WHITE PAPER | 2026 EDITION

Operational Risk Management

Where to Start — and Where to Go Next

Prepared by

Edward T. Hawthorne, Chief Administrative Officer & Partner

CE3 Solutions, LLC

2026 Edition

This white paper is intended for informational purposes. It updates and expands CE3 Solutions' original framework to reflect the realities of the 2025–2026 risk environment.

Starting With the Right Questions

Our earlier article about RISK — what we called the "four-letter word" — generated significant interest and prompted many organizations to ask: where do we begin? This updated edition addresses that question with both the foundational framework that has proven effective for our clients and the new realities of the risk environment in 2025–2026.

I recall the moment I was tapped to serve as Risk Executive for Technology and Operations. After the initial shock, I asked the obvious question: "Why me?" The answer was straightforward — I had direct experience across technology support, change and problem management, application development, information security, business continuity, and disaster recovery. I knew where to look for risk. But knowing where to look is only the beginning.

What followed was a cascade of harder questions:

KNOW	What do I know now — and what do I not know?
ASSESS	What are the likely consequences if these risks materialize?
MEASURE	What is the future probability of occurrence for each identified risk?
CONTROL	Are current controls sufficient to mitigate impact or reduce likelihood?
ACT	What must be done, in what order, with what resources?

> **The Core Challenge**
>
> *These questions are simple to ask and difficult to answer consistently. What has always been missing is a common, repeatable methodology — a shared language and measurement system that works from the ground up, not the top down.*

The Evolving Risk Landscape: What's Changed

The operational risk landscape has always been complex, but the past several years has accelerated its transformation. The risks that earned headlines when this white paper was first written — cyberattacks, AML/KYC failures, third-party incidents — remain highly relevant. They have been joined by an entirely new category of challenges that demand immediate attention.

Emerging and Elevated Risk Areas

Risk Area	Key Considerations for 2026-2027
AI & Algorithmic Risk	Rapid adoption of AI/ML tools introduces model risk, data bias, and governance gaps. Regulators are increasingly scrutinizing AI use in credit, hiring, fraud detection, and customer communications.
Cybersecurity& Ransomware	AI-enhanced attacks, deepfake-driven social engineering, and ransomware-as-a-service have lowered the barrier for sophisticated attacks against institutions of all sizes.
Third- & Fourth-Party Risk	SaaS dependency and cloud concentration risk create systemic exposure. A single vendor failure can cascade across dozens of institutions simultaneously.
Operational Resilience	Regulators globally (DORA in the EU, FFIEC guidance in the US) now expect institutions to prove they can maintain critical services through disruption — not merely recover from it.
AML / Financial Crime	KYC and AML requirements continue to tighten. Sanctions compliance complexity has increased dramatically, and penalties for deficiencies remain severe.
Conduct & Culture Risk	Inappropriate behavior, conflicts of interest, and mis-selling remain persistent. The reputational damage from conduct failures often exceeds the direct financial cost.
Climate & ESG-Related Risk	Physical and transition climate risks are now part of mainstream operational risk frameworks. Regulatory expectations are expanding across all industries.

A Note on Scale

While the largest institutions generate the most news coverage, these risks affect organizations of every size across every industry. In many cases, smaller organizations face disproportionate impact because they have fewer dedicated resources to manage them.

The Foundation: A Shared Taxonomy & Risk Assessment Process

No matter how much the risk landscape evolves, the starting point remains the same: a well-executed risk assessment. Risk assessments analyze threats in terms of consequences and likelihood before the organization decides to accept, mitigate, transfer, or avoid each risk.

As the saying goes: “You can’t manage what you don’t know.” Most risks in any organization are already known — by the people closest to the work. The persistent problem is that Subject Matter Experts (SMEs) lack common processes, tools, and measurement systems to surface, document, and elevate those risks consistently.

This is where leadership decision-making breaks down. When each business unit uses different terminology, different rating scales, and different thresholds, the results are incomparable. Leaders are left choosing between an incomplete picture, their most confident voice in the room, or their own intuition. None of these is a risk management strategy.

The success of a risk assessment hinges on the assessment teams using a shared taxonomy. This permits assessment teams to align terminology with the business, and to aggregate results and most importantly to facilitate decisions that promote successful achievement of business objectives.

