Title: Six Principles of Technology Concentration Risk Management

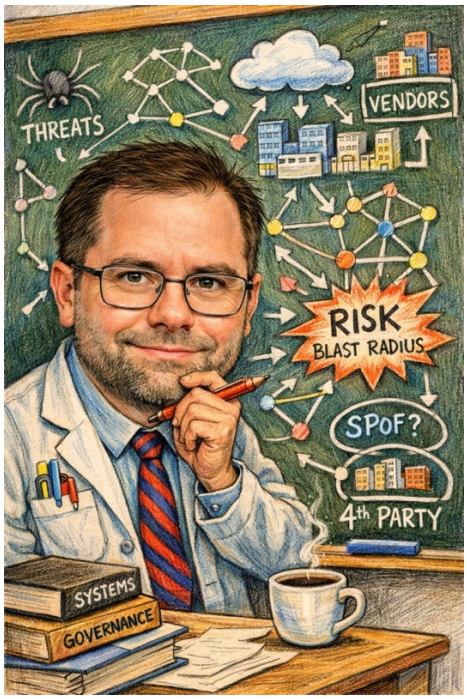
Written by: Ryan Maxwell, PMP, CISA, CISSP, Dept. of War Certified CIO

201-344-3547

ryanmaxwell@tecoris.com

March 4th, 2026

Background of the author: Ryan Maxwell has over 25 years of experience with expertise in risk management, program / project management, cybersecurity, enterprise architecture and software development. He has worked for many of the world's largest banks and on projects for the U.S. Government. He has a BA from Johns Hopkins University, an MS from the National Defense University and has numerous certifications including CISA, CISSP, PMP, AWS and CRVPM. Ryan founded the company Tecoris (TEchnology COncentration RISk) in 2025, which provides a technology concentration risk management software product and consulting services.



Introduction

Modern organizations operate within complex technology environments. Critical services are distributed across internal infrastructure, cloud platforms, outsourced providers, and their subcontractors. While this landscape enables scale and efficiency, it also introduces concentration risk. Technology concentration risk does not arise merely from reliance on specific vendors or platforms, but from structural dependency patterns that can amplify failures, disruptions, and security events. Effective management therefore requires moving beyond traditional inventory-centric approaches toward a more systemic understanding of how technology ecosystems behave.

1. It's about dependencies, not lists

Technology risk management tends to begin with collecting information about assets, vendors and applications. But concentration risk can only be gauged with dependency information. These relationships are the key to analysis. Environments with identical vendor lists, for example, may have significantly different risk profiles depending on these dependencies. Shared identity services, common network paths, centralized management planes, or tightly coupled operational processes can create hidden concentrations. Lists describe what is present; dependency analysis explains how disruption propagate. Concentration risk management must therefore prioritize mapping and understanding dependencies.

2. Distribution does not mean independence

Organizations tend to assume that a hybrid architecture, geographic dispersion or multi-vendor strategies will bring them resilience. While positive in intent, multiple systems may be reliant on shared control planes, databases, or authentication mechanisms. Complexity can mask coupling. True independence exists at the level of failure modes. Shared resources need to be identified and modeled. Effective concentration analysis must test whether components fail independently, not merely whether they appear different.

3. Concentration does not stop at the organization's edge

Traditional risk boundaries are defined by organizational control and contractual relationships. Concentration drivers, by contrast, are systemic. Third-party providers depend on subcontractors. Cloud platforms rely on upstream network operators, hardware supply chains, and regional infrastructure. Software environments inherit common libraries and services. Disruptions originating outside direct supplier relationships can propagate inward with equal or greater impact.

Managing concentration risk therefore requires extending analysis beyond immediate vendors to include fourth-party and ecosystem dependencies. Failure to account for these layers produces structural blind spots precisely where correlated failures are most likely to arise. Concentration risk is indifferent to governance boundaries. It follows dependency graphs rather than organizational charts.

4. Concentration acts as a multiplier of threats, vulnerabilities, and impacts

Technology concentration risk does not live in isolation. Instead, it amplifies existing risk factors. A vulnerability which might normally be considered small and managed, if in a concentration, can become an urgent problem. A threat actor targeting a dominant provider can produce outsized consequences. This multiplier effect alters both probability and impact. Events that might otherwise remain contained can expand into systemic incidents with a large blast radius. In the absence of technology concentration consideration, risk management can produce undersized and incomplete residual risk results.

5. Artificial intelligence alone cannot manage risk

Advances in artificial intelligence are significant and often create the impression that large language models (LLMs) will soon be capable of solving nearly any analytical problem. In the domain of technology concentration risk, this assumption is misplaced. Large organizations maintain exten-

sive, highly structured datasets describing infrastructure, services, dependencies, and control environments. Such data cannot be meaningfully conveyed through conversational prompts alone, nor can its interpretation be assumed to align with the implicit reasoning of a general-purpose model.

Concentration risk analysis requires the application of specialized analytical methods, domain-specific knowledge, and contextual understanding that extend beyond base model capabilities. Even when AI tools assist in processing or summarization, expert judgment remains essential for validating assumptions, interpreting outputs, and distinguishing material concentrations from benign architectural patterns. Results must ultimately be evaluated within the organization's operational context, strategic priorities, and risk tolerance.

Artificial intelligence is therefore best understood as an augmenting capability rather than an autonomous solution. Effective concentration risk management continues to depend on analytics, subject-matter expertise, and human interpretation.

6. Build governance, not just reports

Documents and dashboards are insufficient. Risk reduction requires governance structures capable of influencing architectural decisions, procurement strategies, and lifecycle management practices. This includes defining concentration tolerances, accountability models, escalation pathways, and integration with investment and change management processes.

Without governance, concentration analysis becomes descriptive rather than operational. Reports document conditions; governance shapes them. Effective management occurs when concentration considerations are embedded into decision-making rather than treated as periodic review artifacts.

Conclusion

Technology concentration risk management can seem like an amorphous and elusive animal. Firms pursue redundancy yet create correlated failure. Complexity is mistaken for resilience. Vendor diversification masks infrastructure convergence. Artificial intelligence increases analytical power but not understanding.

For this reason, identifying durable principles and embedding them into risk management practices is essential. Technology concentration risk is not a transient or vendor-specific concern. It is a structural characteristic of interconnected systems operating at scale. As technology ecosystems continue to expand in complexity and interdependence, concentration dynamics increasingly determine how

failures propagate, how threats scale, and how resilience must be designed. Organizations that recognize concentration as a systemic property — rather than merely a supplier attribute — are better positioned to anticipate disruptions and manage risk within modern digital environments.