

THREE TIPS FOR A STRONG THIRD-PARTY RISK MANAGEMENT STRATEGY

By Bill Fortwangler

Adjunct Faculty and Coach, Heinz College of Information Systems and Public Policy

If you want your third-party risk management program to work, you need more than policies and checklists. You need to manage the relationship from the ground up. After decades of working with vendors in complex IT environments, I've learned that the foundation comes down to three things: contracts, statements of work, and performance discipline.

1. GET THE CONTRACTS RIGHT

The master services agreement sets the tone. Make sure termination clauses, licensing models, and Consumer Price Index adjustments are clearly defined. If they're vague, you'll pay for it later. I've seen companies hit with 30–40% price increases at renewal simply because they didn't lock in licensing terms up front.

2. NAIL THE STATEMENT OF WORK

The statement of work is where most organizations stumble. Don't leave deliverables open-ended. Define *what* will be delivered, *when* it will be delivered, and *how* quality will be measured. Tie payments directly to those milestones. Think of it like building a house—you don't pay the builder just because time passed; you pay when the foundation is poured and the framing is complete.

3. MONITOR AND HOLD VENDORS ACCOUNTABLE

Your job doesn't end when the ink dries on the contract. Monitor vendor performance and measure it against the standards you set. Make sure quality metrics are in place, and don't pay for work that falls short. Vendors are partners, but they're also accountable for results.

FINAL THOUGHT

Third-party risk management isn't about paperwork. It's about building strong, enforceable agreements and holding vendors accountable. If you get contracts, statements of work, and performance discipline right, you've already solved most of the risk equation.



Bill Fortwangler is Executive Vice President and Chief Information Officer at Dollar Bank and an adjunct professor in Carnegie Mellon University's Chief Information and Digital Officer (CIDO) Certificate Program. With more than 30 years of IT leadership experience across financial services, manufacturing, and education, he is known for transforming legacy organizations into proactive, value-driven business partners. Recognized as CIO of the Year by the Pittsburgh Technology Council, Fortwangler brings a pragmatic, people-first approach to leading large-scale technology and culture

change—expertise he now shares with CIDO participants preparing to elevate their own impact as digital leaders.

Learn from leaders like Bill Fortwangler in the **Chief Information and Digital Officer (CIDO)** Executive Education Program at Carnegie Mellon University's Heinz College.

EXPLORE THE PROGRAM ►

Lead the Future of Digital Transformation

Carnegie Mellon University's **Chief Information and Digital Officer (CIDO) Certificate Program** prepares leaders to master the expanded and evolving responsibilities of today's digital-first executive - combining technology leadership with strategy, innovation, and enterprise transformation.

Why Choose CMU's CIDO Program?

- Learn from our **world-renowned experts** in technology and policy (CMU is **ranked #1** in Information & Technology Management).
- Gain the **frameworks and tools to drive digital transformation** across the enterprise.
- Explore cutting-edge topics including **AI, data strategy, cybersecurity**, and emerging technologies.
- Build a powerful **peer network** with experienced executives from diverse industries.
- Position yourself and your organization to **thrive in a rapidly evolving digital economy**.

Elevate your leadership. Expand your impact. Become the digital strategist your organization needs.

Program Logistics



~6 months



Hybrid: virtual modules, plus in-person sessions (mid-session and practicum) in Pittsburgh, with virtual option available



Virtual modules are held in the evenings (4 - 9 p.m. ET), generally on Wednesdays

