



*Private equity and venture capital firms often face the threat of risk within their portfolio companies, but are not always certain of their portfolio firm's competency in this area. Risk Management within Information Technology is especially critical as it affects all operations as well as the eventual valuation of the portfolio investment. **CSC, Inc.** specializes in helping investment firms make the best technology decisions for their portfolio company's technology needs.*

This article serves as a primer for PE & VC firms who must ensure that their investments are secure and may need to proactively engage the IT management of their portfolio company. This primer can act as a template for those IT managers that are tasked with developing an IT risk management plan and who need guidelines for the process. It will also provide examples of how to implement each step and a validation structure for the investment firm to follow the process.

I.T. Risk Management Primer

The pervasive nature of technology has increasingly made information the most valuable commodity for the majority of modern organizations. It is because of this that information itself has become one of the most prevalent areas of focus regarding the management of risk within any enterprise-level business. Since risk management is the identification and control of threats that can impact an organization, few things can affect it more than a loss of data or communications.

While many organizations have a designated risk management officer, that officer may not have specific exposure to the management of technology operations. Nor is it the case that all technology managers have extensive understanding of the tenants of risk management. The components of a generalized risk management plan can be found in many well written articles in publication or online; however, the purpose of this article is to provide a step-by-step framework for the technology executive or risk manager charged with developing an IT



risk management assessment and plan for their organization with specific focus on actionable items and reporting procedures to ensure a successful project.

A well executed risk management plan for information technology is primarily a linear process with a focus on the completion of each step as a prerequisite. A recurring theme is the necessity to define terms, methodologies and goals throughout the process in order to maintain a structured and focused plan. It is for this reason that the methodology is presented in the form of the **TRMP (Technology Risk Management Plan) Step-Ladder** (see below) as each step in the process creates a foundation that enables the next step along a gradual move towards completion.



Preparation – “Gathering the Data”



Any successful enterprise risk management plan will begin in the Preparation stage which functions as a preface to the initiation of the project. Preparation focuses heavily on setting the stage for success and involves communications with management to concisely present the project. This may include the Board of Directors, any C-level executives, or whoever will be deemed as a stakeholder in the overall endeavor. It is critical to present the plan as having a clear strategic alignment with the success of the organization in order to gain "Buy-In" from management. Involving management in this stage will ensure that all parties will stay on the same page and that collaborations will be the most productive.

After approval from stakeholders, it is important to engage them in defining the entire process. It will be necessary to gain feedback on the risks faced and the expectations to create a Requirements Definition. The Requirements Definition is a list of needs the organization has identified as well as a concisely written set of goals to be accomplished by the project. Spend as much time as needed to create an unambiguous set of requirements that can be signed-off on by the stakeholders.

Examples:

- Schedule a formal meeting on the overall plan illustrating the process with a flowchart & detailed PowerPoint presentation.
- Consider launching an Intranet site to ensure a collaborative process, with "live" documents & reference materials to include stakeholders in process.
- Intranet-based surveys & questionnaire's are an excellent way to gather useful information.

Identification – "Organizing the Data"

This step of the process involves using the preliminary data gathered from stakeholders & initial meetings to make apparent the risks to the organization. The Requirement Definition document is leveraged to pinpoint the risks to different aspects of the technology department. Each definition established has explicit risks that may affect the ability to fulfill that requirement. For instance, the requirement to maintain availability of networks and data systems entails treating any threat to that requirement; hence, issues such as failure of connectivity, internal or external, power outage, operating system crash, etc. can be clearly identified as risks to be managed. This is a critical stage because the identifications made here will direct the project's efforts and allow the discovery aspects to be properly fulfilled.

The end goal of the Identification phase is to create a Risk Guide document that is a natural progression from the Requirements Definitions. The Risk Guide is a document that summarizes the results of the risk identification showing each of the recognized risks that will be addressed. The document should be concise and definitive regarding these risks so that it can be referenced throughout if there are any questions from stakeholders.

