Security Risk Management Framework for the SEAD Practicum

Professional Project

December 9, 2005

Submitted to:
Professor Dan Likarish

Submitted by:
Janice M. Carney
Certification of Authorship

Regis University
School for Professional Studies
MSCIT Program

Certification of Authorship of Professional Project Work

Submitted to: ______Dan Likarish________

Student’s Name: ____Janice M. Carney________

Date of Submission: _December 9, 2005________

Title of Submission: _Security Risk Management Framework for the SEAD Practicum__

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for the purpose of partial fulfillment of requirements for the MSC 696 or MSC 696B course.

Student’s Signature: ___Janice M. Carney________
Advisor Approval

Regis University
School for Professional Studies
MSCIT Program

Student’s Name: __ Janice M. Carney____________________________

Title: _ Security Risk Management Framework for the SEAD Practicum _

**Advisor’s Declaration**: I have advised this student through the Professional Project Process and approve of the final document as acceptable to be submitted as fulfillment of requirements for the MSC 696A, 696B and 696C courses. The student has received project approval from Advisory Board and has followed due process in the completion of the project and subsequent documentation.

ADVISOR

Name __________________________ Signature __________________________ Date __________________________
## Revisions History

<table>
<thead>
<tr>
<th>Date Submitted</th>
<th>Submission Matter</th>
<th>Date Returned</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/05</td>
<td>1 page Project Proposal</td>
<td>03/08/05</td>
<td>Dan Likarish felt would integrate well with overall group</td>
</tr>
<tr>
<td>03/27/05</td>
<td>Chapter 1 Introduction</td>
<td>04/03/05</td>
<td>Positive feedback, proceed to research</td>
</tr>
<tr>
<td>05/25/05</td>
<td>Chapter 1 &amp; 2</td>
<td>08/17/05</td>
<td>Positive feedback; must write in past tense</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>References on figures</td>
</tr>
<tr>
<td>12/04/05</td>
<td>Final Rough Draft</td>
<td>12/05/05</td>
<td>Positive feedback; add role assignments for next steps</td>
</tr>
<tr>
<td>12/10/05</td>
<td>Final Submission</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Acknowledgments

To Adrian:
Thank you for the meals you cooked, the clothes you washed, and all the emotional support you gave. Without it, I would never have been able to complete this Masters program. This is as much your degree as mine. Here is to at least 28 more years of fun!
I love you!

To Jan, Tony and Ron:
My co-workers, who went through the program at the same time, thank you for being sounding boards. This experience made our department stronger than before. Even though Coosa Valley Tech is breaking us up, we will forever be bound by this experience.
Abstract

To minimize security risks in a technology system, a security plan should begin in the first stages of the software development life cycle (SDLC) and should continue through all phases of the project. This professional project resulted in a preliminary outline to a security risk management framework, as a component of the SDLC framework for developing software as a participant of the Software Engineering and Applications Development (SEAD) practicum. This project proposed the beginnings of a framework to DEAL with risk: Discover risk and vulnerabilities, Evaluate them, take Actions and apply Learned Lessons in the cyclic process. The DEAL plan was based well-known frameworks such as Microsoft Solutions Framework and Microsoft Operations Framework. The security risk management framework has defined a methodology by which security issues at the software development level will be identified and documented. The plan has recommended the use of best practices for secure programming to be followed during all stages of the SDLC.
# Table of Contents

Certification of Authorship........................................................................................................... 2  
Advisor Approval........................................................................................................................... 3  
Revisions History........................................................................................................................... 4  
Acknowledgments.......................................................................................................................... 5  
Abstract....................................................................................................................................... 6  
Table of Contents............................................................................................................................ 7  
Table of Figures............................................................................................................................... 9  

## Chapter 1  
Security Risk Management Framework for SEAD Practicum......................................................... 10  
  Thesis Statement........................................................................................................................... 10  
  Existing Situation........................................................................................................................... 10  
  Constraints................................................................................................................................... 11  
  Research....................................................................................................................................... 12  
Methodology, Deliverables and Estimated Times............................................................................ 12  
  Phase 1 - Discovery....................................................................................................................... 12  
  Phase 2 - Design............................................................................................................................ 12  
  Phase 3 - Develop.......................................................................................................................... 13  
  Phase 4 - Deploy............................................................................................................................ 13  
Next Evolution................................................................................................................................ 13  

## Chapter 2  
Research........................................................................................................................................ 14  
  Introduction................................................................................................................................ 14  
  SOA – Service Oriented Architecture............................................................................................. 15  
    Background................................................................................................................................. 15  
    SOA and Web Services Details...................................................................................................... 17  
  MOF – Microsoft Operations Framework..................................................................................... 20  
    Background................................................................................................................................. 20  
    Details....................................................................................................................................... 20  
    Team Model................................................................................................................................. 21  
    Process Model.............................................................................................................................. 22  
    Risk Management Discipline...................................................................................................... 25  
  MSF – Microsoft Solutions Framework......................................................................................... 26  
    Background................................................................................................................................. 26  
    Details....................................................................................................................................... 27  
    Team Model................................................................................................................................. 28  
    Process Model.............................................................................................................................. 28  
    MSF Project Management Discipline........................................................................................ 29  
    MSF Risk Management Discipline............................................................................................ 29  
ISO/IEC 17799 and BS 7799............................................................................................................ 31  
  Background................................................................................................................................. 31  
  Details......................................................................................................................................... 32  
ITIL – IT Infrastructure Library....................................................................................................... 33  
  Background................................................................................................................................. 33  
  Details......................................................................................................................................... 34
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Source</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MOF Team Model Role Clusters</td>
<td>(MOF, 2004)</td>
<td>22</td>
</tr>
<tr>
<td>2</td>
<td>The MOF Process Model</td>
<td>(MOF, 2004)</td>
<td>23</td>
</tr>
<tr>
<td>3</td>
<td>The process of managing risk</td>
<td>(“Risk Management Discipline“, 2005)</td>
<td>26</td>
</tr>
<tr>
<td>4</td>
<td>The Process Model</td>
<td>(MSF, 2003)</td>
<td>29</td>
</tr>
<tr>
<td>5</td>
<td>MSF Risk Management Process</td>
<td>(MSF Risk Management, 2002)</td>
<td>30</td>
</tr>
</tbody>
</table>
Chapter 1

Security Risk Management Framework for SEAD Practicum

Thesis Statement

To minimize security risks in a technology system, a security plan should begin in the first stages of the software development life cycle (SDLC) and should continue through all phases of the project. This professional project has resulted in a general outline for security risk management framework, which will be a part of the SDLC framework for developing software as a part of the Software Engineering and Applications Development (SEAD) Practicum.

The security risk management framework has defined a methodology by which security issues at the software development level will be identified and documented. The plan has recommended the use of best practices for secure programming to be followed during all stages of the SDLC. The desired result of the security risk management framework has been to minimize security breaches in the software produced by students participating in SEAD.

