



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Everyone's Smart University

Project (Spring 2021)

Student Name	Mohammed Faisal Qabbani	اسم الطالب
Students I.D		الرقم الجامعي

Section

Master

Date

Thursday

18 / 03 / 2021.

Course Code

(PMG510)

Project Risk Management

Instructions:

- اخر موعد للتسليم هو يوم الخميس 2021-05-20 في تمام الساعة ٩ مساءً.
- الإجابة متاحة باللغة الإنجليزية أو اللغة العربية مع مراعاة أن تكون المصطلحات العلمية باللغة الانجليزية.
- يتم تسليم المشروع في صيغة ملف . pdf مع الالتزام نموذج الجامعة ولن تقبل أي مستندات أخرى.
- يجب مراعاة أقسام البحث الرئيسية (مقدمة Introduction، دراسات علمية سابقة Literature Review، طريقة البحث Methodology، النتائج والمناقشة Results and Discussion ، وأخيراً المراجع References . وان كان هناك ملحقات Appendices يتم إضافتها)
- يجب الالتزام بـ Theme موحد كما يلي:
- حجم الخط 12.
- نوع الخط Arial.
- لون الخط أسود.
- المسافة بين الأسطر line spacing 1.5
- عدد صفحات البحث (لا يقل عن ثلاث صفحات ولا يزيد عن ست صفحات).

Instructor's Name: Eng. Mosaab M. Hamed

Project:

Risk Identification and Analysis (Based on the project you chose in APM)

The objective of this report is to identify project risks, prepare a risk probability matrix, and carry out an analysis of selected risks. Referring to the project you select in **Advanced projects management APM course**, your task is to prepare a risk management plan that identifies potential risks in **each stage of the project** and identify risk management strategies.

From the course content and readings, you know that the overall purpose of risk planning is to anticipate possible risk events and be ready to take appropriate action when risk events occur—to eliminate or reduce negative impacts on the project.

You may wish to begin this exercise with a brainstorming about potential risks to get candidate risks “on the table” for consideration. And then identify and refine that wording for risks that have some realistic chance of occurring in this project. For example, potential weather problems present a real obstacle to completing field data collection by the planned completion date. It is also an issue that the project manager will ultimately have to plan for, as opposed to other issues such as a major disaster (e.g., your office burning down), is not a high-enough probability event that requires much time in planning. As described below, you will select several of the identified risks and carry out a risk analysis.

You will use the distilled list of risks to make a risk probability/impact matrix. The matrix will have at least three categories (high/medium/low) for probability and impact.

Remember that it is important to name risks effectively—use words that describe the risk event and point to the impact on the project (e.g., “injury of field technician disrupts data installation work”).

After completion of the risk matrix, document a risk analysis for the selected risks. This detailed documentation for that selected risk will include:

- a description of the risk and potential impacts (schedule, quality of work, cost, etc.) on the project.
- indicators or triggers that would be monitored to help identify the risk as early as possible.
- specific risk response strategies to take.

Using probability and impact matrix calculate the Expected Monetary Value (EMV) for all risks that have the impact in terms of cost \$\$.

Risk Identification and Analysis for IT Data Center

Introduction

Ensuring that adequate and timely risk identification is performed is the responsibility of the owner, as the owner is the first participant in the project. The sooner risks are identified, the sooner plans can be made to mitigate or manage them. Assigning the risk identification process to a contractor or an individual member of the project staff is rarely successful and may be considered a way to achieve the appearance of risk identification without doing it.

Literature Review

A 2015 AFCOM survey of data center professionals identified many trends. Quoting a Gartner Group study, the survey said that, "Global spending on IaaS (Infrastructure as a Service) is expected to reach almost \$16.5 billion in 2015, an increase of 32.8 percent from 2014, with a compound annual growth rate (CAGR) from 2014 to 2019 forecast at 29.1 percent, according to Gartner's latest data. It also shows that in 2014, the absolute growth of public cloud IaaS workloads surpassed the growth of on-premises workloads (of any type) for the first time. Gartner's 2015 CIO survey indicates that 83 percent of CIOs consider cloud IaaS as an infrastructure option, and (10) percent already cloud-first with cloud IaaS as their default infrastructure choice."

Methodology

There are several methods in use for risk identification. The first step in the risk assessment is to identify and evaluate risks. The risk evaluation includes assessment of the site, critical infrastructure, support infrastructure such as fire protection, security, etc., evaluation of existing equipment as it pertains to age, serviceability, capacity, etc., identification of single points of failure, determining the probability of occurrence for individual risks and recommending corrective actions to mitigate the risks.

The next step is to develop a plan for mitigating the risks. This includes developing policies and procedures for infrastructure upgrades and improvements, planning for shutdowns or providing back-up infrastructure to maintain uptime and developing emergency action plan and schedule that aligns with organizational goals. Once the plan is reviewed and approved by appropriate personnel, the plan is executed, and upgrades and improvements are implemented as per the plan. The results of the execution are reviewed on a regular basis and policies and procedures are refined as needed to ensure continuous alignment with the organizational needs.

