

Project Management for Computer Scientists

Open Individual Assessment

Exam number: Y3858851

Question 1

Introduction

The dynamics of a single-person academic project can be very different to those of a team project working in a commercial setting, where many more factors can affect the outcome.

In my personal project, there are no resources to be managed other than myself, very few cybersecurity risks and even less ethical issues.

However, by establishing the project scope, planning, and managing risks correctly, my project can benefit from project management techniques which are applicable to any project.

- Project scope: Firstly, defining a project scope sets out clearly what the goals, timeframes and constraints of the project are. This technique will make it easier to apply other project management techniques, as well as allowing the project owner to have a clear view of what their goals are.
 - Objective
 - Time
 - Constraints
- Planning: Planning is another extremely useful technique for any project, as it allows the owner to see how the project is progressing, and adjust appropriately if it falls off schedule. By setting appropriate product-based milestones using product-led planning and keeping of the necessary steps with an activity list, one can have concrete indicators of how far the project is in its lifecycle and what the next step to take is.

- Product-led planning
 - Activity list
 - **Work flow diagram - not useful**
- **Risks: Include examples of risks** Finally, every project has risks, and keeping track of them is the key to ensuring the project is not derailed by an unforeseen circumstance. Using risk assessment techniques, one can include uncertainty into their planning and actions to maximize the chances that the project is completed successfully. This is implemented in the risk cycle, where risks are continually assessed throughout the project and contingency plans are made to manage, mitigate or remediate the risks. By assigning an exposure value to each identified risk, the relative importance of each risk is put into perspective and will guide the management strategies that are identified.
 - Risk cycle - continually reassess risks
 - Risk exposure + management
 - **Useless:** Not all project management techniques apply to a single person project, however, and in my case my project does not require me to manage any resources, as the only resources involved in my project are me and my laptop.

There are no major cybersecurity issues either, as I will be writing non safety-critical software with no network access and few permissions. Finally there are no ethics or legal issues for me to deal with

- Stakeholders **maybe?**
- CSec
- Resource management
- Ethics

Question 2

Introduction

For a small startup, using AWS instead of having an in-house datacenter provides many advantages, but it does not come without its risks. As YorKlinik

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 [3], but it provides much stronger security than what the YorKlinik development team would be able to achieve.

Points:

- AWS security tools
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 [2].
- YorKlinik's capabilities
 - Development team
As a small company, the development team of YorKlinik might be limited in resources, and they may resort to COTS (commercial off-the-shelf) solutions for ensuring security. These may not be verified or might not work with the security model required for medical data, which could be a large threat.
 - Entire company implications
To bolster security and minimize the risk of attacks, YorKlinik will have to establish security protocols that will encompass everyone in the company. Measures need to be taken to ensure secure access and proper handling of the data. As the data is stored on a cloud server, it is of utmost importance that the access credentials are not intercepted.
- Challenges for a small-scale company working in an enterprise-scale security model
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 [5], 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 [4], 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 failure 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].

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 failure. 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.

References

- [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] 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).
- [4] *How much radiation is dangerous?* Reuters. URL: <https://www.reuters.com/article/us-how-much-radiation-dangerous-idUSTRE72E79Z20110315> (visited on 11/26/2019).
- [5] 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.