Published in AJSE, Vol:21, Issue: 1
Received on 4th January 2022
Revised on 10th April 2022
Accepted on 30th April 2022

AIUB JOURNAL OF SCIENCE AND ENGINEERING
ISSN: 1608 – 3679 (print) 2520 – 4890 (Online)

Risk Identification and Analysis in Software Development in Bangladesh IT Industry: A Hybrid Model

Tania Rahman, Shanto Kumar Saha, Md. Sajjadur Rahman Sohel, Md. Tamim Maula,
Abhijit Bhowmik, Rashidul Hasan Nabil

***Abstract*—Software risk management is a critical and multi-stage process. All over the world, IT Industries face some threats during software risk management processes. Bangladesh is not exceptional. Principal goal of the research is to manage risk for Bangladesh's IT Industry. To gain a clear and transparent idea survey is the most effective way. The research arranged a survey questionnaire and collected data for risk impact areas on Bangladesh IT Industry. A workable and feasible risk management approach prompts an idea for the risk-mitigating plan. In any case, the high proportion of IT project failures demonstrates the futility of risk mitigation activities. From the survey, it is discovered that the most irritating obstructions behind software disappointment for the presence of covered-up and inconspicuous risks and lack of user communication, and lack of proper training on new technology which is overlooked in the greater part of the models. The proposed model works with the improvement of the risk mitigation plan through four phases, the Dynamic Verifier Core (DVC) committee, and the New Unproven Technology (NUT) train-up team. Depending upon the survey replies added another unique feature called the New Unproven Technology (NUT) train-up team. The model considered all four phases of risk management, with the mitigation phase and training on new technologies receiving the greatest attention.**

***Index Terms*—Bangladesh IT Industry, NUT train-up team, Risk impact areas, Software Risk Management, Identify risk.**

I. INTRODUCTION

Software risks are genuine and painfully true for each IT Industries. The software development companies are highly agreed that it is high time to research software risks to reduce software products' failure. It is essential to maintain the critical risks of software products, services however software development. During software interaction, the software management team should be cautious about the management of variant activities. Perhaps the most important yet frequently ignored perspectives in the total interaction are risk and administration [1]. Nothing if not, in every natural environment, the ambiguity and blended danger can be observed. A proper path, techniques, and a systematic model can be dealt with the ambiguity and blended threat [2]. The vast majority of the risk investigation measures are normally multi-phase and for the most part, start with risk distinguishing proof and prompt relief in a constant cycle. According to research, risks can be reduced by establishing prerequisites, plans, designs, and executions [3]. For almost two decades, the research on risk identification and risk analysis is auspicious sector. Also, the industry has received a boisterous repercussion from the researchers and the scholars both globally. Risk is characterized as the opportunity of specific events antagonistically influencing project goals. Recently, the researchers have focused primarily on risk analysis and proposed a deserving or worthy work sequence by different risk models, applications, or techniques for mitigating risks. A sequence of excellent techniques, models, or applications can help project managers make a master decision in software risk identification. Proper risk analysis, identification, and monitoring using the models, techniques, or applications can further develop software products of risk-mitigating problems [4]. The risk reduction technique offers freedom to the software developers in pragmatic circumstances. The models or methods propose appropriate methodologies to handle the software failure that is happening for unwanted risk. The proposed methodologies would help the project managers appraise the effects of different hazards and subsequently raise software products' success rate.

Additionally, the product supervisors need to comprehend different risk alleviation factors and the common connections among them [5]. In any case, it is critical to distinguish the potential risks in all phases of the software risk analysis and overall, the software risk mitigation process. A precise alleviation system makes sure the reduction of the precise level of financial distortion and possible loss.

In this paper, there have been identified such risk impact areas with the help of a survey on Bangladesh IT Industries and mitigated risk by proposing a hybrid model with a new feature that ignored the previous researchers.

II. RELATED WORKS

There has been a lot of exploration and research done on risk identification, analysis, or investigation and there have additionally been many proposed models for risk management and risk mitigation. However, researchers essentially focused on the global IT industry there are very few studies that focus on the Bangladeshi IT industries. So subsequently, the paper has been surveyed those papers are

Tania Rahman is a BSc student of Computer Science Engineering department from American International University-Bangladesh, Dhaka-1229. Email: tania1997rumi@gmail.com.

Shanto Kumar Saha is a BSc student of Computer Science Engineering department from American International University-Bangladesh, Dhaka-1229. Email: shantosaha456@gmail.com.

Md. Sajjadur Rahman Sohel is a BSc student of Computer Science Engineering department from American International University-Bangladesh, Dhaka-1229. Email: sajjadursohel12@gmail.com.

Md. Tamim Maula is a BSc student of Computer Science Engineering department from American International University-Bangladesh, Dhaka-1229. Email: tamimmaula7@gmail.com.

Abhijit Bhowmik is an Associate Professor of the Department of Computer Science, Faculty of Science and Technology, American International University-Bangladesh, Dhaka-1229, Bangladesh. Email: abhijit@aiub.edu.

