Fall 2010

Towards Establishing a Change Management Process at an Academic Research Laboratory Network

Russell Moult
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

ABSTRACT

This report focuses on the evaluation and development of a change management process for the Regis University Academic Research Network (ARNe), and specifically the SEAD Practicum. The author originally proposed expanding on a security audit performed on the ARNe in 2008, and researched, evaluated and presents several risk assessment methodologies. This broad approach was later focused on the practical aspects of developing a change management process for the ARNe/SEAD Practicum, based on researching applicable standards and best-practice guidance. A management questionnaire and user survey were developed and distributed to obtain valuable opinions and perspectives from the individuals most directly involved with the administration and use of the ARNe and SEAD Practicum portal.

ACKNOWLEDGEMENTS

I would like to thank my fellow peers and course facilitators for making this program a rewarding and highly educational experience. I would also like to thank my thesis advisor, Mr. Bob Bowles, for his timely responses, guidance and support on the completion of my thesis, and to Mr. Dan Likarish, coordinator for the Master of Science in Information Assurance (MSIA) program, for his guidance on focusing my thesis topic, and for providing critical input on the roles associated with ARNe and SEAD Practicum administration.

TABLE OF CONTENTS

ABSTRACT ii

ACKNOWLEDGEMENTS iii

INTRODUCTION 4

General 4

Thesis Statement 4

Problem Statement 5

Statement of Goals and Objectives 5

LITERATURE REVIEW 7

METHODOLOGY 33

Qualitative Research Design 33

Case Study 34

Data Collection Methods 35

Data Analysis Methods 44

Change Management Questionnaire Results 47

Change Management Survey Results 48

Presentation 61

CONCLUSIONS 62

Conclusions 62

AREAS FOR FUTURE WORK 64

REFERENCES 65

ANNOTATED BIBLIOGRAPHY 70

APPENDIX A 88

APPENDIX B 91

APPENDIX C 96

LIST OF TABLES

Table 1 – CIS Security Metrics……..10

Table 2 – Tactics for Ensuring Quality Research Design……..45

LIST OF FIGURES

Figure 1- OCTAVE Allegro Roadmap……14

Figure 2 - ITIL Change Management Lifecycle……..20

Figure 3 - ITIL Change Management Workflow …….…...21

Figure 4 – Forward Schedule of Changes…….…...23

Figure 5 - ISO 20000:2005 Structure Diagram……..…..26

Figure 6 – Example Change Request Form for ARNe ……. ….40

Figure 7 – Proposed ARNe/SEAD Practicum Change Management Workflow…….41

INTRODUCTION

General

This report documents and presents the results of my professional project completed to partially fulfill requirements for a Master of Science in Information Assurance through the College for Professional Studies (CPS) at Regis University. The project was undertaken to establish a formal change management process for the Regis Academic Research Network (ARNe)/SEAD Practicum. It builds on prior project work completed by other Regis graduate students and effectively contributes to the body of knowledge concerning change management policies and procedures relative to the ARNe. This project modifies my original proposal dated June 15, 2009, by narrowing the proposal focus to change management processes only.

Thesis Statement

Given the current ARNe architecture, infrastructure and management culture, is it possible to implement a formal change management process to improve the functionality and efficiency of the Regis ARNe, and specifically the SEAD Practicum, by providing a method for effectively tracking and documenting changes to the ARNe architecture, infrastructure and applications?

Problem Statement

Recent project work completed within the SEAD Practicum included a hardware asset inventory, preparation of network diagrams, pilot implementation of a freely available security assessment tool (CIS Benchmarks) to assess the security posture of select network hosts, and completion of a physical security assessment at the five Denver area campuses. Further work identified includes expansion of the security audit metrics to include software products and licensing, data access methods, change management processes, and an evaluation of automated security management products that incorporate centralized, group management functionality.

The ARNe does not currently have a change management process in place. The "state" of the network is not accurately known at any given point in time. This may lead to confusion by system users and unknowingly expose the network to security vulnerabilities.

Statement of Goals and Objectives

There is not currently a formalized or consistent method for tracking changes to the ARNe environment, including any changes made by instructors, students and alumni to the ARNe architecture, infrastructure, applications and system configurations. This may lead to confusion among system users as to the current state of the network, and may also expose the network to unknown security vulnerabilities.

This project intends to improve the overall effectiveness, operation and security posture of the ARNe and SEAD Practicum network by developing a formal change

management process to allow up-to-date tracking and documentation of all changes to the system.

LITERATURE REVIEW

Previous work conducted within the Regis practicum involved the development of an information security audit checklist (Argo, 2008). The checklist consisted of 49 items addressing various physical and technical security metrics related to the ARNe network, as well as an additional 23 assessment metrics related to information security laws and regulations. ARNe security and management policies were not evaluated as part of the prior case study due to time constraints (Argo, 2008). In addition, vulnerability scans, a review of network device configurations (routers, switches), application types, versions and licensing, data access methods, virtual lab configurations and access methods were not included in the prior case study. Wireless and remote access devices and methods were also excluded from the prior study.

A quality security program begins and ends with policy (Whitman & Mattord, 2005). Implementing an information security program begins with the creation and/or review of an organization's information security policies, standards and practices. These form the basis for the selection of an information security architecture and development and use of a detailed blueprint to drive security planning and implementation. Information security is primarily a management issue, not a technical one (Whitman & Mattord, 2005).

Planning is a fundamental step to successful auditing (Cascarino, 2007). An audit should include: tentative objectives and scope; determination of business and control objectives, key performance areas and indicators; assessment of internal and external threats to performance; selection of the audit team; initial communications with auditees

and others; preparation of preliminary audit program and report format; and approval of the auditing approach. Audits may be structured with various intentions, to include assessing the adequacy of internal control system design, tests for compliance with the designed control system, and an evaluation of the effectiveness of the implemented control system.

The security assessment conducted for the ARNe network focused primarily on physical security items and an assessment of effectiveness of physical security controls. Time constraints limited the scope of the security audit. The only area of policy addressed was whether or not a security policy existed (Argo, 2008). A Security Forum Group has reportedly been formed to address policy and management issues related to the ARNe network.

There are various definitions and interpretations of an information system audit versus an assessment. Miles & Rogers (2004) define an INFOSEC assessment as a "baseline measurement of the controls implemented to protect information that is transmitted, processed or stored by a specific system". In essence, a security assessment is a measure of the security posture of a system or organization. An information systems audit, by contrast, may be defined as the process of reviewing system use to determine if misuse or malfeasance has occurred (Whitman & Mattord, 2005), typically in relation to some governing regulation or standard, such as SOX, HIPAA, PCI-DSS or GLBA. Auditing is also a term commonly used in conjunction with the technical configuration of systems and applications that enables the generation and storage of various logs, including security logs. A review and analysis of relevant logs is an important audit function.

It is also useful to distinguish between measurements and metrics. According to Payne (2006), measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing two or more measurements to a pre-determined baseline over time. Using this definition, security metrics may be developed by comparing existing conditions against an established baseline or benchmarks developed from accepted best practices, standards and where applicable, regulations. An improvement in security metrics may be realized by implementing recommended changes based on an initial comparison. A post-implementation comparison is one way to measure improvements in the security posture of a given environment. Metrics are generated from analysis based on an objective or subjective evaluation of the data (Payne, 2006).

The Center for Internet Security (CIS, 2009) has recently published "The CIS Security Metrics, Consensus Metric Definitions, v1.0.0" to provide information security practitioners with widely accepted, defined and standardized metrics for a number of important business functions, including: Incident Management; Vulnerability Management; Patch Management; Application Security; Configuration Management; Financial Metrics.

Twenty (20) security metrics are defined for the six business functional areas. Of particular interest to change management processes are metrics related to Patch Management, Configuration Management and Application Security. Table 1 below presents the security metrics for these three areas.

Table 1 – CIS Security Metrics		
Function	Management Perspective	Metrics
Patch Management	How well are we able to maintain the patch state of our systems?	• Patch policy compliance • Patch management coverage • Mean time to patch
Configuration Management	How do changes to system configurations affect the security of the organization?	• Mean time to complete changes • Percent of changes with security reviews • Percent of changes with security exceptions
Application Security	Can we rely on the security model of business applications to operate as intended?	• Number of applications • Percent of critical applications • Risk assessment coverage • Security testing coverage

This study focuses on change management processes, including changes to system configurations. Patch management and application security, although not individually addressed, will still fall under the change management process umbrella. System changes, including critical updates to operating systems, changes to applications or rollouts of new applications should all be tracked via an established change management process.

The prior case study involving the ARNe included a pilot study implementing the CIS benchmark and scoring tools for the Windows Server 2003 environment. The initial scoring identified a number of security vulnerabilities related to server configuration.

Recommendations were made and implemented resulting in a 40% improvement upon re-evaluation (Argo, 2008).

Various security risk assessment methodologies have been developed and published in recent years. Examples include:

1. National Security Agency INFOSEC Assessment Methodology (NSA IAM)
2. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE®), developed by Carnegie Mellon University CERT
3. Security Consensus Operational Readiness Evaluation (SCORE), a joint effort between the SANS Institute and Center for Internet Security (CIS).

The NSA IAM is the direct result of Presidential Decision Directive 63 (PDD 63) signed in 1998, outlining responsibility for protecting critical infrastructure of the United States. It further defined the framework for the National Infrastructure Assurance Plan, a portion of which required NSA to perform assessments of government systems. This resulted in the development of the IAM and also the development of a training program to provide selected entities the knowledge and skills necessary to lead the IAM process. The goal of the IAM methodology is to assist organizations in improving their security posture. The IAM methodology consists of three phases, defined as:

1. Pre-Assessment
2. On-Site
3. Post-Assessment

The pre-assessment phase focuses on acquiring as much knowledge as possible concerning the target environment, to include key personnel, business objectives and

drivers, business critical information and data, systems and assets. This is also a key, planning phase in preparation for the on-site visit.

The on-site phase may include interviews, group discussions, document research (policies, procedures, guidelines). This is also the phase where several key artifacts of this methodology are defined and agreed on, namely the Information Criticality matrix, Impact Attributes, Impact Definitions, and System Criticality matrices.

Under IAM, two key information characteristics defined include Impact Attributes and Impact Definitions. Mandatory Impact Attributes include the key tenets of information security: confidentiality, integrity and availability. Impact Definitions characterize information into high, medium or low severity, based on the severity of negative consequences to business operations.

Final analysis and document preparation are post-assessment phase activities. (Miles & Rogers, 2004).

The OCTAVE methodology is designed to allow organizations to develop qualitative risk evaluation criteria that describe their operational risk tolerances (Caralli, et al, 2007). Further, it is a methodology to identify mission-critical assets, vulnerabilities and threats to those assets, and evaluate potential impacts resulting from successful exploitation of identified vulnerabilities. The methodology was originally developed to address Department of Defense issues related to HIPAA compliance. There are now three distinct OCTAVE methods available for public use: OCTAVE, OCTAVE-S and most recently OCTAVE Allegro.

The original OCTAVE method is intended for larger (over 300 employees) organizations. A method implementation guide provides procedures, guidance, worksheets

and information catalogs. The method is designed to be facilitated and conducted via a series of workshops involving multi-disciplinary teams representing key business functional areas and personnel of different levels and perspectives. The method may be tailored to suit specific organizational needs, and is conducted in three phases. Phase I focuses on the identification of key information assets, along with existing and required security controls and an identification of threats to security. Phase II evaluates the information infrastructure to further evaluate threats to security and provide input into mitigation strategies developed in the next phase. Phase III focuses on risk identification and the development of a risk mitigation plan (Alberts, 2002).

OCTAVE-S was developed to bring the assessment methodology and approach to small manufacturing companies. It is more structured than the original method, and relies heavily on the institutional knowledge and expertise of the assembled team members.

OCTAVE Allegro, the latest evolution of the methodology, presents a streamlined approach designed to focus on information assets in the context of how they are used, where they are stored, transported and processed, and how they are exposed to threats, vulnerabilities and disruptions (Caralli, et al 2007). The method is supported with guidance, worksheets and questionnaires. This method is also intended for use by individuals, without extensive involvement from or input from others. The Allegro approach consists of eight steps defined within four phases, as shown in Figure 1.

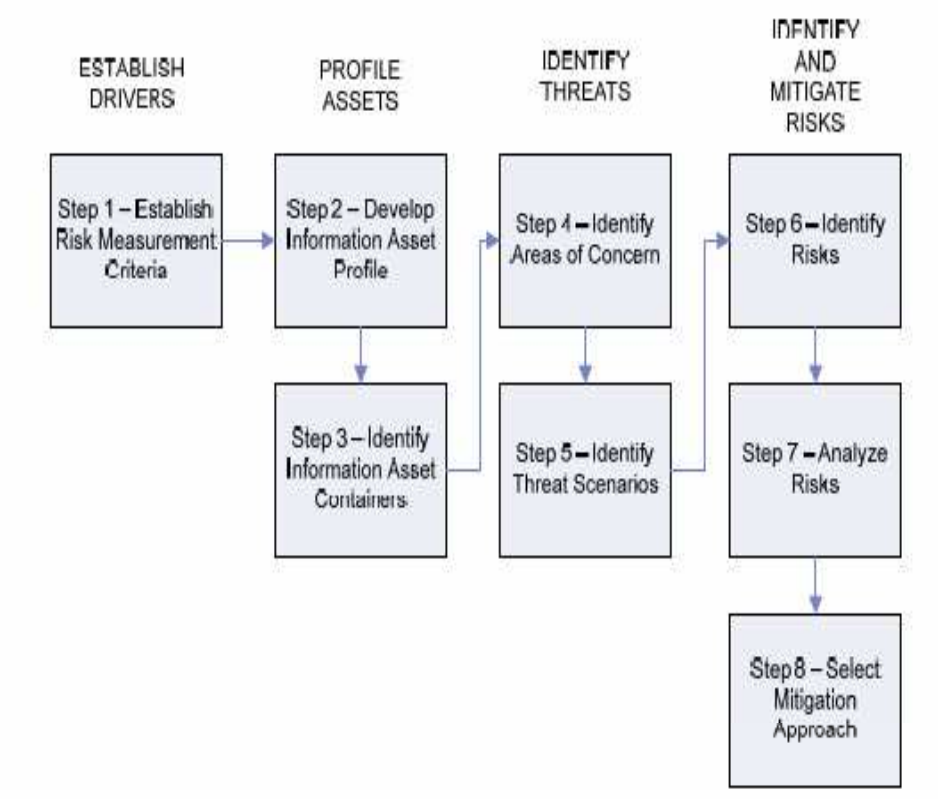


Figure 1- OCTAVE Allegro Roadmap (Caralli, et al 2007)

OCTAVE Allegro uses the concept of information "containers", areas where information is stored, transported or processed (Stevens, 2005). A container may include an individual, object or technology.

As depicted in Figure 1, Phase I involves establishing risk measurement criteria based on key business drivers. During Phase II critical information assets are profiled, along with their containers. Security requirements for each asset are identified during this phase. Phase III involves threat identification in the context of asset containers, or in relation to where assets are stored, transported or processed. Phase IV involves risk identification and development of a risk management plan. The goal of the OCTAVE methodology is to allow organizations to evolve from vulnerability management and

reactive security measures towards incorporating information security risk management into overall business management objectives and strategies.

The SCORE methodology, a collaboration between SANS and CIS, has resulted in the publication of a number of security assessment checklists. Of interest to this study are the Firewall Checklist , Web Application Checklist and the ISO 17799:2005 SANS Checklist.

An inventory of information assets and an assessment of vulnerabilities associated with those assets is a core activity necessary to perform a risk-based analysis and development of a risk management plan. The prior case study focused primarily on an inventory of hardware assets within ARNe and an assessment of physical security controls.

The use of automated security tools assists both in providing a defense-in-depth approach to security and in providing an automated means of identifying security issues, thus reducing the amount of time and human errors inherent in manual reviews (Han, 2003).

The prior study originally proposed conducting a network scan using the open source Network Mapper (NMAP). This type of scanner is useful in identifying active hosts on a network, open ports and services, operating system and applications types and versions, packet filters and firewalls present, and other useful security-related information (Insecure.org, 2009). The decision was made to exclude this type of scan from the prior case study due to time constraints.

