2.4 Risk Management

2.4.2 Risk Identification

2.4.2.1 Legal Challenges

An electronic data discovery request may be made of the Electronic Evidence Management System. A forensic analyst will store chain of custody documentation and observations related to forensic cases in electronic format in the Electronic Evidence Management System. In attacking a forensic analyst, opposing counsel will typically mount an attack on any of the following:

- The forensic analyst's character and level of experience
- The integrity and level of compliance with best practices or best effort for both methodologies and documentation of the forensic analyst and the organization that the analyst represents.
- The integrity of electronic data in the possession of the forensic analyst.

Our proposed system for management and reporting of documentation related to electronic evidence and analyst findings introduces a fourth unique opportunity for opposing counsel:

- Attack the integrity and control of data within our system, to show that data within our system can be altered and provide a misrepresentation of a forensic analysts findings and methodologies.

In attacking our system in this fourth manner, opposing counsel may urge the court to grant a request for data discovery, in which a forensic analyst for the opposing counsel would be granted the right to audit our system for evidence of insecurity and evidence of records manipulation outside of the revision control our system is advertised to provide. Should opposing counsel be granted the discovery request, and without appropriate system design and documentation, our system may be taken off-line for weeks, potentially crippling ICG's forensics department and negatively affecting ICG's relationship with clients engaging ICG in concurrent forensic matters.

2.4.2.2 No Internet Connection Available

It is possible that forensic analysts will perform forensics in a location in which Internet Service Provision for our system's client tablet pc systems is not available.

2.4.2.3 Server Failure

It is possible that our server systems may fail while a forensic analyst is recording notes.

2.4.2.4 Erroneous Data Entry

Even with the capability for a forensic analyst to review data he or she has entered and sign his or her approval of the entered records, there still exists the possibility of human error. Human operators of any system will make mistakes. Mistakes in forensic chain of custody may result in the invalidation of critical evidentiary data that may lead to punitive legal measures against innocent individuals and an inability to legally punish guilty individuals.

2.4.2.5 Database Corruption

The database that will store all records entered into the Electronic Evidence Management System may become corrupted due to hardware failure, operating system software errors, file system errors, and database application software errors.

2.4.2.6 Hacking of the Electronic Evidence Management System

As the Electronic Evidence Management System will be used as a litigation tool, there is a high motivation for the individual or organization

represented by opposing counsel to hack our system in order to demonstrate insecurity or prevent ICG from bringing their evidence to trial against them.

2.4.2.7 Adaptation of System to the Future of Data Forensics

Much of the efforts in computer forensics today deals with the imaging of single hard disk drives. Very rarely do forensic analysts work with RAID storage, Network Attached Storage, or Storage Area Networks. As storage becomes increasingly cheaper and faster, more and more data will be stored electronically, necessitating such large storage systems.

Such large systems make the tried and tested practice in computer forensics of imaging entire hard disk drives impractical and in some cases impossible. Our system will need to record forensic documentation that represents steps taken to extract smaller chunks of data from these large systems. Our system will also need to support forensic efforts related to new storage media as best effort procedures emerge.

2.4.2.8 Time to System Delivery

We are positive that some firms are already using electronic systems to manage forensic documentation for some components of the entire forensic

process. Primarily, these systems support forensic acquisition and forensic preservation. However, ICG is fairly positive that no firm has been able to release such a tool that is used to support field, or on-site, forensic efforts that do not occur at the firms' offices. Additionally, ICG is fairly positive that competing forensic firms do not have tools to document all areas of the forensic process from data enumeration through data presentation.

ICG feels that, though no systems like this exist, competitors likely realize the benefits of a tool like our proposed Electronic Evidence Management System and may currently be working on similar projects. ICG needs to beat these competitors to market with their tool.

2.4.2.9 User Education and Acceptance

ICG's existing paper-based system is very similar to those used by most firms in the computer forensics arena, including most law enforcement agencies. Forensic Analysts seek to minimize differences in the way their work is conducted so as to avoid questions, scrutiny, and legal challenges that arise when non-standard practices are adopted.

Additionally, many experts believe humans are pattern-seeking creatures. Introduction of the Electronic Evidence Management System will necessitate learning to use a new system. There may be resistance from ICG's forensic analysts that our team must overcome.

2.4.3 Risk Measurement

We must decide what are highest risk is so we can focus the bulk of our attention toward that area of the project. Identifying high, medium and low risks will serve to fascilitate the project by allowing us to manage our time more efficiently.

Risk	Level of Complexity	Description
Legal Challenges	Highest	Attack the integrity and control of data within our system, to show that data within our system can be altered and provide a misrepresentation of a forensic analysts findings and methodologies.
No Internet Connection Available	Low	Client systems cannot connect to servers.
Server Failure	Medium	Server Failure may disrupt ICG business continuity.
Erroneous Data Entry	High	Erroneous data entry will need to be corrected in a controlled fashion
Database Corruption	Lowest	Database corruption may occur, invalidating the integrity of forensic documentation stored therin.
Hacking	Medium	There is a heightened motivation of individuals to attach our system as it exists in a litigation environment.
Adaptation of System to the Future of Data Forensics	High	Our system would be a large waste of resources if it is unable to keep pace with ever-changing technology and its associated implications on electronic data forensics.
Time to System Delivery	Medium	Competition may be working on similar systems. ICG should strive to beat the competition to market.
User Education and Acceptance	Medium	It may be difficult to get forensic analysts to accept an electronic system that replaces the existing widely-accepted paper-based systems.

Table 2.16 Risk Measurement

We conclude that our high/highest risks in this project are legal challenges, erroneous data entry and adaptation of system to the future of data forensics.

