Cybersecurity Internal Audit Checklist in India

(SAMPLE)

1. REGULATORY COMPLIANCE & LEGAL FRAMEWORK

Indian Cybersecurity Laws & Regulations

- [ ] Information Technology Act, 2000 (amended 2008) compliance verification
- [ ] Information Technology (Reasonable Security Practices) Rules, 2011 implementation
- [ ] Personal Data Protection Bill (DPDP Act 2023) compliance assessment
- [ ] Reserve Bank of India (RBI) Cyber Security Framework compliance (for financial institutions)
- [ ] SEBI IT Framework compliance (for market intermediaries)
- [ ] Sectoral regulations compliance (TRAI, IRDA, etc.)
- [ ] Critical Information Infrastructure (CII) protection measures (if applicable)

Documentation & Policies

- [ ] Cybersecurity policy document existence and annual review
- [ ] Information security policy aligned with IS/ISO/IEC 27001:2013
- [ ] Data classification and handling procedures documented
- [ ] Incident response plan documented and tested
- [ ] Business continuity and disaster recovery plans
- [ ] Privacy policy and consent management procedures
- [ ] Vendor risk management policy for third-party assessments

2. GOVERNANCE & RISK MANAGEMENT

Organizational Structure

- [ ] Designated Chief Information Security Officer (CISO) or equivalent
- [ ] Information Security Committee with defined roles & responsibilities
- [ ] Cybersecurity governance framework implementation
- [ ] Regular board/senior management reporting on cybersecurity posture
- [ ] Cybersecurity budget allocation and utilization tracking

Risk Assessment & Management

- [ ] Annual cybersecurity risk assessment conducted
- [ ] Risk register maintained with mitigation strategies
- [ ] Threat landscape analysis and threat modeling
- [ ] Business impact analysis for critical systems
- [ ] Third-party risk assessments for vendors and partners
- [ ] Supply chain security risk evaluation

3. TECHNICAL SECURITY CONTROLS

Network Security

- [ ] Firewall configuration and rule review
- [ ] Intrusion Detection/Prevention System (IDS/IPS) deployment
- [ ] Network segmentation and micro-segmentation implementation
- [ ] Virtual Private Network (VPN) security configuration
- [ ] Wireless network security (WPA3, network isolation)
- [ ] Network monitoring and logging capabilities
- [ ] DNS security and filtering implementation

Endpoint Security

- [ ] Antivirus/anti-malware solution deployment and updates
- [ ] Endpoint Detection and Response (EDR) implementation
- [ ] Device encryption (full disk encryption) enforcement
- [ ] Mobile Device Management (MDM) for corporate devices
- [ ] USB port controls and removable media policies
- [ ] Patch management system for operating systems & applications
- [ ] Secure configuration baselines for workstations and servers

Identity & Access Management

- [ ] Multi-Factor Authentication (MFA) implementation for critical systems
- [ ] Privileged Access Management (PAM) solution deployment
- [ ] Regular access review and certification process
- [ ] Role-based access control (RBAC) implementation
- [ ] Single Sign-On (SSO) deployment where applicable
- [ ] Password policy enforcement (complexity, expiration, history)
- [ ] Service account management and monitoring

4. DATA PROTECTION & PRIVACY

Data Security

- [ ] Data classification scheme implementation and labeling
- [ ] Data Loss Prevention (DLP) solution deployment
- [ ] Database security controls (encryption, access logging)
- [ ] Backup and recovery procedures testing
- [ ] Data retention and disposal policies implementation
- [ ] Cross-border data transfer compliance assessment
- [ ] Cloud data security and encryption verification

Privacy Compliance

- [ ] Consent management system implementation
- [ ] Data subject rights fulfillment process
- [ ] Privacy impact assessment procedures
- [ ] Data breach notification procedures (within 6 hours to CERT-In)
- [ ] Data localization requirements compliance (where applicable)
- [ ] Privacy by design implementation in new systems

5. APPLICATION SECURITY

Secure Development

- [ ] Security Development Lifecycle (SDLC) implementation
- [ ] Static Application Security Testing (SAST) integration
- [ ] Dynamic Application Security Testing (DAST) procedures
- [ ] Code review processes for security vulnerabilities
- [ ] Third-party component vulnerability management
- [ ] API security testing and monitoring

