NS ADVANCE

SELF ASSESSMENT

Compliance Readyness Checklist for SMEs

hello@nsasec.com | +358 40 246 3074

Table of Contents

Why this checklist matters?

Dr. Naveen Sharma
CISA, ISO 27001 LA, TOGAF

Cyber threats are increasing, and small and medium enterprises (SMEs) are prime targets due to limited cybersecurity resources. A single cyberattack can lead to financial losses, reputational damage, and compliance fines.

This self-assessment checklist is designed to help SMEs quickly evaluate their cybersecurity posture, identify vulnerabilities, and take proactive steps to strengthen their defenses.

SME Cybersecurity Self-Assessment Checklist

Simply answer each question with Yes, No, or Don't Know and use your score to gauge where improvements are needed.

Awareness

- Are employees aware of cyber risks and trained to avoid threats? □
- Do employees know how to identify and handle suspicious emails and links? □
- Are suppliers assessed for cybersecurity risks? □
- Do employees receive regular cybersecurity training? □
- Is there a formal cybersecurity policy explained to employees? □

Tasks And Responsibilities

- Is there a designated person responsible for cybersecurity? □
- Does this person have the knowledge and authority to take action? □
- Is there a cyber incident mitigation plan in place? □
- Are key employees trained to respond to security incidents? □

Data Protection

- Is sensitive data encrypted, including on mobile devices? □
- Does the company comply with data protection regulations? □
- Is physical access to IT systems secured? □

Backups

- Are regular backups taken for critical data and systems? □
- Are backups stored offline or securely disconnected? □
- Has the backup restoration process been tested successfully? □

Passwords And User Administration

- Are accounts protected with multi-factor authentication (MFA)? □
- Are passwords strong, unique, and changed periodically? □
- Do employees only have access to the systems they need? □
- Are former employees immediately removed from IT systems? □
- If a cyber attack occurs, are passwords updated immediately? □
- Are administrative privileges restricted and monitored? □

Malware Protection

- Does the company use a firewall to protect its network? □
- Are antivirus and anti-malware tools installed on all devices? □
- Is email scanning enabled to prevent malware threats? □

Updates

- Is all business software regularly updated? □
- Are antivirus and security solutions kept up to date? □
- Are firewalls and network security settings updated regularly? □

Secure Communication

- Is company communication encrypted (emails, data transfers)? □
- Is the company WLAN secured and encrypted? □
- Do remote employees use VPNs for secure access? □

Emergency Response

- Is there a clear response plan for cyber incidents? □
- Do employees and managers know what to do in case of an attack? □
- Would vendors and clients inform the company if they were attacked? □
- Does the company have access to an external cybersecurity expert? □
- Is there cyber insurance coverage for IT-related business disruptions? □

Software Development

- Are guest networks separated from company networks? □
- Are responsibilities for software security clearly defined? □
- Are security code reviews performed regularly? □
- Are security tests (penetration testing, black-box testing) conducted? □

Overall Scoring

0 - 10 : High risk, immediate improvements needed.

11 - 24 : Some cybersecurity measures in place, but gaps exist.

25 - 30 : Good cybersecurity hygiene, but further improvements possible.

31 - 39 : Strong cybersecurity posture; continuous monitoring recommended.

How Compliance Challenges Impact SMEs

The Burden of Compliance on SMEs

While large enterprises have the financial and technical resources to comply with evolving cybersecurity regulations, Small and Medium Enterprises (SMEs) often struggle to meet these demands.

SMEs face challenges such as:

- **High Costs of Compliance**: Implementing cybersecurity frameworks, hiring compliance officers, and maintaining security infrastructure can be expensive.
- **Limited Expertise**: Many SMEs lack in-house cybersecurity specialists who can interpret and implement compliance standards effectively.
- **Complex Regulations**: Different regions have varying compliance laws, making it difficult for SMEs operating across multiple jurisdictions to stay compliant.
- **Operational Disruptions**: Failure to comply can lead to regulatory fines, loss of customer trust, and even business shutdowns in extreme cases.

86% Data breaches happen via employees

90% SMEs have no cybersecurity hygeine

80% Cyber attacks happen on SMEs

60% SMEs can not recover from a targetted cyber attack

Our Approach

- ➔ CYBERSECURITY LEADERSHIP
- ➔ COMPLIANCE
- ➔ EMPLOYEE TRAININGS
- ➔ 3RD PARTY RISK MANAGEMENT
- ➔ VULNERABILITY ASSMENT
- ➔ PENETRATION TESTING

» ONE SERVICE INCLUDES EVERYTHING YOUR BUSINESS NEEDS.

WE BRING A HACKER'S PERSPECTIVE TO OVERALL CYBER PROTECTION AND RESILIENCE.

How NS Advance Helps SMEs Stay Compliant

At **NS Advance**, we specialize in making compliance affordable, efficient, and scalable for SMEs. Our services are designed to eliminate complexity and ensure that businesses of all sizes can meet regulatory requirements without overwhelming their resources.