Examples:

- Schedule inclusive meetings to bring stakeholders into the decision-making process regarding the organization's risks.
- Create live poll on the Intranet allowing them to determine definitions from stakeholders input & categorization of threat.
- The Risk Guide document can be in the form of a spreadsheet which shows risks, descriptions, departments affected, systems threatened & key personnel. A Risk Guide can also include a glossary of terms that all parties within an organization have committed to using in order to maintain concise & efficient communications.

Assessment & Prioritization – "Processing the Data"

This section primarily attempts to understand the effects and extent of each risk to the enterprise, and then to create a logical hierarchy or taxonomy to be referenced when later defining the treatment of these risks. A Taxonomy of Risks is an agreed upon structure or hierarchy of risks and sources of risk which allows the risk manager to categorize and prioritize the management process.

Since the Risk Guide contains details of each defined risk, it is important to assess the impact each risk will have on the organization. Each result or impact should be recorded along with the organization's level of vulnerability to that specific risk. In addition to this, it is helpful to determine the likelihood or measureable probability of a risk, if these metrics are available. Whereas many risks and vulnerabilities are quantifiable, some are less easily measured and a qualitative approach is called for using input from the stakeholders.

Now that the risks are ranked in terms of effect and likelihood, an ordered hierarchy can be created in which the most prominent or probable risks are assigned priority. It is usually more manageable to categorize each type of risk with similarly ranked threats to organize the process, which is referred to as "grouping". Each group of risks can be assigned a mode of treatment, which is reflective of each of the data sets including impact, probability, severity and treatability.

Here is a simplified description of the standard types of risk treatment responses. Included are detailed descriptions and IT-focused examples:

Type	Description	Practical Example
Avoidance (eliminate)	Usually an elimination by removing or replacing the process or deficiency causing the risk	Dispose of old/faulty equipment, be proactive as this is the easiest treatment to implement
Reduction (mitigate)	Mitigation of risk to a more reasonable or acceptable degree	Revise the offsite storage procedure, test the Disaster Recovery Plan, upgrade the backup software, upgrade the virus protection, update any security device firmware
Transfer (outsource or insure)	Involves strategically assigning the responsibility to an outsourced provider or insuring against the threat	Reassign the backup process to an offsite provider and automate the process, contact insurance provider and discuss data loss indemnity
Retention (accept and budget)	Accepting a threat either minimal enough to work through or too large to practically resolve or insure against (such as war)	Certain risks like occasional website & internet outages can be shelved, larger risks like terrorist attacks can also be accepted as untreatable

Examples:

- If available, use any statistical metrics from insurance vendors or service providers against these measurements of risk and vulnerability to triangulate threat.
- Balance hard metrics with management’s “gut” feelings about how to prioritize the risks to the organization – this is a crucial area to work with as it represents qualitative input that personalizes the process with stakeholders.

Once the impacts & prioritizations have been established, a functioning Taxonomy of Risks will exist that can be used in conjunction with the Risk Guide to formulate a specific plan according to each of the areas can be addressed.

Planning – “Applying the Data”

The planning stage allows all the preparation and data gathering to be correlated into a workable system. Now that risks are grouped, it is best to establish a process for each level of group hierarchy. The process should include general action items for each type of group dependent on their prioritization. Checklists are highly effective in this aspect as they can detail all the supporting tasks that allow each of the groups to be addressed.

An efficient use of time at this stage is to assign groups for inactivity, designating those groups which will not be addressed for whatever reason. Those risks that are retained, or



simply do not need an action item, can be identified as such and then removed. In the course of any assessment, there are those risks that cannot be addressed, or are strategically placed out of the boundaries of a certain project; these items are then deprioritized to allow emphasis on the others.

Now that the action items for each of the groups have been established, they can be listed in a formal document for the overall process. Address each of the four types of groups by creating specific action plans for each class, and formulate a timeline for each one.

The management of resources is critical in this stage as they will define the level of practical success the plan will have. Resources, human, financial or time allocation, must be evaluated regarding each of the risks and their appropriate treatments. Ensure that each treatment will have the adequate resources by projecting the costs and needs of each step; often, it is wise to include an additional 10% margin to include unforeseen factors.