Web Application Security

- [ ] Web Application Firewall (WAF) deployment and tuning
- [ ] SSL/TLS configuration and certificate management
- [ ] OWASP Top 10 vulnerability assessment
- [ ] Session management and authentication controls
- [ ] Input validation and output encoding implementation

6. CLOUD SECURITY (IF APPLICABLE)

Cloud Governance

- [ ] Cloud security policy and procedures documentation
- [ ] Cloud service provider security assessment
- [ ] Shared responsibility model understanding and implementation
- [ ] Cloud access controls and identity management
- [ ] Cloud workload protection and monitoring
- [ ] Multi-cloud/hybrid cloud security architecture review

7. INCIDENT RESPONSE & BUSINESS CONTINUITY

Incident Management

- [ ] Computer Security Incident Response Team (CSIRT) establishment
- [ ] Incident response playbooks for various scenarios
- [ ] Integration with CERT-In reporting requirements
- [ ] Incident response testing and simulation exercises
- [ ] Forensics capabilities and evidence handling procedures
- [ ] Communication plan for stakeholders during incidents

Business Continuity

- [ ] Business Impact Analysis (BIA) conducted
- [ ] Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined
- [ ] Disaster recovery testing (at least annually)
- [ ] Alternative site arrangements and testing
- [ ] Critical vendor dependency assessment
- [ ] Communication systems redundancy

8. SECURITY MONITORING & OPERATIONS

Security Operations Center (SOC)

- [ ] 24/7 security monitoring capabilities (in-house or outsourced)
- [ ] Security Information and Event Management (SIEM)
- [ ] implementation
- [ ] Log management and retention policy compliance
- [ ] Threat intelligence integration and analysis
- [ ] Security metrics and KPIs tracking
- [ ] Regular security posture reporting

Vulnerability Management

- [ ] Automated vulnerability scanning tools deployment
- [ ] Regular penetration testing (at least annually)
- [ ] Vulnerability assessment and prioritization process
- [ ] Patch management program with defined SLAs
- [ ] Zero-day vulnerability response procedures

9. TRAINING & AWARENESS

Employee Training

- [ ] Cybersecurity awareness training program implementation
- [ ] Phishing simulation exercises and training
- [ ] Role-specific security training for IT staff
- [ ] New employee security orientation program
- [ ] Annual refresher training and assessment
- [ ] Security awareness metrics and tracking

Specialized Training

- [ ] Incident response team training and certification
- [ ] Security tools training for technical staff
- [ ] Compliance training for relevant personnel
- [ ] Third-party security training verification

10. VENDOR & THIRD-PARTY MANAGEMENT

Vendor Risk Assessment

- [ ] Security questionnaires and due diligence process
- [ ] Vendor security certification verification (ISO 27001, SOC 2)
- [ ] Contractual security requirements and SLAs
- [ ] Regular vendor security reviews and audits
- [ ] Fourth-party risk assessment procedures
- [ ] Vendor incident notification requirements

11. PHYSICAL & ENVIRONMENTAL SECURITY

Physical Access Controls

- [ ] Biometric or card-based access control systems
- [ ] Visitor management and escort procedures
- [ ] CCTV surveillance and monitoring
- [ ] Secure areas for critical infrastructure
- [ ] Clean desk and clear screen policies
- [ ] Equipment disposal and sanitization procedures

Environmental Controls

- [ ] Fire suppression systems in data centers
- [ ] Uninterruptible Power Supply (UPS) and backup generators
- [ ] Environmental monitoring (temperature, humidity)
- [ ] Secure cable management and protection

12. AUDIT & ASSESSMENT

Internal Audits

- [ ] Annual internal cybersecurity audit program
- [ ] Security control testing and validation
- [ ] Gap analysis and remediation tracking
- [ ] Compliance audit findings management
- [ ] Audit trail maintenance and protection

External Assessments

- [ ] Third-party security assessments and penetration testing
- [ ] Compliance certification maintenance (ISO 27001, etc.)
- [ ] Regulatory examination preparedness
- [ ] Industry benchmark comparisons