Our SME-Focused Compliance Solutions Include

1. **Regulatory Compliance Audits**
   - Conduct gap analysis against frameworks like GDPR, ISO 27001, NIST, PCI DSS.
   - Provide actionable recommendations for improving security posture.
2. **Automated Compliance Monitoring**
   - AI-driven tools to track compliance in real-time.
   - Automated reporting to simplify regulatory filings and reduce manual work.
3. **Cybersecurity Awareness & Compliance Training**
   - Educate employees on security best practices and compliance responsibilities.
   - Provide phishing prevention training and secure data handling workshops.
4. **Incident Response & Data Breach Management**
   - Ensure SMEs have a rapid-response plan in place for cyber incidents.
   - Assist in forensic investigations and regulatory reporting following a breach.
5. **Affordable vCISO (Virtual Chief Information Security Officer) Services**
   - Offer cost-effective compliance leadership for SMEs who cannot afford a full-time CISO.
   - Provide ongoing advisory services to maintain cybersecurity readiness.
6. **Supply Chain & Vendor Risk Management**
   - Ensure that third-party vendors meet compliance standards.
   - Conduct risk assessments to identify vulnerabilities in partner networks.

How NS Advance Helped an SME Achieve Compliance

Requirement

- A growing fintech startup was struggling with PCI DSS compliance while handling customer payment data. Without the necessary expertise, they risked losing partnerships with banks and payment processors.

Solution

- Conducted a compliance gap analysis.
- Implemented an AI-driven security monitoring system.
- Trained employees on secure payment handling.

Result

- Within three months, the startup achieved full compliance, secured its financial transactions, and built stronger relationships with its banking partners.

The Future of SME Cybersecurity Compliance

With increasing regulatory scrutiny, SMEs can no longer afford to ignore cybersecurity compliance. However, with the right guidance, tools, and support, compliance becomes a manageable and strategic advantage. NS Advance is committed to helping SMEs navigate complex cybersecurity regulations efficiently, ensuring they remain compliant, secure, and competitive in today’s digital economy.

For SMEs looking to strengthen their compliance posture, NS Advance offers tailored security solutions that simplify the process without compromising on security.

Quicker Onboarding & Delivery.

Introduction Call

- Schedule a call to introduce our team and understand your compliance needs and cybersecurity goals.

Proposal and Agreement

- Send a detailed proposal outlining the agreed-upon services, timeline, and pricing.

Kickoff Meeting

- Conduct a kickoff meeting to dive deeper into your business and team introduction.

First Step Towards Holistic Protection

- That is all you need to get onboard with a solid protection from the lurking cyber threats.

Regulatory Compliance Checklist

To help organizations maintain cybersecurity compliance, the following checklist provides common security controls and measures required across most major data privacy and security regulations, including GDPR, ISO 27001, NIST, PCI DSS, and more. This checklist can be customized based on specific regulatory requirements.

1. Governance & Risk Management
   - Appoint a Data Protection Officer (DPO) or compliance lead.
   - Conduct a cyber risk assessment to identify potential vulnerabilities.
   - Develop and maintain a cybersecurity governance framework aligned with regulatory requirements.
2. Data Protection & Privacy
   - Maintain an inventory of personal and sensitive data handled by the organization.
   - Implement data encryption for stored and transmitted sensitive information.
   - Ensure data retention policies align with legal and business requirements.
   - Obtain explicit consent before processing personal data (GDPR & DPDP Act compliance).
3. Access Control & Identity Management
   - Implement role-based access control (RBAC) and least privilege principles.
   - Enforce multi-factor authentication (MFA) for user logins.
   - Maintain logs of user access and privilege escalation activities.
4. Network & System Security
   - Deploy firewalls, intrusion detection systems (IDS), and endpoint security solutions.
   - Regularly patch and update software, applications, and operating systems.
   - Ensure secure remote access policies for remote workers and vendors.
5. Incident Response & Business Continuity
   - Develop and test a Cyber Incident Response Plan (CIRP).
   - Implement real-time security monitoring using SIEM solutions.
   - Establish a data backup & disaster recovery (DR) strategy.
   - Define a breach notification process that complies with regulatory timelines.
6. Third-Party & Vendor Security
   - Conduct vendor security assessments before onboarding third-party providers.

- Ensure third parties sign a Data Processing Agreement (DPA).
- Require vendors to adhere to cybersecurity best practices and compliance frameworks.

7. Security Awareness & Training
    - Provide cybersecurity awareness training for all employees.
    - Conduct regular phishing simulations to assess employee preparedness.
    - Ensure IT staff receive ongoing security and compliance training.
8. Audit & Continuous Compliance Monitoring
    - Schedule regular cybersecurity audits to ensure policy enforcement.
    - Maintain logs of security incidents and responses for regulatory review.
    - Automate compliance reporting using GRC (Governance, Risk, and Compliance) tools.