Rashidul Hasan Nabil is a Lecturer of the Department of Computer Science, Faculty of Science and Technology, American International University-Bangladesh, Dhaka-1229, Bangladesh. Email: rashidul@aiub.edu.

appropriate and closely related to this research.

A. Improving Risk Mitigation Plan through Synthesized Formula

Khatavakhotan et al. [4] developed a model for enhancing a comprehensive risk mitigation plan by focusing on the hidden risks and opportunities connected with risk mitigation decisions, which were mostly ignored in previous models. To get to a successful conclusion, the decision's prospective hazards and prospective possibilities will be assessed at the same time. Through synthesized formula, the model considered the effects of intensified and emerging opportunities. The previously specified recipe is used as part of the estimating strategy. The equation's inputs are verified or historical data as well as survey results.

B. Embedded Dynamic Verifier Core

Khatavakhotan et al. again proposed a model and the paper entitled "Embedded Dynamic Verifier Core Improving IT Risk Management Process; Towards Lowering IT Project Failure." Re-observing the performed activities and creating each stage document in the risk management process increases the model's performance without considering the preexisting technique. The proposed model in this investigation is to identify and eliminate deviations by forming an expert advisory committee with varied capabilities at various phases. Furthermore, making a powerful correspondence interface among task and association workers and Dynamic Verifier Core (DVC) experts works with the administration of new or changed risks. This connection additionally speeds up the distinguishing proof and characterization of the deviations [6].

C. A model with Four Phases including DVC

Khatavakhotan et al. improved their model in [7]. The possibility of errors or blunders at each stage of the process, as well as risk change during risk activities are two common risks experienced during the risk management process. As a result, they presented a system that incorporates highlights in order to combat the two dangers. Examining the exercises performed during the risk management process is one of the major aspects of this research. By creating a verifier core that includes risk supervisors and specialists, the suggested approach reduces risks or dangers. The verification center is dynamic since it can react to each stage, resulting in a productive and current administrative interaction. Risk identification, risk measurement, and assessment make proper autonomy for each step. The result of each stage, be that as it may, is confirmed by the Dynamic Verifier Core (DVC).

D. Simulation Optimization

Another study briefly described two standard techniques, scenario optimization and resilient optimization, which aim to overcome the limitations of traditional optimization approaches for dealing with uncertainty by uncovering excellent arrangements that are feasible in as many different scenarios as possible. Because conventional methods can't deal with issues including a huge number of choice variables and limits, as well as significant levels of uncertainty and intricacy under these conditions, they chose the simulation-optimization route. Furthermore, the cost of the simulation engine's adaptability in terms of describing alternative execution measures and risk profiles as requested by the decision-maker is controlled by the combination of simulation and optimization. The use of simulation and optimization together results in a dynamic apparatus that is quick, cost-effective, and nondestructive. Similarly, simulation optimization creates outcomes that may be easily handed on and grasped, giving the client with a convenient and easy-to-use tool for recognizing improved business options when faced with risk and uncertainty [2].

E. Spiral Development Model

The research paper established a Spiral Development model. The spiral approach is similar to the incremental strategy, but there was concern regarding the project's risk. It was being adopted by a large number of software development firms. Because users are involved early in the process, it can accommodate changes in requirements. The system or product is visualized early in this model. The process management was complex, similar to the iterative approach, because the spiral can go on for an endless period of time, making it unsuitable for short projects [9].

F. Risk Identification, Management and Avoidance Model (RIMAM)

Shahzad et al. [10] exhibited a model the RIMAM (Risk Identification, Management and Avoidance Model) model of software risk management was discussed in this document, which includes a step-by-step execution of the risk handling approach. The model used simple flowcharts to depict how each mitigation/avoidance approach works in relation to any risk factors, allowing the development team to manage the risk on a local level. Depending on the demands of the risk management activity, the organization may or may not choose to follow the RIMAM model in its entirety and may instead choose to implement a component of it. The risk factors inter dependencies were depicted in the dependence diagram in this study. Knowing that there was a danger that is depending on a number of things, it is critical to keep everything in order.

G. Survey and Comparison of Secure Software Development Standards

Ramirez et al. discussed the guidelines, standards, and certifications for software security which support any software development project written in a standardized way. There are numerous criteria and policies in place to ensure secure software development. The Open Group Architecture Framework (TOGAF), Security Assurance Maturity Model (SAMM), Building Security In Maturity Model (BSIMM), Application Security Verification Standard (ASVS), OWASP, and SAFE Code and as are national or international standards organizations such as PCI, NIST, and ISO/IEC. The survey results supported the development of a useful secure software product. Many standard and criterion requirements were not fulfilled when used individually. A standard process for creating secure software must ensure secure software application certification [11].

H. Scrum in Global Software Development: A Conceptual Framework

Projects executing agile practices in Global Software Development (GSD) are increasing rapidly, but project stakeholder distribution in GSD creates a number of issues while using some agile practices. A Systematic Literature Review (SLR) that provides proper guidance in finding papers that discuss Scrum practices in GSD projects. The identification of the main factor taking into consideration global project distribution that modifies the use of Scrum and creates a new approach that may help project managers in overcoming difficulties. A conceptual framework based on a comparison review helped in overcoming problems of Scrum practices in GSD projects [12].

