QOS MSP
Managed Services

# CYBER RISK ASSESSMENT
# STRATEGY GUIDE

Six steps to find, rank, and fix your real security risks — with honest guidance on scope, cost, and what to do first.

+1 (877) 800-7672

www.qosmsp.com

# The Cyber Risk Assessment Strategy Guide

Most organizations discover their cyber risk the expensive way — after an incident. Unpatched systems, weak access controls, phishing exposure, and third-party access quietly accumulate until one of them turns into downtime, data loss, or a ransom note.

This guide is the plain-English alternative: the six steps of a practical cyber risk assessment, what each one produces, and the traps that make assessments useless.

## 1. Identify Critical Assets

You can't protect what you haven't inventoried. Start with the business functions that matter — taking orders, treating patients, making payroll — then map the technology behind them. That mapping is what lets every later finding be judged by what it actually touches.

- Servers and network infrastructure
- Cloud applications and databases
- Customer and financial data
- Business-critical applications
- The accounts and identities that hold access

### The Rule:

If losing it for a week would hurt, it belongs on the list — and the list is usually shorter than you fear.

## 2. Evaluate Threats and Vulnerabilities

Weigh real attack paths against your actual weaknesses. Most compromise is boring: phishing, stolen credentials, unpatched software, exposed remote access — not exotic zero-days. An honest evaluation looks at both what attackers do and what your environment leaves open.

- Malware and ransomware
- Phishing and social engineering
- Credential theft and weak MFA coverage
- Unpatched systems and outdated software
- Misconfigured services and cloud settings
- Third-party and vendor access

### The Red Flag:

A “risk assessment” that’s just a vulnerability-scan export. Scans find weaknesses; assessments weigh them.

## 3. Measure Business Impact

The same vulnerability can be trivial on one system and existential on another. Impact analysis is what turns a pile of findings into priorities — it connects each weakness to the operations, money, and obligations it puts at risk.

- Operational downtime
- Data loss or exposure
- Financial and recovery costs
- Regulatory penalties
- Reputational damage
- Contract and insurance consequences

### The Rule:

Rank risks in dollars and days, not scanner severity scores — nobody budgets by CVSS.

## 4. Prioritize and Remediate by Risk

Fix in order of risk, not convenience. The highest-leverage fixes are rarely glamorous: multi-factor authentication everywhere, prompt patching, access cleanup, network segmentation, endpoint protection, tested backups. A good remediation plan sequences the work, names an owner for every item, and pairs each fix with the risk it retires.

### The Red Flag:

A remediation plan with 200 items and no owner or sequence. That's not a plan — it's a to-do list nobody does.

## 5. Monitor So It Stays Fixed

Risk drifts back: new accounts, new systems, new vendors, new exceptions "just for now." Monitoring keeps the assessment's gains; periodic re-assessment catches the structural changes monitoring can't.

- Log and alert monitoring
- Unauthorized-access detection
- Patch and vulnerability-scan cadence
- Scheduled access reviews

### The Rule:

An assessment is a snapshot; monitoring is the movie. Put the annual re-assessment on the calendar before the first one ends.

## 6. Prepare for the Incident Anyway

No control set gets risk to zero, so response readiness is part of risk management, not an afterthought. The goal is that a bad day stays a bad day — instead of becoming a bad quarter.

- Incident-response procedures
- Escalation and communication protocols
- Tested backup and recovery
- Documented recovery responsibilities

### The Red Flag:

Backups that have never been restored. An untested backup is a hope, not a control.

## How QOS MSP Helps

We run assessments the way practitioners do: hands-on, fixed-fee, with plain-English reporting ranked by business impact — and we stay for the remediation. Founder-led since 2007; recurring assessments are included in our Compliance plan for managed-IT clients. One honest boundary: if what you actually need is a certified audit opinion or a penetration test, we'll say so and help you scope it — the assessment tells you where those are worth aiming.

# The Final Word

Stop treating cyber risk as a feeling. Measured, ranked, and owned — that's a security program. Everything else is reacting.

## Next Step:

Get a fixed-fee assessment scoped. QOS MSP will do the scoping call at no cost: call +1 (877) 800-7672 or visit www.qosmsp.com.