Cybersecurity Diagnostic Report

Overall Score:

260/500 (52.0%)

Category Breakdown:

Access Control: 50/70 (71.43%)

Asset Management: 5/10 (50.0%)

Business Continuity: 0/10 (0.0%)

Compliance: 5/10 (50.0%)

Data Protection: 35/70 (50.0%)

Employee Awareness and Training: 15/70 (21.43%)

Governance and Policies: 45/70 (64.29%)

Incident Response: 10/10 (100.0%)

Incident Response and Recovery: 30/40 (75.0%)

Network Security: 35/90 (38.89%)

Risk Management: 5/10 (50.0%)

Security Awareness: 0/10 (0.0%)

Third-Party Risk Management: 25/30 (83.33%)

Recommendations:

Focus on strengthening key areas: Network Security, Business Continuity, Security Awareness, Employee Awareness and Training.

Suggested Tools for Improvement:

Employee Awareness and Training: KnowBe4, Infosec IQ

Network Security: Snort, Wireshark

Answers Summary:

Q1: No

Q2: In Progress

Q3: In Progress

Q4: In Progress

Q5: In Progress

Q6: Yes

Q7: No

Q8: No

Q9: No

Q10: In Progress

Q11: No

Q12: No

Q13: Yes, strictly enforced

Q14: Yes, annually or more frequently

Q15: Partially enforced

Q16: Yes, annually or more frequently

Q17: Yes, strictly enforced

Q18: Yes, enforced through contracts

Q19: Not Sure

Q20: Yes, with MFA enabled

Q21: Partially

Q22: Yes, but limited budget

Q23: No

Q24: No

Q25: Yes, partially automated

Q26: Yes, but not real-time

Q27: No

Q28: Yes, but infrequently

Q29: Yes, always

Q30: Yes

Q31: Yes, with offsite storage

Q32: No

Q33: Yes, but infrequently

Q34: No

Q35: Yes, but informal

Q36: No

Q37: Yes, but less frequently

Q38: No

Q39: Yes, within 24 hours

Q40: Yes, but without detailed analysis

Q41: Yes

Q42: Yes, with regular compliance checks

Q43: Yes, annually or more frequently

Q44: Yes, but infrequent

Q45: Yes, strictly enforced

Q46: No, but considered

Q47: Yes, strictly enforced

Q48: No

Q49: Yes, for all systems

Q50: No