Comprehensive Security Assessment Checklist

Your Strategic Guide to Enterprise Security Excellence

This comprehensive checklist helps you assess your organization's security posture across seven critical domains. Based on ISO 27001, NIST Cybersecurity Framework, CIS Controls, and real-world implementation experience from Hack23 AB's Information Security Management System.

How to Use This Checklist

- **Check items you have fully implemented**
- ⚠ **Mark items that need improvement**
- **Identify gaps requiring immediate attention**
- **Calculate your security maturity score by domain**

Scoring Guide: - 90-100%: Excellent - Industry-leading security posture - 75-89%: Good - Strong foundation with room for optimization - 60-74%: Fair - Basic controls in place, significant gaps remain - Below 60%: Critical - Immediate remediation required

---

1 Security Architecture & Strategy (20 items)

Strategic Foundation

☐ **Security strategy aligned with business objectives** - Written security strategy document approved by leadership
☐ **Risk assessment framework implemented** - Regular risk assessments conducted (at least annually)
☐ **Security governance structure established** - Clear roles, responsibilities, and accountability
☐ **Executive security awareness** - Board-level security briefings conducted regularly

Architecture & Design

- ☐ **Security architecture documentation maintained** - Current diagrams and specifications
- ☐ **Defense-in-depth strategy implemented** - Multiple layers of security controls
- ☐ **Zero-trust architecture principles applied** - Never trust, always verify approach
- ☐ **Secure-by-design practices followed** - Security considered from inception

Threat Intelligence

- ☐ **Threat modeling conducted for critical systems** - STRIDE or similar methodology applied
- ☐ **Threat intelligence feeds utilized** - Integration with industry threat data
- ☐ **Attack surface mapping performed** - Comprehensive inventory of exposure points
- ☐ **Security metrics and KPIs tracked** - Quantitative measurement of security posture

Standards & Compliance

- ☐ **Security policies documented and approved** - Comprehensive ISMS documentation
- ☐ **Compliance requirements identified** - ISO 27001, GDPR, NIS2, industry-specific standards
- ☐ **Security audit program established** - Internal and external audits conducted regularly
- ☐ **Third-party security assessments completed** - Independent validation of controls

Continuous Improvement

- ☐ **Security roadmap maintained** - Planned improvements prioritized and funded
- ☐ **Lessons learned process implemented** - Post-incident reviews drive improvements
- ☐ **Security awareness program active** - Regular training for all personnel
- ☐ **Vendor security requirements defined** - Third-party risk management framework

---

2 Access Control & Identity Management (15 items)

Identity & Authentication

- ☐ **Multi-factor authentication (MFA) enforced** - For all privileged accounts and remote access
- ☐ **Strong password policy implemented** - Minimum complexity, length, and rotation requirements
- ☐ **Single Sign-On (SSO) deployed** - Centralized authentication

where applicable
☐ **Privileged Access Management (PAM) solution in use** - Secure management of admin credentials

Authorization & Access

☐ **Least privilege principle enforced** - Users have only necessary permissions
☐ **Role-based access control (RBAC) implemented** - Permissions assigned by role, not individual
☐ **Access reviews conducted regularly** - Quarterly or semi-annual access certification
☐ **Automated user provisioning/deprovisioning** - Identity lifecycle management

Account Management

☐ **User onboarding/offboarding procedures documented** - Consistent access grant/revoke process
☐ **Dormant account monitoring and cleanup** - Inactive accounts disabled automatically
☐ **Service account management controls** - Non-human identities tracked and secured
☐ **Session management controls implemented** - Timeout, re-authentication requirements

Directory & Federation

☐ **Centralized directory service in use** - Active Directory, Azure AD, or equivalent
☐ **Federation protocols configured securely** - SAML, OAuth 2.0, OpenID Connect
☐ **Access control audit logging enabled** - Who accessed what, when, and from where

---

3 Data Protection & Encryption (15 items)

Data Classification

☐ **Data classification scheme established** - Public, internal, confidential, restricted
☐ **Data inventory maintained** - Location and sensitivity of all critical data
☐ **Data flow mapping completed** - Understanding data movement and processing
☐ **Privacy impact assessments (PIAs) conducted** - GDPR Article 35 compliance