The Regis ARNe, being an academic research network, is loosely managed by Regis staff, alumni and students. The production aspects of the network are managed

separately through the Regis Computer Systems Development (CSD) group, and are not physically or remotely accessible to non-CSD employees (Argo, 2008).

The ARNe encompasses five different physical locations in the Denver metropolitan area, each comprising its own local area network (LAN). Together they comprise a wide area network (WAN) environment through various Internet service provider (ISP) contracts (Argo, 2008).

The Systems Engineering and Development (SEAD) practicum provides graduate students the opportunity to conduct research on information system projects, with the ultimate goal of completing a Masters thesis in partial fulfillment of degree requirements. The SEAD functions as a simulated information technology company, and provides students the opportunity to gain some practical experience with help desk operations, and also function within operational team environments based on their interests and backgrounds. Teams are currently divided into Systems, Integrated Services and Application Development functions. Periodic meetings keep practicum members current with respect to ongoing projects and developments affecting the ARNe, SEAD and other relevant business of interest.

The SEAD provides a Web-based portal (INSITE) for participants to access, review, post, and edit various documents based on their assigned areas of involvement, responsibilities and permissions. For example, students can post a journal of their activities associated with the SEAD and their respective projects. Recent developments include the establishment of a wiki within the practicum site to provide an area for participants to add content and update various topics, including ongoing projects.

Given the loosely managed and coupled environment, there is not currently an effective change management process in place to track non-production related changes within the SEAD and ARNe environment. Student projects may involve system and configuration changes to equipment and applications that have the potential to impact other systems or services required by other users. In essence the operational state of the ARNe environment is not accurately documented or known at any given point in time. This may lead to some confusion among system users and also potentially exposes the network to unknown security vulnerabilities.

There have been recent efforts to provide up-to-date information on the ARNe infrastructure, including changes made to the network architecture, infrastructure and configurations. This is being loosely implemented by one or more graduate students through various wiki pages, including pages established for Systems, Network and ARNe Change Log. The Systems page lists hardware and configuration information for most, if not all ARNe network hosts at the five Regis campuses. The wiki page "ARNe Change Log" is the first attempt at implementing a method for tracking changes as they are implemented by a system user. The use of the wiki as a collaborative tool to implement a change management process is one viable alternative for the ARNe.

The Information Technology Infrastructure Library (ITIL®) was originally developed in the 1980s by the British Central Computer and Telecommunications Agency (CCTA), forerunner to the present-day Office of Government Commerce (OGC). ITIL has evolved into an international set of best practice guidance documents for IT Service Management. ITIL version 2, released in 2001, established the disciplines of Service Delivery and Service Support. Grouped within these categories, numerous delivery and

support functions are defined. Service Support includes a number of key functions, including: Incident Management; Problem Management; Change Management; Release Management; and Configuration Management. The Service Delivery discipline includes the areas of Service Level Management; Availability Management; Capacity Management, Security Management and Financial Management (OGC, 2001).

The latest ITIL version 3, released in 2007, evolves into defining The Service Lifecycle. This latest version includes six volumes. Aside from the introductory volume, the remaining five core volumes consist of Service Strategy, Service Design, Service Transition, Service Operation and Continuous Service Improvement (Klosterboer, 2009).

ITIL defines Change Management within the Service Transition volume as follows:

> "The goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the number and impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization" (ITIL Open Guide, 2007).

ITIL further defines the change management process as receiving inputs from Request for Changes (RFCs), Forward Schedule of Changes (FSC); and the Configuration Management Database (CMDB). Activities identified within the change management process include filtering changes, managing changes and the change process, chairing the change advisory board (CAB) and CAB/EC, reviewing and closing RFCs, and creation of management reports. (ITIL Open Guide, 2007).

Uncovering and documenting project requirements is a crucial, initial step in defining processes and developing and implementing an effective change management

program. Klosterboer, 2009 classifies requirements into the areas of bad, business, process, system and component requirements. Bad requirements fall into the categories of requirements that are too vague, general or solution specific. An example of a requirement that is too vague or general to be of value might be the statement " We need to control changes" (Klosterboer, 2009). Klosterboer recommends eliminating bad requirements first and then focusing on the discovery of good requirements. Business requirements are the higher–level requirements that state what a project should accomplish. Although at a high-level, they should be as specific as possible. Requirements related to cost, productivity, efficiency and revenue are examples of business requirements.

Process requirements help define characteristics of policies and procedures and serve as guidance in their development. System requirements may define characteristics of tools to be used to automate processes, and may be broken down into functional and non-functional requirements. Functional requirements typically involve features related to human interaction and functionality. Non-functional requirements relate to technology characteristics, such as capacity and performance (Klosterboer, 2009). Requirements discovery should be coordinated and agreed upon with system stakeholders.

In general, a process is a set of sequential, defined actions undertaken to accomplish a desired outcome (Klosterboer, 2009). In terms of process engineering terminology and flow, a process can be divided into a series of sequential steps including the definition and development of process flows, sub-processes, policies, procedures and work instructions. Process and sub-process flows will define the high level sequence of events needed to accomplish a given task. Policies will define and establish rules governing and mandating specific actions and expected behaviors. Policies provide the

framework for more detailed and specific procedures for executing a process. If needed, additional work instructions can be added to complement procedural elements, such as instructions on using a particular toolset.

ITIL defines a change management process flow and lifecycle that includes the following action items: Request a change (RFC), document RFC, evaluate RFC, schedule RFC, implement RFC and review RFC, as depicted in Figure 2.

Figure 2 - ITIL Change Management Lifecycle (Klosterboer, 2009)

Having a formal process for requesting and registering all changes is a key requirement for an effective change management program. Categorizing changes based on urgency and severity, in terms of potential disruptions to service quality, is also extremely important.

A definition of workflows is the next logical step in the change management process. Workflows are discrete, specific steps to navigate through a process, and provide repeatable steps that support automation. Workflows may be developed based on specified categories of changes. Common change management categories include data center, workstation, data, documentation or administrative (Klosterboer, 2009). Another way to define workflows is based on the urgency of a given change. For example, a change may be designated as an emergency change, requiring immediate implementation, non-emergency but urgent, or normal. The workflows for these scenarios will differ. A service-

disrupting incident may require the change process to bypass the initial change request in order to quickly restore critical services. The change would be registered post-implementation. A workflow diagram for a normal change is depicted in Figure 3.

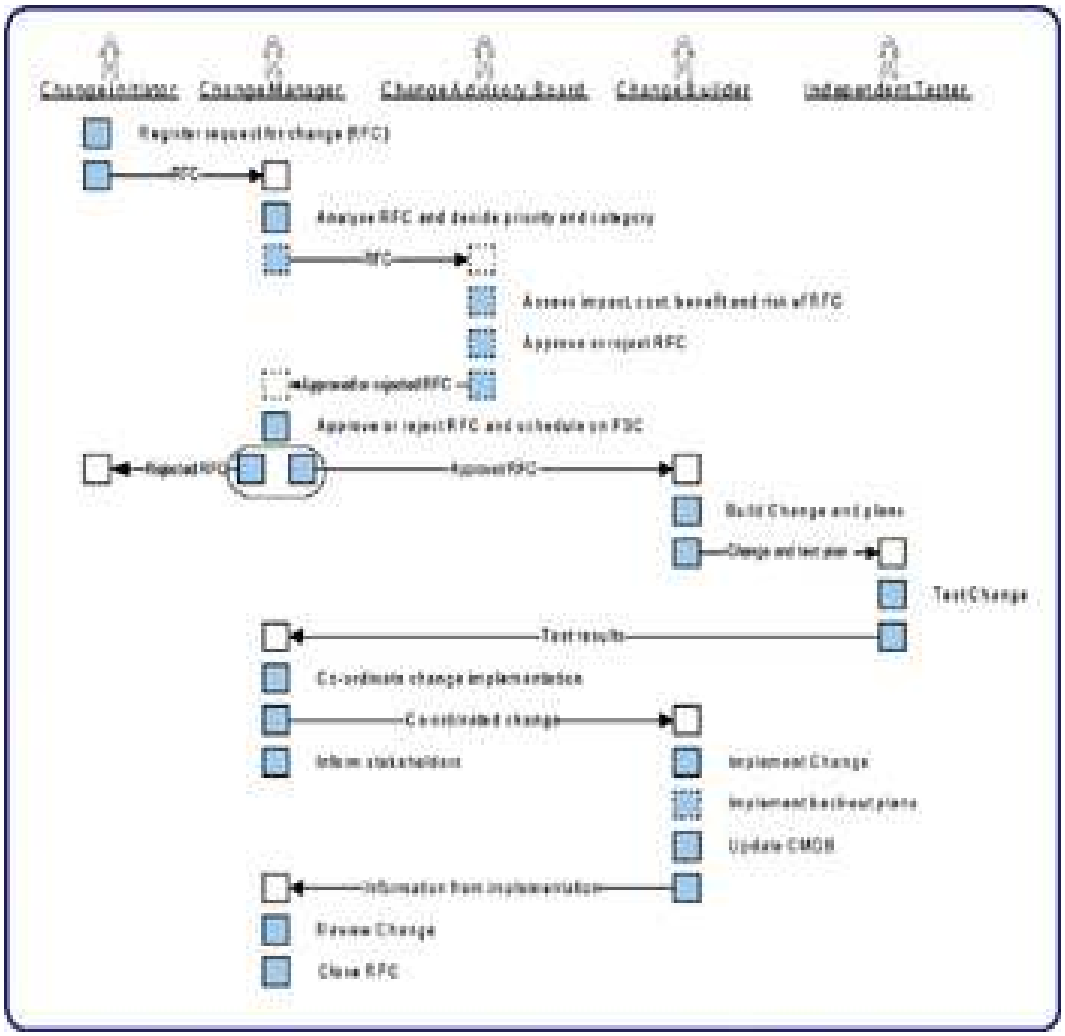


Figure 3 - ITIL Change Management Workflow (Cater-Steel, 2009)

As seen in Figure 3, ITIL defines five roles in the change management process: Change Initiator, Change Manager, Change Advisory Board, Change Builder, and Independent Tester.

The Change Initiator (CI) starts the Request for Change (RFC) process by completing the change request form. The form is forwarded to the Change Manager (CM) to analyze, categorize and prioritize the change. The change is forwarded for review at the next CAB meeting. The CAB will assess the risk, impact, cost, and benefits associated with the proposed change and decide whether to approve or reject the change. This decision is sent back to the CM. The CM either schedules the approved change on the Forward Schedule of Changes (FSC), or notifies the CI of a rejected change. Approved changes are forwarded by the CM to the Change Builder (CB), who builds the change and plans, including a test plan. Within ITIL, an Independent Tester (IT) function serves to test the change before implementation to the production environment.

As mentioned, ITIL defines the forward schedule of changes (FSC) as a best practice in change management. The FSC is a list documenting recently implemented and planned future changes. The actual content of the FSC will vary depending on its primary and ancillary role(s) and operational considerations. For example, the change advisory board (CAB) may use the FSC as a primary tool to review and discuss proposed changes. In addition, the FSC may be used as an operational planning tool and for scheduling purposes. At a minimum the FSC should contain an implementation schedule and identify and describe potential impacts to both IT and business operations. An example of an FSC form is presented in Figure 4.

	Schedule		Impact	
	When	Duration	IT	Business
Past Changes				
This Week's Changes				
This Month's Changes				
Future Changes				

Figure 4 – Forward Schedule of Changes (Klosterboer, 2009)

Implementing an online tool that allows the FSC to be both generated and queried by users is an effective method of automating the FSC process (Klosterboer, 2009).

Control Objectives for Information Technology (COBIT®) was first introduced by the Information Systems Audit and Control Foundation (ISACF) in 1996 and has undergone several revisions since that time. The third edition was released by the IT Governance Institute (ITGI) in 2000. COBIT 4.0 was released in 2005, and represents a complete rework of content with a clear focus on IT governance. The latest version, COBIT 4.1 includes incremental updates (ITGI, 2007).

COBIT provides "good practices across a domain and process framework and presents activities in a manageable and logical structure" (ITGI, 2007. p. 5). From a process perspective, COBIT defines four domains and 34 processes within the areas of plan, build, run and monitor.

Within COBIT, change management falls within the category of general IT controls. In order to assess the status of an enterprise's IT systems, COBIT relies on maturity models, performance goals and metrics, and activity goals. Maturity models, adopted from the Software Engineering Institute's (SEI) model for the maturity of software development capability, are based on a maturity rating system ranging from non-existent (0) to optimized (5). Performance goals and metrics for IT processes are established to assess how well business and IT goals are being met by established processes. Activity goals enable effective process performance.

Looking in more detail from a maturity model perspective, the lower levels are defined as follows:

0 – Non-Existent – There is no defined change management process, and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 – Initial/Ad-hoc – It is recognized that changes should be managed and controlled. Practices vary and it is likely that unauthorized changes take place. There is poor or non-existent documentation of change, and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

In relation to the ARNe environment, the change management process is in the early stages of maturity. There is awareness among the senior ARNe management that a change management process is needed. There are some initial, though not complete or formalized procedures in place, through the use of wiki pages, to document changes to the ARNe .

Within the COBIT framework, the management of changes to IT systems is defined within the Acquire and Implement domain, AI6 – Manage Changes. Specific control objectives defined include:

AI6.1 – Change Standards and Procedures

AI6.2 – Impact Assessment, Prioritization and Authorization

AI6.3 – Emergency Changes

AI6.4 – Change Status Tracking and Reporting

AI6.5 – Change Closure and Documentation

As defined, control over the IT process of Manage Changes is achieved by: defining and communicating change procedures, including emergency changes; assessing, prioritizing and authorizing changes; and tracking status and reporting on changes (COBIT 4.1, p. 97). Further, the effectiveness of the change management process is measured by: the number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment; amount of application or infrastructure rework caused by inadequate change specifications; and the percent of changes that follow formal change control processes (COBIT 4.1 p. 97).

The International Organization for Standardization (ISO) was established in the mid-1940s with the goal of unifying international industrial standards (Mutafelija & Stromberg, 2009). Over this time period, more than 16,000 standards have been published by ISO. ISO 20000:2005, Information Technology – Service Management, outlines an integrated process approach to the delivery of managed IT services.

The structure of this standard is divided into nine sections as depicted in Figure 5.

