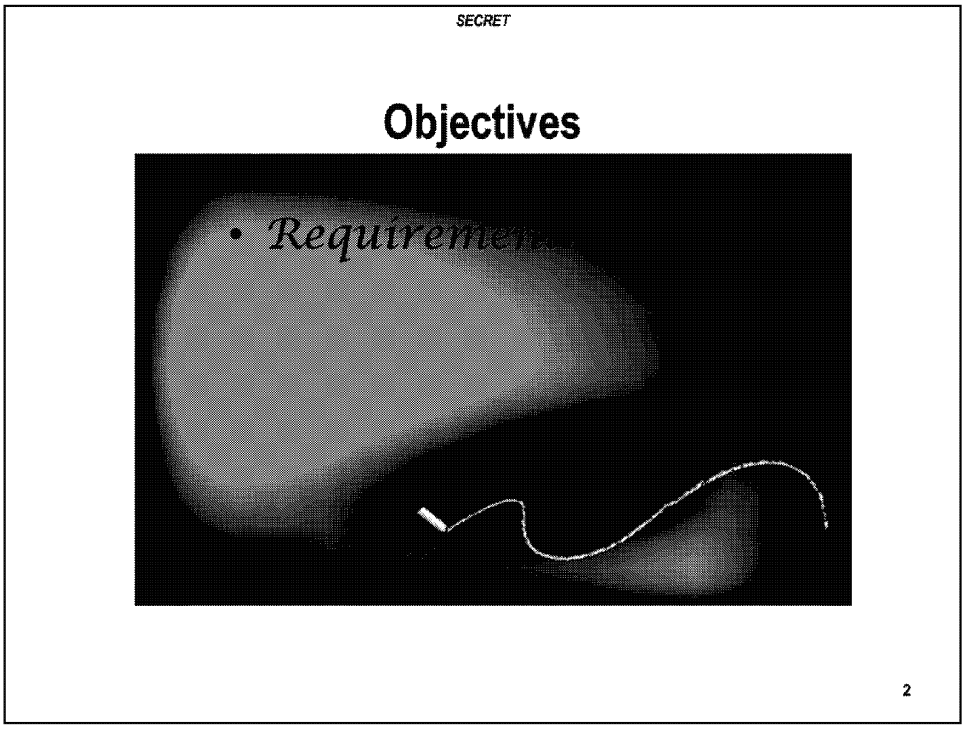
Cyber Defence Policy Awareness Curriculum

