Cybersecurity Diagnostic Report

Total Score: 255/500 (51.0%)

Recommendations:

Fair. Focus on strengthening key areas like access control and incident response.

Category Scores:

Access Control: 55/80

Data Protection: 20/70

Employee Awareness and Training: 50/70

Governance and Policies: 35/70

Incident Response and Recovery: 25/70

Network Security: 40/90

Third-Party Risk Management: 30/50

Detailed Answers:

Q1: In Progress

Q2: No

Q3: No

Q4: No

Q5: Yes, sufficient budget

Q6: Yes

Q7: Yes

Q8: Yes, but not continuous

Q9: No

Q10: No

Q11: Not Sure

Q12: Yes, for some systems

Q13: No

Q14: Yes, strictly enforced

Q15: Yes, real-time monitoring

Q16: No

Q17: No

Q18: No

Q19: No

Q20: Yes, annually or more frequently

Q21: Yes, but less frequently

Q22: Yes, enforced through contracts

Q23: No

Q24: No

Q25: No

Q26: Partially implemented

Q27: No

Q28: Yes, with MFA enabled

Q29: No

Q30: Yes, with regular audits

Q31: Yes, but without security measures

Q32: Yes, within the first month

Q33: Yes, but less frequently

Q34: Yes, but voluntary

Q35: Yes, regularly

Q36: Yes, partially automated

Q37: No

Q38: No, but considered

Q39: Yes, strictly enforced

Q40: Yes, annually or more frequently

Q41: Yes, strictly enforced

Q42: Partially implemented

Q43: No

Q44: Yes, annually

Q45: Yes, at least annually

Q46: Yes, annually or more frequently

Q47: Yes, with regular compliance checks

Q48: Yes, but infrequently

Q49: Yes, but only once during adoption

Q50: Yes, integrated with response tools