PKC

IT Internal Audit Checklist

1. Governance and Compliance

A. IT Policies and Procedures

- [ ] Verify IT policies align with IT Rules 2021, IT Act 2000, and
- [ ] upcoming Personal Data Protection Bill
- [ ] Check compliance with RBI guidelines (financial institutions) and SEBI guidelines (listed companies)
- [ ] Review adherence to CERT-In directives and MeitY guidelines

B. IT Governance Structure

- [ ] Review IT steering committee structure and meeting effectiveness
- [ ] Verify IT strategy alignment with business objectives
- [ ] Confirm compliance with Companies Act 2013 IT governance provisions

C. Regulatory Compliance

- [ ] Assess compliance with digital signature requirements, Aadhaar Authentication rules
- [ ] Verify adherence to GST data requirements, e-invoice standards
- [ ] Check compliance with sector-specific regulations (TRAI, IRDAI, etc.)

2. Data Privacy and Protection

A. Data Management

- [ ] Review data classification and protection measures
- [ ] Verify compliance with Indian data localization requirements
- [ ] Check consent management and data subject rights processes
- [ ] Assess data retention and disposal practices

B. Cross-Border Data Transfers

- [ ] Review mechanisms for international data transfers
- [ ] Verify compliance with RBI data localization for payment systems
- [ ] Check contractual safeguards for cross-border transfers

3. IT Operations and Infrastructure

A. Infrastructure Management

- [ ] Review hardware/software inventory and maintenance processes
- [ ] Assess capacity planning and environmental controls
- [ ] Check compliance with BIS requirements for IT equipment

B. Network and Endpoint Security

- [ ] Verify network architecture, segmentation, and firewall configuration
- [ ] Review endpoint protection, mobile device management, and patch procedures
- [ ] Check intrusion detection systems and TEC standards compliance

4. Access Control and Identity Management

- [ ] Review user provisioning/de-provisioning and access review processes
- [ ] Verify privileged access controls and segregation of duties
- [ ] Check multi-factor authentication implementation
- [ ] Assess Aadhaar-based authentication practices (if applicable)

5. Application Management

- [ ] Review secure coding standards and security testing procedures
- [ ] Verify change approval and testing processes
- [ ] Check compliance with CERT-In application security guidelines

6. Security Monitoring and Incident Management

- [ ] Review security monitoring tools and incident detection capabilities
- [ ] Verify incident response procedures and CERT-In reporting compliance
- [ ] Check vulnerability management processes and penetration testing practices

7. Business Continuity and Disaster Recovery

- [ ] Review business continuity and disaster recovery plans
- [ ] Verify backup procedures, RTO/RPO definitions
- [ ] Check alignment with RBI business continuity guidelines and NDMA recommendations

8. Third-Party Risk Management

- [ ] Review vendor assessment and monitoring procedures
- [ ] Check compliance with IT Rules 2021 for service providers
- [ ] Verify alignment with RBI outsourcing guidelines (if applicable)

9. Cloud Computing

- [ ] Review cloud provider selection criteria and security controls
- [ ] Verify data protection in cloud environments
- [ ] Check alignment with MeitY Cloud Initiative (GI Cloud/MeghRaj)

10. IT Asset Management

- [ ] Review hardware/software asset inventory and licensing compliance
- [ ] Verify e-waste management practices
- [ ] Check IT asset procurement through GeM (for public sector)

11. Mobile and Remote Working

- [ ] Review mobile device management and BYOD policies
- [ ] Verify remote access controls and monitoring
- [ ] Check work-from-home security guidelines

12. Database Management

- [ ] Review database access controls and encryption
- [ ] Verify database backup and patch management
- [ ] Check database audit logging capabilities

13. Indian Regulatory Requirements

A. Financial Sector Compliance

- [ ] Verify compliance with RBI Master Direction on Digital Payment Security
- [ ] Check NPCI security guidelines adherence
- [ ] Review SEBI cybersecurity framework compliance (if applicable

B. Data Localization Requirements

- [ ] Verify compliance with payment data localization
- [ ] Check implementation of data mirroring requirements
- [ ] Review cross-border data transfer mechanisms

C. Critical Information Infrastructure

- [ ] Check if organization falls under CII designation
- [ ] Verify compliance with NCIIPC guidelines (if applicable)
- [ ] Review mandatory security practices for CII entities

D. Public Sector/Government Specific

- [ ] Verify compliance with e-Governance standards
- [ ] Check adherence to Digital India initiatives
- [ ] Review GeM requirements (if applicable)

14. Emerging Technology Risks

- [ ] Review security controls for AI/ML systems
- [ ] Verify blockchain governance (if applicable)
- [ ] Check IoT device security management

15. Information Security Awareness

- [ ] Review security awareness program and effectiveness
- [ ] Check phishing simulation exercises and social engineering controls
- [ ] Verify role-based security training documentation