By following this checklist, SMEs can proactively address cybersecurity risks, reduce compliance gaps, and build a secure operational environment. For detailed checklist and compliance services, please schedule a meeting with us.

Conclusion: Compliance is Now a Competitive Advantage

Cybersecurity regulations are no longer just about penalties and fines—they are shaping how businesses manage risk, build trust, and maintain market credibility. Organizations that proactively embrace regulatory compliance as a core business function will be better positioned to thrive in 2025’s rapidly evolving digital landscape.

Footnotes & Sources

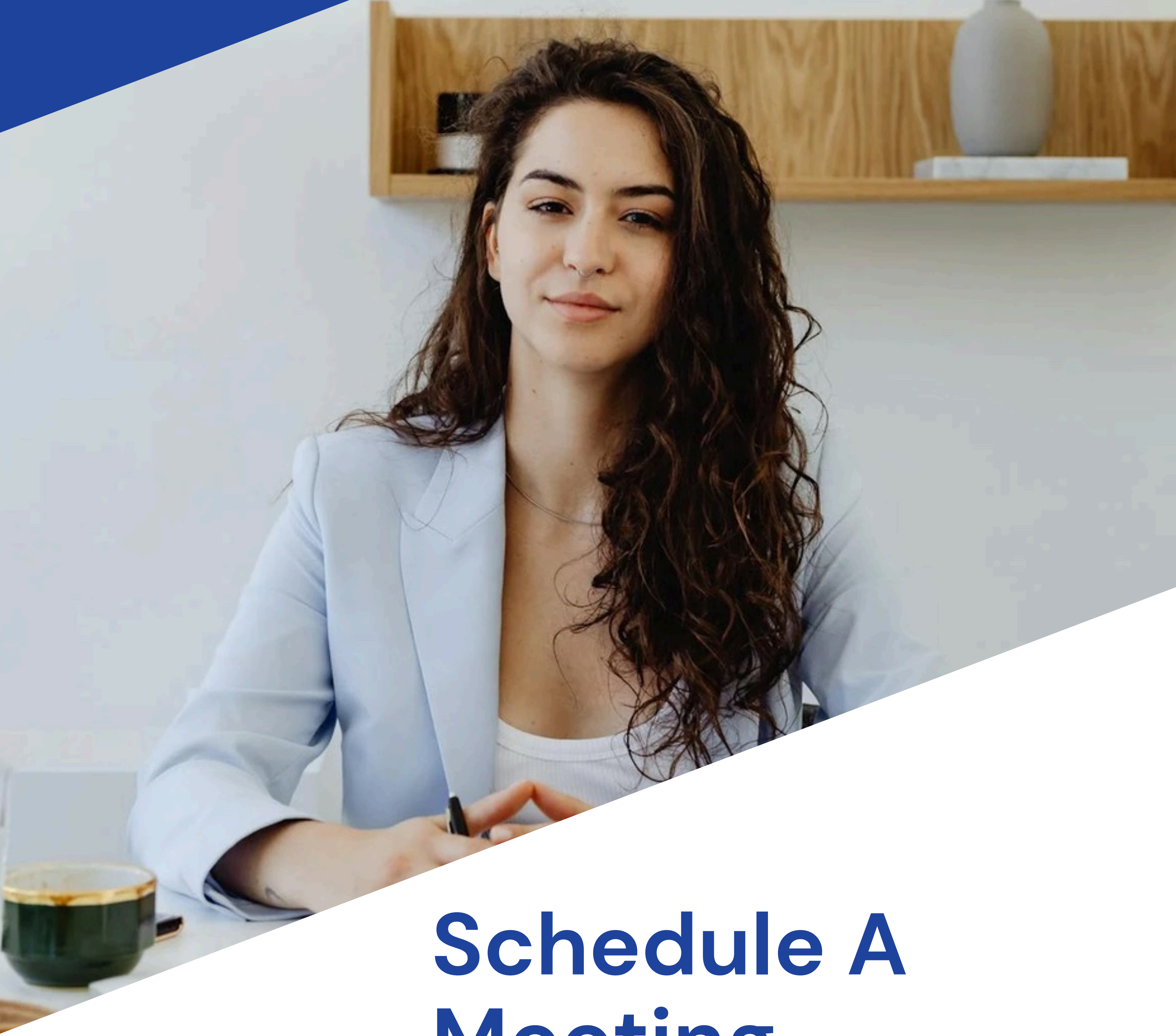
[1] European Commission, "NIS2 Directive: Strengthening Cybersecurity in the EU", 2024.

[2] U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure", 2024.

[3] China National Cybersecurity Administration, "Implementation Guidelines for the Data Security Law", 2024.

[4] Government of India, "Digital Personal Data Protection Act (DPDP)", 2024.

[5] Middle East Cybersecurity Alliance, "Regulatory Developments in Gulf States", 2024.



Schedule A Meeting Today.

NS ADVANCE

PROTECTING WHAT'S GOOD

🌐 https;//nsasec.com

✉ hello@nsasec.com

☎ 040-246-3074