PKC

MIS Audit Checklist

FOR INDIAN ORGANIZATIONS

1. Regulatory Compliance & Legal Framework

IT Act 2000 & Amendments

- [ ] Compliance with Section 43A (data protection and compensation)
- [ ] Adherence to Section 72A (disclosure of personal information)
- [ ] Digital signature implementation as per IT Act requirements
- [ ] Cyber security incident reporting mechanisms in place

Data Protection & Privacy

- [ ] Digital Personal Data Protection Act 2023 compliance
- [ ] readiness
- [ ] Data localization requirements adherence
- [ ] Privacy policy implementation and user consent mechanisms
- [ ] Data breach notification procedures established
- [ ] Cross-border data transfer compliance

Industry-Specific Regulations

- [ ] RBI guidelines compliance (for BFSI sector)
- [ ] SEBI IT regulations adherence (for capital markets)
- [ ] IRDAI guidelines compliance (for insurance)
- [ ] Telecom regulatory compliance (TRAI/DoT guidelines)

2. Information Security Management

Security Policies & Procedures

- [ ] Information Security Policy documented and approved
- [ ] Access control policies and procedures
- [ ] Incident response and business continuity plans
- [ ] Regular security awareness training programs
- [ ] Vendor security assessment procedures

Technical Security Controls

- [ ] Firewall configuration and management
- [ ] Intrusion detection and prevention systems
- [ ] Anti-virus and anti-malware protection
- [ ] Data encryption at rest and in transit
- [ ] Multi-factor authentication implementation
- [ ] Regular vulnerability assessments and penetration testing

Physical Security

- [ ] Data center access controls and monitoring
- [ ] Environmental controls (temperature, humidity, power)
- [ ] CCTV surveillance and access logs
- [ ] Clean desk and clear screen policies
- [ ] Secure disposal of IT assets and media

3. IT Infrastructure & Architecture

System Architecture

- [ ] IT architecture documentation and standards
- [ ] Network topology documentation
- [ ] System integration and interface documentation
- [ ] Disaster recovery site setup and testing
- [ ] Cloud infrastructure governance (if applicable)

Performance & Capacity Management

- [ ] System performance monitoring tools
- [ ] Capacity planning and forecasting
- [ ] Service level agreements (SLAs) monitoring
- [ ] Database performance optimization
- [ ] Network bandwidth utilization analysis

Change Management

- [ ] Change management policy and procedures
- [ ] Change approval workflow and documentation
- [ ] Environment management (Dev/Test/Prod segregation)
- [ ] Version control and release management
- [ ] Rollback procedures and testing

4. Data Management & Governance

Data Quality & Integrity

- [ ] Data quality assessment procedures
- [ ] Data validation and verification controls
- [ ] Master data management processes
- [ ] Data lineage and traceability
- [ ] Data archival and retention policies

Database Management

- [ ] Database security configurations
- [ ] Regular database backups and restoration testing
- [ ] Database performance tuning and optimization
- [ ] Data purging and cleanup procedures
- [ ] Database access controls and audit trails

Business Intelligence & Analytics

- [ ] BI tool governance and access controls
- [ ] Report accuracy and validation procedures
- [ ] Data warehouse architecture and processes
- [ ] Analytics and dashboard security
- [ ] Self-service analytics governance

5. Application Controls & Development

Application Security

- [ ] Secure coding standards and practices
- [ ] Application vulnerability assessments
- [ ] Input validation and output encoding
- [ ] Session management and authentication
- [ ] Error handling and logging mechanisms

Software Development Lifecycle

- [ ] SDLC methodology documentation and adherence
- [ ] Code review and testing procedures
- [ ] User acceptance testing (UAT) processes
- [ ] Application deployment procedures
- [ ] Post-implementation review processes

Third-Party Applications

- [ ] Vendor due diligence and risk assessment
- [ ] License compliance management
- [ ] Third-party application security testing
- [ ] SLA monitoring and vendor performance
- [ ] Data sharing agreements with vendors

