Strike Graph

TISAX Audit Checklist

1. Information Security Management System (ISMS)

Documentation Requirements

- [ ] Information security policy documented and approved by management
- [ ] Risk assessment methodology defined and documented
- [ ] Asset inventory created and maintained
- [ ] Information classification scheme established
- [ ] Security incident management process documented
- [ ] Business continuity and disaster recovery plans in place
- [ ] Change management procedures documented
- [ ] System development lifecycle process documented

Organization and Responsibilities

- [ ] ISMS roles and responsibilities defined
- [ ] Information security officer appointed
- [ ] Management commitment documented
- [ ] Regular management reviews scheduled and documented
- [ ] Information security team structure established

2. Technical Security Controls

Access Control

- [ ] Access control policy implemented
- [ ] User access rights documentation
- [ ] Password policy enforced
- [ ] Multi-factor authentication implemented where required
- [ ] Privileged access management process
- [ ] Regular access rights review process

Network Security

- [ ] Network architecture documentation
- [ ] Firewall rules and configuration
- [ ] Network segmentation implemented
- [ ] Remote access security controls
- [ ] Wireless network security measures
- [ ] Network monitoring tools in place

System Security

- [ ] Server hardening guidelines
- [ ] Endpoint protection deployed
- [ ] Patch management process
- [ ] Vulnerability management program
- [ ] Secure configuration baselines
- [ ] Anti-malware protection

3. Data Protection Measures

Data Handling

- [ ] Data classification implemented
- [ ] Data retention policies defined
- [ ] Encryption standards documented
- [ ] Secure data transfer procedures
- [ ] Data backup processes
- [ ] Data disposal procedures

Privacy Requirements

- [ ] Privacy impact assessments
- [ ] Data processing inventory
- [ ] Privacy notices and consents
- [ ] Data subject rights procedures
- [ ] Data processor agreements
- [ ] Cross-border data transfer controls

4. Physical Security

Facility Security

- [ ] Physical access control system
- [ ] Visitor management process
- [ ] CCTV monitoring system
- [ ] Environmental controls
- [ ] Clear desk policy enforcement
- [ ] Secure areas defined and protected

Prototype Protection

- [ ] Prototype handling procedures
- [ ] Secure storage facilities
- [ ] Transport security measures
- [ ] Prototype disposal process
- [ ] Prototype tracking system
- [ ] Confidentiality agreements

5. Human Resources

Security Awareness

- [ ] Security awareness training program
- [ ] Training records maintained
- [ ] Regular refresher courses
- [ ] Role-specific security training
- [ ] Information security guidelines for employees

Personnel Security

- [ ] Background check procedures
- [ ] Confidentiality agreements
- [ ] Disciplinary process
- [ ] Exit procedures
- [ ] Security responsibilities in job descriptions

6. Incident Management

Response Preparation

- [ ] Incident response team defined
- [ ] Incident classification scheme
- [ ] Response procedures documented
- [ ] Communication templates prepared
- [ ] Emergency contact list maintained

Documentation

- [ ] Incident logging system
- [ ] Investigation procedures
- [ ] Lesson learned process
- [ ] Incident reporting templates
- [ ] Evidence handling procedures

7. Business Continuity

Continuity Planning

- [ ] Business impact analysis
- [ ] Recovery time objectives defined
- [ ] Alternative site arrangements
- [ ] Critical supplier dependencies documented
- [ ] Emergency procedures
- [ ] Regular testing schedule

8. Compliance and Audit

Internal Controls

- [ ] Internal audit program
- [ ] Compliance monitoring process
- [ ] Regular security assessments
- [ ] Non-conformity tracking
- [ ] Corrective action procedures

Documentation

- [ ] Regulatory requirements register
- [ ] Compliance records
- [ ] Audit reports and findings
- [ ] External audit results
- [ ] Improvement tracking system

Pre-Audit Review Checklist:

- [ ] All documentation is current and approved
- [ ] Evidence of implementation collected
- [ ] Key stakeholders briefed and available
- [ ] Sample records prepared for demonstration
- [ ] Technical documentation organized
- [ ] Required personnel trained and prepared
- [ ] Mock audit completed
- [ ] Corrective actions addressed

Remember to:

- Customize based on your specific assessment objectives and desired assessment level (AL1, AL2, or AL3)
- Add company-specific requirements as needed
- Assign responsible parties for each item
- Set realistic deadlines for completion
- Regularly review progress with your project team