# Certifications in IIQ

**Certifications:**

In IdentityIQ, the term "certification" or "certification campaign" refers to an overall campaign to review access for a selected set of users – that is, to create and then complete a set of access reviews. The certification campaign is usually the responsibility of a high-level authority on access, such as a compliance officer, administrator, or manager.

A certification defines what is being reviewed and for which users, who the reviewers will be, what the timeline for the reviews is, and other details. For example, a company's compliance officer may set up a quarterly certification campaign to review and certify all the sensitive financial systems the people in the Accounting department have access to, and require each manager in the Accounting department perform the access review for all the members of his or her team.

The access reviews enable reviewers to:

l Approve access for identities

l Approve account group permissions and membership

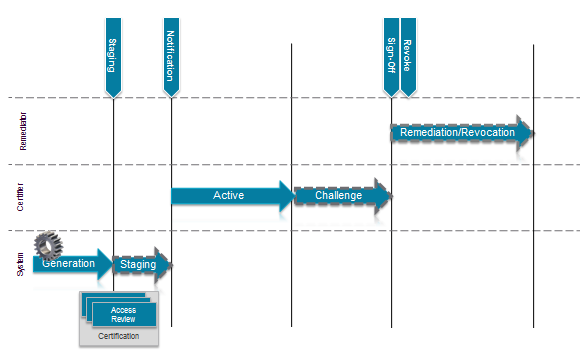
l Approve role composition and membership

l Take corrective actions, such as revoking entitlements that violate policy

l Forward, reassign, or delegate all or part of the access review to another reviewer

For all corrective actions, IdentityIQ can fulfill certification revocations through automated or manual means, depending on the individual applications connector configurations. IdentityIQ can also be configured to integrate with ticketing systems or other provisioning systems to fulfill provisioning requests.

**Life cycle of certification:**



**Certification Schedules**

Certifications can be scheduled to run on a **periodic** basis; they can also be triggered by an **event**, or run as a **one-off** process.

**Periodic Certifications:**

Periodic certifications are scheduled to run on a recurring basis, such as daily, weekly, monthly, quarterly, or annually.

These periodic access reviews provide a snapshot view of the identities, roles, and account groups within your enterprise. Periodic certifications focus on the frequency at which entire entities (identities, roles, or account groups) must be certified.

A periodic certification is considered complete when **all** the access reviews contained within the certification have been completed. The access reviews that make up the certification, in turn, are considered complete when all items, such as roles, entitlements, violations, and application objects, have been acted upon, and those decisions are confirmed by the user to whom that access review was assigned.

Periodic certifications can be created using a multi-level sign-off structure, to allow multiple certifiers to review the access before the review is considered complete.

**Event-Based Certifications:**

Certifications can be configured to run based on "trigger" events that occur within IdentityIQ. For example, you can configure IdentityIQ to automatically generate a certification any time an identity's manager changes. You can also configure the events that trigger the certifications to meet the needs of your enterprise. See Certification Events for more information.

**One-Off Certifications for Identities:**

One-off certifications can be created from the Identity Risk Score, Identity Search Results, or Policy Violation pages.

These one-off access reviews can be run for a single identity, or for multiple identities at once. One-off certifications are most often used in special situations, such as when an access review is required outside of the normal certification cycle. You can also schedule standard IdentityIQ certifications to run on a one-off basis.

# **Types of Certification**

IdentityIQ provides these types of certification:

**[IMG_256Targeted Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

The most flexible type of certification, designed to meet most organizations' full range of certification needs from a single place. In a Targeted Certification you can certify role, entitlement, and account access for a narrowly defined set of your users. The Targeted Certification gives you a high level of flexibility in choosing which parameters to include in the certification, such as who, what, and when to certify.

**[IMG_257Manager Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify that a manager's direct reports have the right entitlements they need to do their job, and no more than that. You can configure a Manager Certification to include all managers in the company, or only specific managers. You can also configure which applications you want to certify as part of the Manager Certification.

**[IMG_258Application Owner Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify that all identities that have access to *applications* for which the reviewer is responsible have the proper entitlements.

**[IMG_259Entitlement Owner Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify that all identities that have access to *entitlements* for which the reviewer is responsible are correct.

**[IMG_260Advanced Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify entitlements and roles for all identities included in a specific population or group.

