Project Management for Computer Scientists

Open Individual Assessment

Exam number: Y3858851

Question 1

Introduction

For a single-person academic project, the techniques of scope management, planning, and risk management can be very useful to ensure that the project is completed on time and all requirements are met. The techniques of stakeholder management and resource management can also be useful, but are less suitable in most cases.

Before the project begins, it is crucial to define the **project scope** in order to have a clear idea of how to apply the remaining techniques. By defining a project scope, the goals, timeframes and constraints of the project are clearly established. For the individual project, the goals and timeframe are provided by the university, and it is important to have them present when going through the various stages of the project. Constraints for this project include the time restrictions imposed by the project being part-time, and the need for learning and background reading before the project work can be done.

Defining a project scope is crucial in order to effectively apply **planning**, an extremely useful technique. By considering various sections of the final paper as products, a comprehensive product list can be constructed. This allows the student to apply activity planning, which can then be used to establish a clear plan of action, as well as due dates for each project. Finally, by using a Gantt chart to visualize the plan, the student can clearly see how the project is progressing and re-plan with enough time to correct if they fall off track.

Throughout the whole project, **risk management** allows the student to keep track of and manage any risks that may arise. Examples of risks that may arise include unlikely events, e.g. hardware failure or a family issue, but also very likely ones, such as time estimate errors[8]. By continually assessing the risks and assigning an exposure value to each one, the student can make changes to their plan depending on which risks have become more or less likely, and develop a contingency plan for when the risks do present themselves.

There are also techniques which are less applicable to the project, namely

stakeholder management and **resource management**. The stakeholders of the project are, in most cases, the project advisor and the university, and the requirements of the project are given out at the start, leaving no need for continual assessment outside of advisor meetings. Managing resources is also less important in such a project where money is usually not a factor, physical resource requirements are small and the staff is reduced to one person.

Question 2

For a small startup, using AWS instead of having an in-house datacenter provides many advantages and reduces cybersecurity risks, but this does not mean that risk does not exist. As YorKlinic will be dealing with medical data, strong cybersecurity practices are a must, due to the strict regulations surrounding patient data and the very negative consequences a data breach would have for both the patients and the company. AWS is not failproof in this regard, as there have been significant data breaches in the past [5], but it provides much stronger security than what the YorKlinic development team would be able to achieve.

For secure environments, AWS provides the Amazon Virtual Private Cloud (VPC), which allows users to define a logically isolated environment in which to run their applications, with advanced security features such as security groups and network access control lists [3]. This seems like a perfect fit for YorKlinic, who might require these features to ensure that data is accessed only by those allowed.

In addition, AWS provides tools for database management and encryption through RDS - relational database system. Data can be encrypted in transit via SSL, which is a must when storing sensitive information, and has granular control over who is able to access the data via AWS Identity and Access Management. This can be run in a VPC for additional security and better interoperability with the other applications [2].

There are a number of setbacks the YorKlinic development team have to take into account when developing their applications in the cloud. Firstly, they have to deal with the risk that their server might be attacked by a malicious agent. This can be minimized by correctly configuring their servers and establishing company-wide policies which aim to protect the access credentials held by employees who use the systems for data entry and access. These policies might include restrictions on password and data sharing.

Second, AWS is an enterprise-scale service which accommodates small-scale companies, but this does not come without costs. Encryption of all data will be required but introduces an overhead in storing and retrieving the data, which is worsened by the fact that it is all stored off-site. However, this also reduces the risk when compared to storing the data on-site, where

a physical threat is more likely and attackers would have more ready access to the infrastructure.

Question 3

For safety-critical applications, it is essential for the supplier to correctly test their software in order to provide a strong guarantee that it is correct. Failure to do so can result in grave issues; nowhere is this more evident than in the Therac-25 accidents [7], where deaths and serious injuries were caused by programming errors and a lack of testing. Since an X-ray overdose can significantly increase the risk of cancer and even cause radiation sickness [6], there are parallels to be drawn to Therac-25, which means that rigorous testing should be performed to ensure that history does not repeat itself.

Stakeholders impacted:

- Patients
  The stakeholder most impacted by the decision of delaying the project or skipping testing are the patients receiving radiation therapy. Were the software engineer to choose not to delay, they would be willingly putting the patients in danger of an overdose. A delay would likely not affect the patients much, assuming that the current software that the x-ray machines use has been appropriately tested.

- Healthcare professionals
  Any issues caused by the x-ray machine would also require the patients' healthcare professionals to expend additional resources in order to heal them.

- Machine operators
  Another negatively impacted stakeholder are the x-ray machine operators. Firstly, a failure of the x-ray machine would render the results useless as the image produced would likely not be usable. In addition to this, were the machine to become unusable after a faliure this would require resources to be used to either repair or replace the machine.

- Company shareholders
  A delay in releasing the product would mainly affect the company's shareholders and executives, as it could potentially cause a loss of revenue due to more developer time needed for the release and a potential decrease in customer engagement. However, a software failure would likely cause heavy reputational damage for the company. Because any failure can put lives at stake, hospitals are likely to revoke their trust

of the company at the first sign that their development practices are flawed.

- Company employees and staff
  Decrease in morale and company trust

- Engineers
  The technical people involved in the project would be negatively affected by a delay, which might make them incapable of continuing their work due to the critical path delay which would presumably be caused by the delay.

- Engineers break the ACM code of ethics
  Finally, the engineer writing the software would be breaching the ACM code of ethics [1] and the BCS code of ethics [4]

Taking all this into account, there are very compelling reasons for delaying the deployment of the software, as every stakeholder involved would be negatively affected by a faliure. The only situation where it might be ethically acceptable to not delay the release is if the code is not safety-critical at all, although this seems unlikely for an x-ray machine.

Bibliography

[1] *ACM Code of Ethics and Professional Conduct*. Association for Computing Machinery. 2018. URL: https://ethics.acm.org/code-of-ethics (visited on 11/21/2019).

[2] *Amazon RDS Features*. Amazon Web Services. URL: https://aws.amazon.com/rds/features/ (visited on 11/27/2019).

[3] *Amazon Virtual Private Cloud*. Amazon Web Services. URL: https://aws.amazon.com/vpc/ (visited on 11/27/2019).

[4] *BCS Code of Conduct*. British Computer Society. URL: https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/ (visited on 11/29/2019).

[5] Peter Cohan. "Will Capital One's 106M Name Data Breach Cut Into AWS's Growth?" In: (). URL: https://www.forbes.com/sites/petercohan/2019/07/30/will-capital-ones-106m-name-data-breach-cut-into-awss-growth/ (visited on 11/27/2019).

[6] *How much radiation is dangerous?* Reuters. URL: https://www.reuters.com/article/us-how-much-radiation-dangerous-idUSTRE72E79Z20110315 (visited on 11/26/2019).

[7] Nancy G. Leveson and Clark S. Turner. "An Investigation of the Therac-25 Accidents". In: *Computer* 26 (July 1993), pp. 18–41. DOI: 10.1109/MC.1993.274940.

[8] Anna Mar. *Why Your Estimates Are Always Wrong*. Feb. 17, 2013. URL: https://management.simplicable.com/management/new/why-your-estimates-are-always-wrong (visited on 11/29/2019).