BIZ PHYX®

TL 9000 EXPERTS

WHITE PAPER

Risk Management

Identifying and monitoring your product and service risks

Jennifer Simcox
Vice President

BIZPHYX, Inc.

Copyright © 2010, **BIZPHYX®**, *Inc.*

Introduction

One of the key additions to the R5 version of TL 9000 is the addition of a risk management requirement. While the requirement is only a single sentence, it is followed by a bulleted note that adds guidance as to the intent. Managing risks that may impact your ability to provide a product or service requested by a customer should be a common business activity; however, the recent experiences in our global economic environment has demonstrated that this effort is not as well managed as it should be. TL 9000 has taken what has long been a part of the automotive standard, TS16949, to manage their supply chain and from CMMI, to best manage projects, and has enhanced the telecommunications standard.

First, let's begin with some basic background on TL 9000. The TL 9000 quality standard is a telecommunications industry specific quality standard based on ISO 9001. It is overseen by QuEST Forum, a not for profit organization comprised of member companies within telecommunications such as AT&T, Verizon, TELUS, Alcatel-Lucent, Corning, Motorola, and many others. One of the guiding objectives of QuEST Forum is to "identify and share best practices to improve operational excellence." With the addition of risk management, we will discuss how this objective is being achieved.

Identification of Risks

All organizations need to identify the risks that can impact their product or service and control these risks to the best of their ability. Each risk is to be managed as part of the project. This can be during the design and development phases, the service delivery phase, or during any other phase that will inhibit an organization's ability to meet the requirements that were agreed upon. Examples of project risks might be a single source supplier that could negatively impact project schedules, lack of availability of qualified personnel, availability of the target network, or even the delay of the customer approval.

The initial steps are to identity the risks for your organization. Consider assembling key managers and process owners involved in your product or service life cycle to determine the potential impacts to cost, schedule, and performance within each aspect of that life cycle. Team members should review performance indicators associated with process measures. For example, if there are identified performance measures related to delivery commitments and delivery is dependent on materials provided by your customers' suppliers, a risk may be that the materials are not delivered and there will be missed due dates for an installation. These risks aligned with defined measures will allow for visibility to monitor performance while providing a context to identify critical milestones. The team should also use brainstorming and other problem solving tools to identify all potential risks including delays due to customer access to secured sites, regulatory approvals, software integration, and experience technicians. By not considering all potential impacts, an organization may miss a critical component.

Additionally, consider past projects and the aspects of the delivery that cause delays or additional effort. These may be areas where there is a new product or there is a need for an additional test or resource expertise. Review project lessons learned or corrective actions for risks that impacted a past project, such as financial obstacles internally or with customers. Lastly, include environmental impacts such as weather or natural disasters. Things like Ice storms or unusually heavy rainstorms must be accounted for when reviewing risks that could cause shipment delays, network outages, and labor shortages.

Events such as flooding, fires, earthquakes, should be assessed as a risk for projects reliant on OSP installations. Verify the alignment with other requirements of the TL 9000, such as disaster recovery and/or business continuity plan, and additional risks may be identified.

Mitigation of Risks

Once risks are identified, the effort of analyzing the impact to your projects must be performed. Again, engaging appropriate managers, process owners, and other subject matter experts is critical for this to be comprehensive. Ensure that the review of each identified risk includes determining what the indicators are for each project in which the risk may occur.

Experiences involving the use of single source suppliers continue to plague the telecommunications industry and jeopardize commitment dates. For instance, recent shortages in power systems and the receipt of damaged or defective fiber have threatened entire network deployments. As these risks are identified, it is imperative that customers consider the impact to their requirements when imposing the use of a single source supplier. Mitigating risks under these circumstances involves the partnership with your customer to determine secondary options before the deployment is impacted.

Consider assigning severity levels to each risk to identify the impact to the project or the customer. This may also take into account the probability or likelihood that the risk may occur. Critical, major, or minor risks can be grouped in order for the risks to have the most critical impact or have the most visibility. This activity will allow you to identify when management attention is required. Categorization levels may also align with your escalation requirement documented for TL 9000.

