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

Network Security

Network Firewall and Segmentation

Deploy a firewall at your internet gateway and between network segments to block unauthorized traffic. Change default passwords/configurations on routers and firewalls. Use network segmentation to isolate sensitive systems.

NIST CSF PR.PT-4; ISO 27001 A.13.1.1; PCI DSS 1.1; SOC 2 CC7

Intrusion Detection & Monitoring

Implement intrusion detection/prevention systems (IDS/IPS) or unified threat management to monitor network traffic and alert on suspicious activities. Use updated threat intelligence and ensure logs are aggregated for real-time monitoring.

NIST CSF DE.CM-1; ISO 27001 A.12.1.1; PCI DSS 11.4; SOC 2 CC7

Secure Remote Access

Require all remote or mobile users to connect via a VPN or other encrypted channel to protect data in transit. Disable insecure remote access services and enforce MFA for remote logins.

NIST CSF PR.AC-3; ISO 27001 A.13.2.3; HIPAA 164.312(e); PCI DSS 4.1

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 Protection

Data Encryption

Protect sensitive data at rest and in transit using strong encryption algorithms. Use AES-256 encryption for data stored on servers or cloud storage and enforce SSL/TLS for all data in transit.

NIST CSF PR.DS-1; ISO 27001 A.10.1; HIPAA 164.312(a)(2)(iv); PCI DSS 3.4; GDPR Art.32

Regular Backups

Maintain regular, reliable backups of critical data and systems, and test your ability to restore them. Follow the "3-2-1" rule: keep multiple copies in different locations/media, including offsite/cloud backups.

NIST CSF RC.RP-1; ISO 27001 A.12.3.1; HIPAA 164.308(a)(7); PCI DSS 12.10

Data Retention & Disposal

Define a data retention policy to keep personal and business data only as long as needed and securely delete it when no longer required. 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

💻 Application & System Security

☐ Patch Management

Keep all operating systems, software, and firmware up to date with security patches. Establish an update schedule (at least monthly, or faster for critical patches) and use automated tools where possible.

NIST CSF PR.IP-12; ISO 27001 A.12.6.1; HIPAA 164.308(a)(5)(ii)(B); PCI DSS 6.3; SOC 2 CC7.1

☐ Vulnerability Scans & Testing

Conduct regular vulnerability assessments and penetration testing on your networks and key applications. Scans should be done at least quarterly and after significant changes. Promptly remediate high-risk vulnerabilities found.

NIST CSF DE.CM-8; ISO 27001 A.12.6.1; PCI DSS 11.2/11.3; SOC 2 CC7

☐ Secure Configurations

Configure all systems and software securely using industry benchmarks (e.g. CIS Benchmarks). Disable default accounts and credentials, remove unnecessary services, and enable security features by default.

NIST CSF PR.IP-1; ISO 27001 A.9.2.5; PCI DSS 2.2

☐ 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 & Recovery

☐ Incident Response Plan

Develop a documented incident response plan that defines procedures and roles for handling cybersecurity incidents. 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

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

Develop and test a business continuity and disaster recovery plan so you can restore operations after an incident. 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

🖥️ Endpoint Security

☐ Anti-Malware on All Devices

Install reputable anti-virus/anti-malware protection on all endpoints (desktops, laptops, and servers) and keep it updated. Ensure solutions are set to scan regularly and update signatures automatically.

NIST CSF PR.IP-3; ISO 27001 A.12.2.1; PCI DSS 5.2; HIPAA 164.308(a)(5)

☐ Endpoint Hardening

Enforce security baselines on user machines: enable host-based firewalls, disable unnecessary software, and require strong login passwords. Limit administrative rights on endpoints and use full-disk encryption.

ISO 27001 A.8.1.1; GDPR Art.32; CIS Benchmarks

☐ Device Physical Security

Remind employees to physically secure their devices and data. Lock workstations when not in use, secure sensitive paperwork, and keep servers in locked rooms with access control.

ISO 27001 A.11.1; Physical security best practices

☐ Mobile/BYOD Controls

If employees use mobile devices or personal devices for work, implement mobile device management (MDM) or equivalent policies. Require strong authentication and the ability to remotely wipe devices if lost.

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

☁ Cloud Security Configuration

- [ ] **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

🤝 Vendor Risk Management

☐ Vendor Inventory and Risk Tiering

Keep an updated inventory of third-party vendors and categorize each by the sensitivity of data or systems they handle. Rank vendors by risk level to focus due diligence efforts.

NIST CSF ID.SC-1; ISO 27001 A.15.1.1; SOC 2 CC9.2

☐ Security Due Diligence

Before onboarding a new vendor, assess their security posture and compliance credentials. Ask for recent security audits, certifications, and independent penetration tests.

ISO 27001 A.15.1.2; HIPAA 164.308(b); PCI DSS 12.8.1

☐ Contracts & Compliance Requirements

Ensure each vendor contract includes necessary security and privacy clauses. For GDPR, require Data Processing Agreements; for HIPAA, require Business Associate Agreements.

GDPR Art.28; HIPAA Business Associate Agreements; Contract security clauses

☐ Ongoing Vendor Monitoring

Treat vendor risk as an ongoing process. Continuously monitor critical vendors, review their security reports annually, and stay alert for data breaches involving them.

NIST CSF ID.SC-4; ISO 27001 A.15.2.1; SOC 2; GDPR

☐ Vendor Termination Procedures

Have a plan to off-board vendors when a contract ends or if they are no longer trusted. Revoke their access, retrieve or confirm deletion of your data, and update documentation.

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.