# IT Audit Kook8

## General Observations

* The documentation of the ISMS is well-structured, but some documents are outdated (last updated in 2021).
* There are clear responsibilities within the IT department, but no written escalation strategy.
* Employees show a basic understanding of data protection policies, but two departments were not included in the training list.

## ISO 27001 Specific Observations

A.10 Cryptographic Controls:

* It was found that full encryption is not used on mobile devices.
* A secure key exchange procedure is implemented but not fully documented.

A.12 Operational Security:

* Server software on critical systems is partially outdated (e.g., Windows Server 2012).
* Regular backups are performed, but there are no disaster recovery tests.

A.13 Communication and Security:

* Firewall rules have not been reviewed for 6 months.
* There are no logs for external connections.

## GDPR Specific Observations

Article 5: Principles of Processing Personal Data:

* Data processing agreements with two external service providers are incomplete.
* Old data (before 2018) is not regularly checked for deletion.

Article 25: Data Protection by Design and by Default:

* Data protection impact assessments have not been conducted for new projects since 2023.
* There is no process for regularly reviewing compliance with the "Privacy by Design" approach.

Article 32: Security of Processing:

* There is no two-factor authentication for remote access to sensitive systems.
* Access to personal data is not sufficiently logged.

## Risks Identified On-Site

High Risks:

* Employees use private devices for work without central management.
* Critical systems lack a contingency plan for failure.

Medium Risks:

* Backup process documented, but recovery not tested.
* Data protection training does not cover all departments.

Low Risks:

* Outdated signage for security zones in the server room.
* No regular tests of access controls.

## Questions and Discussions with the Team

#### Questions:

* "What measures are currently planned to implement encryption on mobile devices?"
* "When was the last backup recovery test conducted?"
* "Is there a clear contact person for data protection impact assessments?"

#### Discussions:

* Possibility of introducing a central solution for device management.
* Establishing an emergency team for IT security incidents.
* Developing a regular audit plan for internal reviews.