Identification of the stakeholders for each risk will ensure there is a clear responsibility for the actions related to the identified risks. Without identification, no one is accountable. These individuals will not only be ultimately responsible for monitoring, but also should provide training and identify the resources needed to respond.

Develop risk plans to determine actions needed and contingency plans. Risk plans will be more detailed based on the criticality of the risk to the project. Risk plans may include qualifying and on-boarding additional suppliers that can supplement the demand of critical equipment, cross-training employees to provide technical expertise with a time sensitive implementation, or outsourcing to gain additional bandwidth for a turn up. Developing test plans as part of a risk plan may also be an invaluable method to verify performance. As part of the risk plans, procedures may be necessary to provide guidance to all that may be involved. Predicting how to respond before the risk is realized ensures the organization is prepared to respond and that the project impact will be mitigated.

Monitoring

In order to best manage the identified risks and ensure they are not realized, ongoing monitoring is necessary. For each organization this will vary as to what method should be used. Traditional FMEA (Failure Mode Effect Analysis) tools have been used and are very effective in organizations with many identified risks and with multiple stakeholders. This tool is a formal guide that is reviewed at identified

phases of a project and is often used in conjunction with the PFMEA (Potential Failure Mode Effect Analysis) developed during project planning.

Less formal methods may be utilized just as effectively. Adding a risk management aspect to management review meetings or even to project reviews may be adequate to review the identified risks and assess their probability.

Ultimately all project risk must be reviewed regularly and in the appropriate detail to recognize and respond. The more critical the risks to the project, the more frequent the review should be conducted. The goal of risk management must always be risk avoidance and risk control.

During review sessions, it may be valuable to provide analysis of the activities and to provide visibility to the risks being monitored. This is especially critical on time sensitive risks or those that have project dependencies such as design development or supplier performance. Consider having stakeholders share not only status and progress, but also milestones where risks were not realized.

Identifying thresholds is also valuable in determining the level of risk. Much like targets for your measurements, these thresholds will allow the organization to respond as needed before there is a project impact.

Monitoring and reporting on the status of the risks identified must be done on a regular basis and must be managed at a top level. Management understanding and involvement in the monitoring activities ensures the appropriate responses are carried out when necessary.

Risk Handling

In the event that an identified risk is realized, ongoing visibility to the steps being taken is critical. Regular reporting should be provided throughout the organization with activities identified, start dates, and anticipated resolution dates. Encourage customers and suppliers to review activities to ensure results are achieved. Many customers monitor scorecard results, but by analyzing actions taken with customers a stronger relationship will emerge. The determination of who should be involved and the steps they should be taking should have been detailed prior to the event.

Once the resulting project impact has been addressed, formal reporting and lessons learned must be captured to incorporate into revised procedures and future plans.

Summary

Once your organization's risks have been identified consider if these risks are unique for a specific project or are these the same risks for each project. You may need to identify risks as your begin each new project. This will be determined by your business and by the dynamic nature of your products and services. Ongoing monitoring of these risks will ensure your business has a plan in place to respond when needed before the risk becomes a hindrance to your business. This addition will prove to be the central goal of a Quality System.

BIZPHYX offers training for TL9000 Release 5.0 as well as specific training on how to implement a Risk Management Program. If you have questions, please call us at (972)429-5560 or e-mail info@bizphyx.com.

Jennifer Simcox is Vice President of BIZPHYX, Inc., a company specializing in quality management system implementation and support for QMS registration. Jennifer has 17 years experience in the telecommunications industry and as a quality professional. She is a member of American Society for Quality, the Oversight and IGQ workgroups for the QuEST Forum, leads the New Member Peer sub-team, and is on the Leadership Council of the QuEST forum as the Secretary of the America's region. BIZPHYX is a selected QuEST Forum trainer. BIZPHYX offers several services including internal auditing, training development, and customized assessments, supplier auditing and others.