**Risk Analysis Case Study**

**Case study:** In recent year, university has computerized its examination system by using various software applications. You as a software expert need to find out Risk involved in implementation and administration.

OR

On-line Exam System is very useful for Educational Institute to prepare an exam, safe the time that will take to check the paper and prepare mark sheets. It will help the Institute to testing of students and develop their skills. But the disadvantages for this system, it takes a lot of times when you prepare the exam at the first time for usage. And we are needs number of computers with the same number of students. The effective use of "On-line Exam System", any Educational Institute or training centers can be use it to develop their strategy for putting the exams, and for getting better results in less time.

**Solution:** Identify various types of risks along with probability (High(1), Moderate(2) & Low(3)) and its effects (Catastrophic(1), Critical(2), Marginal(3) & Negligible(4)) and then decide risk planning strategy.

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Risks:** | | | |
| **Risk** | **Probability** | **Effects** | **Risk planning strategy** |
| The experience staff in the team leave the project before it is finish, or someone was ill | low | Critical | Use more than one staff for each section, which might minimize this risk. Also, manager tries to increase salary for him. |
| The methodology to solve the problem can't work in a proper manner. | high | Critical | Must be study more than one methodology to minimize this risk. |
| Budget does not enough or there is no budget. | low | Catastrophic | Put a condition in the contract if there any more expenses, the funded side must be pay it. To avoid this risk. |
| HW requirement can't come in the time. | moderate | Critical | See if there is any more time to delay the project or not. If there is no more time work by the team computers, to minimize this risk. |
| **Product Risks:** | | | |
| **Risk** | **Probability** | **Effects** | **Risk planning strategy** |
| Packages and Development tools does not enough. | high | Critical | Put a condition in the contract to increase the time of project delivery depends on the problem occur. To avoid this risk. |
| Can't found the suitable components. | high | average | Programmer must have professional programming skills to write a new code, which minimize this risk. |
| **Business Risks:** | | | |
| **Risk** | **Probability** | **Effects** | **Risk planning strategy** |
| Can't found the suitable place for meeting the team. | moderate | average | Monitoring the work by E-mail every day. To avoid this risk. |
| Damage the electricity generator. | high | Critical | There is a spare generator to avoid this risk. |
| Marketing the product system. | low | catastrophic | Distribution of advertisements, which minimize this risk. |

**Risk Case-2**

**Step 1: Identify Risks**

The first step is obvious – identify the risks you face. The trick is *how* you identify those risks. On your own, you might get locked into one way of thinking about risk, such as people suing you, so you become fixated on legal risk. But what about technological risks or funding risks or any other kind of risk?

I found a helpful way to identify the full range of risks is to address risk from three perspectives:

1. *Mission Success* – everything you do to fulfill your organizational purpose. Documents such as a *Theory of Change* or a *Logic Model*, a *Strategy Map* or a *Strategic Plan*, and a list of your programs, can help you think through your mission-related risk in an orderly way. You’ll cover everything from risks dealing with vulnerable people and staff security on the front lines to foreign governments closing access to their countries and governance issues in your own ministry.
   1. Two of the mission-related risks we identified at CCCC were 1) if we gave wrong information that a member relied upon to their detriment; and 2) if a Certified member had a public scandal.
2. *Organizational Health* – everything related to the sustainability of your ministry’s health and viability over the longer term. Think in terms of financial, human, and physical resources, your operating (business) model, and organizational structure.
   1. We listed several risks to organization health for CCCC. Among them were 1) a disaster that would shut down our operations at least temporarily, and 2) a major loss from an innovation that did not work.
3. *Environmental* – everything that is happening outside your organization that could affect either your mission success or organizational health. This includes a scan of the social, political, economic and other environments in which you operate.
   1. We identified a risk related to the sociopolitical environment.

