NET-TECH CONSULTING

Real People, Real Protection, Right Now

Risk Assessment Level 1

Rapid visibility + prioritized remediation — without a multi-quarter initiative.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Why Risk Assessment exists

Decision-grade clarity before risk becomes a business blocker.

Risk is usually discovered late

- Insurer questionnaires
- Customer security reviews
- Audit requests
- Incidents that expose unknown gaps

Most teams lack “visibility + priority”

- Tools exist — evidence doesn’t
- Policies exist — enforcement is unclear
- Remediation plans exist — status is unknown
- Resilience assumptions go untested

What a Level 1 Risk Assessment does

- Evaluate current risk exposure and maturity
- Identify undocumented or unknown policy/procedure gaps
- Cross-check against cyber insurance readiness and regulatory drivers
- Deliver prioritized remediation steps + an executive-ready summary

What the assessment is

A focused engagement that turns “we think we’re covered” into documented proof + a ranked plan.

Operator-built

- Fast discovery
- Clear scope boundaries
- Practical findings (no theory)

Framework-aligned (not framework-obsessed)

- NIST-aligned maturity snapshot
- Insurance readiness baseline
- Evidence format you can reuse

Designed to be reusable

- Executives: clear exposure + priorities
- Auditors/insurers: proof and artifacts
- IT: a sequenced remediation plan with owners

What you walk away with

Concrete artifacts you can circulate and execute against.

Core deliverables

- Risk Summary Dashboard
- Maturity Snapshot (NIST-aligned)
- Cyber Insurance Readiness Scorecard
- Remediation Priorities Matrix

Policy + plan visibility

- Policy & Plan Discovery Tracker
- Gap clarifications (what exists vs. what’s enforced)
- Recommendations for updates / ownership

Delivery close-out

- Executive debrief with report walkthrough
- Supporting documentation bundle (“evidence pack”)
- Clear next steps for remediation or ongoing governance

NET-TECH CONSULTING
Real People, Real Protection, Right Now

How it works

A structured 4-week cadence (typical).

Week 1
Kickoff

- Confirm scope + roles
- Collect diagrams + docs
- Access + logistics

Weeks 2–3
Review

- Security stack review
- Policy + plan review
- Resilience + access checks

Week 4
Draft + QA

- Draft findings
- Internal peer review
- Finalize artifacts

End Week 4
Debrief

- Executive walkthrough
- Priorities + roadmap
- Evidence package

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Assessment routes

We route to the right track based on your driver (insurance, audit, or attestation).

Route A — Business + insurance readiness

- Security stack evaluation
- Policy / compliance review
- Network & resilience assessment
- Executive exposure + remediation priorities

Route B — Eligibility validation (PCI SAQ A)

- Scope validation + payment flow notes
- Architecture review + third-party AOC
- Draft + finalize SAQ A
- SAQ A maintenance guide (optional long-term plan)

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Scope coverage (Level 1)

Four primary domains — reviewed as a system, not a checklist.

1) Security stack evaluation

- Firewall config + patching
- RMM/EDR visibility + alerting
- Backup posture + recovery testing
- SOC coverage vs. best practice

2) Policy + compliance review

- IRP / BCP / DRP / WISP discovery
- BIA + roadmap visibility
- Insurance control mapping
- Gaps + ownership

3) Network & infrastructure resilience

- Connectivity + site dependencies
- Data center dependencies
- Remote access posture + MFA

4) Business alignment + readiness

- Business context interviews
- Insurance documentation review
- Gap scoring + executive summary

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Evidence model

We don’t just identify gaps — we define the proof you’ll be asked for.

Typical evidence artifacts

- Configurations + screenshots
- Policy versions + approvals
- Access/MFA proof
- Backup and recovery evidence
- Ticketing and remediation notes

Designed for reuse

- Cyber insurance renewal
- Customer security questionnaires
- Audit requests
- Board / leadership updates

Result: evidence that travels

- Executive-readable summary + priorities
- A documentation bundle that supports the claims
- A remediation sequence you can execute immediately

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Where Risk Assessment fits

Level 1 gives you the baseline. Remediation and governance keep it from drifting.

Fast-Track Remediation

- Close your top 2–3 gaps quickly
- Document the fixes
- Package the evidence

ThreatLocker implementation

- Control what runs on endpoints
- Reduce application and data-leakage risk
- Enforce least privilege over time

vGRC + vCISO service

- Own the roadmap + evidence cadence
- Track remediation status and exceptions
- Run quarterly governance + tabletop validation

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Next steps

If you want fast clarity, we can start with a short kickoff and a defined 4-week plan.

To get started

- Confirm primary driver (insurance, audit, incident readiness, or PCI/SAQ)
- Identify stakeholders (IT + security + compliance)
- Share what you already have (diagrams, policies, insurance docs)
- We deliver an executive-ready report + evidence pack at close

Contact

Zachary Kinder | Partner
zachary.kinder@net-tech.us | 877-449-8324