Encryption Controls

☐ **Data-at-rest encryption implemented** - Full disk encryption, database encryption
☐ **Data-in-transit encryption enforced** - TLS 1.2+ for all sensitive

communications

☐ **End-to-end encryption for sensitive data** - Protection throughout entire lifecycle

☐ **Cryptographic key management controls** - Secure generation, storage, rotation, destruction

Data Loss Prevention

☐ **Data Loss Prevention (DLP) tools deployed** - Prevent unauthorized data exfiltration

☐ **Email security controls implemented** - SPF, DKIM, DMARC, encryption

☐ **Removable media controls enforced** - USB restrictions, encryption requirements

☐ **Cloud data protection configured** - Cloud Access Security Broker (CASB) or equivalent

Data Lifecycle Management

☐ **Data retention policies established** - Legal and business requirements documented

☐ **Secure data disposal procedures** - Sanitization and destruction standards

☐ **Backup encryption implemented** - Protected backups with tested restoration

☐ **Privacy controls for personal data** - GDPR/CCPA compliance mechanisms

---

4 Network Security (10 items)

Network Architecture

☐ **Network segmentation implemented** - DMZ, internal zones, sensitive data isolation

☐ **Firewall rules documented and reviewed** - Regular audit of allow/deny rules

☐ **Intrusion Detection/Prevention Systems (IDS/IPS) deployed** - Network monitoring for threats

☐ **Secure remote access solution** - VPN with MFA, zero-trust network access (ZTNA)

Traffic Control

☐ **Web Application Firewall (WAF) protecting internet-facing apps** - OWASP Top 10 protection

☐ **DNS security controls implemented** - DNS filtering, DNSSEC validation

☐ **Email authentication configured** - SPF, DKIM, DMARC records published

☐ **DDoS protection mechanisms in place** - Rate limiting, traffic scrubbing

Monitoring & Response

- □ **Network traffic monitoring and analysis** - SIEM integration, anomaly detection
- □ **Wireless network security controls** - WPA3 encryption, network access control

---

5 Vulnerability Management (10 items)

Vulnerability Identification

- □ **Regular vulnerability scanning conducted** - Weekly or monthly automated scans
- □ **Penetration testing performed annually** - External security assessment by qualified testers
- □ **Security code reviews implemented** - SAST (Static Application Security Testing)
- □ **Dynamic application security testing (DAST)** - Runtime vulnerability detection

Patch Management

- □ **Patch management process documented** - SLAs for critical/high/medium/low vulnerabilities
- □ **Automated patching for workstations** - Regular OS and application updates
- □ **Server patching schedule maintained** - Change management integration
- □ **Emergency patching procedures defined** - Response to zero-day vulnerabilities

Remediation Tracking

- □ **Vulnerability tracking system in use** - Jira, ServiceNow, or similar platform
- □ **Remediation verification performed** - Validation that fixes were successful

---

6 Incident Response & Business Continuity (10 items)

Incident Management

- □ **Incident response plan documented** - Roles, procedures, communication protocols
- □ **Incident response team designated** - 24/7 contact information available
- □ **Security incident classification scheme** - Severity levels and escalation criteria
- □ **Incident response drills conducted** - Tabletop exercises at least annually

Detection & Analysis

☐ **Security monitoring and alerting configured** - SIEM, EDR, cloud security tools
☐ **Log aggregation and retention** - Centralized logging with appropriate retention
☐ **Forensic capabilities established** - Tools and procedures for investigation

Recovery & Learning

☐ **Business continuity plan (BCP) maintained** - Recovery time/point objectives defined
☐ **Disaster recovery testing performed** - Annual validation of recovery procedures
☐ **Post-incident review process** - Lessons learned and improvement actions

---

7 Compliance & Governance (15 items)

Regulatory Compliance

☐ **Applicable regulations identified** - GDPR, NIS2, HIPAA, PCI-DSS, SOC2, ISO 27001
☐ **Compliance gap analysis completed** - Understanding current state vs. requirements
☐ **Privacy program established** - Data Protection Officer appointed (if required)
☐ **Data Processing Agreements (DPAs) in place** - Vendor contracts include security terms

