

Access Review Case Study

You work as a busy head of the sales department in a large industry company with many concurrent projects to maximize the income for your company. Your time is limited, and you have sales goals to fulfil. The security teams reminded you via email that your company is legally required (compliance) to review the access of the employees in your department.

Your task will be to review the current authorizations of your employees. For this purpose, you will be provided with a table view like in the example below:

| | | | | |
|---|---------------------------------------|-----------------|----------------|---------------------|
| <input type="button" value="Approve"/> | <input type="button" value="Remove"/> | Belen, Nickolas | Administration | MUC_Access_Extended |
| <input checked="" type="button" value="Approve"/> | <input type="button" value="Remove"/> | Belen, Nickolas | Administration | MUC_Access |
| <input type="button" value="Approve"/> | <input type="button" value="Remove"/> | Belen, Nickolas | Administration | Marketing_Share |

The table shows the current authorizations in your department, with each row containing information about one such authorization. Each row has an Approve and a Remove button, which can be selected to mark your decision if the authorization is necessary (Approve) or excessive (Remove).

The example above shows three authorizations, one is necessary and marked with approve, one is excessive and marked as remove and one is still undecided.

You can alphabetically sort the columns and filter onto specific employees or authorizations via the search bar in the top right corner.

Information for you task:

You must follow the principle of least privilege: Employees must have permissions required for their job, but not more. If you decide to revoke an excessive permission for one of your employees, the employee will no longer be able to access the associated resources by tomorrow.

While the security team points out that any excessive permission poses a security threat, you are aware that missing ones might prevent your employees from working until they reobtain it via a time-consuming helpdesk or self-service request.

Department hierarchies:

- I. Each team has one team lead, who record their teams' used times in the Greyman Time Booking Software.
- II. Additionally, team leads have an annual budget for bonus payments, which they can distribute among their team members based on last year's performance.
- III. Teams might have senior employees, which have additional task that are area specific to a geographic region.
- IV. After a restructuring only the secretary can administer payments to external service distributors.
- V. The trainee is currently working in the Contracts negotiation team. He has worked in the Contracts template creation team in the previous year and will work in the legal consulting team in some years to come.

The sales department consists of three teams:

- I. Contracts negotiation
 - The team has default access and maybe special accesses to the C&C Maker tool.
 - Seniors for a certain region need access to the approval page of the C&C Maker tool.
 - To load a new template into the tool, reading access to the file share of the Contracts template creators' team is needed.
 - Only the team lead can write old contracts into the old contracts file share location.
- II. Contracts template creation
 - The template creators need read and write access to their file share location.
 - They have read access to the corporate design file share location.
 - For software they use CharoLingua, ConciliumC and Adobe Photoshop
- III. Legal consulting
 - Everyone in the team has access to the Pax Pecuniae Software and can access the C&C Tool for legal approval
 - For reference they can read old contracts on the designated file share location

Miscellaneous:

- I. Everybody communicates via Outlook and Microsoft Teams.
- II. Regional specialists may query the company's customer database on their region and acquire the regional company policies.
- III. Everybody can print a coupon for today's deal of the diner next door.

Keep this document close at hand, as you may refer back to it during the review.