Results and Discussion

As discussed previously, the purpose of the risk assessment is to assess the overall site, reliability, critical electrical and mechanical infrastructure, fire protection, communications and security. The assessment identifies single points of failure in the critical electrical and mechanical infrastructure and provides recommendations and estimated costs to mitigate the risks. The assessment report delivers a clear understanding of the capabilities of the existing data center site and can be used as a performance improvement plan to optimize future capital and operational expenditures. There is a negative risk (or threat) with a 10 percent probability of prohibiting the execution of a work package. If that risk happens, the impact of not executing the package is estimated at \$40,000. For the same work package, there is a positive risk with a 15 percent probability and impact estimated at a positive \$25,000. Should you execute the work package?

Answer:

EMV for the threat = $P * I = 10\% * (-\$40,000) = -\$4,000$

EMV for the opportunity = $P * I = 15\% * (+\$25,000) = \$3,750$

Now, the EMV = $-\$4,000 + \$3,750 = -\$250$

Obviously, you do not want to execute the work package, because you will lose money on it. When a work package or activity is associated with a risk, you can find the individual EMV. In other words, you quantify the individual risks.

That covered EMV for an individual work package. How about the overall project risk? A project, after all, will have many work packages, right? To figure this out, you calculate the EMV by multiplying the value of each possible outcome (impact) by its likelihood of

occurrence (probability) and then adding the results which leads us back to our original topic. A common use of EMV is found in decision tree analysis.

Following the initial risk identification phase, the project director should have a working list of risks that have been identified as potentially affecting the project and categories them as follows:

Low Impact, Low Probability

Risks that can be characterized as both low impact and low likelihood of occurrence are essentially negligible and can usually be eliminated from active consideration. The main concern of the owner's project director is to monitor these factors sufficiently to determine that the impact or likelihood does not increase.

High Impact, High Probability

Risks that are characterized as both high impact and high likelihood of occurrence often cause a project to be terminated, or to fail if it is continued despite the risks. In this situation, the owner's management must determine if the project should be terminated or if the project is so mission critical or the potential benefits are so great that taking the risks is justified. Risk management does not imply that no risks are taken; it means that the risks taken should be calculated risks. For example, an owner may decide to proceed if there is a reasonable expectation that enough engineering or management effort can reduce either the impact or the likelihood of the events, such that the risk can become either low impact, high probability or low probability, high impact. Often such a decision is contingent on achieving the necessary risk reductions by some deadline.

Low Impact, High Probability

Low-impact, high-probability risks are those largely due to uncertainties about a number of elements that may be individually minor risks but that in the aggregate could amount to a significant risk. These include uncertainties concerning the actual costs of labor and materials (such as steel), the actual durations of activities, deliveries of equipment, productivity of the workforce, changes due to design development or the owner's preferences, and other uncertainties that are typically considered to lie within the natural variability of project planning, design, construction, and start-up (they do not include

catastrophic events or radical design changes). Each of these uncertainties, taken alone, would have little impact on the project. However, taken together, there is the possibility that many of the estimates of these factors would prove to be too optimistic, leading.

High Impact, Low Probability

High-impact, low-probability events are rare occurrences, and therefore it is very difficult to assign probabilities to them based on historical records. Data do not exist, and so subjective estimates of probabilities are necessary.

Conclusion

Although above model's analysis lack the computational complexity of stochastic risk assessment techniques, for most practical applications they are more than adequate. From the standpoint of the owner, the purpose of project risk assessment is to minimize the impact of uncertainty on the project. How this is best accomplished will vary with circumstances, but, in general, simple direct methods have proven themselves in practice. This does not discount the value of stochastic models, but their application needs to be considered in terms of their contribution to risk management. Probabilistic simulations are of value when data are sparse, and the full range of possible adverse events cannot be easily inferred. Provided that enough simulations are performed, boundaries for total project risk can be established. However, for most projects, it is the committee's collective experience that the simpler models are more useful for generating risk estimates that can be used in day-to-day project management.

References

- FCOM (2015). AFCOM's 2015 State-of-the-Data Center Survey, <http://www.afcom.com/news/dcm-digital-issue-afcoms-2015-state-data-center-survey/>, (Accessed February 22, 2016).
- Burt, C. (2017), Gartner Projects Worldwide IT Spending to Reach \$3.5 Trillion in 2017, <http://www.thewhir.com/web-hosting-news/gartner-projects-worldwide-it-spending-to-reach-3-5b-in->

2017, (accessed November 13, 2017).

Ceballos, J., DiPasquale, R. and Feldman, R. (2012). Business Continuity and Security in Datacenter Interconnection, Bell Labs Technical Journal 17(3), 147–156.

Engemann, K. J. and Henderson, D. M. (2012). Business Continuity