Existing Situation

RegisARN, Regis Academic Research Network (ARN), is a student run and managed internetwork that was established to service the needs of students in the MSCIT program at Regis University. The Networking Lab Practicum (NLP) began in July 2000 as a way to provide graduate students with a networking emphasis a real world experience by actively participating in the support of RegisARN. In 2005, NLP
was renamed to Software Engineering and Applications Development (SEAD) to reflect the current industry naming conventions and updated Regis curriculum. The SEAD practicum is a six month assignment for graduate students where experience can be gained as if working in an IT company and at the same time complete work on professional projects.

SEAD is organized into four groups: data access, network, operations and development. The development group of the SEAD is responsible for the MSCIT Portal, Visual Basic script development and Java Script development including portlets, javalets, and servlets. It is for the development group that this professional paper was created. As a relatively new addition to SEAD at the time of this writing, the development group lacked formal guidelines for work produced by the members. Without a framework in which to work, the development group will not mature or be productive; the group will not be able to withstand the rebuilding of the group every six months that is inherit to the SEAD structure.

As one part of an operational framework, the security risk management plan recommended a method be devised by which developers could identify and document known security issues at the programming level. By consulting a list of known issues and following a best practices methodology, a programmer could produce applications that withstand known security problem areas.

**Constraints**

Two constraints were identified at the onset of this professional project. The first constraint was that this plan was one small part of the overall framework for the operating procedures of the development group of SEAD. Since the operating
framework was concurrently in development, the guidelines set forth by that plan could impact the development of the security risk management framework. The second constraint identified was time. The goal of this project was to create a framework for a security risk management plan. However within the six month timeframe of the SEAD participation, the plan produced that would be incomplete. The next group of SEAD students would be required to continue the research and modify the plan.

**Research**

The structure of the security risk management framework has been designed to follow guidelines promoted by the IT Infrastructure Library (ITIL), ISO/IEC 17799/BS 7799, Microsoft Operations Framework (MOF), and Microsoft Solutions Framework (MSF). The architecture of the development in the SEAD was directed to follow the Service Oriented Architecture (SOA) recommendations. With these frameworks as guidelines, the research for this project included whitepapers, articles and text, which described SOA, MOF, MSF, ISO/IEC 17799 and ITIL.

**Methodology, Deliverables and Estimated Times**

This project consisted of four phases as described below.

**Phase 1 - Discovery**

*Task*: This phase is when the before mentioned research was conducted.

*Deliverable*: Summaries of research.

*Time*: 40 Hours

**Phase 2 - Design**

*Task*: During this phase, the results of the discovery phase were compiled.
Deliverable: The framework components for the SEAD development group were identified.

Time: 60 Hours

Phase 3 - Develop

Task: The security risk management plan was constructed in this phase from the elements identified in the define stage. After this phase, the plan was made available for review.

Deliverable: Security risk management plan drafted.

Time: 40 Hours

Phase 4 - Deploy

Task: Revisions that resulted from the review of the product developed in phase 3 was incorporated to the document during this phase.

Deliverable: Final product.

Time: 40 Hours

Next Evolution

Still in its infancy, SEAD is evolving. With the six-month tenure of each assignment, work on this Security Risk Management framework will need to continue. A method to document security issues will need to be designed, developed and implemented. Best practices will need to be constructed and documented. A methodology of locating and incorporating the best practices will need to be developed. This project has been just the beginning of an on-going process.
Chapter 2

Research

Introduction

Providing security to IT systems is a major issue for all computer professionals. With the growing use of the Internet for e-business, security will continue to be a major concern. In the 2004 E-Crime Watch Survey™ conducted by Carnegie Mellow SEI, 56% of respondents reported operational losses and 25% reported financial losses due to e-crimes (“2004 E-Crime”, 2004).

Many companies have employed firewalls and intrusion detection systems to combat e-crimes. However, these tools only provide a single level of defense. A more in-depth defense mechanism is needed to deal with security issues (Ankolekar, 2003). By drilling down to the programming level, risks can be mitigated and attacks can be minimized. This will help reduce the application maintenance costs and public relations issues (Ankolekar, 2003).

Certain software vulnerabilities that can be addressed in the software development life cycle are well documented. These vulnerabilities have been attributed to poor programming techniques (Ankolekar, 2003). The following is a list of a few of the well known vulnerabilities (Ankolekar, 2003):

• Access control – inadequate input validation allow unauthorized users to access sensitive parts of a system and data.

• Buffer overflows – lack of adequate size checking on input data will allow memory contents to be overwritten. This error leaves an application
unstable and can lead to problems such as Denial of Service attacks or unauthorized code hacks.

- Injection attacks – several different injection attack types exist, but the common theme is script code is entered into an input field. Without proper input validation techniques, the code executes allowing access to backend data and buffer overflows.

Most of the above mentioned vulnerabilities should be addressed as part of a framework of the SDLC by requiring stringent validation processes and other secure programming techniques.

Many frameworks exist which provide guidelines and best practices for managing IT processes. While differing in the methods employed, all frameworks strive to promote a proactive approach to increase the success and survivability of an IT system. Several of these frameworks were researched for this project. They included IT Infrastructure Library (ITIL), ISO/IEC 17799/BS 7799, Service Oriented Architecture (SOA), Microsoft Operations Framework v3.0 (MOF) and Microsoft Solutions Framework (MSF). Since the desired result of the paper was to deliver a security risk management plan for SEAD, the focus on the research was on security and the risk management portions of the researched frameworks.

**SOA – Service Oriented Architecture**

**Background**

Service Oriented Architecture (SOA) is a relatively new paradigm that was developed from lessons learned in programming over the last 50 years. To understand SOA, a brief look back will help. Early computer programs were sequential in nature.
As the programs became more complex, programmers began to use modular design methods. The modular method allowed for the creation of subroutines that could be copied and pasted throughout many systems. This helped in development, but was a maintenance quagmire. If bugs were discovered or the subroutines functionality needed to change, all instances of the subroutine had to be located and changed.

From procedural languages, programming moved to an object oriented approach in the 1960’s. Simula, developed in Norway, is credited with being the first language to use classes and objects (Satzinger, 2002). Object frameworks are sets of classes that are designed with reuse in mind. Libraries of objects are supplied by vendors which can be included in new development (Satzinger, 2002). Java Foundations Classes and Microsoft Foundation Classes are two such libraries. Even though these foundation classes allow for increased productivity in developing a system, several design considerations must be taken into account (Satzinger, 2002):

- The decision on which framework to use must be made before detailed analysis begins.
- The framework imposes the requirement to conform to specific structure and operation.
- If multiple frameworks are required, compatibility and integration testing should be undertaken early.

