

# Detailed Compliance Assessment Results

## Project Information

Project Name	ABC Financial Application
Assessment Date	2024-06-15
Assessor	John Doe
Standards Assessed	ISO 27001, GDPR, PCI DSS

## Summary of Findings

Area	Status	Details
Access Control	Partially Compliant	User access reviews are being conducted but not at required intervals.
Data Protection	Compliant	Encryption in place for data at rest and transit.
Incident Response	Not Compliant	No formal incident response policy established.
Third Party Management	Compliant	Due diligence completed for all external vendors.

## Detailed Assessment Results

### 1. Access Control

- Strengths: Role-based access enforced, multi-factor authentication implemented.
- Weaknesses: Scheduled access review frequency not aligned with policy.
- Recommendation: Implement quarterly access reviews and document procedures.

### 2. Data Protection

- Strengths: AES-256 encryption for sensitive data, regular backups performed.
- Weaknesses: Limited employee awareness training on data handling practices.
- Recommendation: Conduct annual data protection training for all staff.

### 3. Incident Response

- Strengths: Informal workflow observed for reporting incidents.
- Weaknesses: Lack of formal incident response plan and testing.
- Recommendation: Develop and test an incident response plan by Q3 2024.

### 4. Third Party Management

- Strengths: Comprehensive vendor risk assessments documented.
- Weaknesses: Contracts do not specify data protection obligations.
- Recommendation: Update contracts to clarify security and privacy requirements.

## Important Notes

- Assessment results may vary over time as controls and processes evolve.
- This document is intended for internal use and should be kept confidential.
- Recommendations provided are for improvement and risk mitigation purposes.
- Periodic reassessment is advised to ensure ongoing compliance.