ANNOTODE

The Web Anotator.

Risk Management

CS Group 1

Avi Aryan(201451070)

Saurabh (201451017)

Chahat(201451061)

Sunil (201451033)

Mukesh (201451060)

Manikanta (201451022)

Abhilash (201451031)

Mounika(201451062)

Manohar (201451024)

Contents

Revision Table

Revision	Author	Revision Date	Revision Tracking Notes
1	Sunil Yedla	25-9-16	Added images
2	Sunil Yedla	28-9-16	Added references

1 What is risk?

A risk is a potential problem.It might happen or it might not,this is uncertain. We don't know whether particular event will occur or not,but if it does,then definitely it has negative impact on project.So we need to maintain some strategies to reduce these risks that we might encounter.

2 Risk Management Paradigm:

1.Identity:
Searching for the risk before they create a major problem.
2.Analyze:
Understand the nature of risk and gather information about the risk
3.Plan
Creating a risk-management plan
4.Track
Monitoring the status of the risk
5.Control
Correct the deviations and make necessary amendments.
6.communicate:
Discussing about the emerging risks and current risks and plans to be taken.

3 Risk Categorization

3.1 project risks:

- **Inaccurate project estimating:** If we cant estimate the time and budget for the completion of my project,it leads to the project failure.
- **Staff turnover:** If any of my project team memeber is missing due to some emergency situations(sick,drop-out from college.)
- **Too many decision makers:** Among the 9 team members, each one have different way of thinking and different way of implementation.
- **Custom-coding to get features just right.** Sometimes 90 percent of a feature is good enough if delivering on that last 10 percent is going to take 100s of hours of custom coding and testing and cause large time and budget overruns
- Requirements and budget aren't clearly specified

3.2 Technical risks

- On every screen,size and orientation (portrait or landscape). The combinations are almost infinite. Optimising for a specific combination can cause de-optimisation for another.
- Ethical hackers compromising user accounts through brute force attack.Every website authentication page can be brute forced,until there is good enough security.
- Click-jacking: 'iframe' functionality can be applied
- Session management issues:session not getting expiring causes the users Personal information getting leaked.
- Problems in Angular-js code/source code:however how much care we took in designing the Angular-js code still there will

.

3.3 Business risks

- Who might be involved or affected if an incident happens?
- What if the user is facing trouble installing the software?

4 Negative impact of risk

:

- Diminished quality of product
- Increased cost and time
- Project failure

5 Risk management:

5.1 Project risks management:

- Regular project updates ensure that the client is kept informed in the event that estimates and actuals are diverging significantly.
- Ensure that project communications and status reporting are clear, up-to-date and accessible to new project members
- Ensure that project group leaders are sufficiently empowered and supported to make decisions.
- make sure the critical ones are done first before the budget is exhausted

5.2 Technical risks management:

- We ensure that our website is standards-compliant, but still accept that perfect consistency is virtually impossible.we will make sure that the android and web application we are developing is compatible both in mobile and desktop's.
- We will make sure to insert rate limit for authentication so that when hacker tries to brute-force user account it will locout automatically after few trials.we ensure that session ID must be long enough to prevent brute force attacks, where an attacker can go through the whole range of ID values and verify the existence of valid sessions.The session ID length must be at least 128 bits.
- We will include "frame-breaking" functionality which prevents other web pages from framing the site you wish to defend,while we are designing the code.
- While we are developing the code we will make sure that the user will not face any difficuly through our code and the angular-js code will be hidden when the attacker/user tries to view the source code of the webpage(source code is public to everyone by using developer tools.)
-

5.3 Business risks management:

- We will try to maintain a support-staff who will be resolving the security issues faced by user's.if they are facing any difficulty with his account he can submit a token to our support-staff.
- we will give every user/client the "USER MANUAL" which will help the user in his installation and usage of the software.

6 RMMM plan:

- risk management strategy can be included in the software project plan or the risk management steps can be organised into a separate risk
- mitigation,monitoring and management plan.
- RMMM plan documents all the work performed as part of risk analysis and is used by the project leaded as part of the overall project plan.

7 Conclusion:

- to manage the risks we need to establish a strong connection between the user and client.Infact the developer must think as a user and identify the risks he might face as a user when he was reviewing the technical risks
- software tools can he handful in identifying the risks and managing(Ex:RUP)
- Team need to have a strong base about risk management.
- Risk necessarily need not be in negative way and it can be viewed as an opportunity to develop our projects in a better way.

8 References

1. Risk Communication PrimerTools and Techniques. Navy and Marine Corps Public Health Center.
2. https://www.projecttimes.com/articles/project-risk-identification-for-new-project-manager.html
3. https://www.projectsmart.co.uk/10-golden-rules-of-project-risk-management.php
4. https://bia.ca/risk-management-the-what-why-and-how

Reviewedby:
B.Manohar Reddy
CS Group 1
201451024@iiitvadodara.ac.in