It is the integration of multiple frameworks that generate the most problems within object-oriented development (Satzinger, 2002):

Another level of reusable programming came with component based programming standards. Distributed Component Object Method (DCOM) and Common
Object Request Broker Architecture (CORBA) are the most widely used component base methods. As standardized and interchangeable software parts, components differ from object-oriented in that components are binary not symbolic (Satzinger, 2002). For this reason, reusing and implementing components is simplified (Satzinger, 2002).

The next step in this programming evolution is SOA. With the advent of enterprise systems, distributed computing environments need to be adaptable to changes (“Service-Oriented Architecture and Web Services”, 2004). SOA is a design paradigm that advocates breaking systems down into business services that link together through heterogeneous networks (“Service Orientated Architecture”, 2004). The major difference in component based architectures and SOA is that SOA promotes the separation and independence of the service from the technology that provides the service.

**SOA and Web Services Details**

In his IBM Academic Initiative presentation, Kevin R Faughman states “SOA is different things to different people” (“In-demand skills”, 2005). For the business executive, SOA is a set of services that the business uses to interact with customers, partners and within it own organization. For the architect, SOA is a set of principles and patterns for producing systems that are characterized as being modular, encapsulated, loosely coupled, reusable and composed. This architectural style contains three elements: a service, a service provider and a service requestor. Finally for the programmer, SOA is implemented through the use of standards and technology such as Web Services.
It is the use of Web Services technology that makes SOA powerful (“Service-Oriented Architecture and Web Services”, 2004). Built on open standards, services communicate seamlessly even though different languages and applications platforms may have been used to create them. (“Service-Oriented Architecture and Web Services”, 2004) This use of standards based development in distributed computing allows for responsive and flexible services provided to clients and business partners.

Web Services are replacing the web of yesteryear where HTML was used simply as a presentation tool. A Web Service is defined by the W3C Working Group as “…a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.” (“Web Services Architecture”, 2004)

By design, Web Services are autonomous: automating processes and the updates that occur in the processes. (“An Adaptive Approach”, 2004) The exchange of information over the public network by Web Services has been designed for speed not necessarily security. Vulnerabilities exist in several areas, according to the white paper published by ForumSystems. These include:

- The Web Services Description Language (WSDL) documents are scanned without authorization and information is seized.
- Simple Object Access Protocol (SOAP) messages are tampered with and therefore Web Services are disabled or corrupted.
• SQL injections occur which corrupt data or allow attackers to gain unauthorized access to databases.

Several standards are under construction to address the security in Web Services. The standards are addressing issues such as privacy, trust and reliability. ("An Adaptive Approach", 2004) Two groups that are spear heading the development of the standards are WS-I and OASIS.

WS-I, the Web Services Interoperability Organization (www.ws-i.org), is an open industry organization whose charter is to “promote web services interoperability across platforms, operating systems and programming languages.” ("Interoperability", 2004) The Basic Security Profile Working Group deals with transport Security, SOAP messaging security and other Basic-Profile oriented Web Services security considerations. ("Interoperability", 2004)

Oasis, Organization for the Advancement of Structure Information Standards, is an international not-for-profit consortium (www.oasis-open.org). This group is involved in the development of e-business standards. Several Technical Committees (TCs) at Oasis are developing security standards for e-business and Web Services applications. These committees include but are not limited to:

• OASIS Web Services Security (WSS) TC whose focus is on implementing security functions in messages.

• OASIS Security Services (SAML) TC that is defining an XML based framework for creating and exchanging security information between partners.
**MOF – Microsoft Operations Framework**

**Background**

Microsoft Operations Framework (MOF) is an operational framework developed by Microsoft, which is based on the published works of the United Kingdom Office of Government Commerce (OGC). By combining OGCs IT Infrastructure Library (ITIL) guidelines with their own lessons learned, Microsoft has developed MOF to enable organizations to achieve dependable, adoptable, and scalable mission critical systems. (MOF, 2004)

The first version of MOF was created in 1999. As a complement to Microsoft Solutions Framework (MSF), MOF used the ITIL as a basis for providing IT service management. MSF Provided guidelines for solutions and applications development. Once the solution or application is developed, MOF guidelines take over to support the system. MSF are guidelines to “build it right”; MOF are guidelines to “run it right” (MSF, 2003). The current version of MOF is version 3.0. It was released to streamline MOF and align the framework with ITIL v2.0 and MSF v3.0.

**Details**

MOF is comprised of three foundation elements: the Team Model, the Process Model and the Risk Management Discipline. These core components are designed to provide guidance about the people, the processes and risk management in IT service. The focus of each of these elements is on the enabling technologies and best practices in order to achieve the goal of high systems availability, reliability, supportability and manageability on the Microsoft platforms. In addition, MOF provides guidance to achieving interoperability with other technology platforms (MOF, 2004).
**Team Model**

The Team Model deals with the people involved in IT operations. By dividing IT operations into role clusters, even the most complex IT operations of the distributed environments can utilize people’s skills sets more effectively. This division of assignments is based on industry best practices. They are designed to provide flexible, accountable and responsible team roles. By evaluating performance of role clusters, roles can be adapted to provide improvements in effectiveness.

Five primary principles apply to all role clusters in the MOF Team Model (MOF, 2004):

- To provide timely, efficient, and accurate customer service.
- To understand the business priorities and enable IT to add business value.
- To build strong, synergistic virtual teams.
- To leverage IT automation and knowledge management tools.
- To attract, develop, and retain strong IT operations staff.

As shown in the diagram below, role clusters in the MOF Team Model are broken into seven general categories. Associated with each role cluster is a role description. For the focus of this paper, the security cluster was of interest. This cluster’s role responsibilities include ensuring confidentiality, integrity and availability of data. This C.I.A. triangle goes back to the days of mainframes and is considered an industry standard for computer security.
Process Model

The MOF Process Model provides a scheme for managing and maintaining IT services. Microsoft states the MOF Process Model “describes a life cycle” for releases of IT service products of any size and solution (MOF, 2004). The MOF Process Model is broken into four quadrants and each quadrant maintains its own goals and requires an operation management review (OMR). By subjecting significant milestones in the operation file cycle to OMRs, key decisions are well thought out. The OMRs help ensure that when decisions are made, it is with the involvement of proper stakeholders and that necessary information and expectations have been included. In addition, OMRs require all processes to be well documented for future actions.

As shown in the diagram below, Microsoft presents the MOF Process Model as a sequential process. However, Microsoft maintains that several releases, each in a different stage in the IT life cycle may occur at the same time. Each quadrant consists of service management functions (SMFs). Many of the SMFs are based on services...
defined in OGC’s ITIL. Several SMFs are not described in ITIL, as they are specific to the Microsoft platform. This is true of all SMFs in the Operation quadrant and the workforce Management SMF in the Optimizing Quadrant.

Two SMFs in the Process Model of interest in this research were the Security Administration SMF in the Operating Quadrant and the Security Management SMF in the Optimizing Quadrant.

The Security Administration SMF has three goals ("MSF Security Administration", 2005).