I began the risk assessment by reviewing CCCC from these three perspectives on my own. I scanned our theory of change, our strategy map, and our programs to identify potential risks. I then reviewed everything we had that related to organizational health, which included our Vision 2020 document (written to proactively address organizational health over the next five years),  financial trends, a consultant’s report on a member survey, and a review of our operations by an expert in Canadian associations. I also thought about our experience over the past few years and conversations I’ve had with people. Finally, I went over everything we know about our environments and did some Internet research to see what else was being said that might affect us.

With all of this information, I then answered questions such as the following:

* What assumptions have I made about current or future conditions? How valid are the assumptions?
* What are my nightmare scenarios?
* What do I avoid thinking about or just hope never happens?
* What have I heard that went wrong with other organizations like ours?
* What am I confident will never happen to us? Hubris is the downfall of many!
* What is becoming more scarce or difficult for us?

At this point, I created a draft list of about ten major risks and distributed it to my leadership team for discussion. At that meeting we added three additional risks. Since the board had asked for a report from staff for them to review and discuss at the next board meeting, we did not involve them at this point.

**Step 2: Probability/Impact Assessment**

Once you have the risks identified, you need to assess how significant they are in order to prioritize how you deal with them. Risks are rated on two factors:

1. How likely they are to happen (That is, their *Probability*)
2. How much of an effect could they have on your ministry (Their anticipated *Impact*)

Each of these two factors can be rated *High*, *Medium*, or *Low*. Here’s how I define those categories:

* Probability
  + *High*: The risk either occurs regularly (such as hurricanes in Florida) or something specific is brewing and becoming more significant over time, such that it could affect your ministry in the next few years.
  + *Medium*: The risk happens from time to time each year, and someone will suffer from it (such as a fire or a burglary). You may have an elevated risk of suffering the problem or you might have just a general risk, such as everyone else has. There may also be a general trend that is not a particular problem at present but it could affect you over the longer term,
  + *Low*: It’s possible that it could happen, but it rarely does. The risk is largely hypothetical.
* Impact
  + *High*: If the risk happened, it would be a catastrophic or critical life or death situation for the ministry. At the least, if you survive it would change the future of the ministry and at its worst, the ministry may not be able to recover from the damage and closure would be the only option.
  + *Medium*: The risk would create a desperate situation requiring possibly radical solutions, but there would be a reasonable chance of recovering from the effects of the risk without long term damage.
  + *Low*: The risk would cause an unwelcome interruption of normal activity, but the damage could be overcome with fairly routine responses. There would be no question of what to do, it would just be a matter of doing it.

I discussed my assessments of the risks with staff and then listed them in the agreed-upon priority order in six Probability/Impact combinations:

1. High/High – 2 risks
2. High/Medium – 1 risk
3. Medium/High – 2 risks
4. Medium/Medium – 3 risks
5. Low/High – 3 risks
6. Low/Medium – 2 risks

I felt that the combinations High/Low, Medium/Low, and Low/Low weren’t significant enough to include in the assessment. The point of prioritizing is to help you be a good steward as you allocate time and money to address the significant risks. With only thirteen risks, CCCC can address them all, but we know which ones need attention most urgently.

**Step 3: Manage Risk**

After you have assessed the risks your ministry faces (steps 1 and 2), you arrive at the point where you can start *managing* the risks. The options for managing boil down to three strategies:

1. *Prevent*: The risk might be avoided by changing how you do things. It may mean purchasing additional equipment or redesigning a program. In most cases, though, you probably won’t actually be able to *prevent* the risk from ever happening. More likely you will only be able to *mitigate* the risk.
2. *Mitigate*: Mitigate means to make less severe, serious, or painful. There are two ways to mitigate risk: 1) find ways to make it less likely to happen; and 2) lessen the impact of the risk if it happens. Finding ways to mitigate risk and then implementing the plan will take up most of the time you spend on risk assessment and management. This is where you need to think creatively about possible strategies and action steps. You will also document the mitigating steps you have already taken.
3. *Transfer* or *Eliminate*: If you can’t prevent the risk from happening or mitigate the likelihood or impact of the risk, you are left with either transferring the risk to someone else (such as by purchasing insurance) or getting rid of whatever is causing the risk so that the risk is no longer applicable. For example, a church with a rock climbing wall might purchase insurance to cover the risk or it might simply take the wall down so that the risk no longer exists.

