

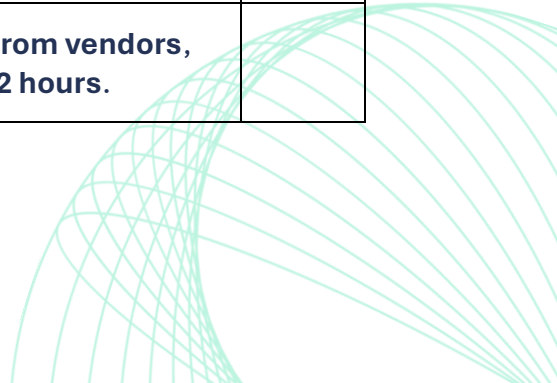
Supply Chain Cyber Security Checklist

Phase 1: Vendor Identification & Risk Assessment

| Security Measure | Action Steps | Status (✓/✗) |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Inventory All Third-Party Vendors | Maintain a centralised, up-to-date list of all vendors, suppliers, and third-party services with access to your systems. | |
| Categorise Vendors by Risk Level | Classify vendors into High, Medium, or Low Risk based on access to sensitive data, network privileges, and history of security incidents. | |
| Assess Vendor Security Posture | Require vendors to provide evidence of security certifications (ISO 27001, SOC 2, NIST 800-161, or similar) and past audit results. | |
| Review Software Supply Chain Risks | Request a Software Bill of Materials (SBOM) from software vendors to identify third-party components and dependencies. | |
| Check for History of Breaches | Investigate whether the vendor has suffered past security breaches and what remediation actions they took. | |

Phase 2: Vendor Security Standards & Controls

| Security Measure | Action Steps | Status (✓/✗) |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------|
| Contractual Security Requirements | Include mandatory security controls, breach notification timelines, and liability clauses in vendor contracts. | |
| Multi-Factor Authentication (MFA) | Require vendors to enforce MFA on all accounts with access to your systems or data. | |
| Secure Software Development Practices | Verify that vendors follow secure coding practices, vulnerability management, and regular penetration testing . | |
| Data Encryption Standards | Ensure all vendor data transfers use end-to-end encryption (TLS 1.2/1.3, AES-256, or equivalent) . | |
| Incident Reporting & Response | Demand a clear incident response plan from vendors , including breach notification within 24-72 hours . | |




Phase 3: Continuous Monitoring & Threat Detection

| Security Measure | Action Steps | Status (√/X) |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------|
| Real-Time Vendor Monitoring | Use continuous security monitoring tools to track vendor access, software updates, and unusual activity . | |
| Automated Threat Intelligence Feeds | Subscribe to threat intelligence services that alert you to vendor security vulnerabilities and active exploits . | |
| Regular Vendor Security Audits | Conduct quarterly or annual security audits to verify that vendors adhere to agreed-upon security practices. | |
| Review & Remove Dormant Vendor Accounts | Regularly review and disable vendor accounts that are no longer in use to prevent unauthorised access. | |
| Check for Leaked Vendor Credentials | Monitor dark web sources and breach databases for leaked credentials associated with your vendors. | |

Phase 4: Access Control & Zero Trust Implementation

| Security Measure | Action Steps | Status (√/X) |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------|
| Apply Least-Privilege Access | Ensure vendors have only the minimum necessary access to your systems and data. | |
| Segment Vendor Access on the Network | Isolate third-party tools, services, and accounts from core business systems using network segmentation. | |
| Zero-Trust Authentication | Implement continuous identity verification for vendor accounts rather than relying on static credentials. | |
| Restrict API & Software Integrations | Limit third-party API access to only necessary functionalities , preventing over-permissioned integrations. | |
| Vendor Employee Security Training | Require vendors to provide security awareness training for employees handling sensitive data. | |



Phase 5: Incident Response & Compliance

| Security Measure | Action Steps | Status (✓/✗) |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------|
| Include Vendors in Incident Response Plans | Ensure vendors are part of your business continuity and incident response planning . | |
| Simulate Supply Chain Attack Scenarios | Run tabletop exercises and red team assessments focused on third-party attack scenarios. | |
| Ensure Compliance with Regulatory Standards | Align vendor security policies with GDPR, PCI DSS, HIPAA, or industry-specific regulations . | |
| Cyber Insurance Coverage for Vendor Breaches | Verify that your cyber insurance policy includes coverage for third-party security incidents. | |
| Establish a Rapid Vendor Termination Plan | Have a procedure in place to immediately revoke vendor access in case of a security incident or non-compliance. | |

