Information Risk Assessment at Boldi AG – Steps 2 & 3

Addressing Security Concerns & Choosing a Risk Assessment Method

Agenda

1. **Overview of Current Concerns** (Step 2)
2. **CIA Analysis (Confidentiality, Integrity, Availability)**
3. **Risk Assessment Approaches** (Step 3)
    - Quantitative vs. Qualitative
4. **Recommendations & Next Steps**

Current Concerns at Boldi AG

Paper Files & Cloud Systems

Inconsistent file formats

Hard to consolidate or compare data for analysis

Access Control Issues

No clear restrictions on who can access these files

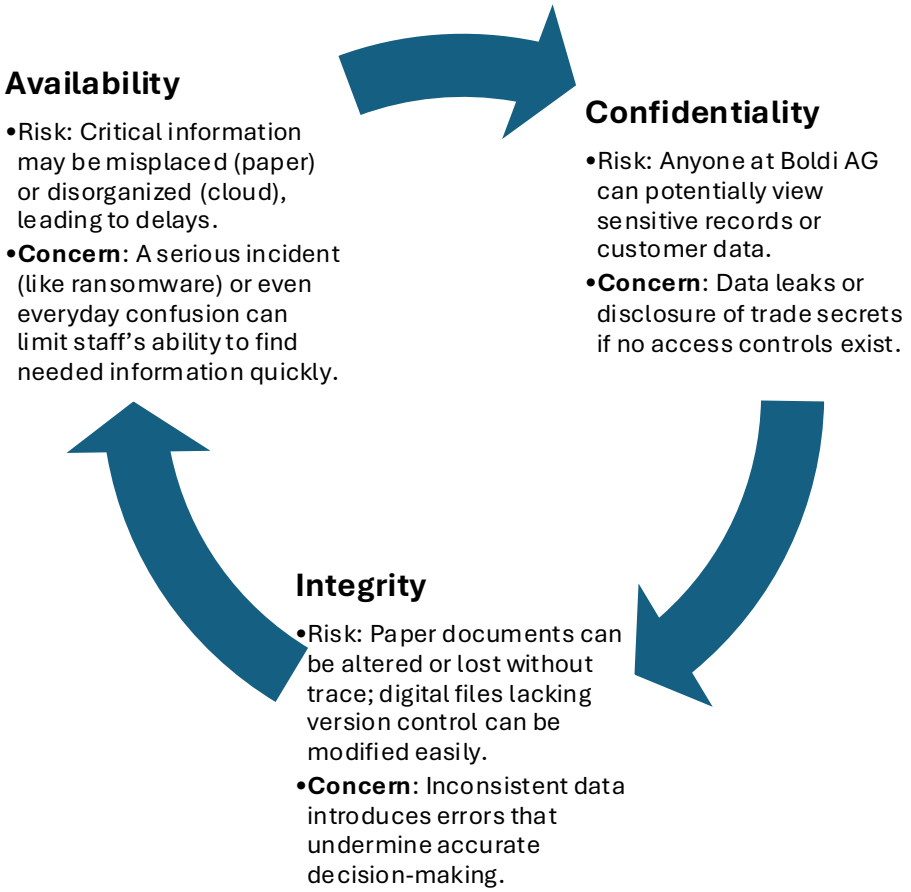
Potential for unauthorized viewing, editing, or sharing

Impact on Risk Assessment

Data scattered across multiple storage methods

Heightened complexity in establishing a complete risk profile

CIA Analysis – Why This Matters



Choosing the Right Risk Assessment Method

Quantitative Risk Assessment

Definition: Uses numerical values (e.g., dollars, time, probabilities) to estimate potential losses.

Reliance: Accurate historical data, reliable statistics, and clear cost metrics.

Challenge: Often difficult in information security due to lack of consistent data on frequency or impact of cyber incidents.

Qualitative Risk Assessment

Definition: Uses expert judgment, categories (e.g., High/Medium/Low), and scenario analysis to gauge risk severity.

Advantages: Faster to implement, can handle incomplete data, widely used in InfoSec.

Drawbacks: Less precise in financial terms and can be subjective.

Which Method for Boldi AG?

Considering Boldi AG's Situation:

- **Data Inconsistency**: Hard to gather accurate numbers for a purely quantitative model.
- **Time Constraints**: The company needs actionable insights promptly given the recent ransomware scare in their industry.
- **Organizational Culture**: Likely more receptive to a structured, scenario-based approach with clear, easily communicated priorities.

Conclusion:

- A **Qualitative Risk Assessment** is probably **more adapted** for this initial evaluation at Boldi AG.
- Over time, if consistent data is collected, **quantitative elements** can be introduced for more precise financial modeling.

Recommendations & Next Steps

Organize & Standardize Data

Digitize or catalog paper files; unify cloud document formats.

Implement clear access control policies.

Initiate a Qualitative Risk Assessment

Interview key stakeholders for High/Medium/Low risk ratings.

Map out critical assets, threats, and vulnerabilities.

Develop a Long-Term Improvement Plan

Gradually add quantitative metrics as data matures.

Introduce formal change management processes to maintain data integrity and availability.

Questions?

Contact: Gabriel Reis Santos

Thank You for reviewing these steps to strengthen Boldi AG’s information security posture.