I. *Measuring Risk of Software Projects*

The paper [13] proposed a model for measuring the financial risk of software. It says the project and financial risk measurement model are of great value measured risk compared to the expected value of risk. This is the software the project is at risk of unlimited cost consequences. Therefore, the maximum risk Software projects can make the experience endless. Software organization cannot be assigned unlimited resources for software project development. Also, not a project this can be done if the project parameters are not defined correctly. For this reason, Risk measurement must consider the maximum cost that a company can tolerate. Invest in the development of software projects. Based on these requirements.

J. *Risk Mitigation System for Managers*

According to [14], Risk mitigation, provides a system for managers to deal appropriately with risk by providing step-by-step execution of the risk management technique, introducing simple flowcharts to convey the working of every mitigation/avoidance process against any risk variables in IT projects. As a result, managers are better able to understand the major zones that need to be addressed in order to reduce the risk to the free and continuous flow of risk data.

This research has been followed three papers [4], [6], [7] to establish a model. This paper has been proposed a hybrid model based on the survey replies by following the concept of previous research. There has been discussed how software risk can mitigate by using the proposed model. The suggested model features an embedded dynamic verifier core and is divided into four phases, each with an embedded core for detecting deviations. In the risk management process, this will result in a better outcome [6]. The risks of the risk management process were given special attention in constructing this model, which was completed by re-monetizing the risks and exercises via the verifier core [7]. The paper has been created the model using a new feature New Unproven Technology train-up team (NUT train-up team) and earlier relevant research. The model was created to be used to create software projects, and it included the best aspects of existing models.

III. Data of Survey

A. *Survey Data Collection*

The [1]survey questionnaires have been created in a sequence so that the paper can relate with the previous literature reviews and proposed a risk mitigating model depending on the survey results. So, the paper had been conducted the [1]survey and sent the [1]survey to various IT and software related companies in Bangladesh. IT has been received a total of 174 responses on this [1]survey.

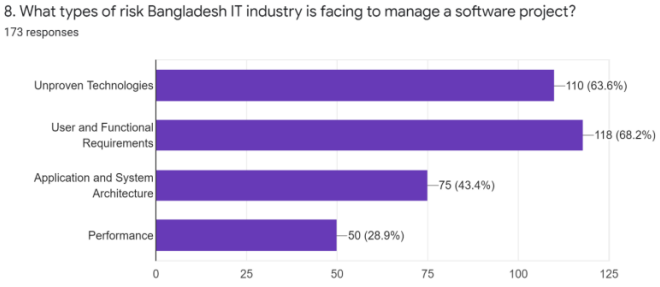

Fig. 1. Information about the Risk of Bangladesh IT industry

[1]https://docs.google.com/forms/d/e/1FAIpQLSc7qJNycnsTn2ast2gBDZgcfTADiIxv_FSZB-0gRTUD-HbYAA/viewform?fbclid=IwAR0DNXMX75dwk3CJ8QMQPWdAaiDMu329jZ2dxFuJ9imQOoXNiskrAJysBgw

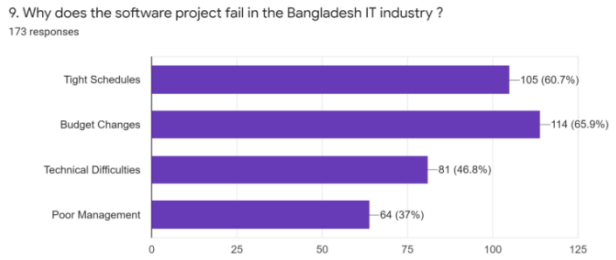

Fig. 2. Feedback about Project Failure

B. *Processing and Analyzing the Collected Data*

After getting all the responses it has been related with the previous literature reviews and identified the risk impact areas depending on the survey results. From this survey result, it has been noticed that most of the time Bangladeshi IT Industries face certain risk impact areas. Such as-

1. Tight schedules (60.7%)
2. Budget changes (65.9%)
3. Technical Difficulties (46.8%)
4. Poor management (37%)
5. Unproven Technologies (63.6 %)
6. User Communication and Functional Requirements (68.2%)
7. Application and System Architecture (43.4%)
8. Performance issue (28.9 %).

As it was targeted to mitigate the risk of software projects of Bangladesh IT Industries firstly, there has been found out the risk impact areas and analyzed them whose are most responsible for the failure of software projects through the survey on Bangladesh IT Industry. From the survey results, it has been notified that the most critical risk impact areas are [Unproven Technologies, User Communication, and Functional Requirements, Tight schedules, Budget changes]. Due to budget constraints, startups hire smart but inexperienced people during their early stages, resulting in software projects failure [8]. Secondly, after identifying and analyzing the survey and previous literature reviews, the paper has been proposed a hybrid model for mitigating risks in the next portion.