6. Operations & Service Management

IT Service Management

- [ ] ITIL/ITSM framework implementation
- [ ] Incident management procedures
- [ ] Problem management processes
- [ ] Service catalog and request fulfillment
- [ ] Configuration management database (CMDB)

Monitoring & Alerting

- [ ] 24/7 system monitoring capabilities
- [ ] Automated alerting mechanisms
- [ ] Performance dashboard and reporting
- [ ] Log management and analysis
- [ ] Root cause analysis procedures

Backup & Recovery

- [ ] Comprehensive backup strategy and procedures
- [ ] Regular backup testing and restoration
- [ ] Recovery time objective (RTO) and recovery point objective (RPO)
- [ ] Disaster recovery plan testing
- [ ] Business continuity planning

7. Financial & Procurement Controls

IT Budget Management

- [ ] IT budget planning and approval process
- [ ] Budget vs. actual variance analysis
- [ ] Cost allocation and chargeback mechanisms
- [ ] ROI measurement for IT investments
- [ ] IT asset capitalization procedures

Procurement & Vendor Management

- [ ] IT procurement policies and procedures
- [ ] Vendor selection and evaluation criteria
- [ ] Contract management and renewals
- [ ] Purchase order and invoice reconciliation
- [ ] Asset warranty and maintenance tracking

8. Human Resources & Training

IT Staffing & Organization

- [ ] IT organizational structure and roles
- [ ] Job descriptions and skill requirements
- [ ] Performance evaluation and career development
- [ ] Succession planning for key IT roles
- [ ] Background verification procedures

Training & Awareness

- [ ] IT skills development programs
- [ ] Security awareness training
- [ ] Compliance training programs
- [ ] Knowledge management systems
- [ ] Training effectiveness measurement

9. Risk Management & Internal Controls

IT Risk Assessment

- [ ] IT risk register and assessment methodology
- [ ] Risk mitigation strategies and controls
- [ ] Regular risk review and updates
- [ ] Integration with enterprise risk management
- [ ] Key risk indicator (KRI) monitoring

Internal Audit & Compliance

- [ ] Internal audit program for IT systems
- [ ] Compliance monitoring and reporting
- [ ] Management information system (MIS) reports
- [ ] Audit trail and logging mechanisms
- [ ] Corrective action tracking and closure

10. Emerging Technology & Innovation

Digital Transformation

- [ ] Digital strategy alignment with business goals
- [ ] Emerging technology evaluation and adoption
- [ ] API management and integration strategy
- [ ] Mobile application security and governance
- [ ] IoT and connected device management

Cloud & Virtualization

- [ ] Cloud governance and security framework
- [ ] Data sovereignty and residency compliance
- [ ] Multi-cloud and hybrid cloud strategy
- [ ] Virtualization security and management
- [ ] Container and microservices governance

11. Audit Documentation Requirements

Evidence Collection

- [ ] Policy and procedure documents
- [ ] System configuration screenshots
- [ ] Access control matrices and user lists
- [ ] Incident and problem management logs
- [ ] Vendor contracts and SLAs
- [ ] Training records and certifications
- [ ] Risk assessments and mitigation plans
- [ ] Compliance certificates and attestations

Audit Trail Requirements

- [ ] User activity logs and monitoring
- [ ] System change logs and approvals
- [ ] Data access and modification logs
- [ ] Administrative privilege usage logs
- [ ] Backup and restoration logs
- [ ] Security incident logs and responses

12. Reporting & Follow-up

Audit Report Components

- [ ] Executive summary with key findings
- [ ] Detailed findings with risk ratings
- [ ] Management responses and action plans
- [ ] Timeline for remediation activities
- [ ] Key performance indicators (KPIs)
- [ ] Compliance status summary

Continuous Monitoring

- [ ] Regular control testing procedures
- [ ] Automated compliance monitoring tools
- [ ] Key control indicator (KCI) dashboards
- [ ] Management reporting and escalation
- [ ] Audit follow-up and closure tracking