- Data confidentiality. No one should be able to view an organization’s data without authorization.
- Data integrity. All authorized users should feel confident that the data presented to them is accurate and not improperly modified.
- Data availability. Authorized users should be able to access the data they need, when they need it.
To achieve these goals, six security requirements are identified by Microsoft. ("MSF Security Administration", 2005)

- Identification - Identification is concerned with user names and how users identify themselves to a computer system.
- Authentication - Authentication is concerned with passwords, smart cards, biometrics, and so forth. Authentication is how users demonstrate to the system that they are who they claim to be.
- Access control (also called authorization) - Access control is concerned with access and privileges granted to users so that they may perform certain functions on a computer system.
- Confidentiality - Confidentiality is concerned with encryption. Confidentiality mechanisms help ensure that only authorized people can see data stored on or traveling across the network.
- Integrity - Integrity is concerned with checksums and digital signatures. Integrity mechanisms help ensure that data is not garbled, lost, or changed when traveling across the network.
- Nonrepudiation - Nonrepudiation is a means of providing proof of data transmission or receipt so that the occurrence of a transaction cannot later be denied.

Microsoft identifies several elements within the scope of the Security Administration SMF which should be part of a systems infrastructure. Of the eight items identified, two relevant aspects are the application security and middleware security. Application security involves determining whether users are authorized to access a
system. Middleware security deals with ensuring that messages passed between services and databases are not viewed, tampered with, or garbled.

The Security Management SMF advocates developing a well defined strategy to maintain security within an organization’s technology structure. A key element in this strategy is policies and procedures that are well documented and communicated to staff and partners. The Security Management SMF uses controls as a way to mitigate security issues. A control can be either computer based or procedural based. Administrative controls are guidelines, defined through policies, standards and procedures, which establish the security framework. A security framework will need to be subjected to a thorough assessment on a regular basis to keep the framework current. The security framework will be the layer in the defense in depth security strategy which defines the security controls at the physical, perimeter, network, host application and data layers (“MSF Security Management”, 2005).

Risk Management Discipline

The third foundation element of the MOF is referred to as a discipline. Microsoft makes the differentiation between a model and a discipline, stating that discipline knowledge may be applied at any time and during any process (“Risk Management Discipline”, 2005). The MOF Risk Management Discipline advocates taking a proactive approach to risk management as opposed to a reactive approach.


- Assess continuously.
- Integrate risk management into all roles and functions.
• Treat risk identification in a positive manner.
• Use risk based scheduling.
• Establish formal process that are documented, understood and used.

Identify, analyze, plan, track, control and learn are the steps outlining by the Risk Management Discipline. At least once, each risk identified will go through each and every step. Risks may actually cycle through the steps multiple times in the process of determining a risk’s effect throughout the life cycle of an IT system. By taking this proactive approach to risk assessment throughout an IT systems life cycle, vulnerabilities can be diminished.

**MSF – Microsoft Solutions Framework**

**Background**

Microsoft Solutions Framework was originally a collection of best practices introduced in 1994. With 25 years of experience in the high-tech industry, Microsoft has drawn on lessons learned from Microsoft product groups, Microsoft Services,
Microsoft’s internal Operations and Technology Group (OTG), partners as well as well-known industry best practices to develop the MSF (MSF, 2003). MSF is an adaptable approach for developing IT solutions on time and within budget.

MSF and MOF work in conjunction with each other to cover the life cycle of a project from conception through production and beyond to eventual retirement. Microsoft advocates using MSF to “build it right” and MOF to “run it right.” MOF and MSF share foundation principles and core disciplines (MSF, 2003). However the application of these principles and disciplines differ. MSF focus if from a “solutions delivery perspective; MOF is from a “service management perspective” (MSF, 2003).

Details

MSF is broken into fire core areas: Team Model, Process Model, Project Management Discipline, Risk Management Discipline, and the Readiness Management Discipline. Using foundational principle throughout the fire core areas, MSF will help developers deliver a successful technology solution. To achieve this end, the MSF describe a “how to” for the following: (MSF, 2003)

- Align business and technology goals.
- Establish clear project goals, roles and responsibilities.
- Implement an iterative, milestone-driven process.
- Proactively manage risks.
- Effectively respond to change.
- Learn from experiences.
Team Model

The Team Model of the MSF defines goal-driven roles and responsibilities for all members of a project. Personnel are divided into team role clusters (or simply roles) and the domain of each role is defined by functionality of skill sets and knowledge areas. The following table depicts role clusters and goals of each.

<table>
<thead>
<tr>
<th>Key Quality Goal MSF</th>
<th>Team Role Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery within project constraints</td>
<td>Program Management</td>
</tr>
<tr>
<td>Delivery to product specifications</td>
<td>Development</td>
</tr>
<tr>
<td>Release after addressing all issues</td>
<td>Test</td>
</tr>
<tr>
<td>Smooth deployment and ongoing management</td>
<td>Release Management</td>
</tr>
<tr>
<td>Enhanced user performance</td>
<td>User Experience</td>
</tr>
<tr>
<td>Satisfied customers</td>
<td>Product Management</td>
</tr>
</tbody>
</table>

There is not a one-to-one correlation between roles and people. On large projects, a role may actually be filled by several people. In a small project, one person may fulfill several roles. Regardless of assignments, a role and stakeholders of the project should be aware of the accountability of each goal.

Process Model

The activity a project goes through from conception to delivery into production is referred to as the life-cycle. Several life cycle methodologies exist. The MSF Process Model pulls on the strength of the traditional waterfall model and the spiral models. The diagram below shows how the MSF Process Model is broken into five phases. Each phase produces a deliverable that marks the end of that phase and the beginning of the next, as in the spiral model. Milestones, as used in the waterfall model, are points in the project where objectives are reviewed to determine if they have been satisfied.
**MSF Project Management Discipline**

The MSF Project Management Discipline is based on well established best practices and standards published by organizations such as Project Management Institute (PMI®), International Project Management Association (IPMA) and Projects In Controlled Environment (Prince2™). The MSF Project Management Discipline outlines steps for distributed project management (PM) responsibilities throughout the teams in a project. The PM role cluster is responsible for coordinating the project processing, planning and scheduling.

**MSF Risk Management Discipline**

Taking a proactive approach, the Risk Management Discipline uses a six step method to mitigate risk within a project. The MSF Risk Management Discipline advocates that risk is a factor in all projects (MSF Risk Management, 2002). To mitigate those risks, a proactive and positive approach is desirable. This approach includes determining root causes of risk and having a well documented resolution structure in place to address issues before they arise. The risk management plan should also be adjusted continuously to reflect lessons learned.
The six steps of identify, analyze and prioritize, plan and schedule, track and report, control and learn are to be continuously followed throughout the entire life cycle of the IT project. In identifying risks, a risk knowledge base is built. Several sources may be used to build a risk knowledge base. These include: lessons learned and publicly available sources such as Carnegie Mellon University's Computer Emergency Response Team (CERT®). Using this information, risks should be categorized to help approach risk management in a well structured manner. Risks identified should then be analyzed and prioritized.