IV. Proposed Model for Mitigating Risks

The survey results indicate the risk factors that occur most for Bangladeshi IT Industries and the most software project do not go ahead towards the success for these identical risks. The proposed model identifies the identical risks of software projects for the Bangladesh IT Industry, and it verifies each stage by a unique committee (Dynamic Verifier Core). Also included is a unique feature New Unproven Technology train-up team (NUT train-up team) that mitigates new unproven technological risks.

A. *Four Phases of Proposed Model*

The paper has been proposed a hybrid model for mitigating risk. It has four phases - risk identification, risk measurement, risk assessment, and risk mitigation and contingency plan. To propose the model, there has been gathered knowledge from Boehm's risk model and his classifications. It also collected the core idea from three papers of Khatavakhotan et al. This proposed hybrid model, then it has been utilized DVC as the core verification of the risk management process [7]. The first phase achieves the collection of data. Depending on requirements the phase identifies the fundamental risks by following certain significant steps and the risk factor agendas are arranged. The second phase estimated

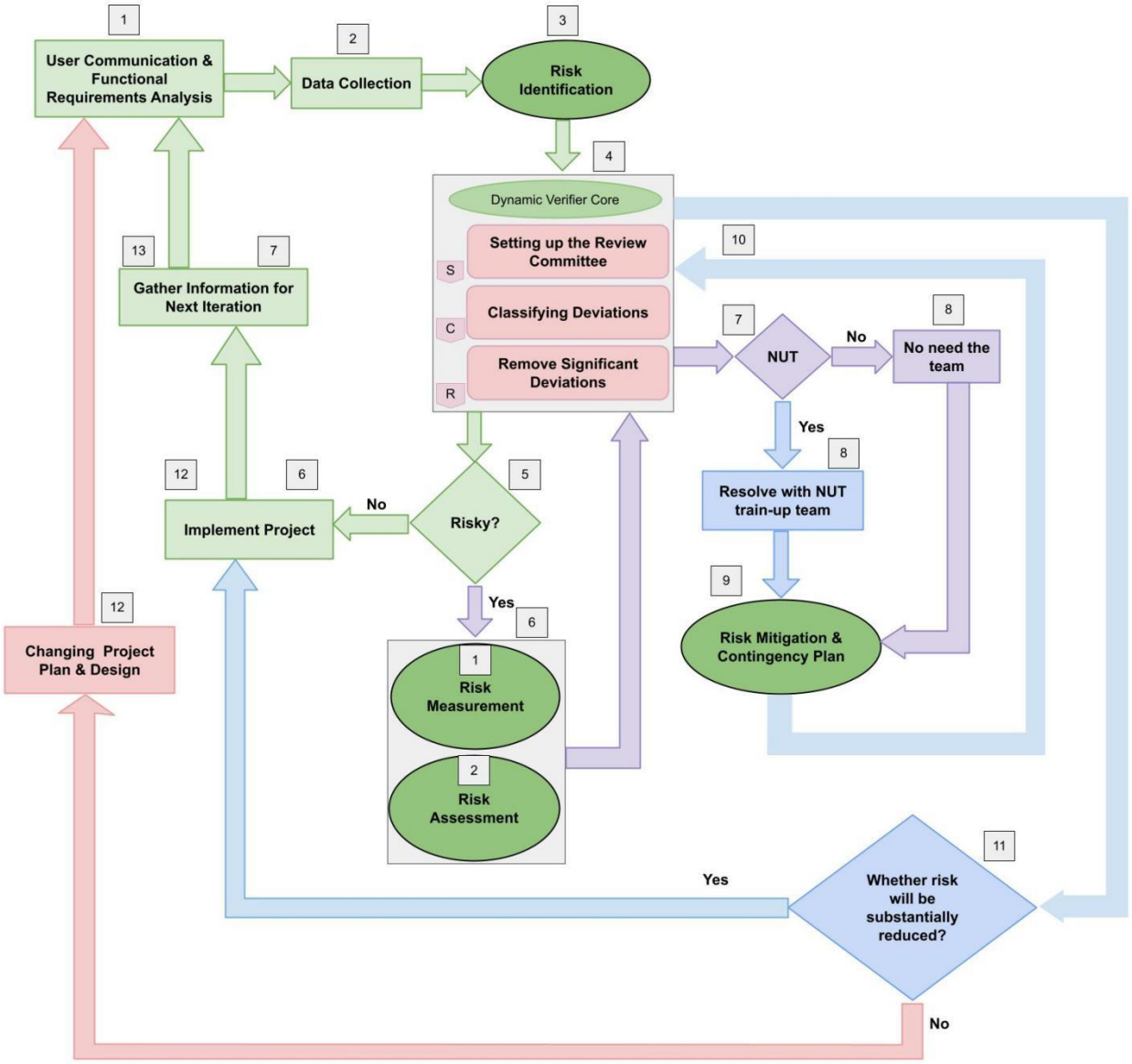

Fig. 3. Hybrid Model for Mitigating Risks

the danger elements' attributes by choosing the qualitative or quantitative method and creating a measurement report. The third phase establishes and prioritizes the level of risk and afterward settles the assessment report and Cost Time Risk (CTR) graph. The fourth phase mitigates the risk by utilizing the "Synthesized Formula" and decides the effectiveness rate of risk mitigation. At last, drive the genuine risks and design an emergency course of action if the further risk has happened.

