IT Security Checklist

Requirements for Completing the Assessment

To effectively complete this assessment, the following resources and steps are needed:

1. **Access to Documentation:**
    - Scope, goals, and risk assessment report.
    - Control categories document for reference on control types and purposes.
    - Compliance frameworks and regulatory documentation.
2. **IT and Security Team Involvement:**
    - Collaborate with IT personnel to verify technical controls.
    - Engage compliance officers to ensure adherence to regulatory requirements.
    - Consult relevant department heads for operational and physical security measures.
3. **System and Infrastructure Review:**
    - Evaluate current security policies and procedures.
    - Assess technical controls such as firewalls, IDS, and encryption methods.
    - Review access control mechanisms and user management policies.
4. **Compliance Verification:**
    - Ensure proper data classification and inventory practices.
    - Check audit logs and reporting systems for monitoring compliance.
    - Validate incident response and disaster recovery plans.
5. **Assessment Completion Process:**
    - Answer each checklist item with 'Yes' or 'No' based on current implementation.
    - Identify gaps and document missing controls.
    - Provide recommendations for improvement.

Controls Assessment

Yes	No	Control
		Least Privilege
		Disaster recovery plans
		Password policies
		Separation of duties
		Firewall
		Intrusion detection system (IDS)
		Backups
		Antivirus software
		Manual monitoring, maintenance, and intervention for legacy systems
		Encryption
		Password management system
		Locks (offices, storefront, warehouse)
		Closed-circuit television (CCTV) surveillance
		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best Practice
		Only authorized users have access to customers' credit card information.
		Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
		Implement data encryption procedures to better secure credit card transaction touchpoints and data.
		Adopt secure password management policies.

System and Organizations Controls (SOC Type 1, SOC Type 2)

Yes	No	Best Practice
		User access policies are established.
		Sensitive data (PII/PHI) is confidential/private.
		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
		Data is available to individuals authorized to access it.