

Internal Cybersecurity Audit Checklist

Planning

- Create an inventory of what is included in the audit
 - Hardware devices
 - Software integrations
 - Database permissions
 - Networks
- Outline Data classified by sensitivity
- Use Threat Modeling to identify threats and possible entry points.

- Anti-virus installed and auto-updates enabled
- Process for regularly reviewing error logs
- Environment variables, code review, and version control best practices reviewed
- Consult a third-party to double-check your IT team's work

Why? Insider threats are among the top 5 threat types in cybersecurity

Employees

- Train employees on security processes and how to detect suspicious activity including:
 - Phishing
 - Social engineering
 - Suspicious links and email spam
 - Password security
 - Processes for managing breaches

Physical Security

- Keep servers in a locked and secure location
- Store your remote backups in a separate and safe location
- Establish a process for regular inspection
- Install biometric or keycard access and security camera systems
- Ensure the process of device and file disposal is safe and permanent

Tip: Send a company-wide email with a suspicious-looking link, employees that click on it receive additional training.

- Establish a standard device policy
 - BYOD: Bring your own device
 - COPE: Company-owned personally enabled
- Determine least privilege access: Employees only have access to information absolutely necessary for their jobs.

Data Security

- Data encryption
 - At rest
 - In transit
- SSL for internet data transfers
- Email

Establish a Process for Auditing at Regular Intervals

- Quarterly internal audits
- Annual external audits

Vendors and Partners

- Understand the privacy policies and data security of all vendors and partners
- Have multiple points of redundancy and backups

Why? Almost two-thirds of breaches are linked to external vendors

IT Department

- Have a plan for system hardening, which is the process of eliminating unnecessary nodes, accounts, permissions, access, or other unused potential vulnerabilities
 - Application hardening
 - Operating system hardening
 - Server hardening
 - Database hardening
 - Network hardening
- Regular penetration testing: simulated cyberattacks to expose potential threats.

