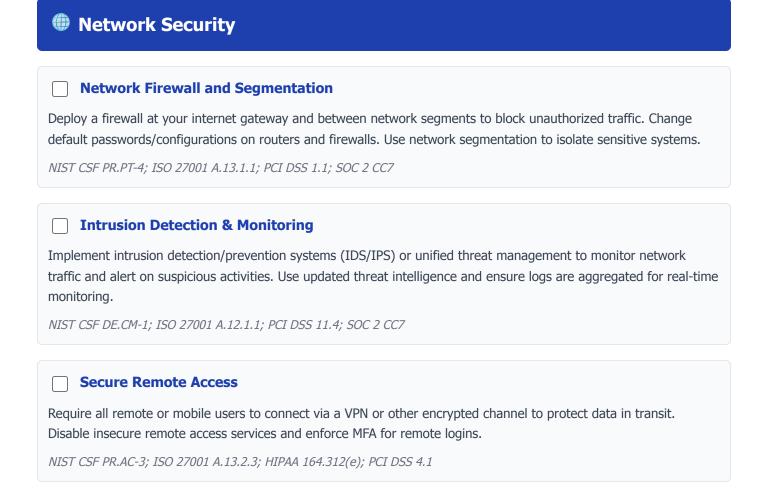
Comprehensive Cybersecurity Self-Assessment Checklist for SMBs

Small and medium-sized businesses should use this checklist to evaluate their cybersecurity posture across core domains. Each item maps to major security frameworks (NIST CSF, ISO/IEC 27001, HIPAA, PCI DSS, SOC 2, GDPR) where applicable.

Access Controls
Implement Strong Authentication
Require unique user IDs and multi-factor authentication (MFA) for all user logins, especially administrators. This reduces risk of credential theft by adding layers beyond passwords.
NIST CSF PR.AC-7; ISO 27001 A.9.4; HIPAA Technical Safeguard; PCI DSS 8; SOC 2 CC6; GDPR Art.32
Enforce Least Privilege
Adopt role-based access control (RBAC) so employees only access what their role requires. Maintain a formal access control policy and grant minimum necessary privileges. Regularly review user access rights and remove or adjust privileges as roles change.
NIST CSF PR.AC-4; ISO 27001 A.9.1; PCI DSS 7; SOC 2 CC5; GDPR Art.25
Timely Provisioning & De-Provisioning
Establish procedures to approve, create, and terminate accounts promptly. Immediately revoke access for departing staff or contractors to prevent unauthorized access.
NIST CSF PR.AC-1; ISO 27001 A.9.2.6; PCI DSS 8.1; SOC 2 CC6.2
Monitor and Audit Privileged Access
Track administrative account use and log all privileged activities. Regularly audit administrative accounts for misuse. Use just-in-time access or session recording for high-risk admin sessions where possible.
NIST CSF DE.CM-3; ISO 27001 A.12.4; PCI DSS 10; SOC 2 CC7.2



Wi-Fi Security

Secure wireless networks with strong encryption (WPA2 or WPA3) and a strong passphrase. Hide your SSID and use a separate guest network for visitors. Change admin default credentials on all access points.

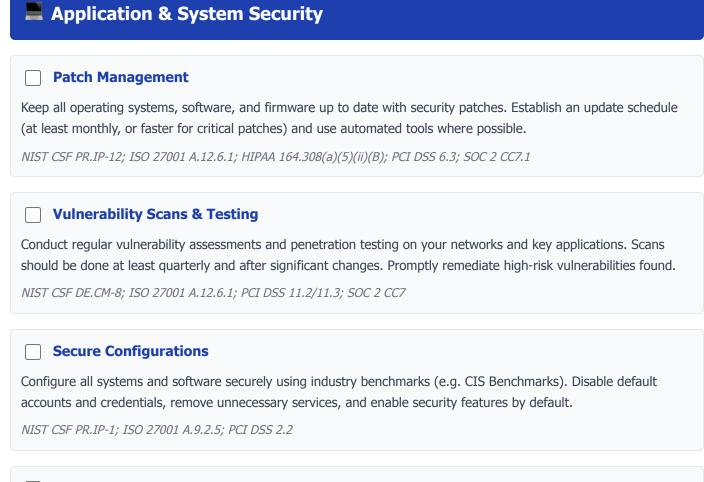
ISO 27001 A.13.1.1; PCI DSS 4.2

Data Encryption	
	st and in transit using strong encryption algorithms. Use AES-256 encryption for data storage and enforce SSL/TLS for all data in transit.
NIST CSF PR.DS-1; ISO 2700	01 A.10.1; HIPAA 164.312(a)(2)(iv); PCI DSS 3.4; GDPR Art.32
Regular Backups	
	ackups of critical data and systems, and test your ability to restore them. Follow the "3-; es in different locations/media, including offsite/cloud backups.
NIST CSF RC.RP-1; ISO 2700	01 A.12.3.1; HIPAA 164.308(a)(7); PCI DSS 12.10
Data Retention &	Disposal
·	icy to keep personal and business data only as long as needed and securely delete it Make sure to dispose of sensitive information properly in compliance with regulations.
ISO 27001 A 8 3: GDPR Art	5 & 17; HIPAA 164.310(d)

Data Loss Prevention

Use Data Loss Prevention (DLP) tools or other controls to monitor and prevent unauthorized data exfiltration. Implement policies and train employees on proper data handling.