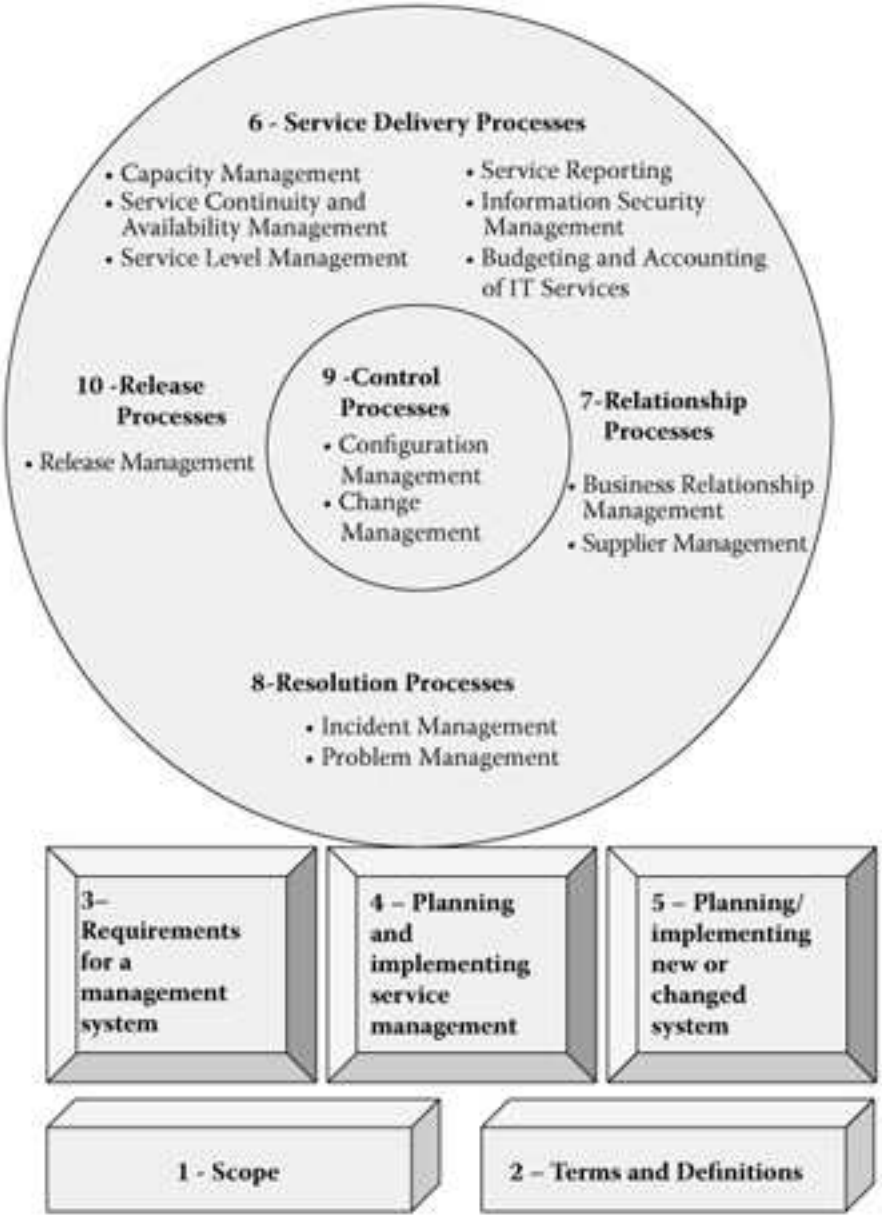


Figure 5 - ISO 20000:2005 Structure Diagram (Mutafelija & Stromberg, 2009)

Section 9 – Control Processes, includes Configuration and Change Management. Within the ISO standard, configuration and change management are considered closely related and integrated from a practical perspective. Configuration management is the process of identifying and controlling components of the service and infrastructure and

maintaining their integrity, while change management involves assessing change requests and implementing approved changes (Mutafelija & Stromberg, 2009).

Some commonalities exist between the reviewed standards and recommended best practices concerning change management. Changes to system architecture, infrastructure, hardware and software configurations, must go through an established change management process. This involves submitting change requests to the authorized individual(s) for review and approval; establishment of the role of change controller or manager and a change review team or board; categorizing changes based on severity and urgency; an evaluation of risks associated with proposed changes; developing a back-out plan; effective communication to system stakeholders and users; and up-to-date documentation of changes. The use of configuration and change management toolsets to automate the processes as much as possible is also an important requirement.

The Information Technology Process Institute (ITPI) is an independent research organization with membership focused on IT operations, security and auditing (ITPI, 2007). ITPI has conducted a number of surveys involving hundreds of IT organizations to assess what IT processes and practices contribute the most to high performance. One such study endeavored to determine which configuration, change and release management processes contributed to high levels of performance. Survey data was collected from 341 IT companies regarding 57 industry-recognized best practices, 15 performance measures and 15 demographic markers. Their statistical analyses revealed 12 sets of best practices that the organizations implemented. Of these, seven sets were predictors of top performance, while five sets did not indicate performance variations. The seven sets of best practices tied to performance improvements include: release scheduling and rollback;

process culture; pre-release testing; process exception management; standardized configuration strategy; change linkage; and controlled production access. Within these seven best practice sets, 30 individual practices were identified that indicate top performance.

Of paramount importance to successful IT service performance is the adoption of an IT process oriented culture. Processes are only effective if they are consistently followed. This takes executive management support, and clearly defined policies and expectations from system users.

With respect to change management, change requests are linked to infrastructure components, business service or need. Further, support personnel are able to access and review change histories to aid in incident and problem resolution and management. Standardized configurations are monitored for unapproved changes or configuration drift. (ITPI, 2007).

Of further interest and relevance to this study, the following sets of best practices were not tied to performance variations: change process routing; multi-function phase gate; change oversight; development integration; and the use of a configuration management database (CMDB). This has interesting implications from a practical standpoint because change oversight, change process routing and the use of a CMDB are identified within ITIL as key measures to implement.

The study concludes that although change management is often identified as a good starting point for ITIL implementation, standardizing on release management is the best way for organizations to realize performance gains from ITIL change and release processes (ITPI, 2007).

Another study conducted by ITPI involved assessing the impact of best practice process maturity as a performance indicator. This study involved 330 North American IT organizations. Key findings of the study indicate that implementing a core set of foundational controls at a high level of process maturity provides significant operational improvements. Twelve of the 53 controls analyzed provided the greatest operational benefit. For smaller companies, which tended to implement fewer controls overall, the greatest benefit was realized from the following controls: defined access control process; defined consequences for knowingly making unauthorized changes; and a defined process for managing known errors. For larger organizations, nine controls produced the greatest benefit, to include: defined root cause analysis process; communicating accurate configuration information to personnel; thorough testing of changes and new releases; defined roles and responsibilities for staff; review of relevant system and security logs to flag unauthorized access; defined process to resolve service level issues; defined configuration management process; a CMDB that includes descriptions of dependencies between infrastructure components (configuration items) (ITPI, 2007).

The study then relates these foundational controls to process maturity and concludes that maturity of process controls has a very significant impact on control effectiveness and operational improvements. In the spirit of the Software Engineering Institute's (SEI) capability maturity model for software development capability, also adopted for use by the COBIT framework, the study requested survey participants to rank the maturity of their foundational processes on a scale of 0 – Not used to 5 – Used very consistently, exceptions have consequences. Not surprisingly, the highest level of performance improvement was obtained from mature control processes (level 4 or 5).

Regis University currently employs Microsoft Office SharePoint® 2007 as a platform to provide an integrated suite of collaboration, communication, process automation and Web-based tools for Regis faculty, students and employees. This application, named Regis University INSITE, provides authorized users a single portal and interface within which to conduct various aspects of their work.

Microsoft SharePoint Server 2007 includes built-in workflow templates for common business-related processes to include: document routing and approvals; document review; signatures; document disposition approval; translation; and three-state, defined as management of high volumes of issues or items (Richman, 2007). Microsoft SharePoint Designer, the successor to FrontPage 2003, allows the development of custom workflow Web pages/forms, and is intended for business process owners/users to have an intuitive, graphical design interface that does not require programming or coding expertise. Professional developers can use the Visual Studio and Visual Studio.NET development platform to extend the Windows Workflow Foundation platform.

Mr. Erich Delcamp, Systems Manager with Regis ITS was consulted concerning change management processes that are currently implemented within the Regis ITS community. Mr. Delcamp informed the author that a web-based change management form and process has been developed and is currently used within his group. A future rollout is planned to other departments in the near future. The change management process developed is modeled after best-practice guidance defined within ITIL and ITPI documents, and addresses the key elements required for effectively requesting, documenting, evaluating, implementing and reviewing changes made within the ITS systems group. The change management forms were developed using SharePoint Designer.

Mr. Delcamp currently serves as the approving authority for changes within his group (Delcamp, 2010). The use of lists within SharePoint provides a means to document, track and review status of all changes.

The basic change management workflow developed for use within Regis ITS is defined as follows: When the Change Owner creates a new RFC, the workflow status is set to “Initiate”. The Change Owner and Change Builder receive an email notification of a new change request. This provides the Change Builder early notification of the request, and provides and opportunity to coordinate and collaborate with the Change Owner. When the workflow status is changed to “Review”, the workflow proceeds. The Change Reviewers, or CAB, are notified via email that a new change is awaiting review. After review, the workflow status is changed to either “Accept” or “Reject”. The Change Owner and Change Builder are notified via email regarding the accept/reject decision. (Delcamp, 2010). The recommended ITIL change management process was modified to more closely align with the Regis ITS Systems Group’s goals and objectives.

The functionality within SharePoint to design custom workflows and the current implementation of SharePoint at Regis, provides an opportunity to develop and implement a Web-based change management process for the ARNe using this existing toolset.

The evolution of the Web has gone from that of merely having a presence (Web 1.0) to a much more inclusive, collaborative environment that includes a rich set of tools and applications. This includes the use of wikis, blogs, social networks, folksonomies and software as a service (SaaS). A wiki represents a collection of Web pages that can be easily edited by anyone given access to the wiki site. Wikis are commonly used by project teams as a means of collaboration. In this capacity, the wiki serves as a repository

for project artifacts (documents, photographs, notes, ideas, lists, forms, etc.). The wiki provides a complete history and record of all entries, and being accessed through a Web browser, does not require any special software.

SharePoint provides built-in wiki functionality, and as stated previously, several wikis have been defined within the SEAD practicum site. The use of a wiki to publish a change management process for the ARNe is a viable alternative taking advantage of established technologies at Regis and the collaborative and information sharing capabilities of Web 2.0 technologies.

Traditionally, project management was focused more on technical issues, while change management focused on sociological aspects of introducing change (Gale, 2008). With the advent of Web 2.0 information sharing and collaborative tools, the differences are fading.

METHODOLOGY

Qualitative Research Design

This project employs a qualitative research design. Qualitative research approaches have two fundamental characteristics: they focus on phenomena that occur in natural settings, and they study those phenomena in all their complexities (Leedy & Ormrod, 2005). Qualitative studies typically are used for one or more of the following purposes (Peshkin, 1993):

1. Description
2. Interpretation
3. Verification
4. Evaluation

Research epistemology refers to the underlying philosophy, perspective and approach the researcher has towards their study. Epistemologies can be categorized as Positivist, Interpretive and Critical (Myers, 1997). The Positivist approach assumes an objective, quantifiable reality independent of the researcher and their activities. Interpretive epistemology assumes there is the potential for more than one correct solution to a problem, although one may be considered more correct or preferable to another. Researchers may interpret data and materials differently based on their personal backgrounds and experiences. Critical researchers operate under the assumption that social reality is historically created and is produced and reproduced by people (Myers, 1997).

Qualitative research methodologies include Case Studies, Action Research, Ethnography, Phenomenology, Grounded Theory, Content Analysis and Historical Research.

Case Study

Case Study research is the most common qualitative method employed for the study of information systems (Orlikowski & Baroudi, 1991). A popular definition of a case study (Yin, 2002) is that a case study is an empirical inquiry that:

1. Investigates a contemporary phenomenon within its real-life context, especially when,
2. The boundaries between phenomenon and context are not clearly evident.

Yin (2009) expands on this definition by stating that a case study:

1. Copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result
2. Relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result
3. Benefits from the prior development of theoretical propositions to guide data collection and analysis.

It is also imperative to define the unit of analysis within the study. The unit of analysis may range from an organization down to an individual. In this case, the primary unit of analysis is the SEAD practicum portal and the ARNe network. Embedded designs involve multiple units of analysis, such as quantitative data collected on a subset or subunit of the case.

In order to direct and focus the research concerning the development of an effective change management process within the SEAD Practicum and ARNe, a number of research questions were developed and proposed based on the literature review. The questions are:

1. How does the currently loosely managed and adhoc nature of managing changes within the ARNe and SEAD Practicum impact the overall operational service levels of the network?
2. What changes to existing change management processes will produce the most benefits to system users?
3. What are the most effective tools or methods for implementing an effective change management process within the ARNe and SEAD Practicum?

These three questions drive the project research.

Data Collection Methods

Yin (2009) identifies six sources of case study evidence as follows:

1. Documentation
2. Archival Records
3. Interviews
4. Direct Observations
5. Participant-observation
6. Physical artifacts

This study uses several methods of collecting data, to include: a review of relevant literature resources; archival records, to include a previous security assessment (Argo, 2008) conducted for the Regis ARNe; a search and review of applicable Internet resources

and vendor and open-source project Websites related to change management tools; guided interviews conducted with key ARNe faculty/administrators; survey of system managers and users to assess their awareness, concerns and level of satisfaction with current change management processes within the ARNe and SEAD practicum.

In order to obtain ARNe management input and perspectives on change management processes within the ARNe and SEAD Practicum, a questionnaire was developed. The questions presented are:

1. What functions do faculty/administrators currently serve in regards to ARNe non-production systems, and within the SEAD practicum portal site?
2. What types of changes do faculty/administrators make to the systems supporting the ARNe and SEAD practicum?
3. Who else currently has authority to make changes to ARNe system infrastructure components, configurations and applications?
4. What safeguards are currently in place to limit negative impacts of changes made to the ARNe network by system users?
5. Is there currently a process in place to request, review, authorize, communicate, implement, and track changes made to the ARNe systems and SEAD practicum portal? If yes, please explain.
6. What types of issues are encountered from current change management processes or lack thereof?
7. What does management perceive as major obstacles to implementing a change management process for the ARNe and SEAD practicum systems?

8. What are the major process improvements deemed the most crucial to providing the greatest improvements in change management within the ARNe non-production network?

System Practicum student participants were asked to respond to a Likert-type survey developed to assess their awareness, concerns and level of satisfaction with change management processes within the SEAD, and also assess the effectiveness of the wiki as a communication and process-enabling medium. They were asked to respond to the survey using the following scaled format:

1 – Strongly disagree

2 – Disagree

3 – No opinion or neutral

4 – Agree

5 – Strongly agree

The following -- survey items were developed and presented to systems practicum participants/users:

1. I am aware of procedures required to make changes to ARNe infrastructure components, configurations and applications.
2. My involvement with the ARNe and SEAD practicum has required me to make changes to network system components, configurations and/or applications.
3. There is a clearly defined process for requesting to make changes to the ARNe environment.

4. I have made changes “at will” to the ARNe environment without an evaluation of potential risks associated with such changes.
5. I’ve made changes to the ARNe environment that have had apparently negative effects on system availability or required a “roll-back” to a previous configuration.
6. I know where to look for up-to-date information on the configuration of the ARNe environment.
7. The adhoc nature of current change management processes is counter-productive to the ARNe user community.
8. My project work within the SEAD has been negatively impacted by service interruptions caused by others.
9. A method of requesting, approving, communicating, implementing and tracking changes made to the ARNe and SEAD environments would be beneficial to the user community.
10. The SharePoint portal is an effective medium for system users to access information concerning changes to ARNe system resources.
11. I’m very comfortable and familiar with Web 2.0 tools and technologies, including wikis and blogs.
12. The use of a wiki as a tool to develop and implement a change management process within the ARNe is a viable alternative and beneficial to the user community.

The author proposed to conduct a pilot study to assess an actual change management process for the ARNe developed by the author. A process was developed

following best-practice guidance promulgated by ITIL and COBIT. Microsoft SharePoint Designer was to be used to develop custom, web-based forms to allow the change management workflow and process to be completed within the SEAD Practicum portal. Developing workflows requires permissions within SharePoint not currently available to the author or non-ITS personnel, therefore, it was decided not to pursue the pilot study.

As stated, developing a process-oriented culture within the ARNe environment is key to a successful change management program. It will only work if it is intuitive and widely adopted by system users and stakeholders.

Figure 6 shows the example master form developed for the ARNe change request process.

