DATA SECURITY AUDIT CHECKLIST

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken

A Data Security Audit is a comprehensive review of an organization's data security practices. It helps to identify vulnerabilities, ensure compliance with regulations, and protect against data breaches. This document outlines a detailed Data Security Audit Checklist to guide you through the evaluation of your data security measures.

1. Data Encryption

Objective: Ensure that data is protected from unauthorized access and breaches through encryption.

Audit Item	Description	Notes/Findings
Encryption at Rest	Verify that data at rest is encrypted using industry-standard methods	
Encryption in Transit	Confirm that data in transit is encrypted (e.g., TLS/SSL)	
Key Management	Assess the processes for managing encryption keys	
Backup Data Encryption	Ensure backup data is also encrypted	

2. Access Controls

Objective: Ensure that only authorized individuals have access to sensitive data.

Audit Item	Description	Notes/Findings
Access Control Policies	Review policies controlling access to data	
Least Privilege	Verify that access is granted based on the principle of least privilege	
Multi-Factor Authentication (MFA)	Check if MFA is required for access to sensitive data	
Access Reviews	Confirm regular reviews of user access to sensitive data	

3. Data Classification

Objective: Ensure that data is properly classified and handled according to its sensitivity.

Audit Item	Description	Notes/Findings
Data Classification Policies	Ensure that data is classified based on sensitivity and criticality	
Labeling	Check if data is properly labeled according to its classification	
Handling Procedures	Review procedures for handling different classes of data	