to show the reports. ✓ Maximum date range of **90 days**

5. What is eDiscovery? Use eDiscovery to export data.

<table>
<tr><td>eDiscovery</td><td>✓ Electronic Discovery
✓ <b>Process/single place</b> of identifying and delivering electronic information that can be used as evidence in <b>legal cases.</b>
✓ Search mailboxes and sites in the same eDiscovery search by using the Content Search tool.
✓ Core eDiscovery cases to identify, <b>hold</b>, and export content found in mailboxes and sites.
✓ Advance eDiscovery for E5 subscription</td></tr>
<tr><td colspan="2">✓ Please Navigate to – <b>SCC</b> > <b>eDiscovery</b> > <b>eDiscovery</b> > <b>+Create a Case</b> > Type Case Name > <b>Open</b>
✓ There you will find three options available to perform – <b>Holds, Searches, Exports</b>
✓ Holds – +Create > fill up <b>choose location, create query</b> > press <b>Save</b>
✓ Searches – +New Search >fill up <b>search query, location</b> (all locations, location on hold, specific location) > press <b>Save</b>
✓ Exports –</td></tr>
</table>