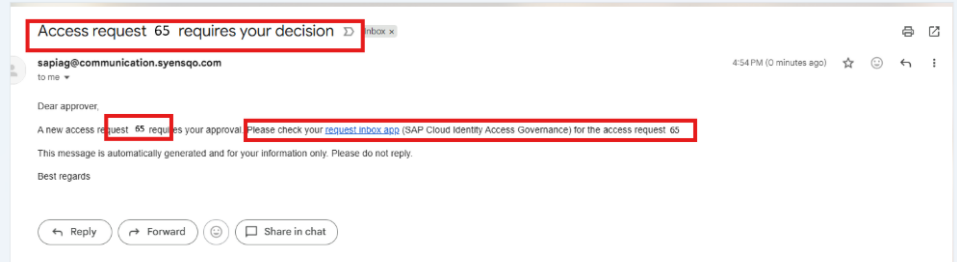
Quick Reference Guide - Approving Privileged Access Requests (Approver Point of View)

Process Overview - Approver POV

> ***Note:*** *Access requests, including PAM (Privileged Access Management), provide elevated permissions and must be approved only for valid business or emergency needs.*
>
> - *Approvers are responsible for validating the **reason, scope of work, and expected activities**.*
> - *Requests with insufficient or incomplete information **must be rejected**.*

Step 1: Receive Approval Notification

- Approver will receive an **email from IAG** indicating a pending access request.



Step 2: Login to IAG

- Click the link in the email or open the **IAG portal.**
- **Dev/QA - https://syw-iag-dev-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#Shell-home**
- **Production - https://syw-iag-prd-eu10.sapciag-ee.cfapps.eu10.hana.ondemand.com/cp.portal/site#Shell-home**

Step 3: Open Access Request Inbox

- Click **Access Request Inbox**.
- Pending approval work items assigned to you will be displayed.

Step 4: Review Request Details

- Select the request to review.
- Verify the following information:
  - **Requestor Name**
  - **Requested User**
  - **Role Requested**
  - **Reason / Justification / Scope of Work**
  - **Duration of access requirement**

Ensure the request is **complete and accurate.**The following PAM roles require the requester to provide a valid justification and specify the assignment duration before the approver can grant access.

> **SAP Ariba PAM Roles**
>
> **Ariba Template Manager** – Creates and maintains sourcing templates.
>
> **Ariba User Admin** – Monitors correct user provisioning from IAG to Ariba.
>
> **Ariba Master Data Manager** – Reviews integration of master data into Ariba.
>
> **Ariba System Admin** – Super user for exceptional tasks or defect fixes.
>
> **Icertis PAM Roles**
>
> **IT Icertis Master Data Admin** – Manages master data only; no system/workflow access.
>
> **IT Icertis User Management Admin** – Administers users, groups, orgs, and technical role assignments; no transactional data access.
>
> **IT Icertis Admin Extended** – Same as Support + access to transactional data (excluding confidential contracts).
>
> **IT Icertis Config Admin** – Full system configuration control; no access to contracts or transactional data; technical roles assigned via User Management Admin.

Step 6: Validate Request

- Confirm the request is for a **valid, active user**.
- Ensure the request aligns with requester's role ownership responsibilities and understand for any impacts of changes in the production system for the access requested.
- Based on validation, approve or reject the request with appropriate comments. The corresponding access decision will be communicated to the user via email notification.