REQUEST FOR CHANGE Regis University Academic Research Network (ARNe) Routine/non-Routine	
Personnel/Roles Involved	
Change Initiator (CI). (Individual requesting changes to system resources)	
CI Department/Job Function	
Change Manager (CM)	
Change Builder (CB)	
Change Advisory Board (CAB)	
Role Responsibilities	
Description of proposed change (CI)	
Systems affected by proposed change (CI)	
Test plan developed (yes/no) (CB)	
Rollback plan developed (yes/no)(CB)	
Change category (administrative, application, hardware, network) (CM)	
Urgency (Routine, Non-routine, Emergency)(CM)	
Risk Assessment (Low, Medium, High)(CAB)	
Impact Assessment (Low, Medium, High)(CAB)	
Assess cost, benefit of proposed change (CAB)	
Accept/Reject proposed change (CAB)	
Communication plan developed (who requires notification and when) (yes/no)(CAB)	
Implementation schedule (CAB)	
CR closed/change review complete (CM)	
Remarks/Comments	

Figure 6 – Example Change Request Form for ARNe

The workflow associated with the change request form and process is depicted in Figure 7 and described as follows:

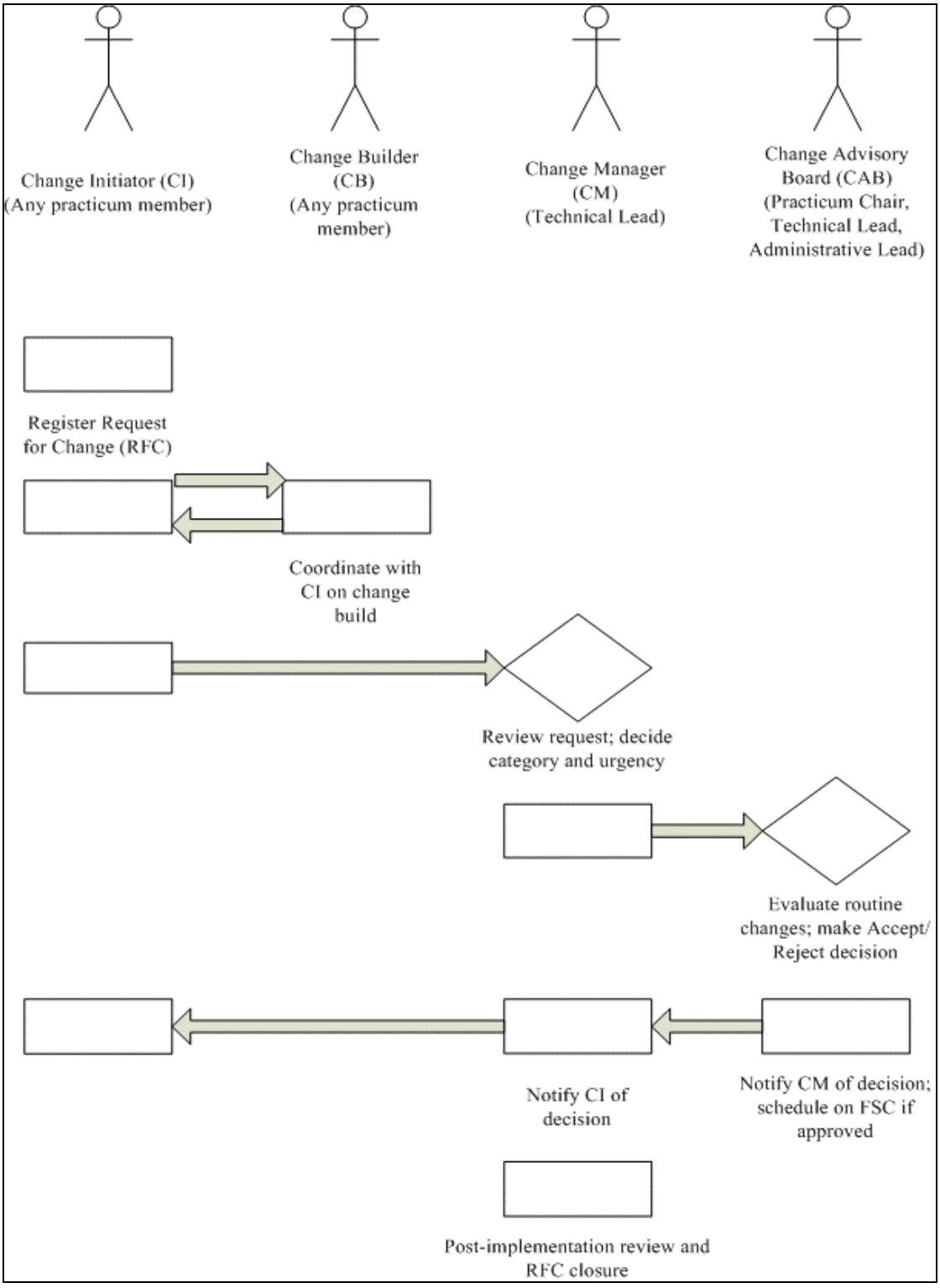


Figure 7 – Proposed ARNE/SEAD Practicum Change Management Workflow

The Change Initiator (CI) starts the process by filling specific sections of a new Change Request (CR) form via the Change Management wiki page. This sets the workflow within Sharepoint to “Initiated”. An email notification is sent in parallel to the Change Builder (CB), along with a link to the CR. The CI and CB have the opportunity to collaborate on the CR before submittal to the Change Manager (CM). Once the initial CR sections are complete, the workflow status is set to “Review”. An email notification is automatically sent to the CM along with the link to the CR. The CM reviews the request, and decides on the category and urgency of the change. Non-emergency changes are then forwarded to the CAB for routine assessment and approval. CAB members are notified electronically of the CR and provided the link. CAB members assess the cost, benefit, risk and impact of the proposed change and make the “Accept/Reject” decision. If approved, the CAB enters the change on the Forward Schedule of Changes (FSC) for implementation. The CI and CB are notified of the decision and schedule. The CB is responsible for developing test and rollback procedures for the change. Upon successful implementation, a post-implementation review is conducted by the CM, and the CR is officially closed.

It is important to note that in this specific environment, one individual may function in more than one role. Current roles defined within the SEAD practicum include the overall practicum Chair (Regis faculty member), Technical Lead, Administrative Lead, and Group Leads for operational groups within the practicum, currently consisting of Systems, Development and Integrated Services. New practicum members are assigned to a group based on their backgrounds and interests. These roles provide the opportunity to assign and tailor change management responsibilities to fit this specific environment. For

example, a change may be initiated by any of these defined roles. The CI role may be a practicum member requesting to change a device configuration to support their research project. They may or may not also build the change (CB). The CM role may be filled by the Technical Lead, responsible for reviewing all change requests and deciding on the change category and urgency. The CAB may consist of the practicum Chair, the Technical Lead and the Administrative Lead, who confer periodically on proposed changes and make final implementation decisions. All change request documentation and routing would be implemented through the SharePoint portal, and specifically within a Change Management wiki. The actual implementation of this process represents an area for future work, and will require adequate permissions within SharePoint to accomplish.

On occasion, it may be necessary to quickly implement a change to restore a system resource. In this scenario, the normal change management process may need to be bypassed. The CM may take responsibility to initiate an emergency change, effectively bypassing the request and CAB approval process. This also typically involves the Incident Management function and process for quickly restoring lost services. The CM in this case may be the manager responsible for incident resolution. The actual change will be recorded post-implementation. Unlike unauthorized or uncontrolled changes, the emergency change process has been approved by management and is controlled by policy. (Klosterboer, 2009).

For the ARNe, incident management is handled through a service desk function implemented using Intuit Track-It!®. Response to problem tickets/incidents may initiate changes to system configurations in an effort to restore lost services. Incidents in this manner are registered, prioritized, tracked, resolved and closed using Track-It.

Data Analysis Methods

In support of data management, analysis and overall method quality, Yin (1994) recommends developing a database and chain-of-evidence to organize, categorize and track all collected data. As described by Pare (2002), the following elements are included within the database: raw material (interview transcripts, field notes, documents collected); coding scheme; coded data; chronological log of data collection. Coding of data serves to organize and allow the rapid retrieval of data related to a specific question, concept or theme. The coding scheme is broken down into three broad categories: contextual conditions; implementation tactics; and implementation success criteria (Pare, 2002).

Project challenges were identified through an analysis of the contextual conditions surrounding the ARNe network (culture, information architecture and infrastructure) relative to the proposed project implementation (change management process). Tactics were developed to address each challenge or problem, or explain why a particular issue forced a re-evaluation and alternate approach to a given situation. For instance, the author's original project proposal was modified to narrow the focus from expanding on the ARNe risk assessment (Argo, 2008) to focusing on change management processes. Further obstacles encountered included not having required permissions through Regis ITS to develop custom workflows within SharePoint, and the recommendation not to utilize surveys as a data collection tool. (The use of a survey was later approved).

A case study protocol includes the instruments (survey questionnaires, interview guides, checklist, etc.) developed to collect data and the procedures and guidelines for using them. A case study protocol should contain the following elements (Yin, 1994):

1. An overview of the case study project (goals and objectives, topics)
2. Field procedures
3. Data collection guides and instruments
4. Report outline

Criteria used to evaluate quality research design include the concepts of construct validity, internal validity, external validity and reliability. These tests have been widely used in social science research. This study employs several tactics for ensuring validity and reliability as adopted from (Yin, 2009), and summarized in Table 2.

Table 2 – Tactics for Ensuring Quality Research Design

Test	Study Tactic	Phase of Study
Construct Validity	• Multiple sources of evidence • Establish chain-of-evidence • Draft report review by key study participants	Data collection Data collection Report composition
Internal Validity	• Explanation building • Address rival explanations • Logic Models	Data analysis Data analysis Data analysis
External Validity	• Theory use	Study design
Reliability	• Case study database • Case study protocol	Data collection Data collection

Once data is collected, (Miles & Huberman, 1994) recommend initial analytic data manipulations to include:

1. Putting data into different arrays.

2. Making a matrix of categories and placing evidence into appropriate categories.
3. Creating data displays to visualize and examine data characteristics.
4. Tabulating the frequency of certain events.
5. Conducting basic statistical evaluations (means, variances)
6. Placing data and information in chronological order or other temporal relationship

Although fine for initial data review, Yin (2009) stresses the need for developing an analytic strategy to guide data collection and analysis. He describes four general strategies for data analysis. The first involves following the theoretical propositions initially framing the case study and data collection strategies. A second strategy involves developing a descriptive framework for organizing the study. Developing a framework requires identifying descriptive categories or sections that incorporate supporting data. A third strategy involves using both qualitative and quantitative data to compliment and enhance the study. For example, in an embedded design, quantitative data may be collected and analyzed on a subset of the overall case, and used to augment higher-level qualitative case data. The fourth general strategy described involves defining and testing rival explanations. Examples (Yin, 2000) include Null Hypothesis, Threats to Validity, and Investigator Bias.

Yin, 2009 further describes five specific data analysis techniques: pattern-matching, explanation-building, time-series analysis, logic models and cross-case synthesis.

This study employs pattern matching as the primary technique to analyze collected data. Empirically based patterns are compared to the predictive patterns established during study design. (Yin, 2009) further states that a quality analysis must satisfy four principles. First, analytic strategies, including rival hypotheses, must address and evaluate all of the evidence, and cover key research questions. Failure to evaluate all evidence may open the door for rival interpretations. Second, the analysis should address all major rival interpretations if possible. Third, the analysis should address the most significant aspects of the study, and fourth, the knowledge and expertise of the researcher(s) should be reflected in the analysis.

Change Management Questionnaire Results

The results of the Change Management Questionnaire resulted in some key insights into the administration, operation and existing management processes of the ARNe and SEAD Practicum portal, from the perspective of faculty/administrators. Important characteristics include the following:

1. There are currently two administrators responsible for the ARNe and a single administrator over the SEAD Practicum portal. (It's important to note the second ARNe administrator is also serving as the Technical Lead for the SEAD Practicum.)
2. Faculty/administrators are primarily responsible for coordinating and performing ARNe system upgrades, to include all hardware, applications, moves. A major initiative currently involves the move to a new DTC location.

3. A committee has been formed via the Regis University Center for Information Assurance Studies (CIAS) to govern major changes to the ARNe environment. The committee is comprised of six representatives, including an outside expert.
4. The ARNe environment has two distinct aspects: a stable production environment and a more volatile student research side.
5. Major obstacles identified for implementing a change management process include lack of resources and the transient nature of the student work force.
6. The single biggest improvement in a change management process is perceived as ensuring up-to-date documentation is maintained on the ARNe system via the wiki.

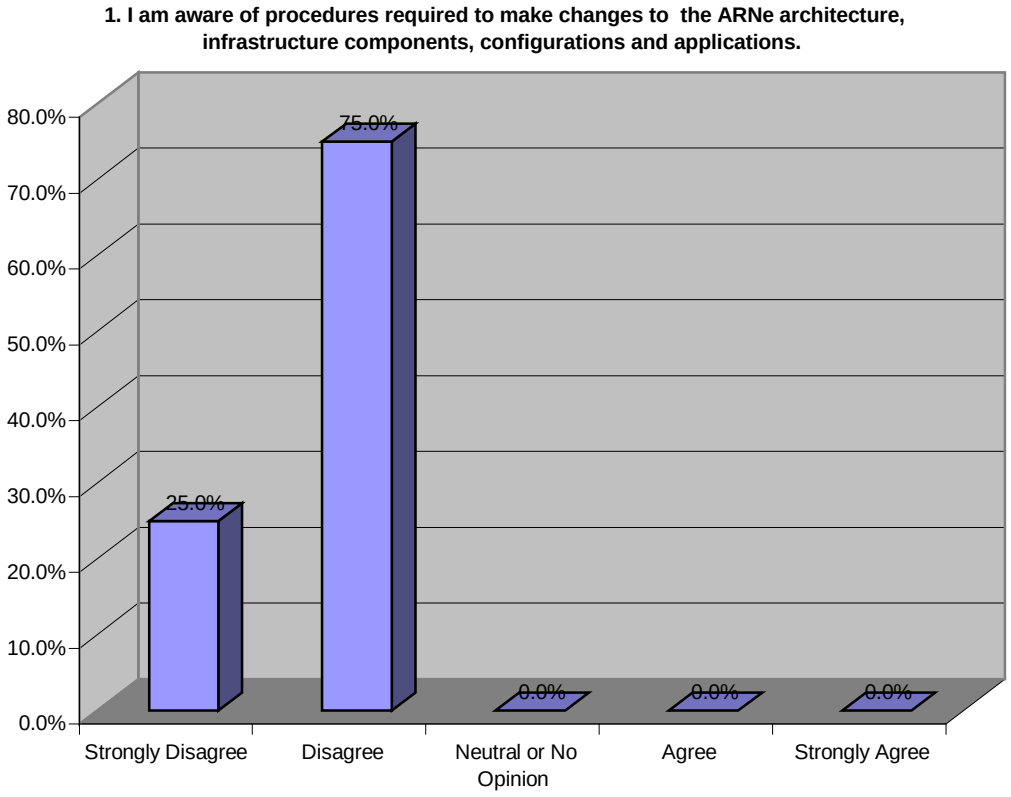
It is important to note the primary focus of this research project is on the non-production SEAD Practicum portal. The concepts developed and eventually implemented for the SEAD Practicum can be scaled to the overall ARNe environment using the same standards-based and best-practice guidance approach.

Change Management Survey Results

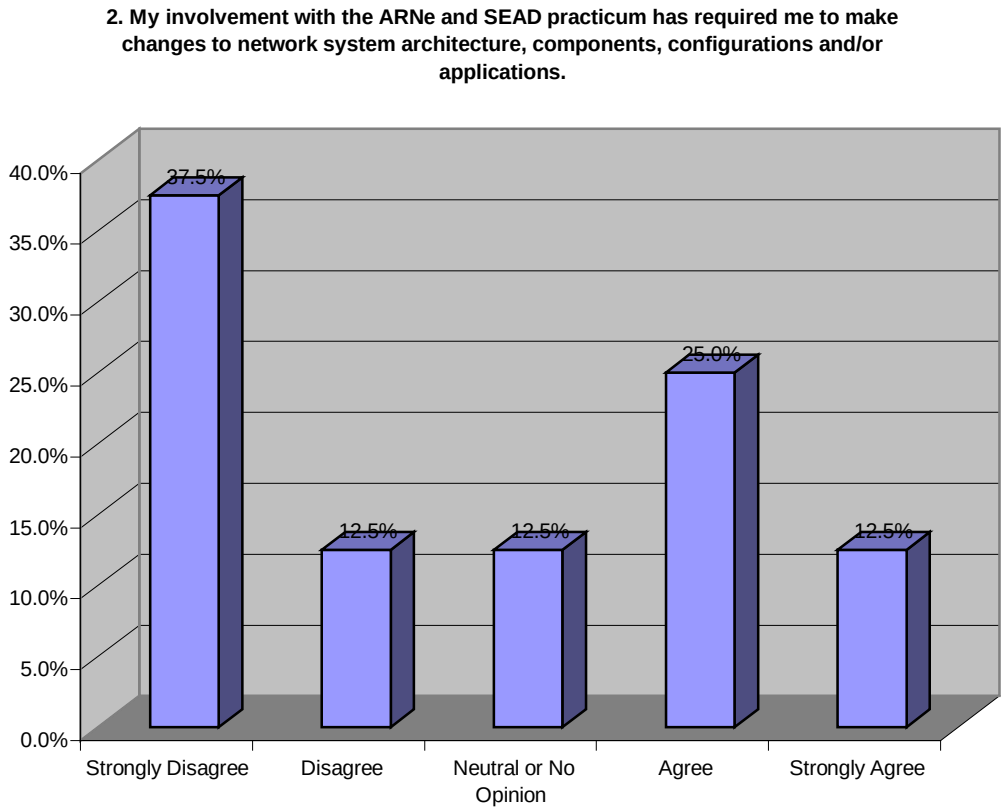
The Change Management Survey was designed to gather SEAD Practicum user input on their perceptions and understanding of change management processes within the ARNe, their comfort level with the use of Web 2.0 tools, and the importance of implementing an effective change management process for the ARNe.