**[IMG_261Account Group Membership Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify that all accounts which make up an account group are correct – that is, are the right accounts in the account group. Account groups that do not have owners assigned are certified by the owner of the application on which they reside.

**[IMG_262Account Group Permissions Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify that all permissions that are granted to an account group for selected application(s) are correct. Account groups that do not have owners assigned are certified by the owner of the application on which they reside.

**[IMG_263Role Membership Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify that roles for which the reviewer is responsible are assigned to the correct identities.

**[IMG_264Role Composition Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

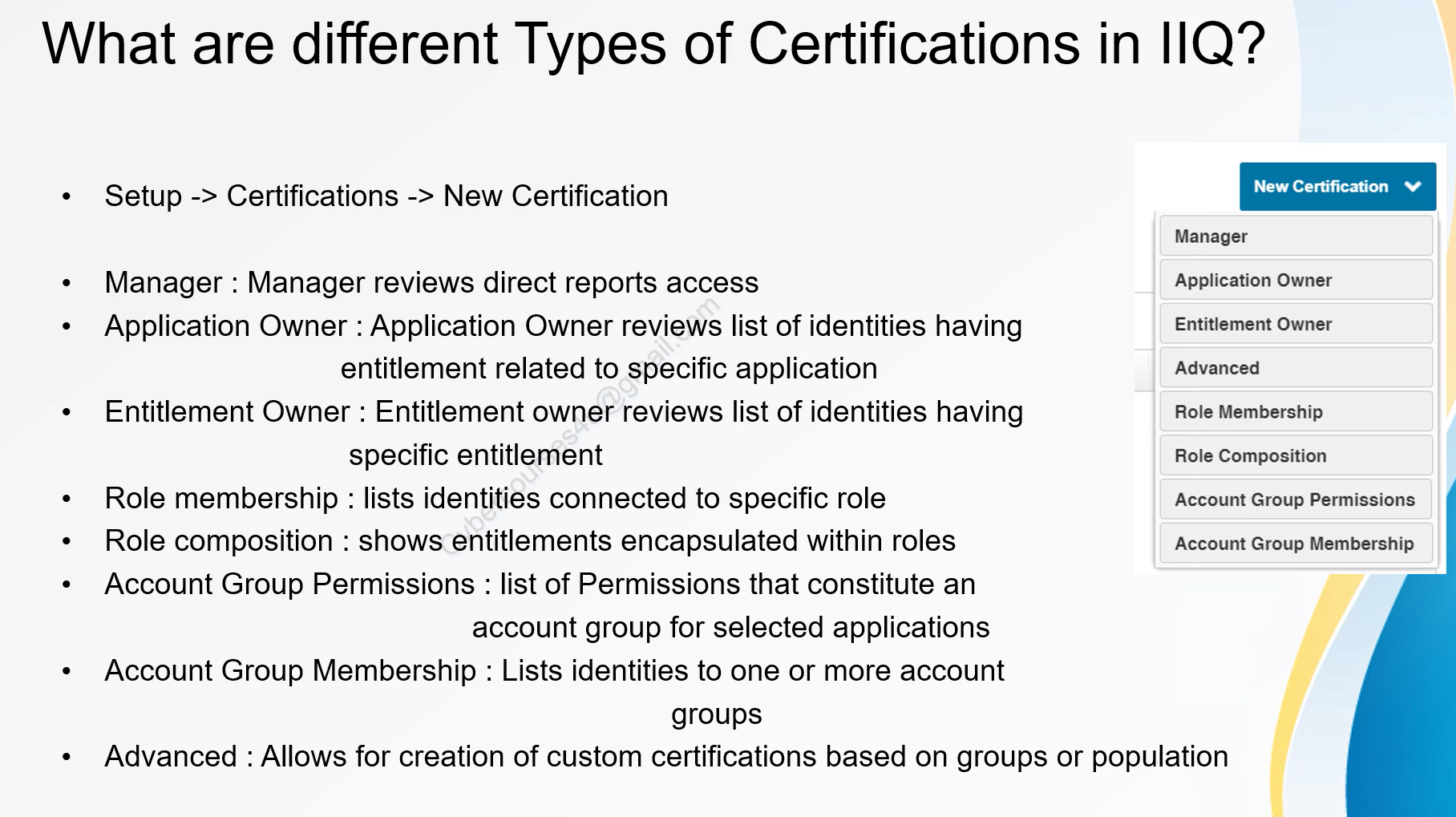
Certify that roles for which the reviewer is responsible are composed of the proper permissions and entitlements.

