CAPTAIN I.T.

Conducting regular IT risk assessments is essential to identify potential vulnerabilities, protect your data, and maintain business continuity. In today's digital landscape, threats like ransomware, data breaches, and system downtime can have a devastating impact on your operations. By proactively evaluating your IT environment, you can uncover hidden risks, strengthen your defenses, and ensure compliance with industry standards.

Use this checklist as a guide to assess the key areas of your IT infrastructure and identify where improvements may be needed.

IT RISK ASSESSMENT CHECKLIST

Security Risks

- [ ] Identify and document all physical and digital assets
- [ ] Assess firewall and antivirus software configurations
- [ ] Evaluate the strength of password policies
- [ ] Confirm multi-factor authentication is enforced
- [ ] Scan for vulnerabilities in the network and endpoints
- [ ] Review access control lists for least privilege enforcement
- [ ] Inspect for outdated or unpatched software
- [ ] Analyze wireless network security (encryption, segmentation)
- [ ] Review remote access configurations (VPN, RDP, etc.)
- [ ] Audit logging and monitoring for security events

Data Risks

- [ ] Identify where sensitive data is stored, transmitted, or processed
- [ ] Evaluate data encryption policies (at rest and in transit)
- [ ] Check backup processes (frequency, coverage, offsite/cloud copies)
- [ ] Test data restore procedures
- [ ] Review data retention and disposal policies
- [ ] Verify compliance with data privacy laws (HIPAA, CCPA, GDPR, etc.)

User & Insider Risks

- [ ] Review onboarding and offboarding processes
- [ ] Check user activity monitoring practices
- [ ] Validate user training on cybersecurity awareness
- [ ] Assess privilege creep (unnecessary access rights)
- [ ] Evaluate use of shadow IT (unauthorized apps or systems)

Third-Party & Cloud Risks

- [ ] Review vendor risk management and security certifications
- [ ] Assess cloud service configurations (AWS, Azure, M365, etc.)
- [ ] Review SLAs and incident response processes with vendors
- [ ] Identify any exposed APIs or integrations
- [ ] Monitor third-party software dependencies

Infrastructure & System Risks

- [ ] Document and evaluate the current network topology
- [ ] Assess patch management and update schedules
- [ ] Review hardware lifecycle and warranties
- [ ] Check for single points of failure in systems
- [ ] Test UPS and power backup systems
- [ ] Evaluate the risk of downtime and disaster recovery planning

Compliance & Legal Risks

- [ ] Identify applicable industry regulations (e.g., HIPAA, PCI-DSS)
- [ ] Review audit trails and compliance documentation
- [ ] Assess security policies and incident response plans
- [ ] Ensure acceptable use policies are signed by employees
- [ ] Confirm insurance coverage for cyber incidents

Incident Response & Recovery

- [ ] Review incident response plan (IRP) documentation
- [ ] Validate communication plans for breach response
- [ ] Test the IRP with tabletop exercises or simulations
- [ ] Verify roles and responsibilities are clearly defined
- [ ] Assess recovery time objectives (RTO) and recovery point objectives (RPO)

Ready to Reduce Your IT Risk?

Don’t wait for a security breach or system failure to find out where your vulnerabilities are. Let Captain IT help you proactively protect your business with a comprehensive IT Risk Assessment.

Contact us for a free consultation!

Hello@CaptainIT.com

(800) 834-9795