Cybersecurity Diagnostic Report

Report Date: 2025

network
cccentro

Category Breakdown

Access Control: 30/70 (42.86%)

Asset Management: 0/10 (0.0%)

Business Continuity: 10/10 (100.0%)

Compliance: 5/10 (50.0%)

Data Protection: 20/70 (28.57%)

Employee Awareness and Training: 30/70 (42.86%)

Governance and Policies: 45/70 (64.29%)

Incident Response: 10/10 (100.0%)

Incident Response and Recovery: 15/40 (37.5%)

Network Security: 50/90 (55.56%)

Risk Management: 5/10 (50.0%)

Security Awareness: 0/10 (0.0%)

Third-Party Risk Management: 10/30 (33.33%)

Recommendations

Governance and Policies

- Complete the development of your cybersecurity policy and seek expert validation.

- Maintain a strong governance framework and review policies periodically.

- Maintain a strong governance framework and review policies periodically.

- Develop formal security policies and ensure organization-wide enforcement.

- Maintain a strong governance framework and review policies periodically.

- Maintain a strong governance framework and review policies periodically.

- Develop formal security policies and ensure organization-wide enforcement.

Risk Management

- Ensure the ongoing risk assessment covers all critical business areas.

Asset Management

- Implement the necessary security measures to mitigate potential vulnerabilities.

Access Control

- Finalize the implementation of security measures and conduct validation tests.

- Continue enforcing strict access controls and review policies regularly.

- Enhance access control measures by implementing multi-factor authentication.

- Implement strict access control mechanisms to prevent unauthorized access.

- Enhance access control measures by implementing multi-factor authentication.

- Enhance access control measures by implementing multi-factor authentication.

- Implement strict access control mechanisms to prevent unauthorized access.

Network Security

- Periodically update and test the incident response plan to address emerging threats.
- Regularly review and update network security configurations and segment networks appropriately.
- Strengthen network security by adding additional monitoring and segmentation controls.
- Implement firewall, IDS/IPS, and network segmentation to improve security.
- Regularly review and update network security configurations and segment networks appropriately.
- Implement firewall, IDS/IPS, and network segmentation to improve security.
- Strengthen network security by adding additional monitoring and segmentation controls.
- Strengthen network security by adding additional monitoring and segmentation controls.
- Strengthen network security by adding additional monitoring and segmentation controls.

Incident Response

- Maintain adherence to best practices and continuously improve security controls.

Business Continuity

- Continue with regular cybersecurity training and introduce phishing simulations.

Security Awareness

- Implement a robust backup strategy to prevent data loss in case of incidents.

Data Protection

- Finalize the implementation of security measures and conduct validation tests.
- Implement encryption and data loss prevention tools to safeguard sensitive data.
- Expand encryption and data protection measures to cover all critical information.

- Implement encryption and data loss prevention tools to safeguard sensitive data.
- Implement encryption and data loss prevention tools to safeguard sensitive data.
- Implement encryption and data loss prevention tools to safeguard sensitive data.
- Ensure encryption standards remain updated and review data protection policies regularly.

Compliance

- Complete the development of your cybersecurity policy and seek expert validation.

Third-Party Risk Management

- Strengthen vendor security assessments and require compliance documentation.
- Strengthen vendor security assessments and require compliance documentation.
- Implement a vendor risk management program to evaluate third-party security.

Incident Response and Recovery

- Expand and formalize the incident response plan with clear response actions.
- Develop and implement an incident response plan to minimize downtime.
- Expand and formalize the incident response plan with clear response actions.
- Expand and formalize the incident response plan with clear response actions.

Employee Awareness and Training

- Develop a mandatory security training program to educate employees on risks.
- Develop a mandatory security training program to educate employees on risks.
- Continue regular security awareness training and phishing simulations.
- Increase training frequency and introduce interactive security awareness programs.
- Continue regular security awareness training and phishing simulations.
- Increase training frequency and introduce interactive security awareness programs.

- Develop a mandatory security training program to educate employees on risks.

Suggested Tools for Improvement

Access Control: Okta, Microsoft Entra ID (Azure AD)

Asset Management:

Data Protection: VeraCrypt, BitLocker

Employee Awareness and Training: KnowBe4, Infosec IQ

Incident Response and Recovery: Splunk SOAR, IBM Resilient

Security Awareness:

Third-Party Risk Management: OneTrust, Prevalent