**[IMG_265Identity Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

This type of certification is used for "one-off" certifications that are launched from the Identity Risk Score, Identity Search Results, or Policy Violation pages. These certifications verify the entitlement information for the identities, typically for at-risk users.

**[IMG_266Event-Based Certifications](https://documentation.sailpoint.com/identityiq/help/certification/types_of_certification.html?Highlight=certification)**

Certify the entitlement information for the identities selected based on events detected within IdentityIQ.

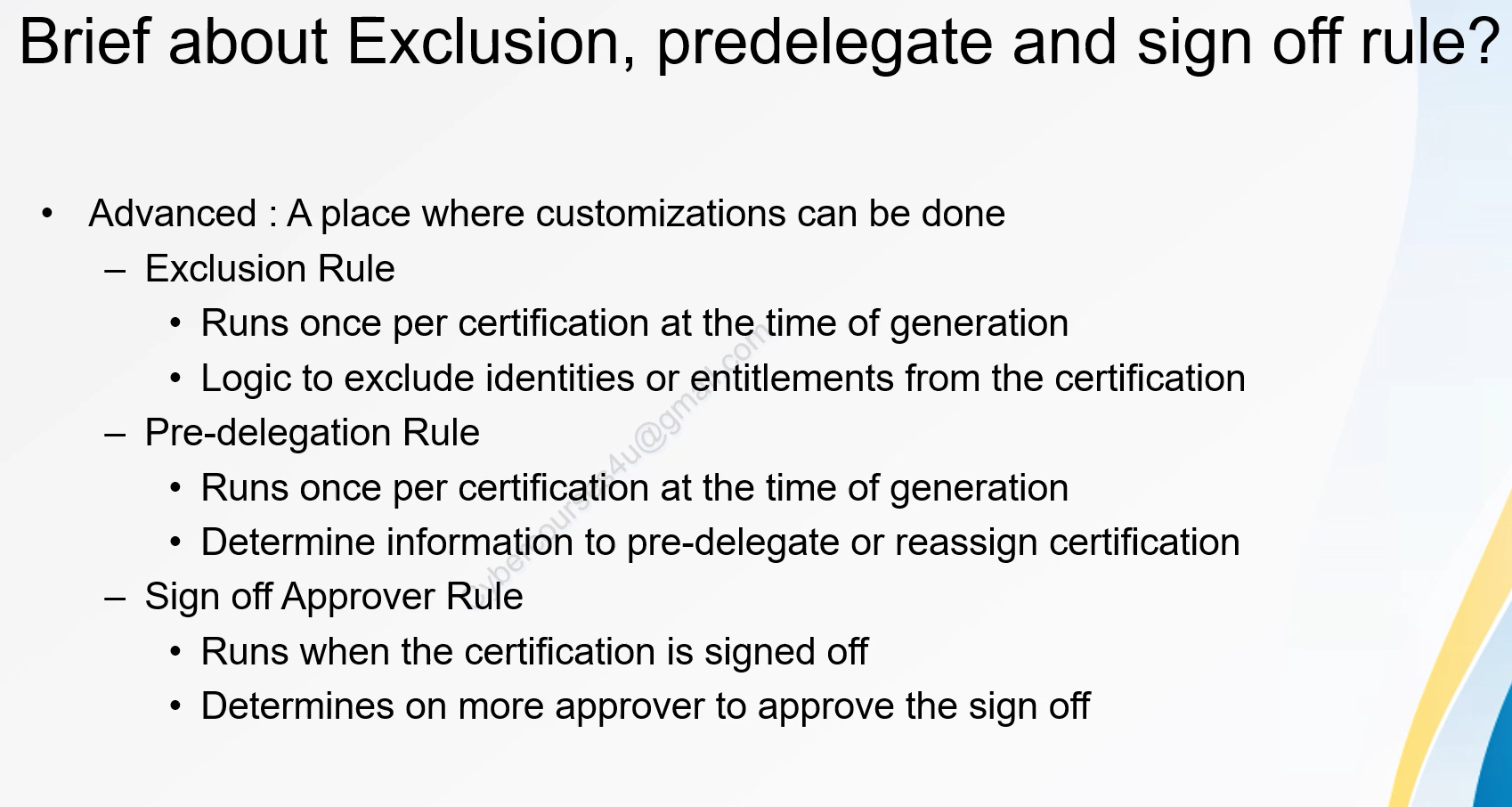


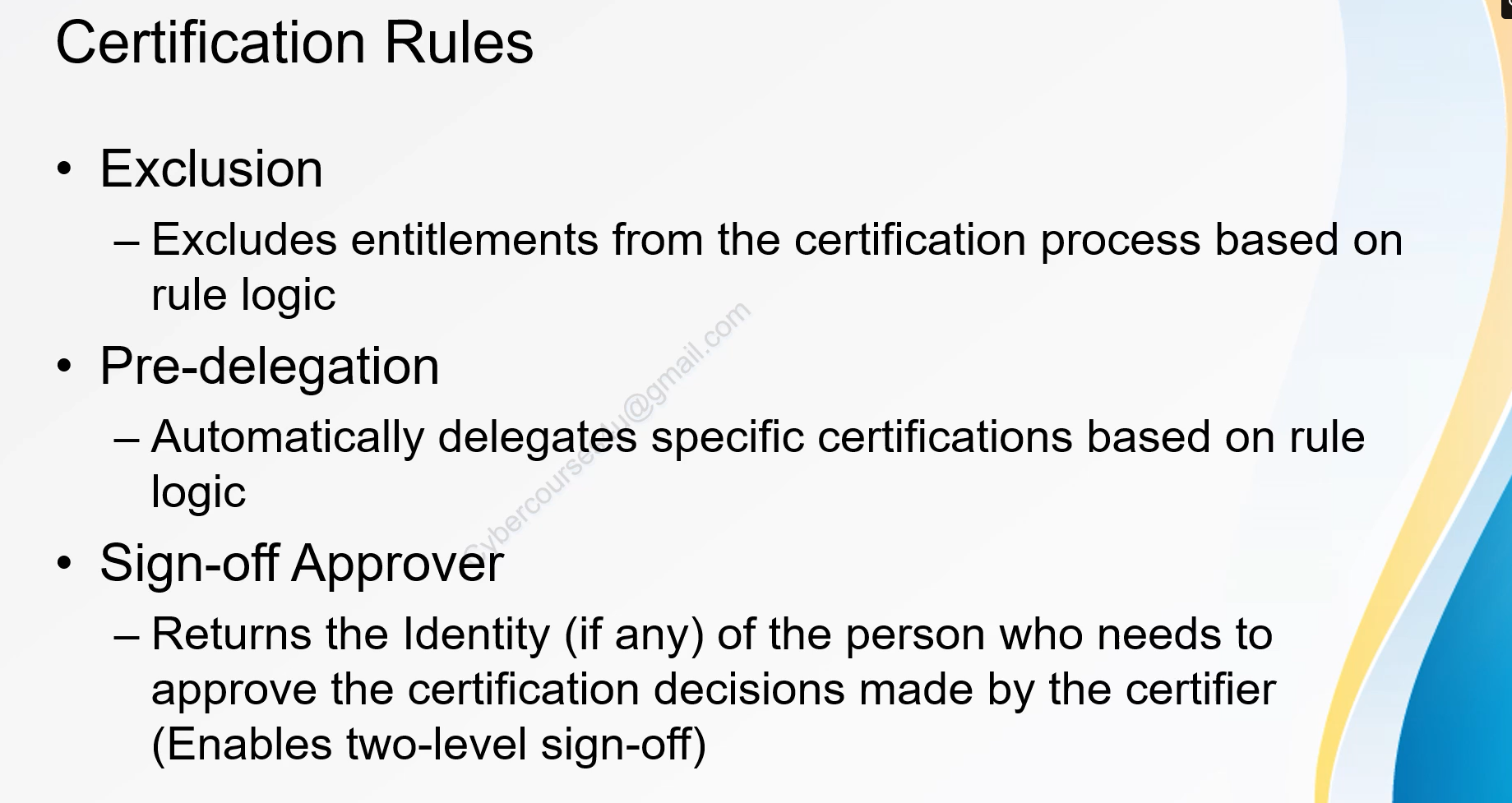
**Interview questions:**

1.What is difference between delegate,forward and Reassign?

Ans: 

1. Explain about Exclusion, Predelegate and Sign Off Rule?





1. What are different Certification Objects?
2. Name CertificationEntity Types?

