Security Management – Case Study 3

Student: Philip Magnus
Student ID: c2410537022
Date: 20.01.2026

Case Study Tasks

1. Describe at least 5 challenges for identity and access management for your organisation (5p)
2. Define an RBAC model for your organization (approx. 5 roles). (5 p)
3. For each role, define at least one scenario and a related permission catalog. (5 p)

Case Study 3 uses the fictional company from Case Studies 1 and 2 as an example: PointPoint GmbH, a SaaS provider headquartered in Vienna with approximately 250 employees.

1. Challenges in Identity & Access Management (IAM)

Identity and access management is a central component of the overall security architecture at PointPoint GmbH. As an organization that provides security-related services itself, weaknesses in IAM would not only pose internal risks but could also damage customer trust and regulatory compliance. Several specific challenges can be identified.

1.1 Complex Role Landscape

PointPoint GmbH is structured into multiple highly specialized departments, including Red Team, Blue Team, Governance, Risk and Compliance (GRC), Cloud & Infrastructure Services, Software Development, Sales, Human Resources, and Management. Each department performs different tasks and therefore requires different access rights to systems, data, and infrastructure.

Without a clearly defined role model, access rights tend to grow over time as employees change positions, support colleagues, or take on temporary responsibilities. This often results in users having more permissions than they actually need to perform their current job. Such over-privileging violates the principle of least privilege and significantly increases the risk of misuse, accidental errors, or successful attacks in case an account is compromised.

1.2 Onboarding and Offboarding

As a SaaS provider and consulting company, PointPoint GmbH frequently hires new employees and engages external consultants for specific projects. New staff members often need access to systems on their first working day to remain productive. At the same time, access rights must be granted in a controlled and documented manner.

The offboarding process is equally critical. When employees leave the company or consultants finish their assignments, all logical and physical access rights must be revoked immediately. If offboarding is delayed or incomplete, inactive accounts may remain enabled. These so-called orphaned accounts represent a serious security risk, as they are often overlooked in monitoring and may be abused without being detected.

1.3 Separation of Duties (SoD)

Separation of duties is an essential security principle at PointPoint GmbH, particularly because the company handles sensitive customer data and security-critical systems. For example, software developers should not have administrative access to production environments. If developers were able to deploy changes directly to production, this could lead to unauthorized modifications, accidental outages, or deliberate abuse.

Similarly, employees responsible for audits and compliance checks must be able to review logs, configurations, and access rights without being able to alter them. If the same person were allowed to both perform and audit security-relevant actions, this would undermine the integrity of the control process. Enforcing separation of duties consistently across all systems is therefore a major IAM challenge.

1.4 Cloud and Hybrid Environments

PointPoint GmbH operates a hybrid IT environment consisting of on-premise infrastructure, public cloud platforms, and various SaaS applications. Each environment may implement identity and access management differently, using local directories, cloud-native IAM solutions, or external identity providers.

Ensuring consistent access control policies across all these platforms is complex. A user who changes roles within the company may require updated permissions in multiple systems. Without centralized IAM governance, inconsistencies can arise, such as access being revoked in one system but remaining active in another. This fragmentation increases administrative effort and creates security gaps.

1.5 Compliance and Auditability

As a company operating in the European Union, PointPoint GmbH must comply with regulations such as the General Data Protection Regulation (GDPR), as well as security standards like ISO 27001. These frameworks require organizations to demonstrate that access to sensitive data is restricted, justified, and regularly reviewed.

From an IAM perspective, this means that all access rights must be traceable, documented, and auditable. The company must be able to answer questions such as who has access to which systems, why this access was granted, and when it was last reviewed. Regular access reviews and detailed audit logs are therefore mandatory, but they also increase the complexity of IAM operations.

2. Definition of an RBAC Model

To address these challenges, PointPoint GmbH adopts a role-based access control model. In RBAC, permissions are assigned to roles rather than directly to individual users. Users are then assigned one or more roles based on their job function.

This approach simplifies access management, improves transparency, and supports key security principles such as least privilege and separation of duties. Based on the organizational structure and business processes of PointPoint GmbH, five core roles are defined: Employee, Developer, Security Analyst, System Administrator, and Management. These roles cover the majority of access requirements within the company while remaining manageable and scalable.

The following RBAC model with five roles is defined:

Role	Description
Employee	Standard employee

Role	Description
Developer	Software and cloud development
Security Analyst	SOC, monitoring, incident response
System Administrator	Infrastructure and platform operations
Management	Strategic and administrative responsibilities

3. Scenarios and Permission Catalogs

3.1 Role: Employee

An employee typically performs standard office tasks such as communicating with colleagues and customers, creating documents, and accessing internal information. In this scenario, the employee requires access to office productivity systems, including email, calendar, and collaboration platforms. Additionally, employees must be able to read internal policies, guidelines, and security instructions.

However, employees do not require access to administrative interfaces, production systems, or sensitive operational data. Restricting access to these systems reduces the risk of accidental changes and limits the impact of compromised user accounts.

Scenario: Daily office work

Permissions:

- Login to office systems
- Access to email and collaboration tools
- Read access to internal policies

3.2 Role: Developer

Developers at PointPoint GmbH are responsible for designing, implementing, and maintaining cloud-based applications. In a typical development scenario, a developer needs access to source code repositories, issue tracking systems, and continuous integration pipelines. The developer must also be able to deploy applications to development and testing environments in order to validate functionality.

Access to production environments and live customer data is explicitly excluded from this role. This ensures that developers cannot directly affect production systems and that all changes must go through controlled release and approval processes.

Scenario: Development of a cloud application

Permissions:

- Access to Git repositories
- Deployment to development and test environments
- No access to production data

3.3 Role: Security Analyst

Security analysts work in the Security Operations Center and are responsible for detecting, analyzing, and responding to security incidents. In an incident response scenario, the analyst requires access to SIEM systems, log data, and monitoring dashboards in order to investigate suspicious activity.

The analyst may also need read-only access to system configurations to understand how systems are set up. However, the role does not include permissions to modify production systems, as such changes must be performed by system administrators following established procedures.

Scenario: Analysis of a security incident

Permissions:

- Access to SIEM systems and log data
- Read access to system configurations
- No modification rights on production systems

3.4 Role: System Administrator

System administrators are responsible for operating and maintaining the IT infrastructure of PointPoint GmbH. In a maintenance scenario, administrators require extensive privileges, including administrative access to servers, networks, and cloud platforms. They are also responsible for managing user accounts and roles within the IAM system.

Despite their broad technical access, system administrators do not have permissions to access HR systems or financial applications. This restriction ensures separation of duties and prevents misuse of sensitive personal or financial data.

Scenario: Maintenance of cloud infrastructure

Permissions:

- Administrative access to servers and networks
- User and role management (IAM)
- No access to HR or financial systems

3.5 Role: Management

Management personnel are responsible for strategic oversight, decision-making, and compliance supervision. In a reporting and compliance scenario, managers require access to aggregated reports, dashboards, and key performance indicators related to security, risk, and operations.

They also require read-only access to audit reports and risk documentation in order to fulfill their governance responsibilities. Management does not require technical administrative access, as their role focuses on oversight rather than operational execution.

Scenario: Compliance and reporting activities

Permissions:

- Access to reports and KPIs
- Read access to audit and risk documentation
- No technical administrative privileges