The Likert-type survey consisted of 12 statements with five possible responses each. A single response was selected per statement.

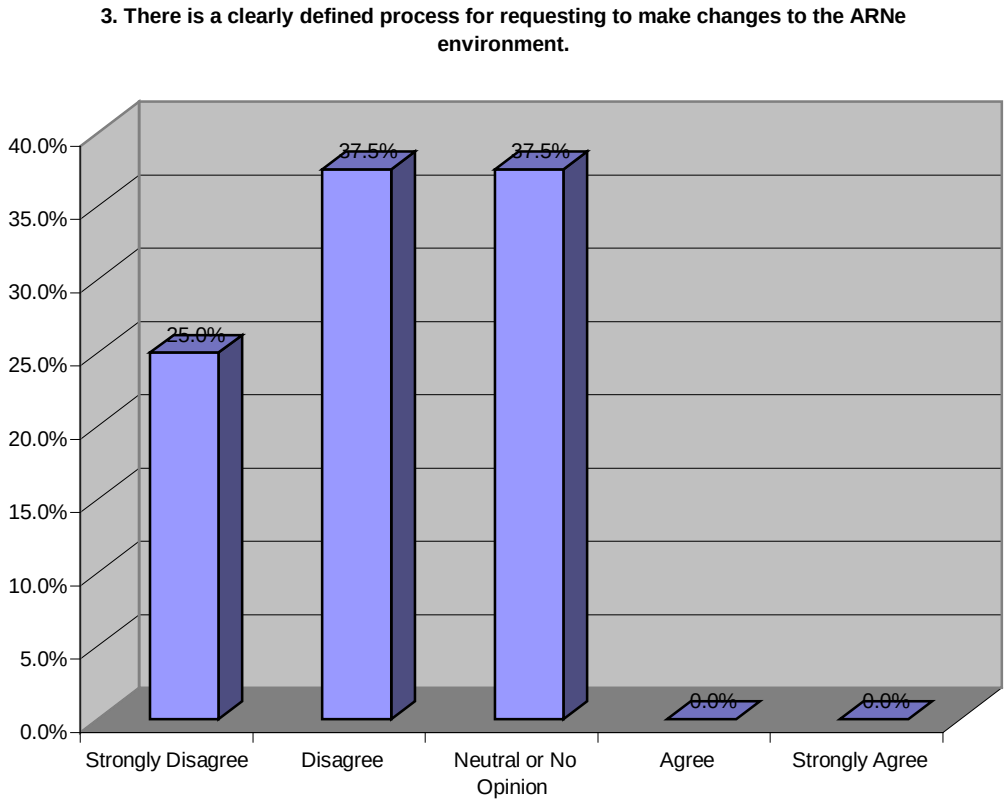
The returned data was analyzed by adding the total number of like responses per question, and then calculating the percentage represented by each total. Some general conclusions were drawn based on this analysis.



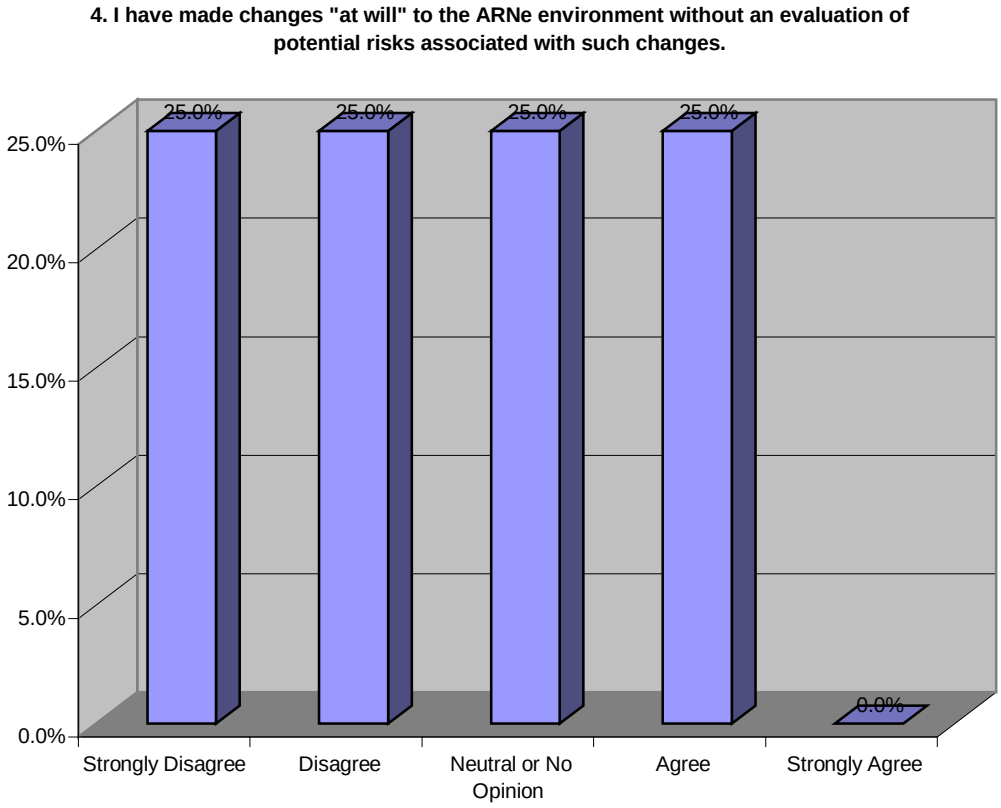
As seen from the above chart, virtually all respondents indicate they are not aware of any procedures required to make changes to the ARNe environment. This clearly points to a lack of a defined change management process for the ARNe,



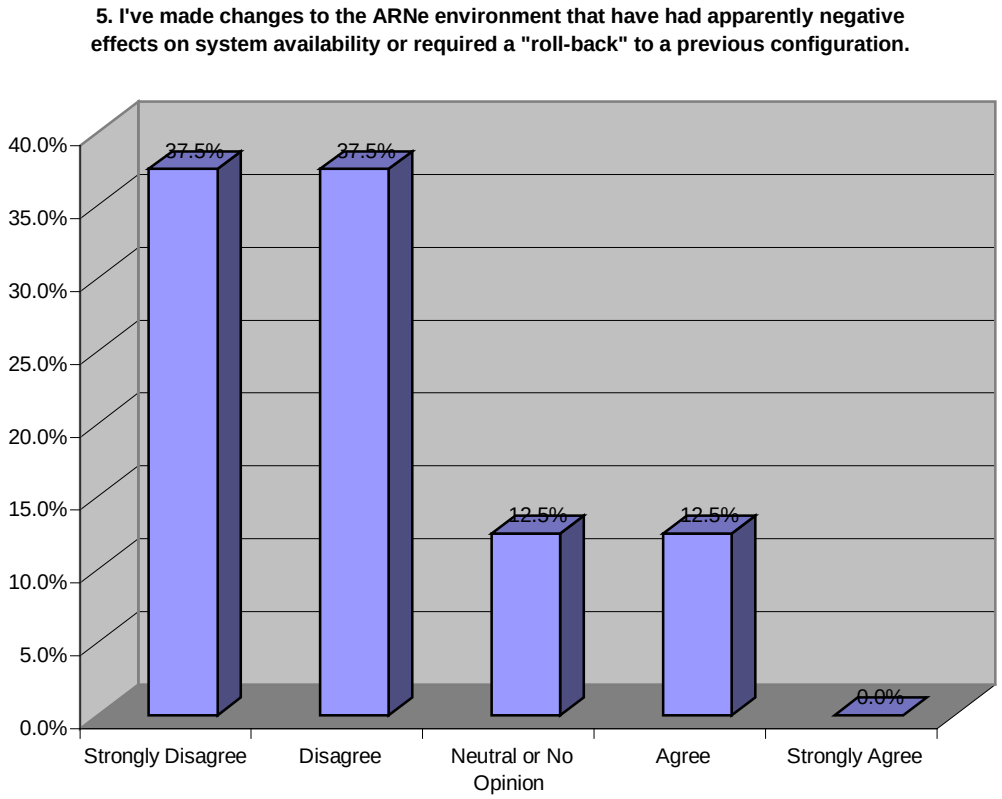
Over a third (37.5 %) of respondents stated they have had to make changes to at least one aspect of ARNe system resources as a result of their involvement with the SEAD Practicum.



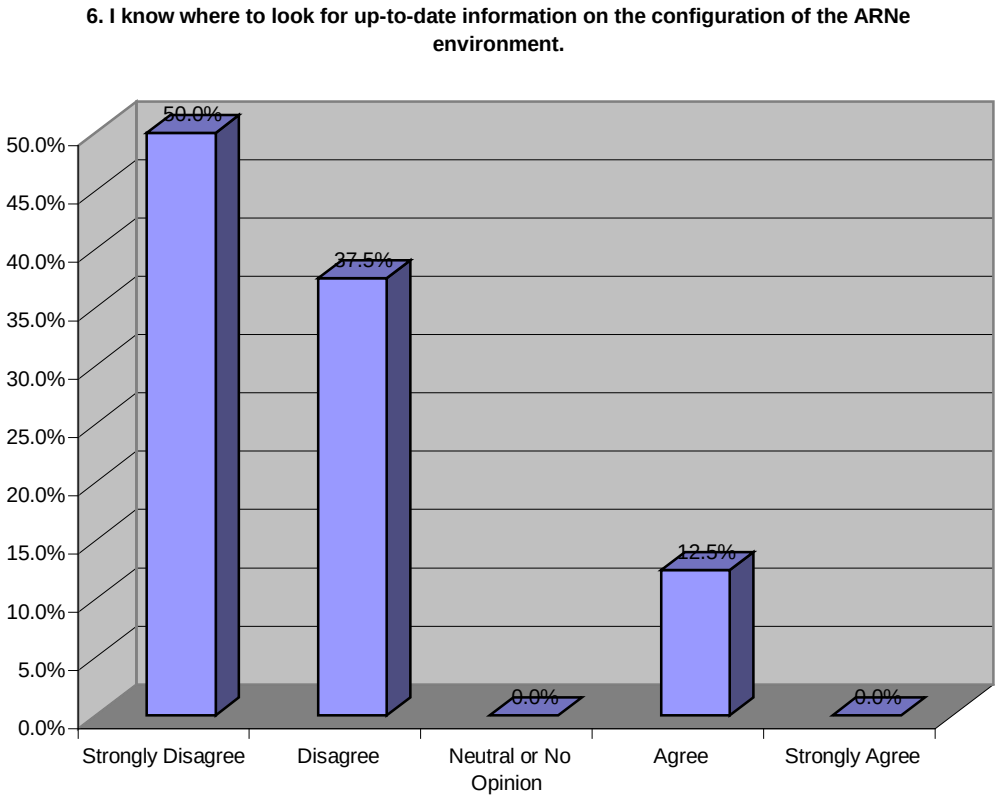
Almost two-thirds (62.5%) of respondents indicate there is no clearly defined change management process currently in place for the ARNe, the remainder were neutral, indicating they were not aware if there was a process or not.



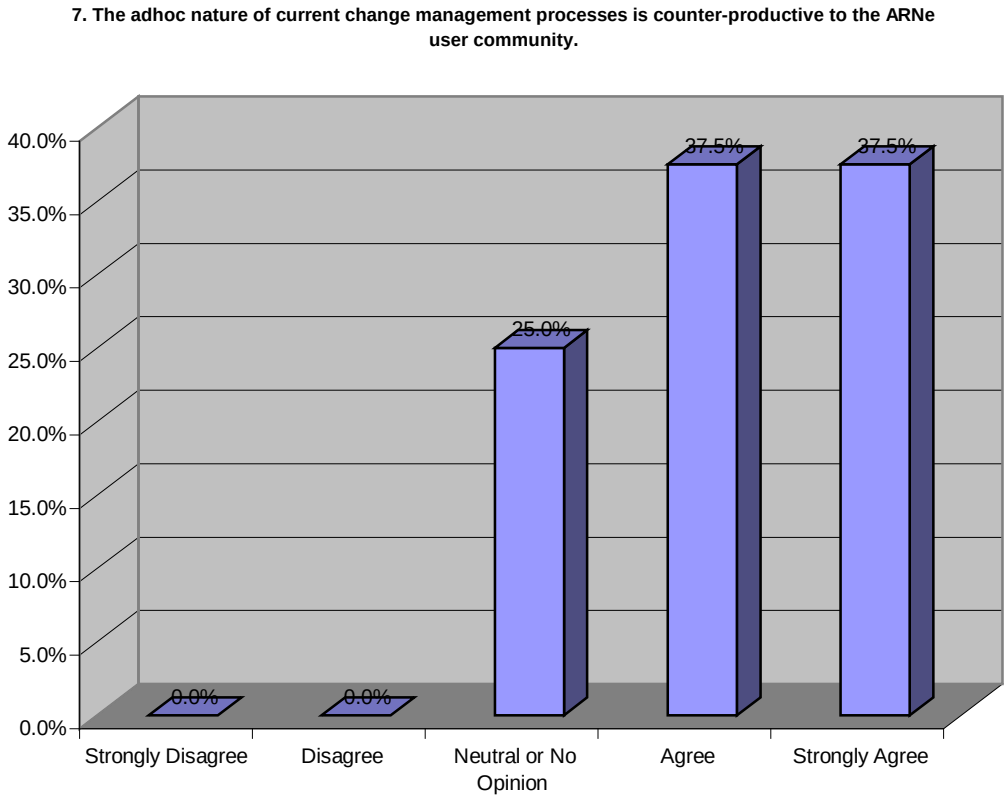
One quarter (25%) of the respondents indicate they have made changes “at will” to ARNe system resources without evaluating potential risks associated with those changes.



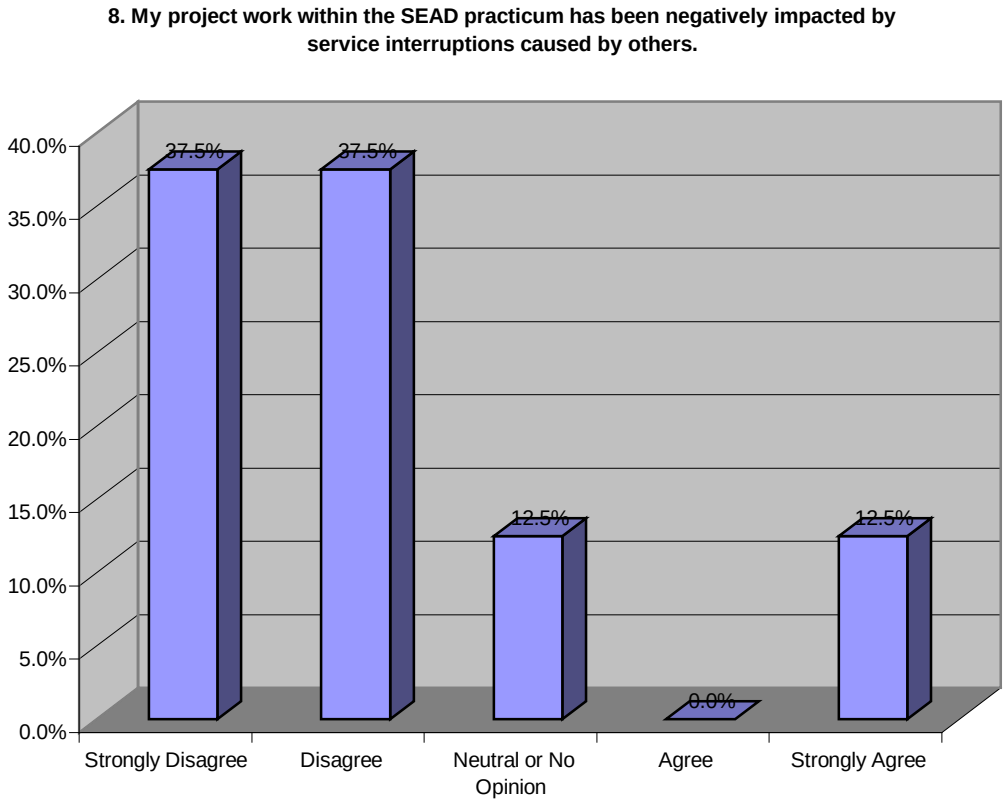
A relatively small percentage (12.5%) of respondents have implemented changes that negatively impacted ARNe system resources requiring backing out or “rolling back” to a prior configuration.