The analysis process will be used to determine which risks are most relevant and therefore should be addressed first. By associating a numerical score to identified
issues, risks can be systematically prioritized. Probability and impact are the two widely accepted components used in determining a risk priority level (MSF Risk Management, 2002). Probability is the measure used to identify a risk will occur and impact is the effect the risk will have on the overall system if the risk does occur. Once a numeric score for each component is identified, a risk exposure metric can be calculated by multiplying impact and probability. This metric can then be used to prioritize risk (MSF Risk Management, 2002). This information is then used to build a master risk list.

The master risk list is used in the risk planning and scheduling phase to create action plans for controlling risk. The action plans detail how and where in the project a risk can be minimized. The next phase of the MSF Risk Management Discipline is to track and report on the implementation of action plans. During this phase, if a risk is identified as needing actions, it triggers a control measure from step five of the Risk Management Discipline. The final step in the MSF Risk Management Discipline is the documentation of lessons learned. These are then used in the continuous cycle of risk management.

**ISO/IEC 17799 and BS 7799**

**Background**

The International Standards Organization (ISO), in conjunction with the International Electrotechnical Commission (IEC) published ISO/IEC 17799 in December 2000 (Whitman, 2005). ISO/IEC 17799 is a non-vendor specific standard whose objective is to “give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their
ISO 17799 advocates a cyclic four step process of Plan, Do, Check and Act. A security risk management system, according to ISO 17799, will consist of ten security controls. These include: (Info-Tech Research Group, 2003)

- Security Policy – A detailed document which maps a company’s security goals.
- System access control – Rules which outline the authorized access level to all assets.
• System development and Maintenance – Build security controls into the entire life cycle of an application.

• Personnel security – Access and assign security responsibilities from recruitment through the full tenure of an employee.

• Physical security – Secure physical areas and work environments of all facilities.

• Organizational security – A forum for reviewing and approving security policies and roles.

• Asset classification and control – Identify and prioritize corporate assets. This control determines ownership and accountability for assets.

• Communication and operations management – Disseminate security instructions to employees to help manage daily operations of IT facilities.

• Compliance – Ensures legal and contractual obligations are maintained.

**ITIL – IT Infrastructure Library**

**Background**

The IT Infrastructure Library (ITIL) was developed in the 1980’s for use in the United Kingdom’s government IT departments (Sturm, 2000). Published by UK’s Office of Government Commerce (OGC), ITIL is widely used in Europe and is gaining recognition in the United States (Sturm, 2000). The evolving library consist of 44 volumes broken into eight core sets which cover best practices, guidelines, and cost effective measures for managing information technology services (Weil, 2004).
Details

The most commonly referenced books of ITIL are the Service Support and Service Delivery books (Weil, 2004). ITIL breaks IT activities into processes. Each process is then approached at three different levels: strategic, tactical and operational (Weil, 2004). At the strategic level, an organization’s objectives are determined and the methods to achieve the objectives are outlined. The strategic plan is then turned into a tactical plan which describes the execution and deployment of processes. It is in the operational level that tactical plans are executed and strategic goals are obtained.

The processes covered by the core sets of ITIL include:

Service Support

- Incident Management – Manage incidents so that the impact on business is minimal and normal levels of service are quickly restored.
- Problem Management – Control future incidents by determining underlying causes of service issues.
- Change Management – A “how to” implement changes quickly with a minimal impact to quality of service.
- Release Management – Managing hardware and software version releases.
- Configuration Management – Management of IT component and services.

Service Delivery

- Service Level Management – Identify client requirements to ensure services are maintained and delivered.
• Capacity Management – Manage IT services to align with current and future requirements of clients.
• Availability Management – Manage IT services to allow business to meet its objectives.
• Service Continuity Management – Maintain IT services in times of disasters.
• Financial Management – Manage IT costs.

The ITIL Information Security Management process defines information security as a cyclic process that should be reviewed and improved on an ongoing basis. The ITIL Information Security Process involves seven steps (Weil, 2004).

1. Identify security requirements using risk analysis.
2. Analyze and determine feasibility of requirements.
3. Define a Service Level Agreement (SLA) of negotiable security requirements in measurable terms.
4. Define an operational level agreement (OLA) which outlines how information security service will be provided.
5. Implement and monitor the SLA and OLA.
7. Modify as necessary.

**Conclusion**

Once all research for the Security Risk Management Framework for the SEAD practicum was completed, it became apparent that risks are a part of any IT system. To mitigate these risks, an organized and well-documented plan should be developed. The
plan should be cyclic in nature with several overlapping phases. The common themes of the researched frameworks included phases of identify, analyze, plan, track, control and learn. These phases helped form the major focus of the Security Risk Management Framework for SEAD.
Chapter 3

Security Risk Management Plan Framework

for SEAD Practicum

Introduction

The development group of the SEAD project is responsible for the MSCIT portal, Visual Basic and Java script development, including portlets, javalets and servlets. The development arm was added to the SEAD project (formerly NLP) in 2005. In its infancy, the group lacked formal guidelines for development. The first team of students to participate in the practicum was tasked with creating documents to serve as a basis for structured and secure applications development.

As one of the first from the 2005 practicum group, the intent of this project was to begin development of a security risk management framework to be used to identify and document security issues at the software development level. However, it is incomplete. This risk management document has merely laid a foundation from which future SEAD participants should build and enhance. Further research is needed, the framework needs to be completed and methodologies need to be developed.

The goal of the security risk management plan was to foster secure programming techniques to be used by all participants in the SEAD development group. This framework was modeled after many well known frameworks which were researched and documented in chapter 2. These frameworks differed in the approach taken to risk management, but all frameworks agreed in several key points. All researched frameworks agreed that risks were a part of all systems and a proactive approach must
be taken to mitigate the risks. A cyclic approach was also recommended by all frameworks. The cycle begins with a discovery process to identify and build a knowledge base of known risks and the process ends with lessons learned. The frameworks proposed adding to the knowledge base from the lessons learned. The documented lessons learned are also used to adjust the risk management plan continuously for improved performance.

Beginning with the software development life cycle, several vulnerabilities can be addressed. These vulnerabilities can be attributed to poor programming techniques. (Ankolekar, 2003) By addressing these during application development, more secure code can be developed. A few of these well known vulnerabilities include: (Ankolekar, 2003)

- Access control – inadequate input validation have allowed unauthorized users access to sensitive parts of a system and to data.
- Buffer overflows – lack of proper size checking on inputed data have allowed memory contents to be overwritten. This error has left applications unstable and susceptible to code hacks and DoS attacks.
- Injection attacks – improper validation techniques on input fields have allowed access to backend data and cause buffer overflows.