Phase 1: Risk Identification

The Risk Identification phase recognizes the sort and category of risks by following a few stages. After the risk identification, the risk will be measured in the following phases. The risk identification steps are described below:

1. Documentation Reviews
2. Brainstorming and interviewing
3. SWOT Analysis (STRENGTH, Weakness, Opportunities, and Threats)
4. Developing and analyzing agendas of dangers
5. Analysis of Root Sake
6. Creating the circumstances and logical results chart

Step 1: Documentation Reviews (Previous and present risk records):

The standard practice to identify risks is looking into project-related documents, for example, exercises learned, articles, authoritative process resources, and so on. The overview of all documentation reported risks in the past stage can compare the risk level also the probability of risks during exploration.

Step 2: Brainstorming and interviewing:

Specialists in each section, in particular, can provide a clearer understanding of the threats. They can also recognize dangers from various parts. This trend emphasizes the importance of holding brief

but vital meetings with important persons, particularly subject matter specialists who are well-versed in current and past threats [7].

Step 3: SWOT Analysis (STRENGTH, Weakness, Opportunities, and Threats):
Identify the strengths and weaknesses of the project. Recognizing project strengths and weaknesses will help to be clear about the opportunities and threats of the project. This procedure assists with identifying risk inside a greater organizational context. This technique uses as a planning tool for analyzing business, opportunities, and threats in the external environment, looking at internal strengths and weaknesses. This technique is additionally utilized in the formulation of strategy. This SWOT technique is incredibly compelling and fruitful for risk identification.

Step 4: Developing and analyzing agendas of dangers:
Fundamental and unmistakable plans should remember the delayed results of studies for previous progresses, which provide information on the name of the danger, the type of dangers, and the IT project assets that may be vulnerable to the dangers (counting business, specialized, time, and executive dangers) [15].

Step 5: Analysis of Root Sake:
Root causes are resolved for the recognized risks. These Root causes are additionally used to distinguish extra risks.

Step 6: Creating the circumstances and logical results chart:
This is the main advance since it incorporates the identification of the reasons for a dangerous event and its results or its effect on the dangers [7].

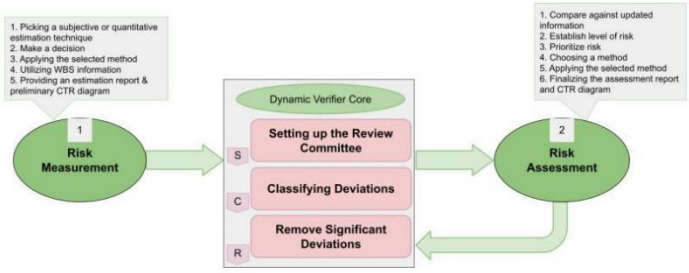

Fig. 4. Risk Measurement and Risk Assessment

Phase 2: Risk Measurement

This phase focuses on the most basic aspect of a risk: measuring or assessing the degree to which risk can affect the various components of a project, work item, or end product. As a result, both subjective and quantitative approaches should be used [7]. Nonetheless, these outlines are mostly divorced from the conceptualization, preceding meetings with subject matter experts, and related writing. This strategy is also employed for Work Breakdown Structure (WBS) because it is more compelling and allows for better implementation. This exemplifies the use of both qualitative and quantitative approaches. Stage 2 is divided into five sections:

1. Picking a subjective or quantitative estimation technique
2. Make a decision
3. Applying the selected method
4. Utilizing WBS information
5. Providing an Estimation Report & Preliminary CTR (Cost Time Risk) Diagram [7]

Step 1: Picking a subjective or quantitative estimation technique:
Quantitative research is more liked than qualitative research since it is more logical, unbiased, quick, centered, and adequate. Notwithstanding, qualitative research is utilized when the analyst has no clue about what's in store. It is utilized to characterize the issue or foster a way to deal with the issue. Quantitative research manages numbers and statistics, while qualitative research manages words and implications. Quantitative methods permit you to test a theory by efficiently gathering and breaking down information, while qualitative methods permit you to investigate thoughts and encounters from top to bottom. Thu-sly, select an appropriate estimating technique ensuing to considering the characteristics of a danger that had been settled in the past stage where the data got in the genuine environment, the time and switching the limitation of budget, and different limits.

Step 2: Make a decision:
After choosing the appropriate measuring method by considering the data of risk identification decide whether it is applicable for applying or not.

Step 3: Applying the chosen technique:
The proposed approach [16] employs the Work Breakdown Structure (WBS) strategy for assessing chances. This is because, rather than true fragments, the evolution of IT projects is based on the required conclusions of each stage. In this manner, the data gathered from each part of an IT task will be useful for risk estimation and assessment [2].

