Addressing Information Security Concerns

01 **Confidentiality:** Lack of access controls and physical security could lead to unauthorized data access.

02 **Integrity:** Inadequate backups and outdated risk analysis could compromise data integrity.

03 **Availability:** Physical security gaps and poor incident response could impact system availability.

Cybersecurity Shortcomings at Boldi AG

- **Content:** Inconsistent File Formats: Paper and cloud-based files are inconsistent, making data analysis and risk assessment difficult.

- **Uncontrolled File Access:** No controls over who can access files, increasing the risk of unauthorized data modification or theft.

- These shortcomings make it difficult to track data changes, identify security threats, and respond effectively to incidents, increasing Boldi AG's vulnerability to cyberattacks.

Quantitative vs. Qualitative Risk Assessments

- Qualitative risk assessment is subjective and relies on expert opinion to assess impact and likelihood.
- Quantitative risk assessment is objective and uses numerical data to calculate risk probability and financial impact.
- Quantitative assessments require historical data and are better suited for well-understood risks.
- Qualitative assessments are more adaptable to new or evolving risks where data is limited.
- For information security, a qualitative assessment is often more appropriate due to the evolving nature of threats.

Qualitative Risk Assessment for Boldi AG

- Asset Identification: Identify critical data, systems, and processes within Boldi AG.
- Threat Assessment: Evaluate potential threats targeting Boldi AG's assets (e.g., unauthorized access, data breaches).
- Vulnerability Assessment: Analyze weaknesses in Boldi AG's systems that could be exploited by identified threats.
- Risk Likelihood and Impact: Assess the probability of each threat occurring and its potential impact on Boldi AG.
- Prioritization: Rank identified risks based on their likelihood and potential impact.