The researched frameworks proposed that an organized method of identifying and evaluating the vulnerabilities would help to mitigate the damage of these risks. Structured actions plans followed by documented lessons learned have proven to improve the survivability of a system. Using the researched frameworks as a basis, this
professional project proposed a proactive four step process for security risk management for the SEAD project:

- Discovery
- Evaluate
- Actions
- Lessons Learned

**Discovery**

The SEAD risk management plan recommended a list of software based vulnerabilities be built during the discovery phase. This list would be checked before any development for SEAD is begun. The goal of this phase was to produce a list of risks and vulnerabilities that is to be consulted during the SDLC of an application project for SEAD. Each risk should be clearly identified and documented.

The discovery phase of this plan has been based on the similar phases of the researched guidelines from chapter 2. It corresponds to the Risk Identification phase of the MSF Risk Management Discipline. The main goal of this phase was to make all members of a project aware of problems that could potentially lead to security breaches. (MSF Risk Management, 2002) This discovery phase reflects of the first step of the ITIL Information Security Process which proposes to identify security requirements using risk analysis. (Weil, 2004)

**Evaluate**

Analysis of risks documented during the discovery phase is to be performed during the evaluation phase. This analysis is to be used to evaluate the affect of the
risks on applications being developed and used to prioritize the risks. The result of this phase is to be used in the next phase.

The evaluation phase is modeled on the Risk Analysis phase of the MSF Risk Management Discipline. Risk analysis in the MSF discipline involves performing a mathematically scoring process on the risks identified in the previous phase. This is done to identify the most relevant and therefore first addressable risks. Probability, the measure of whether a risk will occur, and impact, the effect the risk will have if it occurs, are the two widely accepted components used in determining a risk priority level (MSF Risk Management, 2002). Once a numeric score for each component is identified, a risk exposure metric can be calculated by multiplying impact and probability. This metric can then be used to prioritize risks on a master risk list (MSF Risk Management, 2002).

**Actions**

Identified risk from the discovery phase which were deemed important through the prioritization process of the evaluating phase, are to be addressed in the actions phase. During the actions phase, proper programming strategies are to be developed, approved and incorporated. These actions would mitigate risks and associated vulnerabilities.

This phase corresponds to several phases of the MSF Risk Management Discipline: Risk Planning, Risk Scheduling, and Risk Tracking. It is during these phases that the identified master risk list from the previous phase was processed. Strategies and plans were developed, approved and enacted to manage risks. By tracking risks
and their associated action plans, progress can be monitored and strategies adapted as necessary (MSF Risk Management, 2002).

**Lessons Learned**

The lessons learned phase is to be an important part of the cyclic nature of the risk management plan. During this phase, lessons learned will be documented and added to the knowledge base which is to be used during the discovery phase. Lessons learned will also be used to continuously evaluate the risk management plan and adjust the plan as necessary.

The six months tenure of the SEAD practicum has made this phase especially important. This would be the beginning point for new participants to learn where past SEAD groups have worked. Also, at the end of a SEAD participant’s tenure, the lesson learned knowledge base will be update for the next group.

This projects Lessons Learned is based on a combination of the Risk Reporting, Risk Control and Risk Learning phases from the MSF Risk Management Discipline. It is during these phases that experiences are formally documented to be used in future projects.

**Summary**

This project has begun to lay a foundation for a risk management framework to incorporate secure programming practices when developing applications within the realm of the SEAD development group. The plan proposed to DEAL with risk: Discover, Evaluate, take Actions and Learn Lessons. Drawing heavily upon MSF Risk Management Discipline, a well known risk management discipline, the project proposed a proactive approach to risk management. The project has also recommended a cyclic
approach to risk management, so that lessons learned can be used to build a stronger knowledge base and to continuously improve the risk management plan.
Chapter 4

Project History / Future Direction

Project History

I learned about the NLP Practicum while taking MSCN 662 - Internetwork and WAN Design with Dan Likarish. It was an intriguing idea and therefore I applied. On November 19, 2004 I was accepted into Networking Lab Practicum, NLP, for the first group of 2005. The tenure of the practicum was for the first six months of 2005. I was very excited; it signaled a beginning to the end. I was however anxious about the unknown. On December 4, 2004 I participated in an orientation session which covered the basics of the NLP. We were informed that the NLP had been renamed SEAD, Systems Engineering and Application Development. The following charts showed the organization of the new groups.
I noticed my name on the chart underneath the Development group which struck me as odd since my area of emphasis at Regis had been Networking Technologies. When I talked with Dan Likarish on this matter he stated that since two of my co-workers were also participating in the practicum, he thought it best to keep us together. My co-workers emphasis of study was development. Therefore, I joined them in the Development group. Since I had stated on my application for the practicum that I had an interest in security, I was assigned to the Design and Architecture group with a security focus. The chart below shows the Development group’s structure.

**Development Organization**

![Development Organization Chart]

The development group of the SEAD was tasked with development within the MSCIT Portal, Visual Basic script development and Java Script development including
portlets, javalets, and servlets. As a relatively new addition to SEAD, the development group lacked formal guidelines for work produced by the group. Without a framework in which to work, the development group will not mature or be productive; the group will not be able to withstand the rebuilding of the group every six months that is inherent to the SEAD structure.

The professional papers from this first group of SEAD participants were to build a framework structure for development that could withstand rebuilding every six months. Documented processes for the users would make for a seamless transition from one SEAD group to the next. The individual members in the development group were to design a small portion of an overall framework for development. The papers were to consider the software development life cycle and all aspects therein.

I submitted my thesis proposal on March 7, 2005. My proposal was to develop a risk management plan that identified and tracked security vulnerabilities within software development. The proposed plan would follow the risk management plan documented in the Microsoft Solutions Framework of Identification, Analysis and Prioritization, Planning and Scheduling, Tracking and Reporting, Control, and Learning. The framework would be language independent plan: if a vulnerability exists in one language, it will exist in another. The tracked vulnerabilities would be used in setting up guidelines for how code should be developed to avoid these problems.

Work progressed on the project paper slowly. With teaching full time days, part-time nights, and taking a Regis class every eight weeks, this project was sometimes put on the back burner. The remainder of the submissions was as follows:

<table>
<thead>
<tr>
<th>Date Submitted</th>
<th>Submission Matter</th>
</tr>
</thead>
</table>


Once I got the “picture” of the project in my mind, it proceeded as I originally envisioned. I think this project met the goals I had, but I am not sure it met the goals of the overall goals for the development group. I do wish I had spent more time communicating with other Development group members. With all but 1 member of the development group being online, schedules were hard to coordinate.

The risk management plan submitted was not a completed framework. It was simply an outline for such a plan. It suggested that there is a need to DEAL with risk. The DEAL plan closely followed the Risk Management Discipline of the Microsoft Solutions Framework. Much work is left to be done on the plan by future groups.

