Risk Identification and Countermeasure Analysis of the Emergency Platform R&D Project

Xuan Deng [1] Yinghua Song[2]

[1]School of Management, Wuhan University of Technology, Wuhan, China, 430070
[2]School of Management, Wuhan University of Technology, Wuhan, China, 430070

Abstract

This paper mainly pointed out the necessities of risk management for research and development project, then identified the project risk and analyzed the corresponding strategy for research and development projects of emergency platform in accordance with the sequences of requirements analysis phase, the software development stage and configuration implementation phase.

Keywords: R&D project risk management, emergency platform, risk identification, countermeasures

1. Introduction

Risk is widespread in the world and also exists in the project. Compare with the general project, R&D project tend to have a higher risk. So it is necessary to implement the risk management in the project management for R&D project: According to the statistic, 33% of failed R&D projects are caused by the lost of risk management. In addition, development project, especially the IT project, tends to have a higher risk, so it is important to provide a higher implementation level of project risk management in such a complex system project. In recent years, as the typical manifestation of IT in emergency management, the emergency platform is widely used in the world and its R&D project belongs to IT projects. So it is necessary to implement the project risk management especially in respects of risk identification and corresponding measures.

2. Risk Identification

Initial recognition. Emergency Platform R&D project is an IT class R&D project. Its risk identification can follow the general routine for such R&D project risk identification. For IT class R&D projects, priorities include requirements analysis phase, the software development stage as well as configuration and implementation phase. Requirements analysis phase project refers to the approval, issuance of the plan and all preliminary preparation process. This stage mainly involves with the risk of management; while software development stage refers to the entire emergency platform technology development process, including design, coding, testing. This stage is mainly involved with the technical aspects of risk; Configuration and implementation phase refers to the installation on the device after all software development, and then applied to the actual Emergency Management which, at this stage is the risk of application. The stage and the corresponding risk initially identified as follows:

(1) The needs analysis phase

①Project demand risk. Emergency platform is a game of chess, it relates to the problem of sharing information; the overall

implementation of the framework should be carried out under the unified arrangements. To achieve uniform construction standards and specifications for construction, it is significant to ensure that the system's structure is reasonable, and the design is feasible. The application of this project is mainly to serve the government departments at all levels of decision-making leadership work. As the project progresses, the needs of users continue to be activated, leading to the increase in the content of the work, the project program changes, bringing greater risk to the project.

②The organization and management risk. For instance, reporting delays in approval procedures to the relevant departments and the needs for approvals of a number of directors in various department and/or levels could cause serious impact. At the same time, due to the tight deadlines, the quality of the completion of the project is also bound to be affected; another example is whether the leaders attach importance to it or not, the level of project construction quality as well as project management level and quality of a sense of responsibility to a large extent.

(2) Software development stage

①Systemic risk. When emergencies, especially natural disasters, happen, some traditional information transmission facilities can easily be destroyed, if the emergency platform is entirely dependent on the limited types of facilities, it may be a serious spill-over effect, finally being destroyed. So the emergency platform needs connectivity with video surveillance, rescue communications, rescue command information processing, comprehensive, integrated device, both air and ground combination, a combination of wired and wireless information system, a combination of fixed and motorized; emergency platform grouped by subsystems may use many of the previously existing system in order to simplify the cost, which causes a lot of problems on the interface generated in the integration process, and insight into the internal mechanisms between the individual modules of the system has been built, also the organic integration is not an easy task.

②Outsourcing risk. For the emergency platform some functions may need to be taken during the construction project services outsourcing, so that software developers become vital factors to affect the success or failure of the system. Poor implementation capacity of the software vendors as well as the improper selection of software, information technology projects fail most direct reason. Information technology software market buckwheat mixed, the strength is not strong software company is forced by the pressure of competition, commitment or other non-normal competitive means to undertake the project, by blurring the terms of the contract and technical requirements at very low prices, not personalized development and other ways to deal with the results not only invested too much time and money, cannot achieve the system goals, but the negative impact.

(3) Configuring the implementation phase

①Monitor risk. After the system has been constructed and put into effect, the key of the system would be whether the merits could be applied and has a impact on practice to improve the efficiency of the emergency-responding system. Practice has proved that no matter how advanced information technology projects, how contractor's technical strength is strong, inevitably there will be negligence, unstable system running pre occur, hardware, network failure, technical manager of the day-to-day monitoring environment when the attitude is not serious, business unskilled of system hidden excluded timely, and will give the system's operation and maintenance pose a risk.

②Securityrisk.It is necessary to emphasiz e the data security of the emergency platform system. For a typical emergency platform, mainly rely on network security,

operating system security, database security, and application security, virus prevention, illegal invasion supervision, data change tracking, data security backup and archiving, host room safety management regulations the supervision system administrator to ensure the security of the system. Currently, the prevalence of the community does not attach importance to the security of the system, such as the user's password leaks, super user with too much authority. A direct consequence of the lack of security awareness system loopholes and flaws in the security design, it will lead to the paralysis of the system, and information leakage.

