GENERAL IT CHECKLIST

Security Controls	Check points
Access Controls	☐ User access provisioning and de-provisioning processes are in place. ☐ Access rights are granted based on job responsibilities. ☐ Segregation of duties (SoD) controls are implemented. ☐ Regular access reviews are conducted. ☐ Strong password policies are enforced
Change Management	☐ Formalized change management process is in place for all system changes. ☐ Changes are documented, approved, and tested before implementation ☐ Segregation of duties between development, testing, and production environments ☐ Regular change management reviews are conducted
Backup & Recovery	☐ Regular backups of critical systems and data are performed. ☐ Backup integrity checks are conducted regularly to ensure recoverability ☐ Backup and recovery procedures are documented and tested periodically ☐ Offsite storage of backups is maintained to mitigate risk of data loss
Incident Management	☐ Formal incident response plan is in place to address security breaches and incidents. ☐ Procedures for reporting and documenting security incidents are established. ☐ Incident response team is trained and ready to respond ☐ Post-incident reviews are conducted to identify improvement areas.
Network Security	☐ Intrusion detection/prevention and antivirus systems are deployed. ☐ Network segmentation is implemented to minimize breaches. ☐ Regular network vulnerability assessments and penetration tests are conducted. ☐ Wireless network security controls are in place to prevent unauthorized access

GENERAL IT CHECKLIST

Security Controls	Check points
Data Privacy	☐ Data protection policies are in place for sensitive data. ☐ Data encryption is used for data in transit and at rest ☐ Data classification policies are implemented based on sensitivity ☐ Regular data privacy training is conducted for employees.
Monitoring & Logging	☐ Logging mechanisms are implemented to record security-related events. ☐ Logs are reviewed and analyzed regularly for security incidents. ☐ System performance and availability are monitored to detect anomalies and issues. ☐ Intrusion detection systems are in place to monitor suspicious activity.
Vendor Management	☐ Vendor risk assessments are conducted before engaging third-party vendors. ☐ Contracts with vendors include provisions for security and compliance ☐ Vendor activities are monitored and reviewed regularly ☐ Procedures are in place for terminating vendor access when necessary
Compliance & Audit	☐ Regular compliance assessments and audits are conducted. ☐ IT policies, procedures, and controls are documented and updated. ☐ Remediation actions are implemented for identified control deficiencies or non-compliance issues.