

We will follow models like the NIST Risk Management Framework, which helps identify, assess, and reduce security risks. Data classification is just as important. By labelling data, we know how sensitive it is and how to protect it. To implement risk assessment first we have to define the scope, then we will identify information assets, after that we will identify threats and vulnerabilities. After we apply risk controls and monitor, review and update the risk assessment.

The shadow IT lead to serious risks, including data loss or legal issues. To manage this, we need clear rules for how new tools are approved. We will also use tools like Cloud Access Security Brokers (CASBs) to detect and control unapproved apps. For third-party vendors, we'll require them to follow strict security standards like ISO 27001 and SOC 2 and sign agreements that define their security responsibilities.

Technology alone can't protect data - people must be involved too. We'll train all staff regularly on topics like phishing, safe browsing, and data handling. Campaigns, posters, and short videos can help keep security in everyone's mind. Managers should lead by example, showing that security is important. We'll also reward good behaviour and make it easy for staff to report suspicious activity.

As a Chief Information Security Officer (CISO) of a mid-sized financial services company expanding into Europe, protecting customer data and meeting legal requirements like the general Data Protection Regulation (GDPR) is a top priority. A recent internal audit showed weakness in how we classify data, control access, and respond to incidents.

The main principles of Data Security Governance include accountability, transparency, and continuous improvement. Everyone from leadership to staff - must understand their role in protecting data. Using frameworks like ISO 27001 or COBIT, we can set up a structure that links our business goals with security controls.

Accountability
Clear Policies and Procedures
Transparency
Risk-Based Approach

To meet GDPR requirements, we need to know what personal data we collect, why we collect it, where it's stored, and who has access to it. A data protection impact assessment will help us identify risks. We should appoint a Data Protection Officer (DPO) to manage compliance. We'll make sure data is collected legally, stored securely, and only kept for as long as needed.