Definition of factor.

Clarified risk factor, in accordance with the emergency platform R&D based on three stages, as shown in Table 1.

Table 1. Emergency platform R&D projects risk factor

Phase	Level-1	No.	Level-2
Requirements analysis	Management risks	1	targeting unclear
		2	emphasis lack
		3	cumbersome approval process
		4	management capacity is limited
Software development	Technological risks	5	range of software development technology progress changes
		6	developers link error
		7	outsourcing quality problems
Configuring and implementation	Application risks	8	systematically compatible disorder
		9	Information Security lack
		10	Operating unsatisfactory

3. Coping Strategy

Coping strategy means that how to tackle with the risks distinguished with. There are several methods to be needed during this process, risk aversion, risk deflection, risk mitigation and risk retention. Risk aversion aims at changing the original plan to avoid risks, or changing the conditions of the risk to guarantee the realization of the original goal. Though the project team cannot avoid all the risks, it is able to avoid some specific dangers. Risk deflection means that shifting the burdens of your own crises onto others. During this process, only thing to note here is that risks do not eliminate, but only the subjects change. Risk mitigation is that reducing the probability or the damage of the happening of the risks to the standard, which can be accepted by. Risk mitigation refers to preventive measures. Under this way, it can not only reduce the costs, but also increase the effects. Finally, when it comes to risk retention, it has both positive and negative aspects. It means that the project team does not change the plan but to confront with the risks directly. Once differences are appeared between the process and the original plan, a backup system is to be needed.

(1) The lack of clear target location

Under this situation, risk mitigation needs to be selected. Here are the general coping strategies: enhance the communication with the application unit situation; sufficiently to understand business requirements; discussing the overall structure of the system, planning schemes and the design for the system functions; and accomplishing the minimum risks for demand fluctuation.

(2) The lack of enough attention

Under this situation, there are several measures, which can be used. Firstly, enhancing the communication with the leaderships can get the support from them and bring positive support for them. Then it is useful for the configuration of people, capital and goods. Secondly, enhance the responsibility of the leadership of the specific department. From the primary construction to the maintenance stage, there must be these leaders taking part in directly. It can be enhanced through signing in the responsibility books.

(3) The authorizing procedures complicated

Measures are as followed. According to the requirement of the planning management, enhance the communication with the functional departments, fund the system to adjust work, try to get the

support from these departments, speed up the bureau approval of the leadership, and make the base for the application of the project.

(4) The limitation of the management ability. Here are the measures. Fund the powerful and strong planning team to build the system of risk management. The people, who responsible for need to be smart, and make decisions under the previous situation. They can also be able to adjust all the resources make complete plans as well.

(5) The change of the process. The measures are, make the decision for the change possibility, which can make the evidence for the change; communicate with the business sections, which can help clarify the limitation. However, due to hasty plan and the change of progress, strategy selection is also a "Risk Remission". There some measures should be taken are : have full communications with the application unit , have full understanding of the business requirement, give sufficient time to make the entire project plan, preparation may quicken the work; supervise the complete situation of stage target , and hire a supervision company according to the clear requirements in the contract.

(6) Outsourcing Quality Problems.
In order to response to this "Risk transfer" choice of strategy,
the detailed measures are as followed:
require Pre-qualification; make specific and detailed requirements in the contract; employ information technology Services Company to consult.

(7) System Compatibility Disorder
In order to response to this "Risk Remission" choice of strategy, the detailed measures are as followed: Set standard criterion, to apply single standard at system port, different data properties can inter-convert within internal system.

(8) Missing information security
In order to response to this "Risk Retention" choice of strategy, the detailed measures are as followed: Set network isolation mechanism, to build a good system running environment, Set disaster recovery mechanism, to apply the method of dual-computer among different network segment simultaneously. To enhance dual-power supply, multilink back-up, ceaseless power supply concurrently.

(9) Poor Operation Skills.
In order to response to this "Risk Retention" choice of strategy, the detailed measures are as followed: Implement better training, conduct pre-qualification to ensure the quality of operation.

4. Conclusion

The role and functionality of emergency platform towards emergency management is irreplaceable, its complexity leads to t he high risk when constructing the progra m. This article will position it as an IT pr oject, while applying risk recognition and countermeasure analysis of key steps acc ording to common routines. It focuses on the determination on the nature, meanwhi le the systematic exploration of index qua ntification is insufficient.

5. References

[1] Yuhua Xu, Limin Zhou. Study on Large-scale scientific research project risk management [J]. Aviation science and technology,2004(4).

[2] Yan Jiang. scientific research project risk control based on the project capability maturity model [J]. Soft science,2009,23(6).

[3] Deying De. Risk management security system design of IT project [J]. Business research, 2006(10).

[4] Song Ying-hua. *Introduction to Emergency Management*[M]. China Economic Publishing House, 2009.