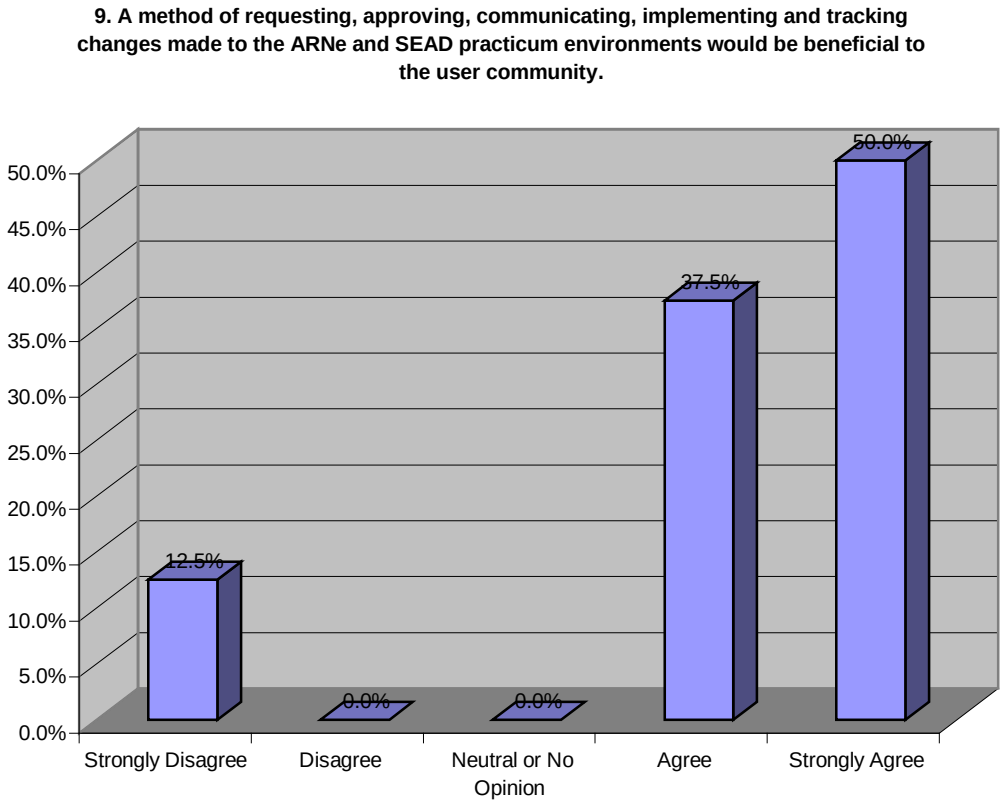
The majority of respondents (87.5%) have no idea where to look for up-to-date information related to the configuration of the ARNe.



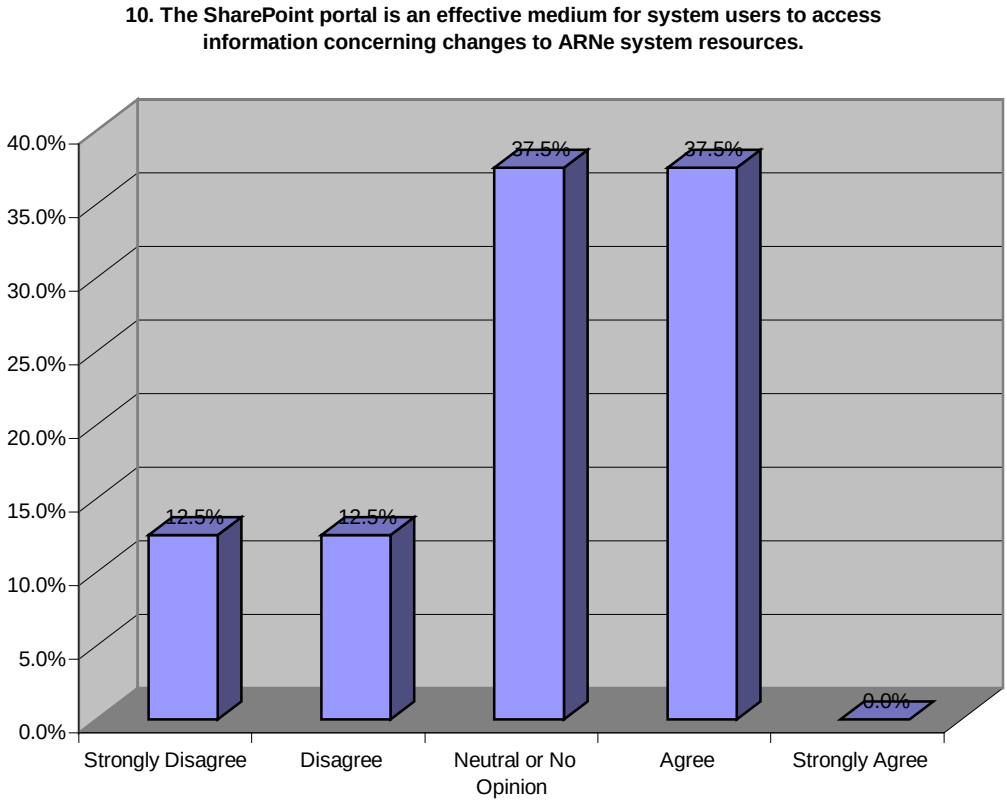
The majority of respondents (75%) indicate the adhoc nature of current change management processes is counter-productive to the ARNe user community.



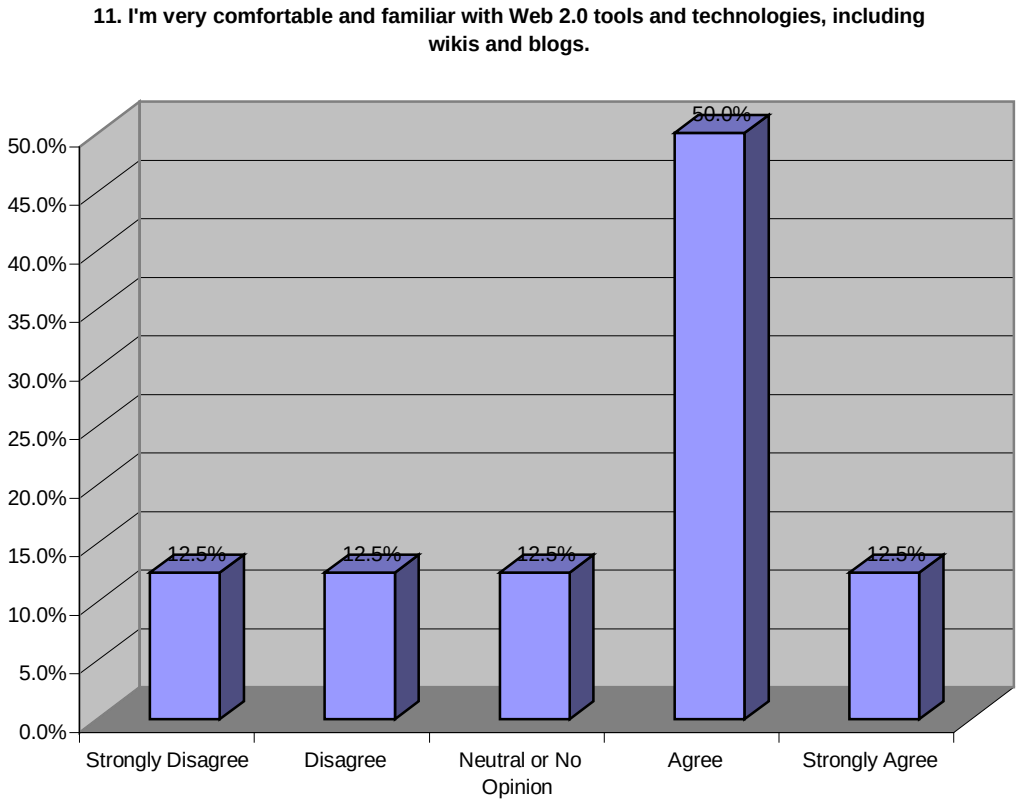
The majority of respondents (75%) have not experienced any negative effects from service interruptions to the ARNe, however, 12.5% of respondents strongly agree that they have experienced services interruptions.



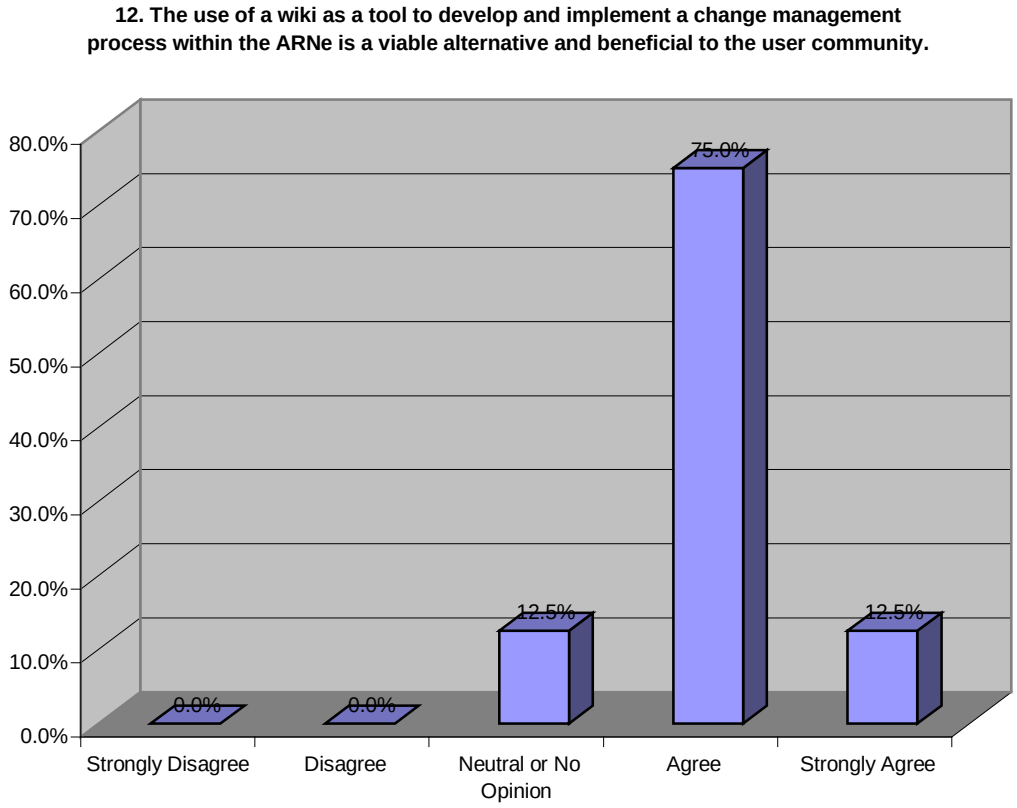
The majority of respondents (87.5%) indicate a formal change management process implemented for the ARNe and SEAD Practicum would be beneficial to the user community.



Over one third of respondents (37.5%) indicate the SharePoint portal is an effective medium for communicating system changes to the user community. One quarter (25%) indicate this is not an effective medium for this purpose.



Over one-half (62.5%) of respondents indicate they are very comfortable using Web 2.0 tools and technologies; one quarter (25%) indicate they are not.



A majority (87.5%) of respondents indicate that a wiki is a viable alternative for implementing a change management process for the ARNe and would be beneficial to the user community.

Based on the results of the user survey, the author draws the following general conclusions.

1. SEAD practicum users (Users) are not aware of any procedures or processes currently in place to request to make changes to ARNe system resources.
2. Users do not know where to look for information on the current state or configuration of ARNe system resources.
3. Users currently make uncontrolled changes to ARNe system resources without an evaluation of associated risks.

4. Users have either implemented changes to the ARNe environment that have had negative impacts on system resources, or have experienced negative impacts caused by others.
5. The overwhelming majority of Users think implementing a formal change management process would be beneficial to the ARNe and SEAD practicum user community.
6. The overwhelming majority of Users think using Web 2.0 tools, such as a wiki, is a viable alternative to implement a change management process.

Presentation

The results of the study are documented and presented in this technical report of findings. There is not currently a standardized or widely used report format for case studies. The report follows the recommended format presented on the Regis University SEAD Website. The evidentiary database is attached to this report in the form of the Annotated Bibliography and References.

CONCLUSIONS

Conclusions

This project was undertaken to develop a change management (CM) process for the ARNe/SEAD Practicum, thus addressing a practical operational problem resulting from allowing uncontrolled and unauthorized changes to network resources. The process was developed after extensive research into industry standards and best-practice guidance including ISO 2000:2005, ITIL, ITPI and COBIT. In addition, earlier project research involved an analysis of standards and best-practice guidance related to risk assessment processes.

The CM process developed, if implemented in the future, will provide a means for ARNs/SEAD Practicum stakeholders to effectively manage and track changes to system architecture, infrastructure and component configurations, thus reducing adverse impacts associated with uncontrolled changes.

Project limitations included not implementing an actual CM process on a limited, pilot scale basis. In spite of this limitation, the author was able to assimilate and evaluate a great deal of information and data related to CM processes, in the form of archival documents, technical reports, books, best-practice guidance documents and published standards, and in the process learned a great deal in the areas of risk assessment and IT service management. Research into IT service management, and specifically change management, included delving into the related areas of process engineering and workflow design. The management interviews and user surveys provided useful insight into how system stakeholders view the current nature of change management procedures within the

ARNe/SEAD Practicum, and gain input from stakeholders on their perceptions of using Web 2.0 tools and techniques to implement a change management process.

AREAS FOR FUTURE WORK

This project focused on the development of a change management process for the ARNe/SEAD Practicum, without testing an actual implementation. Implementing the process and developing metrics to measure the effectiveness of the process would be a natural continuation of this project.

REFERENCES

Alberts, Christopher & Dorofee, A. (2002). Managing Information Security Risks: The OCTAVE® Approach, Boston, MA: Addison-Wesley

Argo, Annette (2008). ARNe Security Case Study and Review of the EBK Framework. Professional Project. Regis University School for Professional Studies. Retrieved May 22, 2009 from https://in2.regis.edu/sites/scis/IT/SEAD/Shared%20Documents/Forms/AllItems.aspx

Carelli, Richard A., Stevens, James F., Young, Lisa R. & Wilson, William R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. [Electronic version]. Retrieved October, 18, 2009 from www.**cert.org**/archive/pdf/07tr012.pdf

Cater-Steel (ed), Aileen (2009). Information technology governance and service management: frameworks and adaptations. IGI Global. © 2009. Books24x7. Retrieved April 5, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_28491/book.asp

Cascarino, Richard (2007). Auditor's Guide to Information Systems Auditing. Hoboken, NJ: John Wiley & Sons, Inc.

