SharePoint Server 2019 ISO 27001 & Security Compliance Checklist

1. Governance & ISO 27001 Alignment

- Define scope: limit to campus web hosting, exclude personal data.
- Implement ISMS: establish policies, risk assessments, and control monitoring.
- Maintain asset inventory of servers, databases, and web applications.
- Perform periodic internal audits and management reviews.

2. Technical Controls

- Apply latest SharePoint, Windows Server, and SQL Server patches.
- Use least-privilege service accounts and role separation.
- Enforce HTTPS/TLS with strong cipher suites; disable TLS 1.0/1.1.
- Integrate AD authentication, enable Kerberos, and enforce MFA for admins.

3. Server & Network Hardening

- Apply CIS Benchmarks for Windows and SQL Server.
- Disable unused services and legacy protocols (SMBv1, Telnet).
- Implement firewall rules and endpoint protection (Windows Defender ATP).
- Use DMZ for WFE servers and restrict Central Admin access by IP.

4. Monitoring & Incident Response

- Centralize logs (ULS, Event, IIS, SQL) in SIEM (Sentinel/Splunk).
- Set alerts for privilege escalation or configuration changes.
- Maintain and test incident response procedures regularly.

5. Backup & Continuity

- Perform encrypted farm and SQL backups; test restoration regularly.
- Document disaster recovery plan with RTO/RPO objectives.
- Ensure backup retention and offsite storage compliance.

6. Framework Alignment

- CIS Benchmarks: SharePoint, Windows Server, SQL Server.
- NIST SP 800-53: control mapping for U.S. compliance.
- OWASP Top 10: web application security alignment.
- Microsoft Security Baselines: validate via Security Compliance Toolkit.

7. Documentation & Audit Readiness

- Maintain architecture diagrams and access control matrices.
- Keep patch records, backup logs, and audit trails.
- Retain risk assessments and corrective action records for auditors.