**Future Direction**

Since this professional project has only begun to outline the framework for the Security Risk Management plan, the majority of the work on the framework will be left to future SEAD participants. Each of the DEAL phases will require work that will include completion of the framework, guidelines are to be developed, and policies and procedures will need to be documented.

**Discovery**

Items to be addressed to see the discovery phase to completion include:

- Finalize the framework of the discovery phase
- Develop guidelines of the research and discovery phase
- Identify sites such as [http://www.riptech.com](http://www.riptech.com) and [http://xforce.iss.net/](http://xforce.iss.net/) to be researched
• Develop a mechanism for storing, searching and documenting risk and vulnerabilities

**Evaluation**

Items to be addressed to see the evaluation phase to completion include:

• Finalize the framework of the evaluation phase
• Develop guidelines for ranking impact and probability values
• Develop guidelines of the mathematical score used for risk exposure metric
• Develop a mechanism for storing, searching and documenting information used in prioritizing risk and their importance

**Actions**

Items to be addressed to see the actions phase to completion include:

• Finalize the framework of the actions phase
• Develop guidelines of the actions phase
• Develop a mechanism for storing, searching and documenting current projects and the implementation of the actions identified
• Develop a mechanism for re-evaluation of actions so as to adapt action plan as necessary

**Lessons Learned**

Items to be addressed to see the lessons learned phase to completion include:

• Finalize the framework of the lessons learned phase
• Develop guidelines of the lessons learned phase
• Develop a mechanism for storing, searching and documenting lessons learned in a knowledge base
Job Roles

The next group of SEAD participants would need to take an aggressive role in order to continue this project on to completion. The next group of students should complete the framework and begin development of the guidelines used in the Risk Management Plan. Below is a chart showing the next groups responsibilities.
Summary

This project has resulted in an outline for a Security Risk Management Framework for the development group of the SEAD practicum. Much work is needed to see this framework to fruition. However, once completed and implemented, the framework and resulting methodologies will provide a method to DEAL with risk in the software development projects that will take place with in SEAD.
Chapter 5

Lessons Learned

Working on this project has been an interesting experience. The lessons I learned in completing this project range from educational to professional lessons. There are some things I would change, but overall I would proceed in the same manner.

Experiences

The educational lessons I learned included performing research. Locating valid resources and obtaining the information I needed was difficult at first. However, after many hours of combing the online library resources of Regis and other online resources, research became a natural process and has actually continued into everyday life. As an instructor at a two year college, this has been a lesson I have passed along to my students. I have also learned the importance of a writing style such as APA. The consistency of citing sources, formatting a document and listing references proved tedious, but I understand the necessity of the standardization.

The technology lessons learned have been tremendous. Before the tenure in this practicum, I had not heard of SOA or ITIL and was only briefly familiar with MOF and MSF. Again I have developed a great appreciation for such frameworks and the resulting methodologies used to implement the strategies outlined in the frameworks. I also gained experience with VoIP technology with Team Speak, help desk applications with TrackIT and with portal software with SharePoint.

I also learned that even though online learning offers great convenience, some things would be better experienced in-person. I know I could have had a greater
learning experience during the term of the practicum if I had been able to be on campus for the monthly meetings, the server relocations and RegisARN support.

If I was starting this project next week, I would change a few things. First, I would have not taken other courses at the same time I participated in the practicum. I have learned that even though I try to multitask, I do much better single tasking. Each of the classes I took while in the practicum was 90% research and writing papers. It was difficult for me to conduct the two researches simultaneously. Second, I would have requested more structured meetings within the project team. Possible bi-weekly meetings would help the team focus and therefore would have helped keep me on task. I believe greater communication between the participants within the development group would have produced a more cohesive total framework.

Expectations

The initial expectations of this project were to develop a framework to help identify risk factors and vulnerabilities at the software development stage. The framework was designed to minimize security breaches in the software produced by students participating in SEAD. The research reported on in this document supports the importance of this and also documents frameworks currently advocating this approach. It was a constraint of this project that this framework would not be complete and it is not. This project has laid a foundation which can be built on by future groups.

The expectation is that the next evolution of the project should include building on this foundation. The framework should be finalized. Then guidelines and methodologies will need to be developed. The more time spent in designing the framework, guidelines and methodologies, the stronger the Security Risk Management
Framework will be. Once this strong foundation is complete, the next step would be to develop the tactics used to implement the procedures defined. Decisions will need to be made on the mechanisms used to research and store known risk factors, how risk are evaluated and prioritized, develop secure programming actions to take, and how lessons learned will be documented.

Conclusions

This project has included many hours of research and design. The framework is not complete but it was known in the beginning that this would be the case. Many more hours need to be put into the framework to carry it to the next step. It will require constant re-evaluation, as threats and risk management are constantly evolving. Over time, this project could prove to be beneficial to the development arm of SEAD.
References