Center for Internet Security (2009). The CIS Security Metrics: Consensus Metric Definitions v.1.0.0. Retrieved August 12, 2009 from https://www.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.0.0.pdf

Gale, Doug (2008). Change Management Meets Web 2.0. Campus Technology. Retrieved July 15, 2009 from http://campustechnology.com/articles/2008/09/change-management-meets-web-20.aspx

Han, Sang Jin (2003). Demystifying Security Tools. Should I Use Commercial or Freeware? SANs Institute. InfoSec Reading Room. Retrieved June 10, 2009 from http://www.sans.org/reading_room/whitepapers/tools/demystifying_security_tools_should_i_use_commercial_or_freeware_1060?show=1060.php&cat=tools

Insecure.org (2009). Featured News. Nmap Network Scanning. Retrieved June 10, 2009 from http://insecure.org/

IT Governance Institute (2007). COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. Retrieved June 18, 2009 from http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

ITIL Open Guide (2007). Open Guide: Change Management. Retrieved June 21, 2009 from http://www.itlibrary.org/index.php?page=Change_Management

IT Process Institute (2007). Change, configuration and release: What's really driving top performance? [Electronic version]. Retrieved February 15, 2010 from http://www.itpi.org/home/white_papers.php

IT Process Institute (2007). Process maturity matters: The key to unlocking the power of IT controls. [Electronic version]. Retrieved February 15, 2010 from http://www.itpi.org/home/white_papers.php

IT Process Institute (2007). The Visible Ops Handbook. Implementing ITIL in 4 practical and auditable steps. Revised First Edition. [Electronic version]. Retrieved February 20, 2010 from http://www.itpi.org/home/visibleops2.php

Klosterboer, Larry (2009). Implementing ITIL change and release management. [Electronic version]. IBM Press. © 2009. Books24x7. Retrieved April 5, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_30900/book.asp

Leedy, Paul D. & Ormrod, Jeanne E. (2005). Practical Research. Planning and Design (5th Edition). Upper Saddle River, NJ: Pearson Education, Inc.

Miles, Matthew B. & Huberman, Michael A. (1994). Qualitative Data Analysis: An Expanded Source Book (Second Edition). Thousand Oaks, CA: Sage Publications.

Miles, Greg, and Russ Rogers. Security Assessment: Case Studies for Implementing NSA IAM [Electronic version]. Syngress Publishing. © 2004. Books24x7. Retrieved August 18, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_7165/book.asp

Mutafelija, Boris & Harvey Stromberg (2009). Process Improvement with CMMI v1.2 and ISO Standards. Auerbach Publications. © 2009. Books24x7. Retrieved April 5, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_26466/book.asp

Myers, Michael D. (1997). Qualitative Research in Information Systems. Association For Information Systems. Retrieved June 15, 2009 from http://www.qual.auckland.ac.nz/

Orlikowski, W.J. & Baroudi, J.J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research 2,* 1-28.

Pare, Guy (2002). Enhancing the Rigor of Qualitative Research: Application of a Case Methodology to Build Theories of IT Implementation, *The Qualitative Report 7 (4)*, retrieved June 20, 2009 from http://www.nova.edu/ssss/QR/QR7-4/pare.html

Payne (2006). A Guide to Security Metrics. SANS Institute INFOSEC Reading Room. Retrieved August 18, 2010 from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

Peshkin, A. (1993). The goodness of qualitative research. *Educational Researcher, 22* (2), 23-29.

Richman, Evan (2007). Transforming Your Business With SharePoint Products and Technologies. Retrieved August 18, 2010 from http://www.microsoft.com/downloads/details.aspx?FamilyID=cf5bb5e2-909d-4910-a8bb-3f4718bee8f7&displaylang=en

SANS (2010). Security Consensus Operational Readiness Evaluation (SCORE). Retrieved August 18, 2010 from http://www.sans.org/score/

Whitman, Michael E. & Mattord, Herbert J. (2005). Principles of Information Security, Second Edition. United States: Thomson Course Technology.

Yin, Robert K. (2009). Case Study Research: Design and Methods (4th Edition.). Thousand Oaks, CA: SAGE, Inc.

ANNOTATED BIBLIOGRAPHY

Argo, Annette (2008). ARNe Security Case Study and Review of the EBK Framework. Professional Project. Regis University School for Professional Studies [Electronic version]. Retrieved May 22, 2009 from Regis University SEAD Practicum Website: https://in2.regis.edu/sites/scis/IT/SEAD/Shared%20Documents/Forms/AllItems.aspx

This thesis report was prepared by a Regis CPS graduate student, and focuses several areas, including documenting the results of a physical risk assessment at the five Regis area campuses; conductance of a pilot study using CIS benchmarks related to Windows 2003 server security. The report provides a good description of the Regis University ARNe architecture and infrastructure, and its relation to the SEAD practicum management and operational environment.

Arora, Ashish Hall, Dennis, Pinto, C. Ariel, Ramsey, Dwayne & Telang, Rahul (2004). Measuring the risk-based value of IT security solutions [Electronic version]. *IEEE IT Professional, 6 (6),* 35-42.

The authors present a new framework to help evaluate the costs and benefits of security solutions based on a company's risk profile. The framework bases benefit on avoided risk. Lawrence Berkley National Lab (LBNL) reportedly uses this framework as a

demonstration that it is much less expensive to accept some damages from security incidents than try to prevent all incidents. They define “risk-based benefit” as the reduction in expected loss from security failure incidents. The described framework uses a risk management approach to integrate risk profile with actual damages and implementation costs. They state this approach requires voluminous incident data. Two key concepts introduced are “incident type” and “bypass rate”.

Brykczynski, B. & Small, R.A. (2003). Reducing Internet-based intrusions: effective security patch management [Electronic version]. *IEEE Software, 20 (1),* 50-57.

The authors are both associated with the Software Productivity Consortium. The consortium has focused on four key security defense areas against Internet-based threats, including: security patch management, system and application hardening, network reconnaissance and enumeration, and tools against malicious software. They stress that the process of patch management has not been adequately addressed in the literature.

The authors describe eight key steps they consider fundamental to effective, systematic and repeatable patch management and propose performance metrics for evaluating a patch management program. Key practices include: establish policies, procedures and responsibilities; maintain awareness of IT infrastructure; maintain vulnerability alert resources; monitor vulnerability alerts; assess and respond to alerts; test and evaluate patches; install patches; measure and improve the process.

Carelli, Richard A., Stevens, James F., Young, Lisa R. & Wilson, William R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. [Electronic version]. Retrieved October, 18, 2009 from www.**cert.org**/archive/pdf/07tr012.pdf

This technical report prepared for Carnegie Mellon's Software Engineering Institute (SEI) introduces OCTAVE Allegro, an evolution of the Operationally Critical Threat, Asset, Vulnerability Evaluation (OCTAVE®) risk assessment methodology developed by the CERT® Survivable Enterprise Management team. The OCTAVE method was orginally developed for the Department of Defense (DOD), as an aid in addressing information security concerns related to the Health Insurance Portability and Accountability Act (HIPAA). OCTAVE Allegro was developed as a streamlined and optimized method of assessing information security risks.

Cater-Steel (ed), Aileen (2009). Information technology governance and service management: frameworks and adaptations. IGI Global. © 2009. Books24x7. Retrieved April 5, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_28491/book.asp

The author is a senior lecturer in information systems at the University of Southern Queensland, Australia. The book focuses on the importance of IT service management to IT governance, and emphasizes the benefits of service management to overall business competitiveness. The book provides an overview of IT governance literature and research,

provides several case studies related to the implementation of IT governance best-practices, delves into the relationship between IT governance and various other frameworks, and describes IT service management frameworks.

Chaboya, David J., Raines, Richard A., Baldwin, Rusty O., & Mullins, Barry E. (2006). Network intrusion detection: automated and manual methods prone to attack and evasion. [Electronic version] *IEEE Security & Privacy*, *4(6)*, 36-43.

The authors are all associated with the Air Force Institute of Technology, three as professors. They provide a discussion of intrusion detection techniques, evasion techniques, and suggest methods for improving the trust relationship between server and analyst. They suggest the key to improving trust and validating server response is to analyze attacker shell code. They describe three techniques of doing this, to include: reverse engineering the shell code; cataloging known shell code and analyzing payload size. They conclude each technique has its strengths and weaknesses. They are also testing Linux systems using the Metasploit framework, and developing payload size and code matching filters for Snort.

Devanbu, P., Gertx, M. & Stubblevine, M. (1999). Security for automated, distributed configuration management [Electronic version]. Retrieved June 17, 2009 from http://www.cs.ucdavis.edu/~devanbu/files/tcm.pdf.

The authors discuss security issues related to software configuration management, discuss the need to maintain privacy, integrity, authentication, and protection of proprietary information when employing automated, distributed configuration management tools. They go on to state they are developing a flexible, retargetable architecture that addresses these security needs, and describes the issues and requirements to be met by such an architecture.

For example, integrity issues include software, configuration and message integrity. Key research issues to be addressed include: security aspects of configuration management languages; cryptographic techniques; messaging infrastructure; formal underpinnings, and retargetability.

Flowerday, S., Blundell, A.W., & Von Solms, R. Continuous auditing technologies and models: a discussion (2006) [Electronic version]. *Computers & Security*, *25*, 325-331.

The authors are all affiliated with the Nelson Mandela Metropolitan University in South Africa, two as graduate students, with Professor von Solms being the Director of the Institute for ICT Advancement at the University.

The authors discuss the need for real-time auditing techniques and technologies within three different continuous auditing models. The models all strive to obtain real-time functionality. They employ different technologies to achieve the same goal. For example, error and fraud detection may be accomplished through Computer Aided Audit Tools and Techniques (CAATS), digital agents or expert systems.

They discuss problems encountered when trying to implement continuous auditing tools, such as disparate file and record systems, and technologies to overcome these obstacles. Technologies like XBRL can be used to standardize reporting formats. Intelligent technologies like Financial Reporting and Auditing Agent with Net Knowledge (FRAANK) can be used to convert older reports into XRBL.

They discuss the importance of continuous auditing addressing both the testing of internal controls and transactions, and then provide their opinion of the future of continuous auditing.

Higby, Charles & Bailey, Michael (2004). Wireless security patch management system [Electronic version]. *Proceedings of the 5th conference on information technology education. Security III*, 165-168.

The authors discuss security issues with increased use of wireless devices on college campuses and propose an automated security patch management system to ensure mobile device configurations are current and in compliance with campus security policies before being granted access to the campus network.

Their system includes a patch management and antivirus software system, and a RADIUS server and Certificate Authority to authenticate users. They provide specific details on the hardware and software comprising the system and how the process flows. They state research is continuing on the quarantine aspect of the system.

Hill, John M.D.; Carver, Curtis A. jr.; Humphries, Jeffrey W. & Pooch, Udo W. (2001). Using an isolated network laboratory to teach advanced networks and security [Electronic version]. *Proceedings of the thirty-second SIGCSE technical symposium on computer science education, 33(1),* 36-40.

The authors describe an approach to teaching network security that emphasizes practical, laboratory-based exercises rather than classroom lectures. The approach employs "persistent cooperative teams" broken down into attackers and defenders of networked systems. The lab is isolated from other campus network resources to prevent the potential for negative consequences. They describe the lab topology and the tools used by the teams to attack, analyze and defend the network. The authors conclude this approach is a very effective way to teach practical security techniques and methods.

Hu, Ji; Meinel, Christoph; & Schmitt, Michael (2004). Tele-lab IT security: an architecture for interactive lessons for security education [Electronic version]. *Proceedings of the 35th SIGCSE technical symposium on computer science education, Computer Security, 36(1),* 412-416.

The paper describes the user interface, architecture and functional components of the Tele-lab IT Security system developed at the University of Trier, Germany. The system provides both a web-based tutoring system and virtual laboratory to teach students practical application of information security methods. The system employs virtual machine technology (VNC), and topics covered include cryptography, digital certificates and secure

email, authentication and scanning techniques and tools. The authors provide a good overall description of the system components and architecture; future work identified relates to dynamically adapting content based on user behavior tracked in their profile.

IT Process Institute (2007). The Visible Ops Handbook. Implementing ITIL in 4 practical and auditable steps. Revised First Edition. [Electronic version]. Retrieved February 20, 2010 from http://www.itpi.org/home/visibleops2.php

The Visible Ops Handbook describes four phases to implement ITIL best practices based on surveying hundreds of IT organizations and determining what practices result in the greatest efficiencies and effectiveness, or otherwise stated, what implemented practices result in a high performing IT organization. The book provides a road map towards becoming a high performing IT organization.

Klosterboer, Larry (2009). Implementing ITIL change and release management. [Electronic version]. IBM Press. © 2009. Books24x7. Retrieved April 5, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_30900/book.asp

The author is a certified IT architect working for IBM's global services delivery team as a lead systems engineer. The book describes ITIL service management processes, focusing on change and release management. He outlines and describes a structured approach to discovering requirements, defining processes, building change and release management workflows, and developing an implementation plan. He further describes

operational issues, including issues with the Forward Schedule of Changes (FSC), and discusses the business benefits of implementing a change and release management program.

Mattord, Herbert J. & Whitman, Michael E. (2005). Planning, building and operating the information security and assurance laboratory [Electronic version]. *Proceedings of the 1st annual conference on information security curriculum development, Academic Papers* 8-14.

The authors, both faculty members with Kennesaw State University, describe current practices in establishing information security laboratories. The authors feel that laboratory exercises are a core component of an InfoSec program, and provide the opportunity to learn and implement computer and network security tools and techniques, along with the more challenging aspects of vulnerability assessment and penetration testing. They describe what they consider as best practices in the design and implementation of a lab architecture, and types of software including the use of VMWare and Microsoft Virtual PC to enable use of multiple OS images. They further discuss lab curriculum structure, content and preparation.

Millet, Jean-Marc (2004). Security improvement of a wide and heterogeneous set of network devices: a global approach [Electronic version]. *SANS Conference.* London, 2004. Retrieved June 25, 2009 from http://www.sans.org/reading_room/whitepapers/networkdevs/security_improvement_o

f_a_wide_and_heterogeneous_set_of_network_devices_a_global_approach_1550?show=1550.php&cat=networkdevs

The author describes elements of a case study that addresses security in multi-platform network environments. The environment includes Cisco routers, Nokia firewalls and as well as other devices. They describe how to establish a security baseline through a network scan, and group and prioritize devices based on risk. State of the art security configuration tools and best practices are described. Various techniques, to include Cisco Router Auditing Tool (RAT), audit checklists and ad hoc scanning are described. The network scan is considered the default security control. The author states a network scan is the cheapest way to assess weak configuration and obsolete software issues. Instead of Nessus, a proprietary (ITCORP) scanner was employed for the scan. The scan was evaluated in two ways: by network environment and by vulnerability frequency. Multiple scans were run, to establish the baseline and document improvements after implementing corrective actions.

The author concludes that securing individual network hosts is not an adequate approach, and that the network must be viewed as a single entity. He poses several questions in this regard, including: are automatic tools available to validate perimeter firewall rules? What tools and methods are available to check and measure network, rather than component, security? He also concludes that relying on one vendor's equipment is a less secure infrastructure than implementing a heterogeneous, multi-vendor platform.

Miles, Greg, and Russ Rogers. Security Assessment: Case Studies for Implementing NSA IAM [Electronic version]. Syngress Publishing. © 2004. Books24x7. Retrieved August 18, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_7165/book.asp

The authors are co-founders of Security Horizon, Inc., a private information security consulting firm based in Colorado. They both are Air Force veterans and have experience working as security consultants and contractors for various Federal agencies, including NSA, Air Force and NASA.

The book focuses on case studies for fictional organizations related to the implementation of the NSA's Information Assurance Methodology (IAM). The IAM was developed in response to Presidential Decision Directive 63 (PDD-63) and increased demand for an INFOSEC assessment methodology. The book provides useful examples and a structured, methodical approach to conducting an INFOSEC assessment based on the methodology and the authors' practical experience.

Mitropoulos, Sarandis, Patsos, Dimitrios & Douligeris, Christos (2006). On incident handling and response: A state-of-the-art approach [Electronic version]. *Computers & Security, 25,* 351-370.

The authors propose a detailed management framework and structured methodology containing best practices for handling security incidents. They state that

incident response is often overlooked by security administrators. They further propose a generic incident response process within a corporate environment.

They further describe both passive and active (traceback) incident response methods, identify and provide a detailed discussion of the different phases of the incident response process, based on published and recognized standards. They include recommended best practices applicable to each stage. They describe different traceback methods, including: IP marking traceback, IP tunneling traceback, ICMP-based traceback, host-based and application based traceback methods. They then describe the importance and applicability of digital forensic techniques and methods to the realm of incident response, and describe various forensic approaches (computer, network and software forensics).

