IT Security Audit Checklist for PCI DSS Compliance

Ensure your organization meets all requirements with our comprehensive **IT security audit checklist** for PCI DSS compliance. This checklist guides you through critical security controls to protect cardholder data and maintain regulatory standards. Regular audits help identify vulnerabilities and strengthen your overall security posture.

PCI DSS Audit Checklist

1. **Build and Maintain a Secure Network**
   - Install and maintain a firewall configuration to protect cardholder data.
   - Change default system passwords and security parameters.
2. **Protect Cardholder Data**
   - Protect stored cardholder data with strong encryption.
   - Encrypt transmission of cardholder data across open, public networks.
3. **Maintain a Vulnerability Management Program**
   - Use and regularly update anti-virus software on all systems.
   - Develop and maintain secure systems and applications.
4. **Implement Strong Access Control Measures**
   - Restrict access to cardholder data by business need to know.
   - Assign a unique ID to each person with computer access.
   - Restrict physical access to cardholder data.
5. **Regularly Monitor and Test Networks**
   - Track and monitor all access to network resources and cardholder data.
   - Regularly test security systems and processes.
6. **Maintain an Information Security Policy**
   - Maintain a policy that addresses information security for all personnel.

Best Practices

- Schedule regular PCI DSS self-assessments.
- Educate employees on compliance requirements and security awareness.
- Document all processes and audit findings thoroughly.
- Remediate vulnerabilities as soon as possible after identification.

References

- PCI Security Standards Council
- PCI DSS Requirements and Security Assessment Procedures