Step 4: Utilizing WBS information:
Other than fast project breakdown in WBS, likewise gain admittance to instruments like Gantt, Resource and Task Management, Time Tracking, and Earned Value Management - accessible for individual users and groups.
These incorporated into one solution that follows Easy Project Management Philosophy:

- Abstract the project scenario "makes it Easy"
- Visualize it
- Plan it
- Manage tasks
- Evaluate it

In the estimating interaction, each hazard will be requested either as Catastrophic, Critical, or Marginal. Huge monetary lack or specialized execution are requested as disastrous dangers. Basic dangers wrap up minor deferrals in programming alterations and some danger alleviation in specialized execution; in any case, Marginal dangers are irrelevant to a little danger decrease in specialized execution and monetary assets [17].

Step 5: Providing an estimation report:
The deliberate qualities of the danger elements will be added to the information in previous plans, and they will be evaluated and announced using various time and cost units [7].

Phase 3: Risk Assessment

Risk assessment is the first step toward effective risk management [7]. The risk assurance step will assign risk priority to each risk by contrasting the probability level (high, medium, low) and effect level. Risk management in expanded endeavor frameworks makes out of utilizing risk sharing, control and avoidance, and financial instruments to diminish the impacts of the coordinated operational chain chances and their financial consequences [18]. Based on the information and estimates acquired in the previous phase, the risks will be analyzed and positioned in this step. If the appraisal is incorrect, allocating resources, planning, and deciding on an alternative course of action will be extremely difficult [15]. In phase 3, from the start, compare the refreshed data and past bits of risk records and set up the risk level at that point focus on them, pick a

method to lessen the risk, apply the picked method, and finalize the assessment report and CTR diagram.

Phase 4: Risk Mitigation and Contingency Plan

The primary goal of risk management supervisors is to improve risk mitigation decisions. Other than risk reduction activities, it is necessary to address the mitigation of known risks, expected circumferential risks, arose opportunities, and amplify opportunities to make an effective decision [4]. This phase makes use of the data gathered in the preceding phase. This phase is divided into two parts: mitigation strategies and contingency plans. Phase 4's steps are as follows:

1. Identifying the hazardous risk
2. Characterizing plausible decisions for risk mitigation
3. Deciding the activity for every decision
4. Diminishing the occurrence probability and results of risks
5. Applying the utilization of mathematical formulas:

• measure the advantages of the parallel impacts of each activity
• measure the recently arisen opportunities
• Measure amplified opportunities
• select decisions dependent on the acquired results of the formulas

• states the ideal risk mitigation decision's efficiency rate

6. Driving the actual risks
7. Designing Contingency Plan [4], [7]

Decisions for the Best Mitigation:

The following steps are included in the model that optimizes risk mitigation decisions [4]:

To begin with, the model has identified major hazards from the previous phase. The model will then identify the activities for each choice, including actions that lower risk occurrence probability and actions that minimize risk outcomes once they have occurred. Use mathematical formulas to calculate the benefits of the sidelong effects of each activity, as well as the recently discovered and amplified opportunities from previous phases of the project. Finally, make decisions based on the formulas acquired aftereffects.

Synthesized Formula:

The 'Synthesized Formula,' which is provided for this model, asserts the risk mitigation optimum decision's efficiency rate [4].

$$\text{EDAi} = \sum_{k=1}^{all\ actions} [(RRA\_Net)_k + OBA_k - (OICA\_Net)_k - C_k]$$

Whereas:

$$OBA_k = \sum_{n=1}^{all\ arisen\ opportunities} (ARO_{kn}) + \sum_{n=1}^{all\ amplified\ opportunities} (AMO_{kn})$$

$ED_i = EDA_i – GICA$

Variables and descriptions:

GICA = General Inconvenient Consequences Amount regarding decision i
EDA_i = Efficiency of Decision i regarding the Actions
ED_i = Efficiency of Decision i
C_k = Cost of action k
RRA_k = Risk Reduction Amount regarding action k
$(RRA\_Net)_k$ = RRA_k Considering its Probability
$OICA_k$ = Other Inconvenient Consequences Amount regarding action k
$(OICA\_Net)_k$ = $OICA_k$ Considering its Probability
OBA_k = Opportunity Benefit Amount regarding action k

For each key decision, this formula takes into account the risk mitigation likelihood as well as the rate of consequence reduction. Simultaneously, the activities' likely opportunities will be calculated in detail. Finally, for each action, the chance and loss number of circumferential risks will be computed. By focusing on the cost of each activity, the algebraic total of the previously described issues reveals the effectiveness of each action.

Actual risks are being driven: If a risk has happened, the contingency plan will be implemented. To begin the big adjustments, the agendas and reports are given to the Dynamic Verifier Core (DVC) at the same time.

Creating a contingency plan: If a risk happens, the plan specifies what steps should be performed to reduce the effects [7].