Definition of Acronyms

ARN – Academic Research Network

MOF – Microsoft Operations Framework

MSF – Microsoft Solutions Framework


ITIL – Information Technology Infrastructure Library

MSCIT – Masters of Science Computer Information Technology

NLP – Network Lab Practicum

RegisARN – Regis Academic Research Network

SDLC – Software Development Life Cycle

SEAD – Software Engineering and Application Development

SOA – Service-Oriented Architecture
## Addendum 1 - Calendar of Events

### SEAD

**Calendar of Events**

**Jan Carney**

<table>
<thead>
<tr>
<th>Date</th>
<th>Activity</th>
<th>Description</th>
<th>Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/19/04</td>
<td>Acceptance into NLP Practicum</td>
<td>Email from Dan Likarish</td>
<td>Excited - the end is near</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Scared – what do I do?</td>
</tr>
<tr>
<td>12/04/04</td>
<td>Orientation Session</td>
<td>Tactical Task Development to take on the web resources both remotely and at the DTC (practicum web site is underdevelopment, trackit, IM during the meetings, topica listserv, ftp, sharepoint) Ops to take on 1) the role of user setup during the change over between terms, 2) management of the helpdesk tickets during the term Storage interns for the HDS equipment at SNIA</td>
<td>1-800 phone conferencing Hard to hear remotely Confused – it will get better Received organization chart showing my placement in the development group; Question Dan Likarish on this, his response was to keep the CVTC crew together</td>
</tr>
<tr>
<td>12/12/04</td>
<td>Sharepoint login</td>
<td>Email from Vicki Scoefiled</td>
<td>Nice place to store documents</td>
</tr>
<tr>
<td>01/08/05</td>
<td>Optional Meeting for NLP2005a Mandatory Meeting for NLP2004</td>
<td>Dan Likarish gave presentation on research resources at Regis Dan also gave a presentation on paper outline</td>
<td>1-800 phone conferencing Hard to hear remotely Sharepoint for centralized document storage, recordings of meeting, training,</td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>01/15/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>1-800 phone conferencing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dan Likarish shared strategic goals:</td>
<td>Hard to hear remotely</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Place for students to finish their projects</td>
<td>MSN used for IM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Production at MSCIT</td>
<td>IM nice to ask questions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Research projects</td>
<td>The more I see this TrackIT tool, the more I like it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Build a lasting operational structure that can withstand rebuilding every 6 months</td>
<td>I will have to find a topic which incorporates security into the development. I am considering a risk management plan for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lead Assignments:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network (Mike Atkinson)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dev (Ronnie Bradford)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems (Vicki Scofield)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ops (Scott Shadler)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Each of the four groups responsibilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mgp storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Regis has great research facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I may also use Galileo, a research tool available to Georgia schools / students</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TrackIT is a great tool – CVTC needs this tool</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>02/12/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>S. Legere gave presentation on documentation procedures in SEAD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WebCT used for communication chatroom</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sharepoint for centralized document storage, recordings of meeting, training, mgp storage</td>
<td></td>
</tr>
<tr>
<td>03/07/05</td>
<td>Submitting project proposal</td>
<td>One page Project proposal was submitted via email to Dan Likarish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>I sure hope I am on the right track. I have proposed a Security Risk Management plan for SEAD software development. What I envision is a DB that tracks security risks due to poor app development. A developer would check this during design phases and will incorporate secure development techniques into a SEAD project.</td>
<td></td>
</tr>
<tr>
<td>03/08/05</td>
<td>Response from Dan Likarish</td>
<td>Dan Likarish responded to the project proposal. He feels it “will integrate security requirements into the overall development cycle that Ronnie, Jim and Bob are managing. Seems like a great fit.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Good news about fitting well. I still do not feel I know what I am doing. I need to talk with Jim Ochse. This was just a one page, give him the idea of what I am doing. Now I have to really put things together on what I going to do for first chapter.</td>
<td></td>
</tr>
<tr>
<td>03/09/05</td>
<td>WebCT chat</td>
<td>Much time spent discussing IBM presentation on SOA and firewalls</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This chat was wasted on me</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Still not sure of what my role is</td>
<td></td>
</tr>
<tr>
<td>03/12/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>Discussed role of TrackIT in IT; about ITIL and MOF frameworks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VOIP Teamspeak used by some…I think I will try it next time</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>03/27/05</td>
<td>Ch 1 submitted</td>
<td>Chapter 1 was submitted today to Dan Likarish; copied Jim Ochse</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jim emailed me his vote of confidence on 3/28/05</td>
<td></td>
</tr>
<tr>
<td>04/03/05</td>
<td>Response from Dan Likarish</td>
<td>Dan Likarish responded about Chapter one</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Very positive comments. Now I am on to research.</td>
<td></td>
</tr>
<tr>
<td>04/09/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>Dan Likarish gave an overview of the IBM presentation “The State-of-the-Practice in Designing and Building Service-Oriented Solutions” by Alan W. Brown</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visio documents referenced. Dan Likarish seemed to think we all had these. I have not seen them before.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOA is interesting framework. Things have changed since I was a programmer 20 years ago!!</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Need to email someone about those Visio documents. Bryon Meuller email next day stated the documents had been uploaded to Sharepoint.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used VOIP Teamspeak I had no microphone, just head phones; was really</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>05/14/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>Presentation on TrackIT Synchronization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used VOIP Teamspeak again</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Love this Teamspeak</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WebCT used for communication chatroom</td>
<td></td>
</tr>
<tr>
<td>05/25/05</td>
<td>Submitted Chapter 1&amp;2</td>
<td>Submitted Ch 1&amp;2 to all via email</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WOW! A lot of work doing the research, HOWEVER, I now have a better</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>understanding of SOA, MOF, MSF. Frameworks lead to guidelines lead to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policies and procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>We really need to implement this at my school for service</td>
<td></td>
</tr>
<tr>
<td>06/11/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>Anthony Ayodele presented his presentation on Vlab and curriculum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>support (MSCT660)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installation of Apache and Tomcat on the VM server;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Eddie Lopez was to present on SANS status – could not attend or we</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>could not hear him in Teamspeak</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used VOIP Teamspeak again</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Love this Teamspeak</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WebCT used for communication chatroom</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sharepoint for centralized document storage, recordings of meeting,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>training, mgp storage</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Details</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>07/09/05</td>
<td>Mandatory Meeting for NLP2005a</td>
<td>Last Mandatory meeting for NLP2005a; preparing for NLP2005b</td>
<td>Used VOIP Teamspeak again</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dan Likarish pushed us to finish up last chapters; will post to SharePoint folder</td>
<td>Love this Teamspeak</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HDS installed at SNIA</td>
<td>WebCT used for communication chatroom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN and Sonicwalls are installed and running (testing)</td>
<td>Sharepoint for centralized document storage, recordings of meeting, training, mgp storage</td>
</tr>
<tr>
<td>08/17/05</td>
<td>Ch 1&amp;2 returned</td>
<td>Ch 1&amp;2 was returned today from Dan Likarish</td>
<td>I am concerned with completing this paper within the next six months with Regis classload and CVTC class load</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Evidently my paper got lost in a shuffle somewhere…either with all the submittals at once to Dan or in returning to me with my work email. Anyway…..</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Feed back is positive. Must research writing in third person.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I am concerned about time to work on this in the next three months. With teaching 5 classes next quarter with four of them having new books, I will be swamped. Oh well, it will get done.</td>
</tr>
<tr>
<td>09/17/05</td>
<td>Began work on Ch 3</td>
<td>Ch 3 is Methodology. For my methodology I have chosen <strong>DEAL</strong> with risk:</td>
<td><strong>DEAL</strong> with risk is my plan for risk management. Very much based on the MSF Risk Management Discipline.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Actions to take</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Activity</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>11/26/05</td>
<td>Began work on Ch 4&amp;5</td>
<td>Chapter 4 – Project History</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chapter 5 – Lessons Learned</td>
<td>My quarter of teaching at CVTC has been so heavy I have not had time to work on this. I really wanted to be done by now, but life got in the way. This was an interesting time. Helped pull everything together. I really feel I have learned a lot. Hope this project will continue in future practicums.</td>
</tr>
<tr>
<td>12/3/05</td>
<td>Consolidate paper</td>
<td>Pull all the pieces together to submit final rough draft</td>
<td>This is the tedious work.</td>
</tr>
<tr>
<td>12/4/05</td>
<td>Submitted final rough draft</td>
<td>Final rough draft submitted; GoToMeeting.com meeting scheduled with Dan Likarish on 12/5/05</td>
<td>Beginning PowerPoint presentation</td>
</tr>
<tr>
<td>12/5/05</td>
<td>GoToMeeting.com</td>
<td>Met with Dan Likarish - Need to add role assignments for future SEAD group</td>
<td>GoToMeeting tool is nice collaboration tool;</td>
</tr>
</tbody>
</table>