2.4.4 Risk Minimization Table

A breakup of the risks at different stages of the project.

Phase	WBS Task	Risk Identification	Risk Elimination Milestone
Phase I	Project Initiation	1. Team is not formed	
		2. Team does not like project	
		Overview	Team Certification
		3. Important information	NDA Signed by each team member
Phase II	Project Planning	1. AS-IS analysis not possible	
		2. Project is not technically feasible	
		3. Project is not economically feasible	Team Roles and Responsibilities
Phase III	Requirements	1. All stakeholders are not identified	
	Analysis	2. Delay in gathering requirements	
		3. Improper mapping of functional	
		requirements	
			Midterm Documentation
Phase IV	System Design	1. Paper based form to online forms	Prototype 1
	Implementation	2. Digital Check point for prototype I	Prototype 2
		3. Prototype 3 is not completed	Prototype 3
		4. Final Product is not integrated	Final Document
		1. Test cases do not test entire	
Phase V	Testing	functionality	
		2. Test cases cannot be executed	Final Product

Table 2.17 Risk Minimization

Here is break down of how we are going to attack our risks.

2.4.4.1 Legal Challenges

Legal challenges are obviously the most critical risk that our team must take into account when designing the Electronic Evidence Management System. Our team will take the following steps to mitigate the issue and reach of discovery requests and minimize interruptions of ICG's ability to deliver promised work to their clients:

- Well documented system functionality will assist ICG in minimizing the reach or necessity of a discovery request targeting the system.
- Independent auditing of our system by an organization such as the National Institute of Standards and Technology (NIST) Computer Forensic Tool Testing (CFTT) Division will reduce the ability for opposing counsel to have the court approve an electronic discovery request targeting the system.
- We will package small thermal printers to travel with the Tablet PC client systems such that an audit trail of data entered at the client level can be printed at the time of data entry, and later used to audit data stored server-side. The lack of this functionality has hindered the adoption of electronic voting machines.

- We will implement fully redundant database servers that will mirror all records in the records storage database of the Electronic Evidence Management System. In this way, ICG will be able to maintain business continuity should one server be taken offline for forensic analysis by an outside firm.

2.4.4.2 Erroneous Data Entry

To account for human error, our system will incorporate a document and record revision control system. An analyst will be able to review initially entered data and sign records as being correct, at which point and time, the data is locked into the system such that the analyst may not alter that version of the documentation. To account for error, the analyst must be able to propose revisions to the locked documentation and provide a reason why the documentation was incorrect and note why he or she initially certified the erroneous data as correct.

The analysts' project managers must be able to review, approve, and add notes to the proposed revised documentation. The project manager must be able to add his own notes regarding the errors, then approve or disapprove the changes and authenticate the decision with a signature. At this point and time, the data is

locked into the system such that the project manager may not alter the new version of the documentation.

Changes to the project manager's approved changes will require a similar process to be carried out by the head of the forensics department, or a member of the organization's executive staff.

2.4.4.3 Adaptation of System to the Future of Data Forensics

The Electronic Evidence Management System will be extensible in that data enumeration, acquisition, preservation and analysis templates and the associated data storage templates may be incorporated into the system. This will let our system support forensic efforts related to new storage media and data acquisition techniques as best-effort and best-practice procedures emerge.

2.4.4.4 Hacking of the Electronic Evidence Management System

Any security models and software incorporated into our system will be well established, tested, and frequently-audited technologies. Though no system connected to any network is fully secure, this system will be as secure as best-effort and best-practice security models are able to provide.

2.4.4.5 Time to System Delivery

We will develop the system leveraging a spiral development model and rapid application development techniques to focus on delivering functional prototypes as quickly as possible, so ICG can develop a training program, conduct test usage sessions, and help us to develop a system as quickly as is possible so that ICG can beat their competition to market.

2.4.4.6 User Acceptance and Education

To encourage user acceptance, our system must take extra care to far surpass the existing paper-based system in terms of user-experience, ease of use, and reduction of data that must be entered by an analyst. The Electronic Evidence Management System will include the following features that we feel will ease transition and benefit the analyst.

2.4.4.7 On-Line Help System and Knowledge Base

ICG's system will include a help system that explains each data entry field, and offer help on how to forensically obtain the information that should populate a given field. Additionally, a forum-like user comments section on each data entry

page will let our users share tips, do's, and do not's with each other. As the user-driven knowledge-base grows, it will include help even for items our development team would never have been able to predict and help ICG to train new analysts in a shorter amount of time. ICG can be more confident in sending new analysts out to perform field work.

2.4.4.8 Server Failure

To minimize the interruption of business continuity that could result from one of our records servers crashing for any number of reasons, we will deploy a redundant, synchronous server environment and use dynamic DNS to automatically send data to the first available server.

Additionally, our system will include a script to completely package our applications and data into a small number of archive files for backup on ICG's existing data archival systems. Our system will also include a script to restore the data to a new server with minimal information technology staff interaction.

2.4.4.9 No Internet Connection Available

To minimize these occurrences, the client Tablet PC systems will have all necessary interfaces to utilize most common types of network adapters. Additionally, system cost will include subscriptions to various Internet Service

Providers(ISPs) each covering a different network technology. Though these measures can minimize such situations, our electronic system will still need to be complimented by an off-line paper-based component and have a post-live interface to for the entry of data on paper-based documentation into the Electronic Evidence Management System.

2.4.4.10 Database Corruption

The system will automatically monitor itself for data corruption and notify information technology staff when and if the database needs to be repaired or restored from a backup. This functionality already exists in most enterprise database server software today.