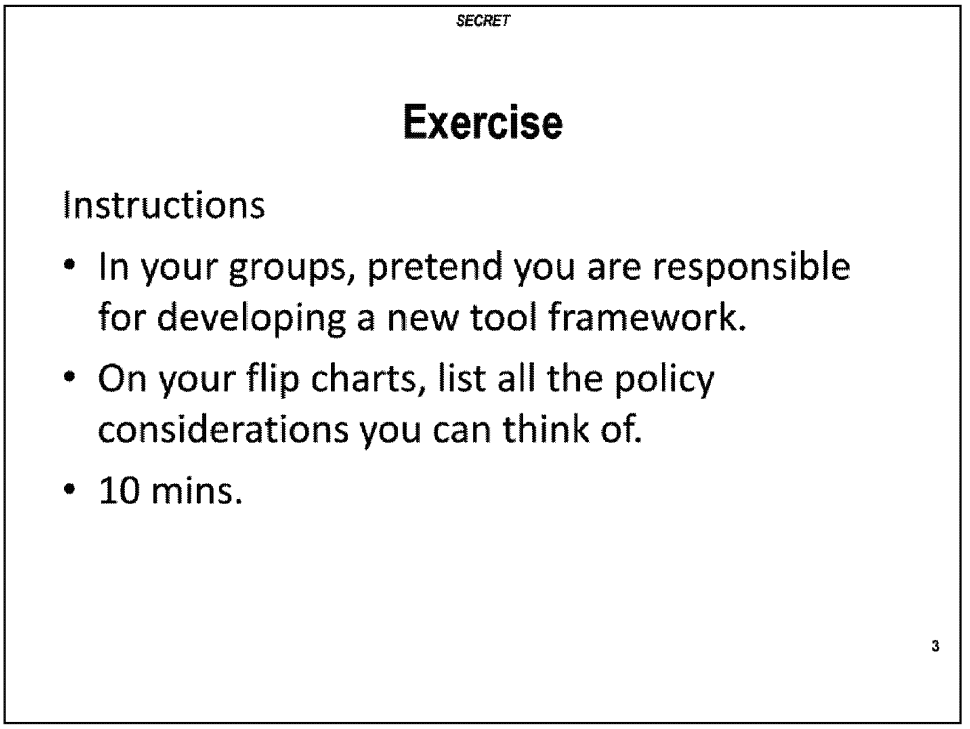
DEVELOPMENT

1

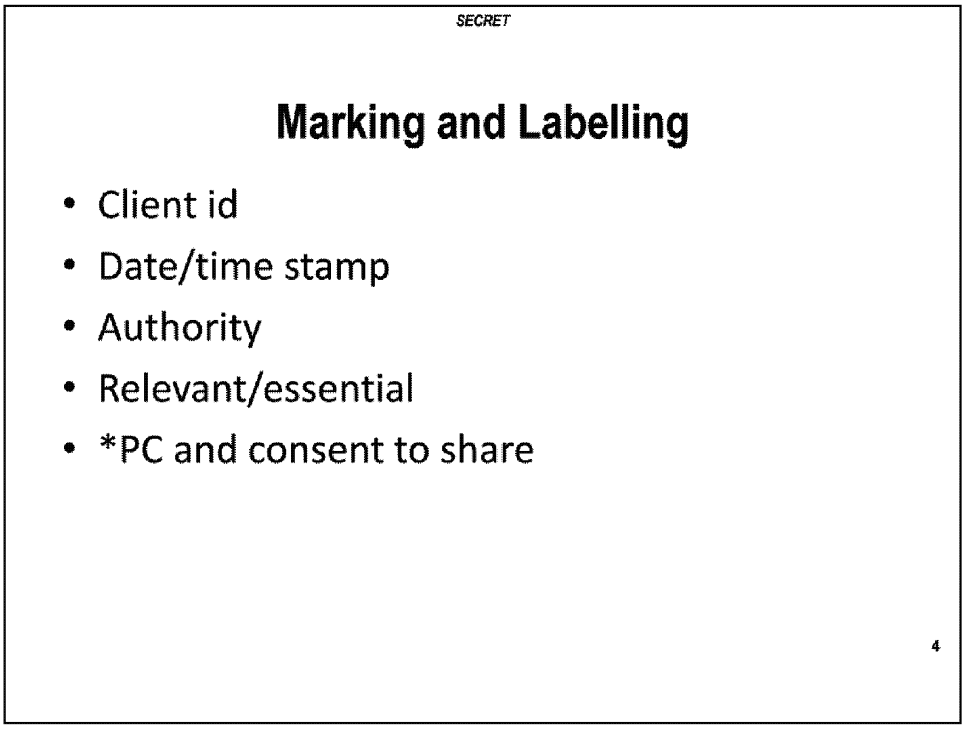


The development portion of this course is relatively short as there is really no new information to be presented. But it is a very good lesson to finish off the curriculum as it takes into consideration everything that was already presented in the previous lessons.

So, to start this lesson off, I'm going to put you all to work!



Have each group present their considerations and have them explain why each was important.