What a Strong Risk Assessment Must Deliver

1. Identify threats to the organization's business operations and strategic objectives
2. Evaluate and prioritize risks using consistent, well-defined taxonomy and measurement criteria
3. Surface connections between risks that compound each other when they co-occur
4. Align risk findings with strategic goals so that leaders can make informed trade-off decisions
5. Reduce and continuously monitor threats so they remain at or below agreed tolerance levels

Why Most Risk Programs Fail to Deliver

The risk management industry has a credibility problem. Over the past two decades, global risk programs and enterprise tools have over-promised and under-delivered — generating confusion, low adoption, and false confidence.

- Top-down over bottom-up: Programs imposed from the boardroom rarely reflect the operational realities that front-line teams understand best. Risk is found and understood where the work actually happens.
- Inconsistent taxonomy: When each department rates risks using different criteria, you cannot compare or prioritize across the enterprise. Aggregated results become meaningless.
- Tools without process: Technology cannot compensate for the absence of a clear methodology. Risk software deployed into a process vacuum produces reports, not insight.
- Governance without teeth: Identifying risks means nothing without accountability, escalation paths, and executive ownership of outcomes.
- Point-in-time thinking: A risk assessment done once a year is a historical document. Continuous monitoring is not optional — the environment changes faster than your assessment cycle.

The Real Solution

The solution is not a better tool. It is a sound, repeatable methodology implemented with genuine organizational commitment — one that engages SMEs closest to the work while maintaining clear executive accountability.

What Good Looks Like: Key Diagnostic Questions

Organizations that manage risk effectively can answer yes to each of the following. If your answer is uncertain or no, that gap is where to begin.

✓	Does your company have a documented, repeatable risk assessment methodology?
✓	Do you have adequate, knowledgeable resources and tools to execute it consistently?
✓	Does your process effectively surface, analyze, and prioritize operational risks — not just catalogue them?
✓	Are identified key risks explicitly aligned with your company's strategic goals and objectives?
✓	Does the process facilitate timely updates to your risk profile as the business environment changes?
✓	Does the process ensure continuous monitoring of identified risks against agreed control limits?
✓	Are your AI tools, third-party vendors, and cloud platforms included in your risk inventory?
✓	Can you demonstrate operational resilience — not just recovery capability — for your most critical processes?

CE3's Risk Management Approach: Empower

CE3 Solutions has established a streamlined approach to Risk Management, particularly suited for complex organizations with a challenging Operational Risk environment. **Empower** is an integrated risk management approach to proactively identify, evaluate, and mitigate the risks that matter to your organization. Just as importantly, it guides you in identifying risks that may limit your ability to innovate and grow.

Empower's value proposition and fundamentals are centered around:

- Taxonomy
- Assessment
- Action
- Integration
- Culture
- Governance

These fundamentals are further defined and discussed in other CE3 White Papers available at:

CE3 Solutions - Home

How CE3 Solutions Can Help

CE3 Solutions is a boutique management consulting firm whose partners have collectively over 100 years of experience directly managing operational risk, customer experience, employee engagement, and business optimization across numerous Fortune 500 organizations and institutions of all sizes.

We work with clients starting from scratch and those who have a program in place that is not delivering results. Our engagements are practical and grounded — we have led these processes ourselves, which means we move faster and more effectively than teams working through these challenges for the first time.

Our approach is built on a bottom-up methodology that engages your SMEs, establishes consistent taxonomy and measurement, and connects risk findings directly to strategic decision-making — without the overhead and complexity that too often get in the way of actual results.

Our Core Service Areas

- **Risk Management:** Assessment methodology design, risk inventory development, control evaluation, governance framework build-out
- **Operations & Service Optimization:** Process redesign, operational resilience planning, third-party risk management
- **Customer Experience Enhancement:** Risk-aware CX strategy, complaint analysis, regulatory alignment
- **Employee Engagement:** Embedding risk culture, SME enablement, leadership alignment
- **Human Resources:** Conduct risk frameworks, policy development, workforce planning

> **Ready to Start?**
>
> *Contact us at ce3solutions.net to discuss your risk management needs. The right starting point is a conversation.*

About the Author

Edward T. Hawthorne is Chief Administrative Officer and Partner with CE3 Solutions, LLC. He has extensive experience as a Risk Executive for Technology and Operations, with a background spanning technology support, change and problem management, application development, information security, business continuity, and disaster recovery. CE3 Solutions partners have collectively over 100 years of experience directly managing risk, customer experience, and operational excellence with Fortune 500 organizations and businesses of all sizes.