B. Dynamic Verifier Core (DVC)

Figure 2 shows how DVC can be divided down into three pieces. The prearranged reports, computations, and documents are provided to the DVC core without considering the pre-owned strategy to assess and detect possible deviations from objectives, programs, and actions at the conclusion of each level in the risk process. Finally, the required procedures will be taken to prevent similar errors. DVC is divided into three stages [6]:

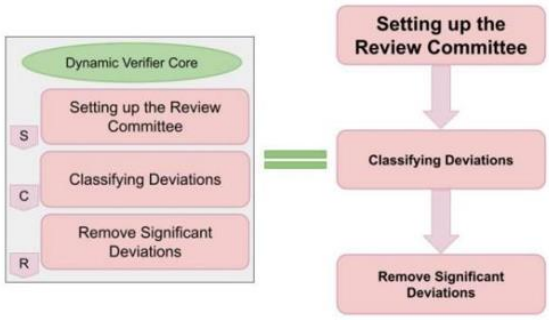

Fig. 5. DVC (Dynamic Verifier Core)

The review committee is made up of a few people with varied skills and duties at different phases of the process. In light of the aforementioned challenges, the review committee should be included at the conclusion of each phase of the risk process, including risk identification, measurement, assessment, mitigation, and contingency planning. When each phase is done, the data is transferred to the DVC using pre-planned structures. Any possible deviations were classified during the review. Finally, the committee decided to update the checklist and remove the significant differences.

C. Unique Feature of the Proposed Model

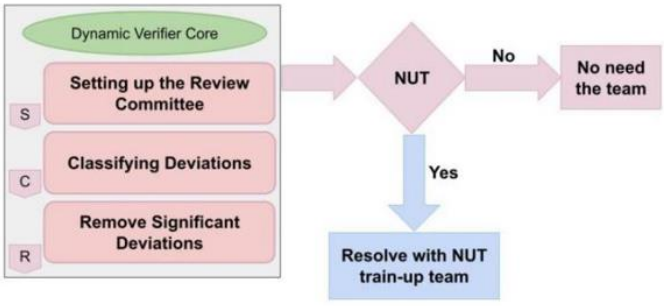

Fig. 6. NUT train-up team

New Unproven Technology (NUT) train-up team:

The unique team (DVC) will be considered and verified the three phases of risk characteristics and declare whether the new unproven technology is necessary or not. If the risk will be reducible without using the new technology, then no need for the NUT train-up team. If the new technology is necessary, then follow the below steps:

1. Make a team by providing proper training on each new-unproven-technology so that the train-up team can properly use the new technology.
2. The team must keep proper information/knowledge about the previous and present risk impact areas records.
3. Identify the type of technology.
4. Compare with previous and present risk records for new unproven technology.
5. Resolve the technical problem.
6. Pass the updated solution to DVC (Dynamic Verifier Core).

D. Advantages of Proposed Model

The proposed model has the following advantages:

i. The model follows a sequential manner. If one stage is done it goes to the next stage. So, the model simply follows a simple path, and it has simplicity.
ii. It has transparency for new technology. NUT train-up team training up continuously for new technology and so the model has an effective solution for new technology that is ignored in the previous models.
iii. There is no possibility of a decision mismatch because each phase is checked by the same individuals.
iv. The model is concerned with user communication and functional requirements.
v. The gradual appearance of the risk effect areas [7], as well as the transparency of each phase.
vi. It is a comprehensive model because it encompasses all stages of implementation, mitigation, and contingency planning [7].
vii. There has a chance for changing the project plan and design before the failure of software projects.

V. Solution Verification

The proposed model is concerned about user communication and also clients' requirements at the same time. The model has been notified of the phases of risks and DVC verifies each phase. After the verification of DVC, the same committee decides whether risk happened or not and what should be avoidable, or what should be include-able. This has been noticed from the survey and the previous literature reviews, when the software projects face the necessity of new technology then for the lack of proper training on new technology most of the software projects do not go ahead towards success, they failed in the middle. In this model, there has been also included a new feature that is the NUT train-up team. The DVC also decided that whether the use of new unproven technology is necessary or not. If necessary, then the NUT train-up team will solve the related problem by using their previous and present knowledge and then the DVC will verify the results again and provide a decision. As a result, software project failure will be reduced substantially as a proper train-up team is frequently training up on new technology. Furthermore, as a unique committee (DVC) check and decide for every risk phase and stage so the possibility of decision mismatch will be reduced substantially. Additionally, the Synthesized Formula declares the risk mitigation optimum decision's efficiency rate [4]. Finally, by overall justification, it can say that the goal of risk mitigation is successful.

VI. Conclusion

The goal of this paper was the reduction of software risk in the Bangladesh IT Industry. The model has been conducted the goal through two teams i) DVC (Dynamic Verifier Core) and ii) NUT train-up team. The DVC demonstrates the four risk phases and suggests decisions. The NUT train-up team facilitates the new technology which is ignored in the other models. To take risk mitigation decisions it has been used "Synthesized Formula" in Phase 4 (Risk Mitigation and Contingency Plan) [4]. The use of "Synthesized Formula" has strongest the model to mitigate the risks. The Synthesized Formula declares the risk mitigation optimum decision's efficiency rate [4].

On the other hand, the model identifies potential risks at all phases of the software development process, allowing a good mitigation approach to be implemented at the right level to minimize potential cost and time losses.

References

[1] B. Roy and R. Dasgupta, "A study on software risk management strategies and mapping with SDLC," in Advanced Computing and Systems for Security, Springer, 2016, pp. 121-138.