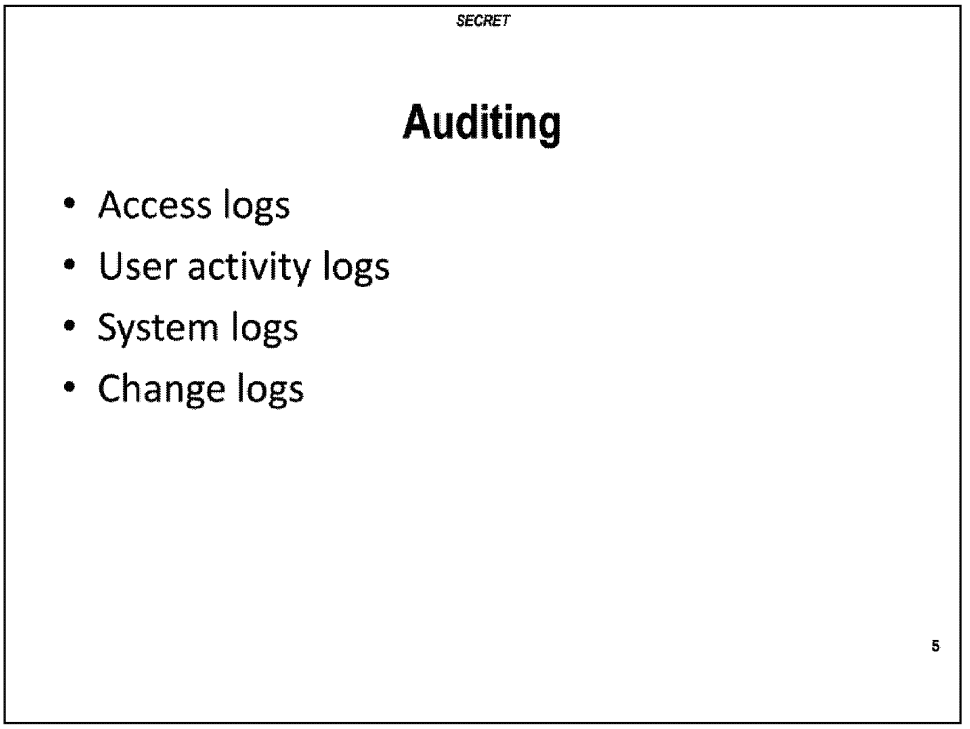


If the tool framework stores data, it must mark the data with appropriate tags.

All data obtained during Cyber Defence Activities must be marked with a client id, date/time stamp and the authority under which the data was obtained.

Data that is used and retained must be properly marked as either relevant or essential.

For Non-MA operations, data must be marked to show if it's a PC, a PC with recipient consent to share, or other data.

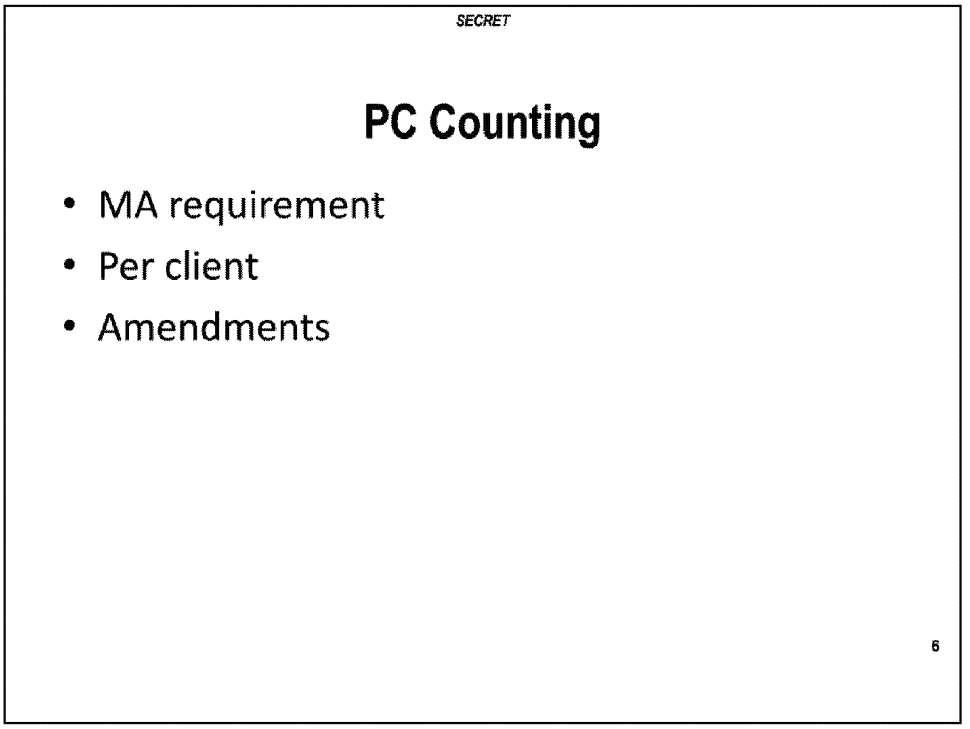


Policy doesn't specifically state how to ensure auditability, just that it is required. Some examples of what to incorporate into tools would be access logs, user activity logs, systems logs and change logs.

The specific requirements will depend on what is being developed and what type of data is being used.

i.e. If the tool allows users to access raw data, you'll want more stringent and detailed auditing than if the tool \only access used and retained data.

At the end of the day, ask yourself, "can I piece the story back together?".



As an MA requirement, CSE must count all recognized PC retained during cyber defence operations under MA.

