Security Verification Checklist

Use this checklist to validate your cybersecurity on a recurring basis, with network and application scanning, vulnerability management and continuous reviews of your key processes in compliance with NIST CSF, ISO 27001:2022 & applicable data protection legislation.

1. Network Security

- ❑ Network Segmentation: Verify that network segmentation is in place to isolate critical systems and limit the spread of potential breaches.
- ❑ Firewall Configuration: Ensure that firewalls are properly configured to block unauthorized access while allowing legitimate traffic.
- ❑ Intrusion Detection and Prevention Systems (IDPS): Confirm that IDPS are installed and regularly updated to detect and prevent malicious activities.
- ❑ Encryption: Check that data in transit is encrypted using secure protocols such as TLS/SSL.
- ❑ Access Controls: Ensure that network access is restricted to authorized users and devices through the use of strong authentication mechanisms.

2. Application Security

- ❑ Code Review and Testing: Conduct regular code reviews and application security testing to identify and remediate vulnerabilities.
- ❑ Input Validation: Verify that all applications implement proper input validation to prevent common attacks such as SQL injection and cross-site scripting (XSS).
- ❑ Secure Development Practices: Ensure that developers follow secure coding practices and guidelines.
- ❑ Application Firewalls: Confirm that web application firewalls (WAF) are in place to protect against web-based attacks.
- ❑ Patch Management: Check that all applications are up-to-date with the latest security patches and updates.

3. Vulnerability Management Programs

- ❑ Regular Scanning: Conduct regular vulnerability scans to identify and assess vulnerabilities in systems and applications.

- ❑ Prioritization: Verify that identified vulnerabilities are prioritized based on risk and potential impact.
- ❑ Remediation: Ensure that a process is in place to remediate vulnerabilities in a timely manner.
- ❑ Verification: Confirm that remediation efforts are verified through subsequent scanning and testing.

Other Recommendations to add to Your Cybersecurity Verification Checklist

- Regular Patching: Ensure all software is regularly updated and patched to protect against known vulnerabilities.
- Password Security: Enforce strong password policies, including the use of complex passwords and regular password changes.
- Multifactor Authentication (MFA): Implement MFA for all critical systems and applications to add an extra layer of security.
- Employee Training: Continuously educate employees about cybersecurity best practices and how to recognize phishing and other social engineering attacks.
- Incident Response Plan Testing: Regularly test and update the incident response plan to ensure it is effective and current.
- Audit and Compliance: Conduct regular audits to ensure compliance with internal policies and external regulations.

Interested in risk assessment? Ask about Verify™.
https://www.securityassessments.ca

DATARISK CANADA