Managing the Practical Risk Assessment

Jane smiled as she signed the contract—it had been a long time coming. Data availability and data integrity for her organization's advocacy work had always been an issue. Available public information was controlled by the entities her organization was trying to monitor. Detail was lacking, timeliness was nonexistent. Now their watchdog group would change all that by developing their own data analytics tool for fact-based evidence that could be acted upon. Not that Jane was ready to toast the occasion yet. Although the new contract for a vendor-developed custom data tool would bring the organization from conversation to action, she knew the project posed risk to the tiny advocacy group. Did they have the know-how to pull this off, even with a savvy software vendor? What if the budget projections were off and more capital was needed? And, what if, after all the data collection, the results were inconclusive, or the data integrity was suspect? How would they even know how to detect errors? Jane knew they had taken a huge leap and a risk that everyone was ready to accept, but did they all understand what that risk really was? She thought of the old saying, "be careful what you wish for."

ISACA® professionals know that all risk is not the same. Industry dynamics, enterprise culture, and department risk tolerance all impact what an organization is willing to do. But risk is more than a willingness to take something on. Risk needs to be reviewed and scored based on the organization's objectives, while fact checking the objectives against market trends, regulatory requirements, and more. So how can a risk professional help someone like Jane?

Practically Speaking, Culture Matters

Successful risk management is all about operational acceptance and feasibility. Industry culture plays a significant role in determining risk priorities, and having a structured risk assessment approach is crucial, regardless of industry or organization size. That said, the structure must be tailored to suit the audience. Oftentimes, the leadership teams inadvertently make risk decisions without careful deliberation on benefits and consequences. To an IT professional familiar with the rigor of methodical development, business continuity, and other technology disciplines, it seems inconceivable that planning based on prioritized value and need might be overlooked, but it often is. The standard portfolio of risk categories must be outlined and assigned ratings of importance, including these categories:

- **Financial risk**—Does the project have a clear business case outlining the required expense/

CINDY BAXTER | CISA, ITIL FOUNDATION

Is Conservation Manager for Friends of Belle Isle Marsh. She works with environmental organizations, the community, and with developers to promote compliance for a green and resilient environment for the only remaining salt marsh in the city of Boston, Massachusetts. Her work also involves collaboration with municipal and state officials to move legislation forward with the innovation that green technology provides. Baxter is pleased that technology has allowed her to reinvent her career and continue learning at every step. She had the privilege of learning technology and managing Fortune 100 client relationships at AT&T. Baxter then applied her expertise as an IT operations director at Johnson & Johnson before moving to compliance and risk management roles at AIG and State Street Corporation. Baxter continues to accept select consulting assignments through her business What's the Risk LLC, focusing on environmental risk management, inspection, and compliance enforcement. Baxter is pleased to serve as Operations Officer on the ISACA New England Chapter and is a board member on the Nantucket Lightship LV-112 Museum.

capital with projected benefits? If so, that business case can be used to determine what activities may pose too great a financial risk to be considered. If not, a business evaluation is needed to manage general project cost, funds for potential rework, or issues against the expected value to the organization.

- **Market risk**—What is the risk of losing market share by either completing or not completing the project? This risk challenges teams as they consider financial risk, since one must often spend money to get or keep a competitive edge. Understanding the competitive landscape and how actions will positively or negatively impact market share must be evaluated as risk, including financial risk, is identified.
- **Reputational/client risk**—How will the project impact the existing client base and potential new clients? A technology organization may be expected to take a risk and innovate, reducing the potential negative impact from clients. An insurance company may have a very different investor base, one which expects a conservative approach, thereby requiring a higher risk rating for cutting edge projects.
- **Regulatory/compliance risk**—Industries falling under regulatory scrutiny such as banking or healthcare must prioritize regulatory requirements with a high risk score. What might seem like a great idea from a market share perspective may be tempered by what is permissible within the confines of the law or even industry best practices.
- **Security/privacy risk**—A critical risk for many organizations across industries, this risk still varies in priority based on information used to perform the work. Privacy does not become a major concern if all information used is publicly available, for example.
- **Operational risk**—Operational risk includes all the risk factors inherent in getting the work done: employee absence, volunteers who don't show up, machines that break down, systems that fail, and unforeseen conditions such as weather or utility emergencies. Operational risk must be defined and prioritized to determine appropriate budget allocations for resources to adequately cover the risk while balancing the need to spend wisely across many organizational objectives.

It seems like a lot of work to research and discuss up front, which is why many organizations do a less than thorough job of building a risk framework. Business ideas are raised, teams get excited, and risk isn't reviewed. Yet doing nothing to assess risk is the biggest risk of all.

> It seems like a lot of work to research and discuss up front, which is why many organizations do a less than thorough job of building a risk framework.

Overcoming Barriers to Successful Risk Management

ISACA professionals can help organizations overcome the major barriers to risk profiling by providing and executing a risk framework that's feasible and practical for each organization. A feasible framework is one that the organization can execute because it has the tools and resources to perform the risk evaluation. A practical framework is one that provides enough value to the organization to merit using resources and tools versus using them on something else. Using resources, whether budget or manpower that is best used elsewhere, only devalues the benefit of the risk assessment. It is an extra step, but understanding what else is going on, what money can be spent, and what the organization's expectations are will help right-size the risk framework used. The example of Jane's advocacy group shows what must be considered by the ISACA professional to ensure that the risk assessment itself is valued and prioritized. Taking the following steps for Jane's not-for-profit can help:

- **The risk consultant must know the client and their industry well.** Knowledge, whether researched, acquired through interviews, or based on experience is the starting point before all other considerations.
- **Collaboration is crucial.** The enterprise, IT, and any vendors involved must review and assess the risk together. In some cases, legal and regulatory will participate to avoid missing any required

LOOKING FOR MORE?

- Use the *Risk Scenarios Toolkit: https://www.isaca.org/risk scenarios*
- Learn more about, discuss, and collaborate on risk and audit in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

guidelines. For a more structured evaluation of who should participate, using a responsible, accountable, consulted, and informed (RACI) grid can help ensure that all aspects are covered.

- **Adequate time must be spent to evaluate all risk factors.** Making time, with all the necessary stakeholders present, is a big request to make of any organization. Everyone is busy, but when a decision is needed regarding what risk is the right one to take, all opinions add value and save on potential rework.
- **Evaluating risk must be a repeat event.** Successful risk management occurs when people involved plan to participate more than once. A standard risk review cadence, whether annually, twice a year, or more must be established based on how fast the business or customer base is changing. Looking back at the prior risk ratings to see how close they were to reality also makes the risk review a practical, valuable undertaking.

End Results

Jane did end up hiring a risk professional after signing the data analytics contract. Practically speaking, she knew this was a huge opportunity for her organization to become a trusted advisor to the communities impacted by the big business Jane's organization monitored. Success required a solid financial assessment, especially for add-on features and functionality they might want. Data integrity was paramount, so a thorough review of security and operational risk were also key priorities for project success. All information used was public, and her organization was a small advocacy group, but the organization they monitored was regulated and Jane wasn't sure how to tackle compliance risk. It made sense to bring in a knowledgeable professional to not only educate the team and vendor on risk management, but also to help operationalize a risk plan, with appropriate controls and auditing. The result was that risk was prioritized adequately from the start and corrective action was taken in a timely manner for the high priority areas. It was worth the risk of taking on a risk consultant.