Managing IT Risk

White Paper

COMPUTER AID, INC

Managing IT Risk

White Paper

Managing IT risks is a critical component of the overall IT business plan. As today's businesses become increasingly dependent on the Internet and IT systems, the job of mitigating risks associated with the maintenance of these systems becomes more crucial and far more visible than ever before. Effective risk management provides a wide variety of benefits for the IT organization and by default the entire enterprise. Examples of those benefits include:

- Improved alignment with business objectives
- Improved quality
- Reduction in wasted effort and time
- Improved customer satisfaction within the central enterprise as well as its clients, partners, and supply chains
- Improved regulatory compliance (business and IT)

A risk is simply a problem that has not occurred. Managing risks requires the ability to anticipate problems before they occur, identify the possible impacts, and determine the probability of occurrence. Once this information is known, a decision can be made regarding the steps to prevent or mitigate the risk. For example, if the impact is low, the probability of occurrence is low, and the cost of mitigation is high, the appropriate decision may be to ignore the risk and deal with the problem if or when it occurs.

Within the IT arena, anticipating problems and mitigating risk is difficult because of the wide variety of possibilities. This is further complicated by the fact that technology changes rapidly, business requirements are in a consistent state of flux, and industry best practices are still evolving. While the constant changes increase the likelihood for problems they also make it difficult to identify and mitigate risks.

From a business perspective, a risk is the possibility that a commitment will not be realized. Commitments take many forms. For an IT organization, supporting and enabling business goals is a key commitment. In order to support this commitment, IT must ensure a processing capability along with required infrastructure and data. Government or industry regulations also impose commitments on the IT organization. Finally, there are project or support level commitments that the IT organization must achieve. Examples include completion dates, effort estimates, and time to resolve problems by priority.

IT risks are related to IT's ability to enable the tactical objectives and strategic goals of the enterprise, providing a processing capability, complying with regulations, completing projects, and supplying the required support services. A structured five-step process will ensure the visibility and understanding of all IT risks.

1. **Step 1:** Identify all commitments and the measurements or criteria for meeting the commitment. Differentiate commitments and expectations. Expectations may be unreasonable or impossible. Success requires managing expectations, making reasonable commitments, and meeting those commitments.
2. **Step 2:** Obtain agreement for all commitments and measurable success criteria.
3. **Step 3**: Ensure the organization's "Ability to Deliver" is sufficient to meet the commitments. The ability to deliver consists of technology/infrastructure, tools, staff size, staff skills, and processes all with respect to the expected completion date. Gaps between the available ability and the required ability constitute risks.
4. **Step 4:** Establish ongoing management oversight to provide the visibility and control required to track progress, ensure compliance with processes, identify issues, and mitigate risks.
5. **Step 5:** Risk identification and monitoring is an ongoing activity and must be incorporated into planning and operational processes.

The application of steps can be applied to the London Stock Exchange's TAURUS (Transfer and Automated Registration of Uncertified Stock) program. This program was developed to simplify stock ownership and make trading more efficient for all parties involved. By utilizing a central database, the LSE hoped to reduce costs for shareholders, eliminate paper waste, and cut transaction times. Prior to the advent of this undertaking, no risk management systems were ever considered or set in place. However there were no clearly delineated commitments and measurements for meeting those commitments. Without this framework no viable agreement existed for the TAURUS program and as a result the potential for a risk to be realized was exacerbated.

Soon the program became extremely complex and cumbersome. LSE was forced to rewrite almost 60% of its systems in order to reach the desired end result. The outsourcing of this entire project led to a lack of quality controls and a surplus of communication issues. After seven years of trying to complete the project, management cancelled the effort in 1993. The total estimated cost of this IT blunder was found to be $600 million.

Had LSE employed a structured risk management framework throughout the project's lifecycle, they would have avoided these issues and experienced success. Not only would the goals of the project been achieved...resulting in the planned efficiency's, but untold hours of effort and money would have been saved both directly and indirectly. While this is a well documented and extreme case of poorly built risk management framework, it clearly proves the point that defined and agreed to commitments coupled with the necessary resources is critical to a project's success. But without ongoing management oversight and visibility on an ongoing basis to monitor project activities and status against a framework, the chance of a projects success is extremely limited.