Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2JcQc5p

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

Q Our organization is considering multiple projects for developing and implementing IT-based solutions. I have checked on various websites, but could not get a detailed list of generic risk scenarios for IT-related projects. Can you help?

A Project management is a specialized area of knowledge about completing work that involves various kinds of resources within the constraints of deliverables, cost and time. Considering the proliferation of IT as an enabler for almost all areas of a business, most organizations initiate IT-related projects at one time or other. To leverage project management techniques to deliver on time and within costs, it is imperative for the organization to have a project and program management framework. (A program is a group of projects with a larger scope and a common objective.) If such a framework is not available, implementing one should be the starting point. A standard framework can be obtained from the *Project Management Body of Knowledge (PMBOK) Guide, Sixth Edition.*[1]

Key aspects of project management are identification of risk and the strategies that could be used to either mitigate or minimize the impact due to risk. ISACA's *COBIT® 5 for Risk*[2] is an excellent resource on how to manage risk. In addition, ISACA® has also published *Risk Scenarios Using COBIT® 5 for Risk*.[3] However, it is important to understand that every organization needs to develop its own scenarios depending upon internal (within the organization) and external (i.e., competition, legal, regulatory) risk factors and the nature of the project deliverables, their time lines and budget.

Listed below are a few sample generic areas of risk associated with IT-related projects that may be useful.

Project Planning and Schedule

Project planning is a key for successful completion of the project. Poor planning is the main reason for project failure. Planning requires understanding of all aspects of the project deliverables and constraints for execution of the project. The following risk factors must be considered while planning a project:

- Resource availability schedules by the project sponsor do not match the project time lines.
- The project plan is prepared considering most optimistic effort estimates.
- The work breakdown structure (WBS) omits some tasks.
- The project plan depends upon specific resources.
- Unrealistic time lines are used.
- Existing technology does not support deliverables.
- Tight time lines create pressure, resulting in reduced productivity.
- The project sponsor arbitrarily changes time lines and resource schedules.
- Staff is not familiar with the new technology required for the project deliverables.

Project Organization and Management

To execute the project plan, the project manager needs management skills to address issues arising out of risk materialization. Risk scenarios include:

- The project sponsor is not appointed by the business, and the project lacks top management support.
- Tasks take longer than pessimistic estimates.
- Resources leave the project halfway.
- Project budget is deferred/reduced.
- Specific technology is proposed that is not available locally.
- Personal issues exist among team members.
- Decision/review by management/sponsor at milestones is slow.
- Expected/mandated infrastructure is not available for testing/deployment.
- A user acceptance test resulted in a lack of acceptance.
- The go-to-market time lines are arbitrarily proposed by management, impacting the quality.
- Changes in requirements make rework necessary.
- There are delays in procurement of infrastructure required for project/testing/implementation.

Outsourcing/Third-Party Issues

Many projects require hiring third-party resources or vendors. The following situations, at the minimum, must be considered:

- The third-party (vendor) selection process does not consider the capability of vendor.
- The quality of supplies from the vendor is very low.
- Selected vendor does not have the appropriately skilled resources.
- Vendor management is out of the purview of the project manager.
- Vendor-supplied tools/hardware/services have a high learning curve or are not user-friendly.
- The contract and service level agreement (SLA) with the third party contain weaknesses such as:
  – Absence of a nondisclosure agreement
  – Undefined service levels or service levels not in line with project time lines
  – Absence of monitoring of the third party.
  – Noninvolvement of legal department, resulting in an unenforceable agreement
- Cost of outsourcing was not considered in budget.

Project Requirements Specifications

Almost all IT-related projects suffer from risk associated with scope creep due to various factors including:

- The requirements and scope have not been frozen and signed-off.
- The requirements specifications are poorly defined, resulting in frequent changes.
- The technical requirements are defined vaguely, resulting in gap in understanding.
- The project requirements specifications are signed off, but the change management process is not defined.
- The security requirements specifications are not defined in scope.

Deliverables and Quality Requirements

The quality of the deliverables depends heavily on the skills and experience of the architects, designers and developers involved in the project. Some of the issues faced when the resources are not up to expected levels are:

- Designs result in error-prone/faulty products requiring rework.
- Poor-quality software requires additional design, testing and implementation efforts.
- The specifications of the user interface are not met.
- Extra functions/modules that are not required are included.
- Response/execution speed/capacity requirements are not considered during design creating issues.
- Compatibility and interface with legacy and other systems require more effort for testing, design and implementation.
- Use of unproven, latest technology results in frequent changes in design and development.
- A requirement for a platform-independent solution takes longer to satisfy stakeholders.
- The final production environment is not available for testing and implementation.
- The testing/production environment is not configured as per policy.
- Deliverable milestones are unrealistic and affecting the quality of the deliverables.

Read more about risk factors of IT-related projects in the expanded HelpSource column which can be found exclusively online *(www.isaca.org/journal/archives/Pages/default.aspx)*.

Conclusion

The risk scenarios listed here are generic and one may use them as guidance. It is not complete list of project-related risk. The project manager needs to develop a list of possible risk scenarios depending upon the associated risk factors.

Endnotes

[1] Project Management Institute, *Project Management Body of Knowledge PMBOK Guide, Sixth Edition*, USA, 2017, *https://www.pmi.org/pmbok-guide-standards/foundational/pmbok/sixth-edition*

[2] ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/cobit/pages/risk-product-page.aspx*

[3] ISACA, *Risk Scenarios Using COBIT® 5 for Risk*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Risk-Scenarios-Using-COBIT-5-for-Risk.aspx*