Security Protocols for Data Migration

Objective:

1. Implement SFTP servers
2. Implement strict authentication policies for secure data transfers during migration

Steps taken to reduce the risk of data exposure during the migration:

Steps	Actions	Outcome
Define Security and Compliance Requirements	Collaborate with the InfoSec and Compliance teams to document requirements for data encryption, access controls, and auditing.	Create formal security requirements document that will drive the configuration and policies for the SFTP solution.
	Identify sensitive data types (e.g., CSV files, HR data extracts) and define the level of protection needed (e.g., TLS encryption, key-based authentication)	
Define and Document Strict Authentication Policies	Establish authentication methods, favoring key-based authentication over passwords, and consider implementing two-factor authentication (2FA) where possible.	Create a clear authentication policy document that specifies how users gain access and how their activities are monitored.
	Develop policies for account creation, periodic password/key rotation, access review, and session timeouts.	
Deploy the SFTP Server Environment	Provision for a dedicated server in a secure network segment in your organization's infrastructure.	A hardened SFTP server ready for secure file transfers
	Integrate the SFTP server with your organization's authentication infrastructure (e.g., Active Directory or LDAP).	
Implement Monitoring, Logging, and Auditing	Configure logging to capture all access attempts, file transfers, and authentication events.	Continuous monitoring and auditing to ensure compliance and detect anomalies immediately.
	Integrate these logs with the existing Security Information and Event Management (SIEM) system for real-time monitoring.	

	Set up alerts for suspicious activity or repeated failed login attempts.	
Conduct Testing and Pilot Transfers	Develop Standard Operating Procedures (SOPs) for file transfers, including instructions on generating and managing keys.	A fully operational and well-understood SFTP solution with trained personnel ensuring secure and efficient file transfers.
	Train the relevant teams (migration, IT, and end users) on how to securely use the SFTP server.	
	Schedule a go-live date and communicate the plan and expected impact to all stakeholders.	
Post-Implementation Review and Continuous Improvement	Schedule periodic reviews of access logs, update authentication policies as needed, and conduct regular audits.	Ongoing assurance that the SFTP environment remains secure and compliant throughout the migration.
	Adjust configurations based on feedback and emerging threats.	

Technical Teams Involved

- **IT Security Team:** To define requirements, conduct risk assessments, and perform security audits.
- **Systems Administrators/DevOps Engineers:** To deploy, configure, and maintain the SFTP server.
- **Network Engineers:** To ensure that the SFTP server is deployed in the correct network segment and configured with necessary firewall rules.
- **Integration Specialists:** To link the SFTP server with existing authentication systems (Active Directory/LDAP).