Mohan, Kannan, Xu, Peng & Remesh, Balasubramaniam (2008). Improving the change management process [Electronic version]. *Communications of the ACM, 51 (5),* 59-64.

The authors describe issues with the software change management process, and a general lack of inclusion of certain artifacts such as requirements and design documents in the process. They state that software configuration management (SCM) and traceability tools, although having common objectives, are often employed independently of one another. They propose integrating SCM and traceability techniques and tools as a means to improve configuration management processes in software development. They conduct a case study on an organization that develops embedded software systems. The

case study reportedly identified issues with SCM and the need to augment SCM with traceability. They propose a framework for integrating SCM and traceability and validate their results by obtaining feedback from several software professionals. They conclude that project managers should implement process and tool integration to improve configuration management processes.

Mutafelija, Boris & Harvey Stromberg (2009). Process Improvement with CMMI v1.2 and ISO Standards. Auerbach Publications. © 2009. Books24x7. Retrieved April 5, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_26466/book.asp

Both authors have extensive private sector experience in the area or process improvement, having helped organizations improve their process maturity levels based on established standards and best-practice guidance. They provide an excellent description of International Standards Organization (ISO) standards, including ISO 20000:2005 specific to IT service management. The book describes CMMI v 1.2 and maps various components of the ISO standards to CMMI.

Romney, Gordon W. & Stevenson, Brady R. (2004). An isolated, multi-platform network sandbox for teaching IT security system engineers [Electronic version]. *Proceedings of the 5th conference on Information Technology Education. Security* 19-23.

The authors, graduate students at Brigham Young University (BYU) describe the successful deployment and operation of an academic research laboratory to teach Information Technology (IT) Security System Engineers. The laboratory is an isolated ("Sandbox"), multi-platform environment where students can practice the design and implementation of security techniques and methods without the concern of adversely impacting external networked systems. Students designed the laboratory network architecture and also developed security courses and laboratories. The architecture is modular to allow creation of multiple network nodes containing related host devices (servers, routers, switches, firewalls, IDS, etc.). They go on to provide a more detailed description of the architecture. A student Security Team was established to administer the laboratory.

The authors describe the apparent lack of trained security professionals, academic programs and researchers, while the demand only continues to grow in these areas. They further describe the BYU security initiative in response to the need for trained professionals, and provide a generic job description for a Security System Engineer. Future work identified includes augmenting the Sandbox with a network that employs controlled Internet access. The use of Honeypots is suggested as a subject for further research.

Sahinoglu, Mehmet (2005). Security Meter: A practical decision-tree model to quantify risk [Electronic version]. *IEEE Security & Privacy*, *3 (3),* 18-24.

The author proposes a probabilistic security model to quantify security risks in information systems. The author states a quantitative risk assessment provides hard

numbers that management can relate to, as opposed to qualitative methods that are easier to implement but provide less concrete results. He states a quantitative risk measure calculated as a percentage can be tested, improved, compared and budgeted, as opposed to less tangible descriptions such as high, medium or low. The presented Security Meter model includes a description of inputs and outputs in a probabilistic decision-tree diagram. A modified or hybrid approach is also presented to account for scenarios where all necessary quantitative data is not available.

Stanton, Jeffrey M., Stam, Kathryn R., Mastrangelo, Paul & Jolton, Jeffrey (2005). Analysis of end user security behaviors [Electronic version]. *Computers and Security, 24,* 124-133.

The authors present the results of a survey of end user information security practices. They began by interviewing 110 information security professionals with knowledge of end user behaviors, continued with a behavior rating exercise with 49 subject matter experts, and finally conducted a survey of 1167 end users to obtain self assessments and password related behaviors.

The results were used to categorize and map end user results against both technical expertise and intentionality of behaviors. A two-factor taxonomy of end user security behavior was tabulated. They further developed a listing of the ten most extreme behaviors relative to technical expertise.

The authors conclude that end-user training, awareness, knowledge of monitoring, and rewards resulted in improved basic security conscious behaviors.

Theoharidou, Marianthi & Gritzalis, Dimitris (2007). Common Body of Knowledge for Information Security [Electronic version]. *IEEE Security & Privacy, 5 (2),* 64-67.

The authors, both associated with the Athens University of Business and Science, present an information security (InfoSec) common body of knowledge (CBK) aimed at information security curriculum development. They surmise current efforts at presenting a CBK actually focus on security sub-domains and therefore present limited understanding and narrow perceptions of the overall domain.

Their work involved a survey of educational programs in Africa, Asia, Europe, South America and North America that offered undergraduate, graduate, and/or courses in information security. They grouped programs into seven different security categories and then present skill sets for information security professionals. They present ten InfoSec domains that include technical domains such as Network and Telecommunications Security and non-technical domains like Social, Ethical and Legal considerations. A future area of interest to the researchers is the development of a Master of Science program in information security and critical infrastructure protection.

Ward, Peter & Smith, Clifton L. (2002). The Development of Access Control Policies for Information Technology Systems [Electronic version]. *Edith Cowen University, School of Engineering and Mathematics.* Retrieved January 29, 2009 from http://www.sciencedirect.com.dml.regis.edu/science?_ob=ArticleListURL&_method=list&_ArticleListID=860083495&_st=13&_sort=d&sisrterm=auditing&_acct=C

000055361&_version=1&_urlVersion=0&_userid=1922016&md5=86d7d68ec21adcaa89e59dc192508f31

The authors are both affiliated with Edith Cowan University in Australia. The authors propose a high-level approach to implementing security policies through assigning responsibilities, accountability and other baseline access control security policies.

They discuss the transition from centralized mainframe computing to distributed computing, and how security vulnerabilities and risks have changed as a result. They identify security risks inherent in distributed computing environments.

The authors then discuss key information security concepts, including risk management, defense in depth, separation of duties and also issues such as accountability, dual control and the concept of need-to-know.

They then present an outline for a strategic plan to implement security policies within an organization. The plan outline specifies roles and responsibilities for management, asset owners, asset owner representatives, users and service providers.

They further provide outlines for various types of information security policies including management accountability, information systems security policy, system access control policy, personnel security policy, physical and environmental security policy, telecommunications security policy, information classification policy, business continuity planning policy.

Yin, Robert K. (2009). Case Study Research: Design and Methods (4th Edition.). Thousand Oaks, CA: SAGE, Inc.

The author, Dr. Yin, is a recognized expert in the case study methodology. This book represents the fourth edition of the original work published in 1984. As such, it contains more material and reportedly more practical value than earlier editions. Its goal is to guide the researcher through the process of rigorous case study research. The book provides a detailed description of the case study methodology, and also encompasses the breadth of the methodology. It further refers to numerous useful case studies to exemplify the methodology.

APPENDIX A

SEAD PRACTICUM FACULTY/ADMINISTRATIOR QUESTIONNAIRE

CHANGE MANAGEMENT QUESTIONNAIRE

SEAD Practicum Faculty/Administrators

August 2010

The following questionnaire is being presented to support research associated with my professional project and thesis focusing on change management processes within the ARNe environment.

(Please email responses as an attachment to moult879@regis.edu)

Thank you for your time! Russell Moult

1. What functions do faculty/administrators currently serve in regards to ARNe systems administration, and specifically within the SEAD practicum portal site?

2. What types of changes do faculty/administrators typically make to the systems supporting the ARNe and SEAD practicum?

3. Who else currently has authority to make changes to ARNe system architecture, infrastructure components, configurations and applications?

4. Is there currently a process in place to request, review, authorize, communicate, implement, and track changes made to the ARNe systems and SEAD practicum portal? If yes, please explain.

5. What safeguards are currently in place to limit negative impacts of changes made to the ARNe network by administrators and users?

6. What types of issues are encountered from current change management processes or lack thereof?

7. What does management perceive as major obstacles to implementing a change management process for the ARNe and SEAD practicum systems?

8. What are the major process improvements perceived as being the most crucial to providing the greatest improvements in change management within the ARNe and SEAD practicum site?

APPENDIX B

SEAD PRACTICUM USER SURVEY

CHANGE MANAGEMENT SURVEY

SEAD Practicum User Community

August 2010

The following survey is in support of my research project and thesis focusing on information technology change management processes, specifically within the Regis University ARNe and SEAD practicum environment. Please respond to the following Likert-type survey by selecting the single choice that best describes your opinion on each statement.

Please save your selections and email your responses back as an attachment to moult879@regis.edu.

Thank you for your time! Russell Moult

Change Management Survey

Select the single answer that best describes your opinion on the following statements. The five possible choices are:

1 – Strongly disagree

2 – Disagree

3 – No opinion or neutral

4 – Agree

5 – Strongly agree

1. I am aware of procedures required to make changes to the ARNe architecture, infrastructure components, configurations and applications.

1 - Strongly Disagree

2. My involvement with the ARNe and SEAD practicum has required me to make changes to network system architecture, components, configurations and/or applications.

1 - Strongly Disagree

3. There is a clearly defined process for requesting to make changes to the ARNe environment.

1 - Strongly Disagree

4. I have made changes “at will” to the ARNe environment without an evaluation of potential risks associated with such changes.

1 - Strongly Disagree

5. I’ve made changes to the ARNe environment that have had apparently negative effects on system availability or required a “roll-back” to a previous configuration.

1 - Strongly Disagree

6. I know where to look for up-to-date information on the configuration of the ARNe environment.

1 - Strongly Disagree

7. The adhoc nature of current change management processes is counter-productive to the ARNe user community.

1 - Strongly Disagree

8. My project work within the SEAD has been negatively impacted by service interruptions caused by others.

1 - Strongly Disagree

9. A method of requesting, approving, communicating, implementing and tracking changes made to the ARNe and SEAD environments would be beneficial to the user community.

1 - Strongly Disagree

10. The SharePoint portal is an effective medium for system users to access information concerning changes to ARNe system resources.

1 - Strongly Disagree

11. I’m very comfortable and familiar with Web 2.0 tools and technologies, including wikis and blogs.

1 - Strongly Disagree

12. The use of a wiki as a tool to develop and implement a change management process within the ARNe is a viable alternative and beneficial to the user community.

1 - Strongly Disagree

APPENDIX C

IRB DOCUMENTATION

APPLICATION FOR REVIEW/APPROVAL
RESEARCH INVOLVING HUMAN SUBJECTS
(Word Version, FORM A)

TO: IRB, Regis University
Main Hall, Room 206, Mail Code H4

Date: __08/16/2010_____

Principal Investigator(s): ___Russell Moult_____

_55 Shamrock Loop_____

Address: **__Byhalia, MS 38611_____**

_____

Telephone: __662-838-3021_____ Email: moult879@regis.edu

Academic Department or School: __CPS - MSCIT_____

Faculty Advisor (student projects):_Bob Bowles_____

Project Title: Towards Establishing a Change Management Process at an Academic Research Laboratory Network_____

_____

_____

1. Are investigational drugs to be used?

Yes _____ No __X_____

2. Will you be using patients and/or facilities of a health care agency as a part of this study?

Yes _____ No ___X____

If **YES**, after approval by this Committee your proposal must also be approved by the appropriate review board within that facility.

Materials addressing numbers three through seven are to be either filled in under the questions or, if appropriate, attached.

3. Project description in relation to human subjects. Attach a brief summary of the problem to be investigated, the questions being asked, the methods or instruments to be used, the subject population to be studied, and the method of subject selection and recruitment. Include sufficient detail, including samples of protocols and/or data collection instruments, that the Committee can assess any potential hazards.

I propose to email a simple form questionnaire to SEAD practicum faculty/administrators (one or two individuals) to obtain their perspectives on change management processes within the ARNe and SEAD practicum portal. (A copy of the questions is attached).

I further propose to email a Likert-type survey to a limited group of SEAD practicum peers/users to obtain input on their perspectives related to change management processes within ARNe and the SEAD practicum. (A copy of the survey is attached).

4. Risk/Benefit assessment. Assess the risks and potential benefits of the investigation.

The risks associated with this investigation are low to non-existent. The questions and survey statements are designed to elicit valuable information concerning IT change management that will benefit the ARNe and SEAD practicum by initiating the development of a change management process. When implemented the process, based on industry best-practices and tailored for the specific environment, will improve operations by providing a method of requesting, approving, implementing and tracking changes to system resources.

5. Provision for informed consent. Provide details of informed consent procedures to be used, including samples of project descriptions to be given to subjects and consent forms to be used.

Informed consent will be obtained by having investigation participants sign off on the attached form.

6. Additional ethical considerations. Describe provisions for anonymity or confidentiality and any additional measures not previously addressed taken to protect the rights and safety of subjects.

I propose to have investigation participants complete the questionnaire or survey and email it back to my Regis.edu mail account. This investigation is limited to SEAD individuals directly involved in the systems practicum. The questionnaire for faculty/administrators is essentially a structured interview. The survey asks users to make a selection to each statement ranging from Totally Disagree – Totally Agree. Some very simple statistical analyses will be conducted on survey responses. Responses will not be tied to individual users, nor will individual users be identified in my report.

7. Research funding. If research is supported by grant, give source of funding.

Note: Research must be resubmitted for approval, if changes are made in the research plan that significantly alter the involvement of human subjects from that which is described by this application.

Signature of Principal Investigator: ____Russell J. Moult_____

(Note: if this document is being sent electronically, your typed signature will be considered as your signature)

Date _____08/16/2010_____

Signature of Faculty Advisor _____

Note: if this document is being sent electronically, the faculty advisor may send an email affirming his/her approval. This email should (1) indicate that the faculty advisor has read the application and (2) agrees with the information provided on the form.

Date _____

The space below this line is for the use of the Institutional Review Board.

Action of Institutional Review Board:

1. Exempt according to condition _____

2. Approved by expedited review _____
(reviewer, date)

3. Approved in general and specific details.

4. Approved in general with specific details to be resubmitted.

5. Disapproved for the following reasons:

Signature:

_____

Chair, Institutional Review Board Date

INFORMED CONSENT FORM FOR SURVEY PARTICIPANTS

RESEARCH PROJECT

Title of Research Project: Towards Establishing a Change Management Process at an Academic Research Laboratory Network

You are invited to participate in a study that is focusing on the research and development of a change management process for the ARNe and SEAD practicum. This study is being conducted to fulfill the requirements of a Thesis Project. The study is being conducted by Russell Moult, who can be reached at 662-838-3021 or e-mail moult879@regis.edu. This project is supervised by the student's Thesis Advisor, Bob Bowles, Regis University, 3333 Regis Boulevard, Denver, Colorado 80221-1099, rbowles@regis.edu.

Participation in this study should take about 10 – 15 minutes of your time. Participation will involve responding to 12 statements about change management processes.

Participation in this project is strictly voluntary. The risks associated with this project are minimal. If you experience discomfort you may discontinue the survey at any time. We respect your right to not answer any questions that may make you feel uncomfortable. Refusal to participate or withdrawal from participation will involve no penalty or loss of benefits to which you are otherwise entitled.

Your responses will be identified by numbered selection only and will be kept separate from information that could identify you. This is done to protect the confidentiality of your responses. Only the researcher will have access to your individual data and any reports generated as a result of this study will use only group averages and paraphrased wording. However, should any information contained in this study be the subject of a court order or lawful subpoena, Regis University might not be able to avoid compliance with the order or subpoena. Although no questions in this interview address it, we are required by law to tell you that if information is revealed concerning suicide, homicide, or child abuse and neglect, it is required by law that this be reported to the proper authorities.

If you have any concerns or complaints about how you were treated during the survey, please contact Mr. Bud May, the director of the Regis University Institutional Review Board at (303-458-4206).You may keep this page for your records. Please sign below if you understand and agree to the above. If you do not understand any part of the above statement, please ask the researcher any questions you have.

I have read and understood the foregoing descriptions of the study called Towards Establishing a Change Management Process at an Academic Research Laboratory Network. I have asked for and received a satisfactory explanation of any language that I did not fully understand. I agree to participate in this study, and I understand that I may withdraw my consent at any time. I have received a copy of this consent form.
Note: If this document is being sent electronically, your typed signature will be considered your signature.

Signature _____ Phone Number _____
Date _____