Security Controls Framework

☐ **Security controls mapped to frameworks** - ISO 27001, NIST CSF, CIS Controls
☐ **Control effectiveness testing performed** - Evidence of control operation
☐ **Security audit trails maintained** - Immutable logs for compliance evidence
☐ **Compliance reporting automated** - Dashboards and periodic compliance reports

Documentation & Evidence

☐ **Security policies reviewed annually** - Current and approved documentation
☐ **Security procedures documented** - Step-by-step implementation guidance
☐ **Security awareness training tracked** - Completion records maintained
☐ **Vendor security assessments documented** - Third-party risk evaluation

Continuous Monitoring

☐ **Continuous compliance monitoring implemented** - Automated

control validation
- □ **Security metrics dashboard available** - Real-time visibility into security posture
- □ **Compliance calendar maintained** - Tracking audit dates, renewal deadlines

---

Calculate Your Security Maturity Score

Score by Domain: 1. Security Architecture: _____ / 20 = _____% 2. Access Control: _____ / 15 = _____% 3. Data Protection: _____ / 15 = _____% 4. Network Security: _____ / 10 = _____% 5. Vulnerability Management: _____ / 10 = _____% 6. Incident Response: _____ / 10 = _____% 7. Compliance & Governance: _____ / 15 = _____%

Overall Security Maturity: _____ / 95 = _____%

Next Steps Based on Your Score

If You Scored 90-100% (Excellent)

You have an industry-leading security program. Focus on: - Continuous improvement and optimization - Advanced threat hunting capabilities - Security automation and orchestration - Thought leadership and knowledge sharing

If You Scored 75-89% (Good)

Strong foundation with optimization opportunities. Prioritize: - Closing identified gaps in lower-scoring domains - Automating manual security processes - Enhancing security monitoring and response - Advanced security controls implementation

If You Scored 60-74% (Fair)

Basic controls in place but significant gaps. Focus on: - Immediate remediation of critical vulnerabilities - Implementing missing foundational controls - Establishing formal security processes - Building security awareness culture

If You Scored Below 60% (Critical)

Immediate action required to reduce business risk: - Conduct comprehensive risk assessment - Prioritize critical security controls - Consider engaging external security expertise - Develop rapid remediation roadmap

---

How Hack23 Can Help

At **Hack23 AB**, we don’t just provide checklists—we help you implement comprehensive security programs that are transparent, effective, and aligned with business objectives.

Our Expertise Includes:

Security Architecture & Strategy - ISO 27001 ISMS implementation - Risk assessment and threat modeling - Security roadmap development - Public ISMS documentation (see our GitHub)

☁ **Cloud Security & DevSecOps** - AWS security architecture (Advanced level) - DevSecOps integration into CI/CD pipelines - Infrastructure as Code security - SLSA Level 3 supply chain security

Compliance & Governance - GDPR, NIS2, SOC2 compliance programs - Security policy development - Audit preparation and support - Continuous compliance automation

Secure Development - Secure SDLC implementation - Code quality and security analysis - Automated security testing - Developer security training

Why Choose Hack23?

- **Transparent by Design:** Sweden’s only cybersecurity consultancy with fully public ISMS on GitHub
- **Expert Credentials:** CISSP, CISM, AWS Security Specialty certified
- **Real-World Experience:** 30+ years in enterprise IT and security (Stena Group, Polestar, WirelessCar)
- **Practical Approach:** Security that enables innovation, not blocks it

Ready to Improve Your Security Posture?

Contact us for a free 30-minute security consultation:

- Email: james.pether.sorling@hack23.com
- LinkedIn: https://www.linkedin.com/in/jamessorling/
- Website: https://hack23.com
- Public ISMS: https://github.com/Hack23/ISMS-PUBLIC

Additional Resources

Learn More About Security Best Practices: - Hack23 Security Blog - Expert insights and implementation guides - Public ISMS Repository - Real-world security policies - CIA Compliance Manager - Open-source security assessment platform - Secure Development Policy - DevSecOps implementation guide

Security Frameworks Referenced: - ISO/IEC 27001:2022 - Information Security Management - NIST Cybersecurity Framework 2.0 - CIS Controls v8 - OWASP Top 10 and ASVS - AWS Well-Architected Framework (Security Pillar)

This checklist is provided for educational purposes. For specific compliance requirements, consult with qualified security professionals and legal counsel.