

Shrimambary Ujaleet shalkh -2419481

(500 W)

Introduction (50 words)

Ans: Key Principle of data security and how they apply to this scenario.

Accountability & Responsibility weakness in data classification, access control, risk management which is applied by suggesting data stewards, governance committees & it aligns with GDPR

Ans: Steps to ensure GDPR and other regulations. Europe triggers GDPR requirements.

Ans: risk management and data classification.

- poor data classification and access control.
- it helps identify the data and financial risks.

Ans: discovery tools, usage policies, risk assessments & GDPR compliant - control. which are regulatory for compliance and security.

Ans: security training, simulations, executive support, security championship.

these all are proven practises from COBIT, ISO, 27001 and industry experience. leadership should be an example.

Conclusion (50 words)

CISO of a mid-sized financial services and company expanding into the European market, establishing a robust data security governance and compliance framework is critical. The internal audit has highlighted key vulnerabilities - specifically in data-classification access control, and incident response - alongside unvetted a third-party cloud service.

The key principal of data security governance and their applications are accountability and responsibility release their clear ownership for data assets which is assign stewards in each department responsible for data integrity and protection. Transparency is Documented publish data and handling policies. Ensure that subjects understand how data is used in line with GDPR emphasis on lawful Processing.

Risk management has been implemented continues processes to evaluate threats to data confidentiality integrity and availability.

Compliance and monitoring is regularly audit data handling and process against GDPR and other application standards.

There are some steps to ensure GDPR and regulatory compliances :

Data inventory and mapping conduct a data protection impact Assessment to map all personal data flows across the organization. Identify where data is stored, processed or transferred - including by third-party vendors.

lawful processing and consent are review and update Privacy notices and consent mechanism. Ensure that data collection align with GDPR's lawful bases.

Data subject rights are implemented mechanism to support data subject rights such as access, rectification, erasure and portability.

Security measures and Breach Response plan.

There are few risk Assessment and data classification. an effective data protection strategy begins with knowing the data what you have and understanding the risks associated with.

Risk Assessment and Data classification and access control. Here the shadow IT - unauthorized use of cloud services poses significant compliances and security risks to manage this; policy enforcement, vendor risks management, Discovery monitoring.

Further, we have to build a culture of security awareness and accountability. There is some technical measures along with insufficient without a strong security culture. security awareness training, phishing simulations, leadership and ~~phishing~~ Accountability, incident reporting culture and metrics and KPIs.

To conclude, in European market while maintaining data security and regularly compliances, our company must implement a multi-faced data security governance. By fostering a security-aware culture and enforcing strong technical and administrative controls, we have build trust with clients and stock holders in our new market.