ChecklistGuro

Insurance Cyber Risk Assessment Checklist

Data Inventory & Classification

Identify and categorize sensitive data assets, including personally identifiable information (PII), financial data, and confidential business information.

Description of Data Type (e.g., PII, Financial, Medical)

Write something...

Data Sensitivity Level (Confidential, Internal, Public)

- [ ] Confidential
- [ ] Internal
- [ ] Public

Approximate Record Count

Enter a number...

Data Retention Policy Applied

- [ ] Yes
- [ ] No

Data Location (Specific System or Database)

Write something...

Data Categories (Select all that apply)

- [ ] Name
- [ ] Address
- [ ] Financial Information
- [ ] Health Information
- [ ] Policy Details

Last Data Classification Review Date

Enter date...

Network Security Controls

Evaluate firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and other network security measures.

Firewall Rule Count

Enter a number...

Firewall Vendor

- [ ] Cisco
- [ ] Palo Alto
- [ ] Fortinet
- [ ] SonicWall
- [ ] Other

Enabled Security Features (IDS/IPS)

- [ ] Signature-Based Detection
- [ ] Anomaly Detection
- [ ] Protocol Filtering
- [ ] Application Control

Last Intrusion Detection System (IDS) Signature Update

Enter date...

VPN Type

- [ ] IPsec
- [ ] SSL VPN
- [ ] Other

Number of VPN Connections

Enter a number...

Endpoint Security

Assess antivirus/anti-malware protection, device encryption, and mobile device management (MDM).

Antivirus Software Installed?

- [ ] Yes
- [ ] No
- [ ] N/A

Last Antivirus Scan Date (Days)

Enter a number...

Endpoint Detection & Response (EDR) Deployed?

- [ ] Yes
- [ ] No
- [ ] N/A

Last Patch Management Date

Enter date...

Full Disk Encryption Enabled?

- [ ] Yes
- [ ] No
- [ ] N/A

Endpoint Security Controls Implemented (Select all that apply)

- [ ] Firewall
- [ ] Intrusion Prevention
- [ ] Data Loss Prevention
- [ ] Application Whitelisting

Application Security

Review secure coding practices, vulnerability scanning, and penetration testing of applications.

Secure Coding Practices Implemented?

- [ ] Yes
- [ ] No
- [ ] Partially Implemented

Last Vulnerability Scan Score (0-100, 100 being best)

Enter a number...

Which Vulnerability Scanning Tools are Used?

- [ ] OWASP ZAP
- [ ] Nessus
- [ ] Qualys
- [ ] Burp Suite
- [ ] None

Date of Last Penetration Test

Enter date...

Is a Web Application Firewall (WAF) in Place?

- [ ] Yes
- [ ] No
- [ ] Planned

Describe any identified vulnerabilities and remediation efforts.

Write something...

Third-Party Risk Management

Evaluate the cybersecurity posture of vendors and service providers who handle insurance data.

Vendor Risk Tier Assessment

- [ ] High
- [ ] Medium
- [ ] Low

Last Vendor Risk Assessment Date

Enter date...

Security Standards/Frameworks Used by Vendor

- [ ] SOC 2
- [ ] ISO 27001
- [ ] PCI DSS
- [ ] NIST CSF

Number of Active Users (Vendor)

Enter a number...

Vendor Security Questionnaire Responses

Upload File

Vendor Audit Frequency

- [ ] Annual
- [ ] Bi-Annual
- [ ] Upon Request

Incident Response Planning

Assess the readiness of incident response plans, including data breach notification procedures.

Incident Response Plan Document Location

Write something...

Primary Contact Role (Incident Commander)

- [ ] IT Security Manager
- [ ] Claims Director
- [ ] Legal Counsel
- [ ] Designated Incident Commander

Secondary Contact Role (Communications)

- [ ] Public Relations
- [ ] Legal Counsel
- [ ] Marketing Manager
- [ ] Designated Communications Officer

Last Incident Response Plan Review Date

Enter date...

Estimated Time to Contain Incident (Hours)

Enter a number...

Stakeholders to Notify (Check all that apply)

- [ ] Executive Management
- [ ] Legal Counsel
- [ ] Regulatory Agencies
- [ ] Law Enforcement
- [ ] Cybersecurity Insurance Provider

Briefly Describe Initial Containment Steps

Write something...

Employee Training & Awareness

Verify that employees receive regular cybersecurity training and are aware of phishing scams and other threats.

Most Recent Training Completion Date

- [ ] Within Last 3 Months
- [ ] 3-6 Months Ago
- [ ] 6-12 Months Ago
- [ ] Over 12 Months Ago

Training Topics Covered (Select All That Apply)

- [ ] Phishing Awareness
- [ ] Data Privacy
- [ ] Secure Password Practices
- [ ] Social Engineering
- [ ] Incident Reporting Procedures

Average Score on Cybersecurity Quiz

Enter a number...

Feedback on Training Program

Write something...

Date of Next Scheduled Training Session

Enter date...

Data Backup & Recovery

Check the effectiveness of data backup and recovery procedures to ensure business continuity.

Frequency of Full Backups (Days)

Enter a number...

Frequency of Incremental/Differential Backups (Hours)

Enter a number...

Backup Storage Location (Onsite/Offsite/Cloud)

- [ ] Onsite
- [ ] Offsite
- [ ] Cloud

Last Successful Full Backup Date

Enter date...

Description of Backup Software Used

Write something...

Retention Policy (How long backups are kept)

- [ ] 30 Days
- [ ] 60 Days
- [ ] 90 Days
- [ ] Custom (Specify in Long Text)

Last Backup Verification Report

Upload File

Cloud Security

Review security configurations and controls for cloud-based infrastructure and applications.

Cloud Provider Security Certifications

- [ ] SOC 2 Type II
- [ ] ISO 27001
- [ ] PCI DSS
- [ ] HIPAA
- [ ] None

Encryption at Rest Strength (bits)

Enter a number...

Multi-Factor Authentication (MFA) Status

- [ ] Enabled for all users
- [ ] Enabled for privileged accounts only
- [ ] Disabled

Cloud Security Group Configuration Details

Write something...

Last Cloud Security Audit Date

Enter date...

Cloud Security Tools Deployed

- [ ] Vulnerability Scanning
- [ ] Intrusion Detection/Prevention
- [ ] Data Loss Prevention (DLP)
- [ ] Security Information and Event Management (SIEM)

Compliance & Legal Requirements

Ensure adherence to relevant regulations, such as GDPR, CCPA, and state-specific data breach laws.

Applicable Regulations (e.g., GDPR, CCPA, State Laws)

- [ ] GDPR
- [ ] CCPA
- [ ] HIPAA
- [ ] State Data Breach Laws (Specify)
- [ ] Other (Specify in Long Text)

Specific Legal Requirements Addressed

Write something...

Last Compliance Assessment Date

Enter date...

Number of Data Subject Access Requests (DSARs) Received in Last Year

Enter a number...

Data Breach Notification Threshold (Specify Legal Requirement)

- [ ] State Specific
- [ ] Federal Requirement
- [ ] Company Policy

Documentation of Compliance Efforts

Write something...