Risk Assessment Document for Team TerraUser

The Web-based User Management Project

Michelle Harr
Naoko Tsunekawa
Daniel Wallace

2 December 2001
Revision 1.0

1. INTRODUCTION

This document is a risk analysis of the TerraUser web-based user management software.

Our client is Deborah Lee Soltesz from US Geological Survey (USGS) Terrestrial Remote Sensing Group at the Flagstaff Field Center. USGS work with satellite multispectral, airborne photos, shipborne sidescan sonar, and DEM digital images. This team does such things as digital mosaicking, extraction and mapping of earth science information, geometric and radiometric calibration and corrections, and multitemporal change detection. The team has set up TerraWeb as a way for people to access this information along with a way to organize and manage some of their data.

Currently USGS TerraWeb applications have minimal security. Users are not required to log on to access these web applications. No current user management system is in place. Data management and data analysis/manipulation is the main function of many of these applications, and it is imperative that if work is going to be done using these systems that there be some sort of security standards.

The objective of the project is to design and implement an efficient and secure interface to other USGS TerraWeb applications, along with a stand-alone application used to administer the user management system. The software will allow users to securely and easily access other interactive TerraWeb applications.

This document characterizes the possible risks during the design, implementation, and testing phase in three different categories: project risks, product risks, and business risks. The risks are also analyzed for their probability and overall effect to identify possible strategies for success of the project.

Risk analysis will help us to focus on events that have a reasonable chance of occurring and that would directly affect the success of our project.

2. RISKS

After analyzing the problem, Team TerraUser had identified the following as being potential risks.

2.1 Project Risks

Risk	Risk Description
Time Management	Group members all have different and busy schedules, finding time to meet might be difficult.
Hardware issues	Hardware, which is essential for the project, might fail or be unavailable.
Requirements change	Numerous changes on the requirements that were not anticipated.
Security	Changing security standards in the field.
Compatibility	Compatibility issues on web server, operating system, browser, and database.
Interface specification availability	Essential interface specifications not available on schedule.
Size underestimation	Underestimation of size and complexity of system.
Lack of experience	There is a lot of technology that group members need to learn and master in order to successfully complete the project.

Table 1: Project Risks

2.2 Product Risks

Risk	Risk Description
Interface specification	Interfacing to a variety of USGS TerraWeb applications.
Security	Security issues with bugs, viruses, hackers.
Speed issue	The network cannot process as many transactions in a reasonable speed as expected.
Flexibility	Product is not flexible for future modification.

Table 2: Product Risks

2.3 Business Risks

Risk	Risk Description
Changes in technology	Some new technology might come out that supersedes the technology on which the system is built.
Product competition	Product might already exist.
Data management	Different TerraWeb applications might need TerraUser to keep track of some unique piece of information.

Table 3: Business Risks

3. RISK ANALYSIS

The risks we have identified are a few of the many risks the project may face. We have analyzed the major risks and in doing so, we have projected the probability of each risk happening and the overall effect of the problem actually occurring. The only critical risk we have identified is the underestimation of development time. We are confident, however, that this risk will be closely monitored and that the team is devoted to overcoming any obstacle to prevent it from happening. The following table shows the major risks along with the probability of each happening and the corresponding effect.

Risk	Probability	Effects
Time to develop software is underestimated.	High	Serious
Learning curve is high on required technology.	Moderate	Tolerable
The size of the software is underestimated.	High	Tolerable
The network or database or server cannot process as many transactions as expected.	Low	Catastrophic
Cannot perform open searches on database.	Low	Serious
Unexpectedly high number bugs to fix during test phase.	Moderate	Tolerable
Key team members are unavailable or ill at critical time in project.	Moderate	Serious
Changes to the requirements are made causing major design and implementation changes.	Moderate	Serious

Table 4: Risk Analysis

Risk Mitigation

Key risks have been identified and possible strategies have been identified to manage these risks. Solutions to some potential risks follow:

Risk	Risk Analysis/Mitigation
Hardware failure on server.	Could lose valuable data and code if there was a major hardware failure on server. Make a back up plan of critical files and document the setup.
Failure to find most efficient and effective way to interface from lack of experience.	Team members will research and try to get up to date on interfacing issues.
Efficient data management can be a challenge.	Sometimes data management can get messy and confusing. One way to avoid this is to follow guidelines and standards set forth by the industry.
Consistency among browsers is related to how the web-application functions.	Decide on some sort of standards and stick to them.
Overwhelming amount of bugs found in software.	If testing of software is done consistently and intensely through out the process, major bugs can be minimized and avoided.
Underestimated development time.	Work harder on prioritizing important tasks to be completed.

Table 5: Risk Management

Risk Monitoring Strategies

Throughout the project the risks will be reassessed and updates will be made to risk mitigation strategies. The risks will be discussed during periodic project reviews and status reports.

Risk monitoring will consist of the following:

- To track changes in the technologies that we are using, weekly monitoring of technology news websites will be done.
- To monitor how we are doing with regards to the schedule, we will look at the current schedule and calendar and make updates as needed.
- To keep track of bugs and software problems, we will use a bug track log and then have other group members verify that problem is corrected after the bug fix. We will test related functionality to make sure other things did not break once the bug fix was applied. Verifications will be logged too.
- By constant use of development box we will know if a hardware failure occurs. To be safe we will make a weekly backup.
- To keep up to date on what each team member is doing, each team member will write a weekly status report and email it to the team.

By logging bugs, making backups of our data, constantly updating schedules and timelines, getting constant communication from group members through email, and monitoring news and technology websites we hope to minimize our risks.

5. Risk Summary and Conclusions

Through detailed documentation, constant communication, quality tracking and constant research we hope to be able to avoid most of the identified risks.

When we identified the risks, we recognized that time management is significant since the project must follow the college capstone curriculum timeline. Also, changes in technology are fast, and it is important to be aware of and to keep up with them. Security issues are always a major issue in computer networking, and we should have a good knowledge of it to be confident with our product.

By identifying the possible risks associated with the project and ways for minimizing or mitigating them we feel confident that we will not have any major surprises. Although we have identified many risks we feel better prepared to deal with problems should they arise. The overall project seems to have a moderate to low risk associated with it.