NIST CSF PR.DS-5; ISO 27001 A.13.2.1; GDPR Art.25



Secure Development (if applicable)

If you develop or customize applications, integrate security into the SDLC. Follow secure coding practices to prevent common flaws (e.g. OWASP Top 10 web app risks). Require code reviews and use security testing tools.

PCI DSS 6.6; ISO 27001; OWASP Top 10

☐ Incident Response Plan			
Develop a documented incident response plan that defines procedures and roles for handling cybersecurity incident			
Include steps for preparation, detection, analysis, containment, eradication, recovery, and post-incident lessons.			
NIST CSF RS.RP-1; ISO 27001 A.16.1.5; HIPAA 164.308(a)(6); PCI DSS 12.10			
Communication & Notification			
Communication & Notification			
Incorporate clear communication protocols in the IR plan for both internal escalation and external notifications. Know your obligations for breach notification (GDPR: 72 hours, HIPAA: 60 days).			
GDPR Art.33; HIPAA 164.408; State breach notification laws			
_			
Training and Drills			
Train your team on incident response procedures and conduct periodic drills or tabletop exercises. Simulate realistic attack scenarios to test your response plan and readiness.			
NIST CSF RS.IM-1; ISO 27001 A.16.1.6; SOC 2 CC7.3			
Detection & Logging			
Deploy centralized logging and monitoring (SIEM) to aggregate system and security logs and flag anomalies in real time. Implement alerting for suspicious activities.			
NIST CSF DE.CM-3; ISO 27001 A.12.4.1; PCI DSS 10.6			
Recovery and Continuity			
Recovery and continuity			
Develop and test a business continuity and disaster recovery plan so you can restore operations after an incident.			

Incident Response & Recovery

Identify critical systems and data, and prioritize their recovery.

NIST CSF RC.CO-1; ISO 27001 A.17; HIPAA 164.308(a)(7); SOC 2 CC8



NIST CSF PR.AC-5; ISO 27001 A.6.2.1; BYOD policies

Cloud Account Management Apply strict access controls in cloud platforms just as you would on-premises. Use least privilege IAM roles and unique accounts for each user/service. Enable MFA for cloud console logins. NIST CSF PR.AC-4; ISO 27001 A.9.2; SOC 2 CC6.3 **Secure Cloud Configurations** Continuously review your cloud resource configurations for misconfigurations. Use security groups and firewall rules to restrict traffic – adopt a default deny stance and only open required ports/IPs. Cloud Security Alliance; CIS Cloud Benchmarks **Cloud Monitoring and Assessment** Enable cloud-native monitoring services and send logs to a central SIEM for real-time oversight. Use threat detection services to catch anomalous behavior in the cloud. ISO 27017/27018; SOC 2; Cloud provider security standards **Cloud Data Protection** Leverage your cloud provider's security features to protect data. Enable encryption for cloud storage and databases. For regulated data, verify your cloud provider can support compliance. PCI DSS 3.4; GDPR Art.32; HIPAA Business Associate Agreements

Cloud Security Configuration

Keep an updated inventory of third-party vendors and categorize each by the sensitivity of data or systems they nandle. Rank vendors by risk level to focus due diligence efforts.		
credentials. Ask for recent security		
For GDPR, require Data Processing		
, review their security reports annually		

Vendor termination best practices; Data deletion requirements

User Awareness and Training **Security Awareness Training** Implement a comprehensive security awareness training program for all employees on a regular basis. Cover topics like phishing, social engineering, safe internet use, and incident reporting. NIST CSF PR.AT-1; ISO 27001 A.7.2.2; HIPAA 164.308(a)(5); PCI DSS 12.6 **Phishing Simulations and Drills** Regularly test your employees with simulated phishing attacks and social engineering exercises to gauge their vigilance. Use results as teachable moments to improve training. SOC 2 CC3.2; GDPR Recital 39; Security awareness best practices **Strong Password Hygiene** Enforce a robust password policy and educate users on proper password hygiene. Require long, unique passwords and consider providing a password manager to help users manage credentials. NIST SP 800-63; ISO 27001 A.9.4.3; PCI DSS 8.2; GDPR Art.32 **Clear Policies and Reporting Culture** Establish clear acceptable use, security, and privacy policies and ensure all personnel read and sign off on them. Foster a culture where employees feel responsible for security. NIST CSF; ISO 27001; Security culture frameworks

How to Use This Checklist:

- 1. Review each section and check off items that are already implemented
 - 2. Identify gaps in your current cybersecurity program
- 3. Prioritize improvements based on your risk profile and compliance requirements
 - 4. Regularly revisit this checklist to adapt to new threats and requirements

Remember: Cybersecurity is an ongoing process. This checklist aligns with best practices from major compliance frameworks including NIST CSF, ISO 27001, HIPAA, PCI DSS, SOC 2, and GDPR.

For professional penetration testing and security assessments, contact Inventive HQ.