At this point in the plan generation, a framework for implementation should be in place, including list of risks grouped by class and prioritized with a detailed tasks list for each one. It will be necessary to create a palatable presentation for stakeholders to be able to move forward. Schedule a meeting to present findings and the risk management plan to the stakeholders, with a focus on the mission-critical results. A persuasive presentation will facilitate the stakeholder Buy-In. Obtaining approval is the completion of the step.

Examples:

- Certain groups like Disaster Recovery risks are mission critical, so this level of priority should have a very detailed listing of actionable items and the process for mitigation such as:
 - upgrade connectivity between sites
 - refresh all hardware and software at DR site
 - formulate real-time test of DR Plan
- Generate a step-by-step process for each type of treatment for each group in the form of a flow chart that can be distributed to the team members, or kept on an Intranet.

Implementation – “Leveraging the Data”

Once the plan is ready, it becomes necessary to establish a structure that will allow it to be put into action. Accountability is critical as the results of the risk management project will affect the entire enterprise. Determine who will be part of the team or the Steering



Committee responsible for executing the plan. Again, in order to preempt unforeseen factors, create a stage within implementation that allows for reevaluation of any risk group and its treatment by establishing a re-assessment protocol that allows for an emergency convening of the Steering Committee to address such issues. While it is impossible to plan for all events, having a process to assess, adapt and respond, mitigates this occurrence.

An announcement or Kick-Off meeting sets the stage to move forward, and effectively communicates with members of the organization to put the plan in motion. Initiate the plan according to priorities that were assigned in earlier stages. Start with highest priority groups and schedule to roll out implementation. Notify team members associated with each group and move forward with the scheduling, in order to keep the plan on track. Make sure to generate timely updates that serve as documentation and proof of progress.

Examples:

- Generate a flowchart to represent hierarchy of responsibility and contact information
- Create plan implementation scheduling and post it publicly (Intranet) to ensure all members are aware of the process
- Show definitive progress by creating timely updates and notifications via Intranet
- Monitor the implementation plan's cycle to confirm it is succeeding; adapt and change plan as necessary

Finalization – “Communicating Results from the Data”

This last stage includes preparatory steps needed to wind down the project for an organized and documented completion. A guideline would be to begin organizing the finalization step after 80% of the project's risk treatments steps have been implemented.

Generate documentation that formally states how the treatments were applied successfully, and how these risks are officially retired from the risk management process. Use this information to update the Risk Guide, which will reflect how the treated risks were handled. This effectively shows the success of the overall risk management plan, and documents it for the organization. Communicate to the stakeholders that the final stages of the risk management plan are scheduled, and that the resolution is in sight.

After the last and lowest priority risks & groups have been treated according to plan, prepare the final reporting and updates. Create a final Risk Guide that will provide closure, and document all the processes used to treat the risks, and the status of each risk after the project is completed. Schedule a Wrap-Up meeting with all stakeholders and all members of



the risk management plan team to provide the final documentation and results. A formal final presentation will convey a sense of closure for the project as it is finalized.

Finally, it is also good practice to have a post-implementation procedure in place in case issues or questions arise. Final versions of the documents, including Requirement Definition, Risk Guide, and Taxonomy of Risks, should reside in a static format (PDF) in an easily accessible location such as the Intranet, as well as in hard copies in the organization's archives. In the event of a revision or formulation of a new risk management plan, all original documentation will be on hand to be updated, adapted or modified to align with any new developments. This post-step also allows for access of information for third-parties, such as auditors and insurance personnel.

Examples:

- Create detailed PowerPoint presentation for a Wrap-Up meeting utilizing graphics that illustrate how the impact of risk has been managed
- Include printed & bound hardcopies that the stakeholders can take away so that they have solid evidence of success. Such copies should also exist in the archives for use by auditors, etc.
- Schedule a semi-yearly (twice a year) meeting to review the existing plan, confirm whether there are any new developments, and if an update is necessary

For more information on how CSC can help your firm make better investments and manage the technology of your portfolio companies, please visit our website at www.techcsc.com or contact us at info@techcsc.com

