

CHECKLIST

Vendor & Third-Party Risk Assessment Checklist

A practical guide for evaluating and monitoring the security risk your vendors and service providers introduce to your business.

You inherit the cyber risk of your vendors. A breach at a supplier with access to your systems or data can be just as damaging as a breach of your own network — but far harder to see coming. Use this checklist to build a repeatable vendor risk review process.

Vendor Inventory & Classification

- ☐ **Maintain a current inventory** of all vendors with access to systems, networks, or data.
- ☐ **Classify vendors by risk tier** based on data sensitivity and level of system access.
- ☐ **Identify critical vendors** whose outage or breach would materially disrupt operations.

Security Due Diligence

- ☐ **Request evidence of security controls** (SOC 2 report, certifications, security questionnaire) before onboarding.
- ☐ **Review the vendor's incident history** and breach notification track record.
- ☐ **Confirm sub-processor and fourth-party relationships** are disclosed and reviewed.

Contractual Protections

- ☐ **Include data protection and security requirements** in every vendor contract.
- ☐ **Require breach notification obligations** with a defined notification timeline.
- ☐ **Define right-to-audit clauses** for critical or high-risk vendors.
- ☐ **Confirm cyber insurance requirements** are specified for vendors handling sensitive data.

Ongoing Monitoring

- ☐ **Re-assess vendor risk on a defined cadence** — annually at minimum for critical vendors.
- ☐ **Monitor for vendor security incidents** via news alerts or threat intelligence feeds.
- ☐ **Track expiring certifications and attestations** (SOC 2, ISO 27001, etc.).

Offboarding

- ☐ **Revoke vendor access immediately** when a contract ends or scope changes.
- ☐ **Confirm data return or destruction** in writing at contract termination.

Vendor risk is reviewed once and forgotten more often than any other control area — put a recurring calendar cadence behind this checklist, not a one-time exercise.

Need Help Managing Vendor Risk?

Cenova Cyber helps businesses build and run a right-sized vendor risk program.

Contact us to get started.

www.cenovacyber.com