[2] M. BETTER, F. GLOVER, G. KOCHENBERGER, and H. WANG, "SIMULATION OPTIMIZATION: APPLICATIONS IN RISK MANAGEMENT," International Journal of Information Technology & Decision Making, vol. 7, no. 4, p. 571–587, 2008.

[3] D. Reifer, "Ten deadly risks in Internet and intranet software development," IEEE software, vol. 19, no. 2, pp. 12-14, 2002.

[4] A. S. Khatavakhotan and S. H. Ow, "Rethinking the Mitigation Phase in Software Risk Management Process: A Case Study," in 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation, Kuala Lumpur, 2012.

[5] N. C. Pa and B. A. Jnr., "A Model of Mitigating Risk For IT Organisations," in 2015 4th International Conference on Software Engineering and Computer Systems (ICSECS), Kuantan, Pahang, Malaysia, IEEE, 2015, pp. 49-54.

[6] A. S. Khatavakhotan and D. S. H. Ow, "Improving IT Risk Management Process by an Embedded Dynamic Verifier Core: Towards Reducing IT Projects Failure," in 2012 Third International Conference on Intelligent Systems Modelling and Simulation, IEEE, 2012, pp. 684-687.

[7] A. S. Khatavakhotan and S. H. Ow, "DEVELOPMENT OF A SOFTWARE RISK MANAGEMENT MODEL USING UNIQUE FEATURES OF A PROPOSED AUDIT COMPONENT," Malaysian Journal of Computer Science, vol. 28, no. 2, pp. 110-131, 2015.

[8] Fatema, K., Syeed, M. M., & Miah, M. S. U. Demography of Startup Software Companies: An Empirical Investigation on the Success and Failure. International Journal of Computer Applications, 957, 8887.

[9] A. E. Chowdhury, A. Bhowmik, H. Hasan and M. S. Rahim, "Analysis of the Veracities of Industry Used Software Development Life Cycle Methodologies," AIUB Journal of Science and Engineering (AJSE), pp. Vol. 16; Issue 2; June; pp 1-8, 2017.

[10] B. Shahzad and A. S. Al-Mudimigh, "Risk Identification, Mitigation and Avoidance Model for Handling Software Risk," 2010 2nd International Conference on Computational Intelligence,

Communication Systems and Networks, 2010, pp. 191-196, doi: 10.1109/CICSyN.2010.82.

[11] A. Ramirez, A. Aiello and S. J. Lincke, "A Survey and Comparison of Secure Software Development Standards," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges (51275), 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322704.

[12] E. Hossain, M. A. Babar, H. Paik, and J. Verner, "Risk Identification and Mitigation Processes for Using Scrum in Global Software Development: A Conceptual Framework," 2009 16th Asia-Pacific Software Engineering Conference, 2009, pp. 457-464, doi: 10.1109/APSEC.2009.56.

[13] M. Uzzafer, "Measuring the Risk of Software Projects," International Journal of Software Engineering and Its Applications, vol. 9, no. 11, pp. 247-262, 2015.

[14] M. Jakub and J. Gorski, "Software support for collaborative risk management," in proc. of 8th International Conference on Advanced Computer Systems, 2001, pp. 17-19.

[15] D. Wu and D. L. Olson, "Introduction To The Special Section On Optimizing Risk Management Methods And Tools," Human & Ecological Risk Assessment, vol. 15, no. 2, pp. 220-226, 2009.

[16] J. G. Zhao, "Significance Of WBS In Contingency Modelling," AACE International Transactions, pp. 5.1-5.5, 2006.

[17] W. T. LI, Z. Jian, and Y. X. WANG, "Research on Software Risk Assessment Based on Grey System Theory," Computer Technology And Development, vol. 23, no. 5, pp. 124-126, 2013.

[18] A. M. Sharif and S. Basri, "Software Risk Assessment: A Review on Small and Medium Software Projects," J.M. Zain et al. (Eds.): ICSECS 2011, Part II, CCIS 180, p. 214–224, 2011.

[19] S. G. Sutton, D. Khazanchi, C. Hampton and V. Arnold, "Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships," Journal of the Association for Information Systems, vol. 9, no. 3-4, pp. 151-174, 2008.

[20] C. Radut, "The Enterprise Information System And Risk Management," Annals of the University of Oradea, Economic Science Series, vol. 18, no. 4, pp. 1030-1034, 2009.

[21] B. W. BOEHM, "Software Risk Management: Principles and Practices," IEEE Software, vol. 8, no. 1, pp. 32-41, 1991.

[22] C. G. Pan, Y. W. Chen and W. Hao, "Overview of the study on theories and methods of software project risk management," Control and Decision, vol. 22, no. 5, p. 481-485, 2007.

[23] A. Y. Abdihafid, Software Project Failure in Bangladesh, Daffodil International University, 2019.

[24] P. C. Yong and M. Phil, "Software Risk Management based on Software Development Life Cycle," Thesis of Zhejiang University, Zhejiang, pp. 11-17, 2002.