

1. Governance Requirements:

- **Company policies & SOPs, such as:**
 - Information Security Policy
 - IT Governance Policy
 - Data Privacy Policy
 - Access Control Policy
 - Incident Management Policy

- **Defined roles & responsibilities**
 - System Owner
 - Information Security Officer
 - Admin/User roles

- **Management approval** of policies (signed & dated)

- **Vendor / Third-Party Risk Management policy**

2. Risk Management Requirements

- **Risk Assessment Report**
 - Application risks
 - Infrastructure risks
 - Data risks
 - Cybersecurity risks

- **Risk Treatment / Mitigation Plan**

- **Threat modeling**

- **Business Impact Analysis (BIA)**

- **Disaster Recovery (DR) & Business Continuity Plan (BCP)**

- **Backup & Restore procedure**

3. Compliance Requirements

- **RBI IT Framework for Banks**
- **ISO 27001 (Information Security)**
 - Certificate preferred, or at least ISO-aligned controls
- **CERT-In guidelines**
- **IT Act 2000 & DPDP Act (India Data Protection)**
- **OWASP Top 10** (for application security)

Documents/evidence needed:

- Compliance mapping document
- Secure SDLC process
- Data encryption details (at rest & in transit)
- Password & authentication standards
- Logging & monitoring policy

4. Security & Technical Audit Requirements

- **VAPT (Vulnerability Assessment & Penetration Testing)**
 - Conducted by a CERT-In empanelled auditor
 - Both Application VAPT and Infrastructure VAPT
- **Source Code Review**
- **Audit closure report** (all high/medium issues fixed)

Artifacts required:

- VAPT Report
- Remediation report
- Re-test confirmation

5. Application & Data Security Controls

- Role-based access control (RBAC)
- MFA / strong authentication
- Session management
- Audit logs (who did what, when)
- Data masking (if PII is involved)
- Encryption (TLS, AES, etc.)
- Secure API design

6. Operational & Process Evidence

- Change management records
- Incident response mock drill
- User access review reports
- Backup logs
- DR drill report
- Patch management records