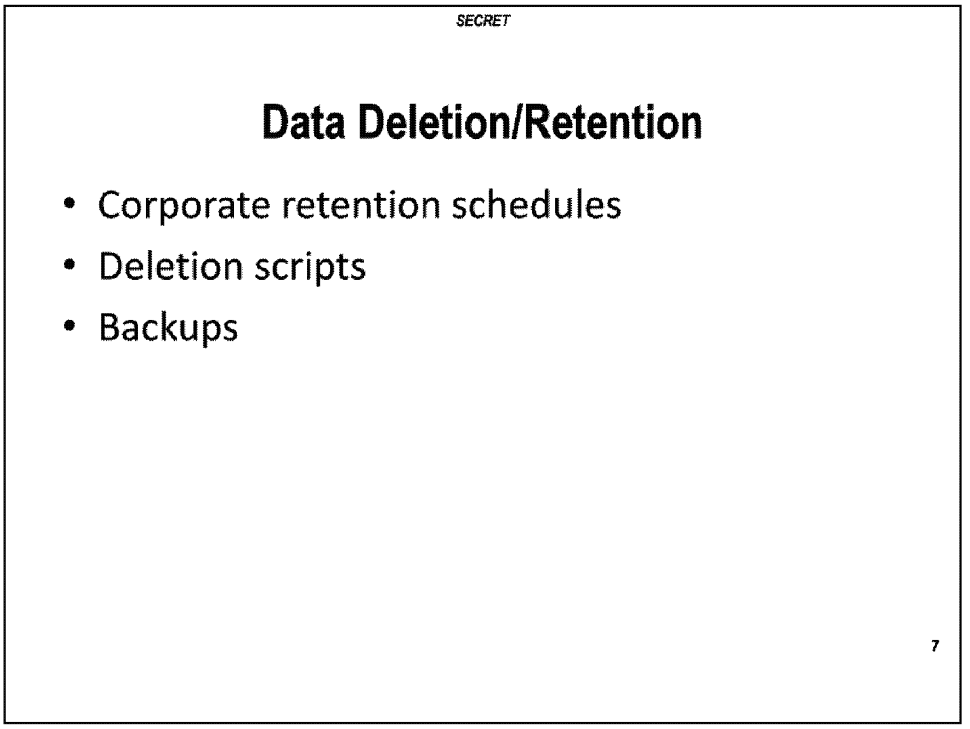
The total count of retained PC must be calculated on a per client basis.

Sometimes analysts will have to amend the PC count. If that happens, the system must be able to take that into account. i.e. As part of the PC count report, [redacted] actually indicates if there were any changes to PC numbers from the last period.

Every individual email retained are counted as one.

If data from multiple identical emails is used and retained, then you have to could each of the emails. Think SPAM sent to multiple people.

For other types of data recognized as PC, every individual data flow or, IP packet for non-data flow, is counted as one PC. Think chat session.

