Cybersecurity Audit Prep Checklist

Use this checklist to prepare for your security audits, privacy assessments and risk reviews, ensuring that your organization's processes remain in compliance with NIST CSF, ISO 27001:2022 & applicable data protection laws.

1. People

- ❑ Security Awareness Training: Ensure all employees have completed security awareness training, covering topics like phishing, password security, and data protection.
- ❑ Role-Based Access Control (RBAC): Verify that access to systems and data is granted based on roles, ensuring that employees have the minimum necessary access.
- ❑ Background Checks: Conduct thorough background checks for employees in sensitive positions, in compliance with company policy and legal requirements.
- ❑ Incident Response Team: Ensure that an incident response team is established, trained, and familiar with the organization's incident response plan.
- ❑ Third-Party Vendor Management: Verify that third-party vendors have undergone security training and adhere to the same security standards as internal employees.

2. Process

- ❑ Policy and Procedure Documentation: Ensure all security policies and procedures are documented, up to date, and accessible to relevant personnel.
- ❑ Regular Audits and Assessments: Conduct regular internal audits and risk assessments to identify and mitigate vulnerabilities.
- ❑ Incident Response Plan Testing: Regularly test and update the incident response plan, ensuring it includes communication strategies, roles, and responsibilities.
- ❑ Data Protection and Privacy Policies: Ensure compliance with data protection laws and regulations, such as GDPR, and maintain up-to-date privacy policies.
- ❑ Change Management Process: Implement a change management process to control and document changes to the IT environment, including hardware and software updates.

3. Technology

- ❑ Network Security: Ensure the network is segmented and protected by firewalls, intrusion detection/prevention systems (IDS/IPS), and secure configurations.

- ❑ Encryption: Verify that sensitive data is encrypted both at rest and in transit using strong encryption standards.
- ❑ Patch Management: Ensure that all systems and applications are regularly updated with the latest security patches.
- ❑ Access Control: Implement multi-factor authentication (MFA) for all critical systems and ensure access controls are in place.
- ❑ Backup and Recovery: Verify that data backup procedures are in place, tested regularly, and that backups are stored securely offsite.

Shareable Recommendations

- Continuous Monitoring: Implement continuous monitoring tools to detect and respond to security incidents in real time.
- Compliance with Standards: Ensure all practices align with NIST CSF, PCI DSS, and ISO 27001 requirements.
- Penetration Testing: Conduct regular penetration tests to identify and fix security weaknesses before they can be exploited.
- Vulnerability Management: Implement a robust vulnerability management program to regularly scan, assess, and remediate vulnerabilities.
- Logging and Monitoring: Ensure comprehensive logging of all critical systems and regular review of logs for suspicious activity.
- Physical Security: Verify that physical access controls are in place to protect data centers and sensitive information.

This checklist will help your organization prepare for a cybersecurity audit and ensure compliance with NIST CSF, PCI DSS, and ISO 27001 standards.

Let's help you prepare for your next security audit:
https://www.securityaudits.ca

DATARISK CANADA