**Step 4: Final Assessment**

Armed with all this information, it’s time to prepare a risk report for final review by management and then the board. I’ve included a download in this post to help you write the report. It is a template document with an executive summary and then a detailed report. They are partially filled out so you can see how it is used.

The following chart is an executive summary of the complete risk analysis. Directors who would like more details on a particular risk can read the detailed analysis which follows.

|  |  |  |
| --- | --- | --- |
| Risk | Significance (Category/Impact) | Mitigation/Strategy |
| 1. Donation Revenue | Catastrophic/High | New campaign to raise monthly donors  • Consultant hired to help us develop a strong case for support |
| 2. Social media | Critical/Medium | • Media training • Learning from our peers who have suffered attacks • Responses to known issues drafted in advance • Testing of positions with peers and opponents |
| 3. Innovation | Marginal/Medium | • Financially strong • Prudent risk takers • Incremental innovation as much as possible • In-house development as much as possible |
| 4. Physical disaster | Critical/High | Comprehensive, tested, disaster plan • Back-up mirror website • Rigorous walls up to protect against electronic infiltration • Daily back up of all drives with offsite storage • Laptops equipped with Lo-Jack for tracing and wiping |

**1. Donation Revenue Falls**

Risk: Describe what the risk is

Significance: High Probability/High Impact. Explain why you made this assessment.

Mitigating Factors: Explain what you have already done to avoid the risk or at least minimize it.

• Cash reserve sufficient for three months of expenses Strategy/Action: Explain what you will do to avoid the risk, for example:

• New campaign to raise monthly donors

• Hire consultant to help us develop a strong case for support

**2. Social Media outrage**

Risk: Describe what the risk is

Significance: Medium Probability/Medium Impact. Explain why you made this assessment.

Mitigating Factors: Explain what you have already done to avoid the risk or at least minimize it. • Media training

• Learning from our peers who have suffered attacks Strategy/Action: Explain what you will do to avoid the risk, for example:

• Responses to known issues drafted in advance

• Testing of positions with peers and opponents

**3. Major loss from innovation**

Risk: Describe what the risk is

Significance: Medium Probability/Medium Impact. Explain why you made this assessment.

Mitigating Factors: Explain what you have already done to avoid the risk or at least minimize it. With each factor, expand with the point with the strategy/action/details you will implement.

• Financially strong

• Prudent risk takers

Strategy/Action: Explain what you will do to avoid the risk, for example:

• Incremental innovation as much as possible • In-house development as much as possible

**4. Physical Disaster**

Risk: Describe what the risk is

Significance: Low Probability/High Impact. Explain why you made this assessment. Mitigating Factors: Explain what you have already done to avoid the risk or at least minimize it.

• Comprehensive, tested, disaster plan

• Back-up mirror website

• Rigorous walls up to protect against electronic infiltration Strategy/Action: Explain what you will do to avoid the risk, for example:

• Daily back up of all drives with offsite storage • Laptops equipped with Lo-Jack for tracing and wiping

After preparing your report, review it and consider whether or not the mitigating steps and recommendations are sufficient, Do you really want to eliminate some aspect of your ministry to avoid risk? Do you believe that whatever action has been recommended is satisfactory and in keeping with the ministry’s mission and values? Are there any other ways to get the same goal achieved or purpose fulfilled without attracting risk?

Finally, after all the risk assessment and risk management work has been done, the ministry is left with two choices:

1. Accept whatever risk is left and get on with the ministry’s work
2. Reject the remaining risk and eliminate it by getting rid of the source of the risk

**Step 5: Ongoing Risk Management**

On a regular basis, in keeping with the type of risk and its threat, the risk assessment and risk management plan should be reviewed to see if it is still valid. Have circumstances changed? Are the plans working? Review the plan and adjust as necessary.