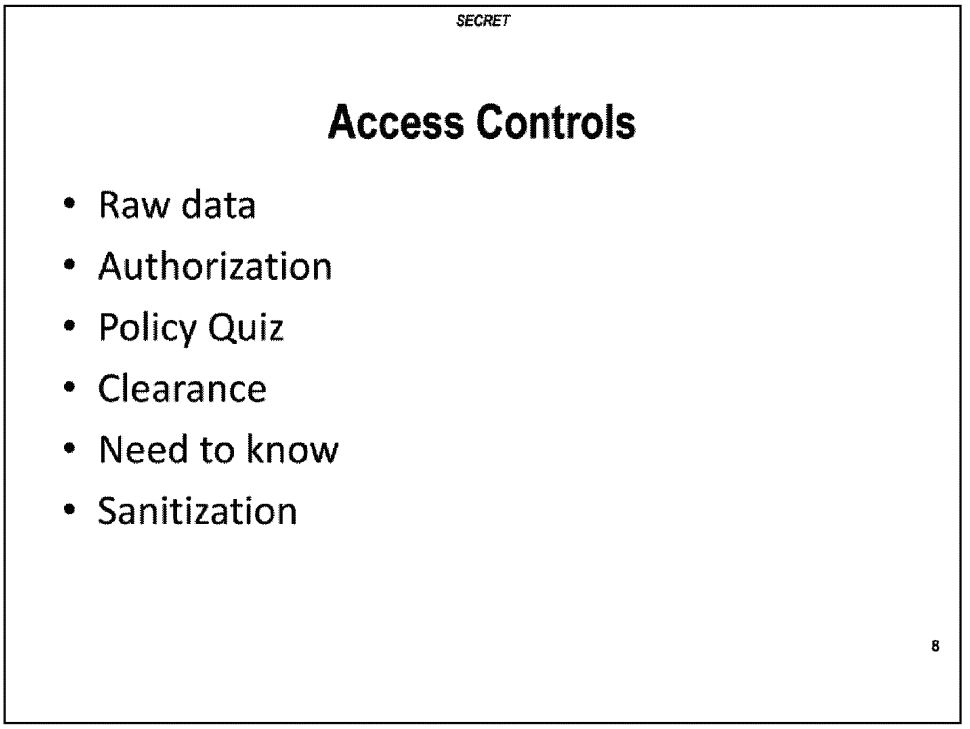


Depending on the source (MA or Non-MA) raw data can only be kept for a limited time. [redacted] for data collected under MA, [redacted] for metadata under MA and [redacted] after the completion of requested assistance for non-MA activities.

Any used and retained data must follow the corporate retention.

Any tool that stores data must have scripts in place to ensure data is not kept for any longer than allowed.

You also should have backups in case the script doesn't run. This could be manual checks, an auto generated warning or even a second script.



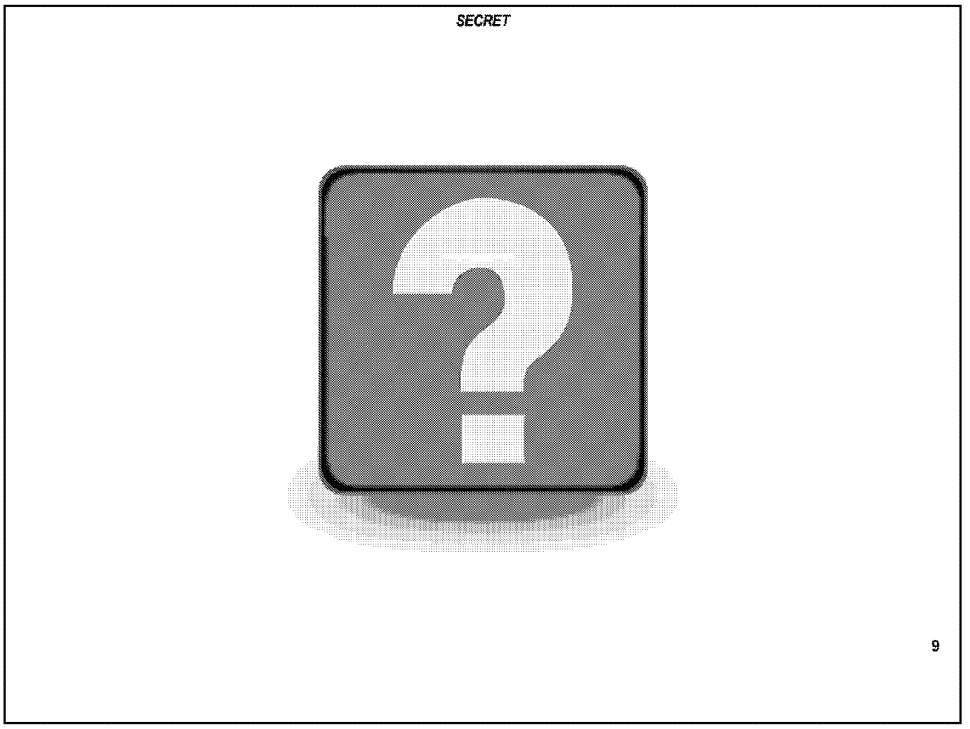
Raw data can only be accessed by those who have been authorized to conduct or support cyber defence activities by DG Cyber Defence.

Once authorization has been granted, those personnel must completed an ITS policy quiz before being put on the "ALPR" list.

So, as a developer, you need to make sure that there is a way to restrict access based on this list. It can be an automatic process fed by LDAP, or a manual process. The problem with the manual process is that the ALPR list changes as people move positions, so it would be require constant updating.

Other than the ALPR list, you have to take into consideration security clearances, ECIs as well as need to know.

What about suppression? Is there unsuppressed CII which is viewable by everyone?



Remember, the goal of this lesson was not to tell you what to do when involved in developing a system, service or tool. The goal was to get you understand that there are many factors that need to be considered. The best thing to do is to engage IPOC early in the process so we can give you the proper policy advice and guidance as you move forward.

Questions?