ITS a BeAR

Masters Project Report
ITS a BeAR

IT Security for
Berkeley Academic Resources

By:
Matthew W. Chew Spence
Bindiya Jadhwani
Lawan Likitpunpisit
Meghalim Sarma

MIMS, Class of 2008

Professor: Eric Kansa

Team Members

Matthew Chew Spence

Matthew Chew Spence, a second year masters student in the UC Berkeley School of Information, has over 10 years work experience as an on-site contractor at NASA Ames Research Center. He was recently recognized by NASA for his role in helping Ames become the first NASA center to reach 100% Federal Information Security Management Act (FISMA) compliance. Under the aegis of the Center IT Security Manager, he provided FISMA compliance guidance, including developing and reviewing IT security policy & procedures, leading risk assessments and reviews of existing controls, and developing control testing procedures for complex systems such as wind tunnels, supercomputers, materials test labs, and center IT infrastructure. He was the system architect for NASA's secure advanced collaborative environment, was on the Orbital Space Plan RFP review committee, and was a multidisciplinary engineer on the NASA Research and Education Network. He is currently a member of the NASA PKI team.

Bindiya Jadhwani

Bindiya Jadhwani is a second year Masters student at the School of Information. Her areas of focus include Needs and Usability Assessment, Project Management and Business Analysis. She has interned in the technology division of Goldman Sachs & Co in the project management space and performed market research and strategy planning for OKAPI, an Open Knowledge and Public Interest initiative on campus. As an undergraduate, she held the positions of Public Relations Officer and Vice Chairperson of her campus IEEE chapter, and served as a delegate in the UC Berkeley Graduate assembly.

Lawan Likitpunpisit

Ms. Lawan Likitpunpisit, a second year graduate student in the School of Information, has over 5 years work experience in the leading business and IT consulting firm. She has experience in business architecture blueprint and roadmap design, IT processes improvement, and IT system implementation projects for leading telecommunication industry leaders. She had also worked part-time as a system capacity planning analyst for eBay, where she had been awarded the eBay Summer Intern Award in recognition of her exceptional contribution to the team.

Meghalim Sarma

Meghalim Sarma is a second Masters student in the School of Information. She has over 5 years of work experience in the area of SOA and Business Process Management. During her 5 years of software career with Oracle Corporation, she was engaged with software development and beta program management for Oracle SOA suite products. Her core expertise includes XML data modeling, Web Services and business process modeling.

Table of Contents

Table of Figures

Table of Tables

1 Executive Summary

The free exchange of information is a key tenet of higher education. However sensitive information must be protected, as its compromise could cause harm to the university or to individuals. UC Berkeley experiences thousands of network attacks every second, and a single successful compromise can cost the university hundreds of thousands of dollars. In the last 5 years, several such incidents at Berkeley have received national press coverage, illustrating the need to improve IT security at UC Berkeley. But the decentralized nature of the university makes it difficult to ensure security awareness across campus, let alone ensuring effective security measures on those resources that contain sensitive information. The UC Berkeley office of the CIO has limited visibility into what information systems exist within the units on campus, and what measures are being taken to protect them.

Most IT resources on campus are managed by academic units or individuals. People may be unaware of all the security requirements for the systems they manage or use. Specific safeguards to protect sensitive information measures may be mandated by law, regulation, or policy. The mandates that apply in a particular situation may be determined by the context under which the data was initially collected as well as the inherent nature of the data itself. It is not easy for unit technical staff to find guidance. The specific requirements, known as controls, are spread across UC and campus policies. Different policies may use differing terminology for the same role or control. Within the policies, controls are described at a very high level, leaving the concrete steps up to the interpretation of the reader. There is no single source of requirements, recommended practices, or appropriate campus resources that can assist with compliance.

These issues are addressed by the ITS a BeAR security plan generator, which is a proof of concept web-based system that walks those responsible for an IT resource through discovering and documenting the security controls needed. It asks questions about the system and generates a security plan at the end. It generates of a list of appropriate controls based on their answers, helps users understand policy terminology, and gives guidance on how to implement controls. The generated security plan provides a concrete list of requirements that can be used by the unit to understand their security posture and justify security expenditures to decision makers. Similarly, it provides visibility to campus the CIO into the nature of the IT resource, identifies who fulfills key roles, and what security measures are in place or are planned.

The heart of ITS a BeAR system is a catalog of controls distilled from an analysis of key university-wide and campus policies. Each catalog item identifies the conditions that mandate it, and may include recommended practices and campus resources. The system decision logic uses the catalog to auto-generate the list of controls and create a security plan using our proposed standard format. The catalog, decision logic, and security plan template will be provided to the UC Berkeley office of the CIO so that future use of our methodology is not dependent on production implementation of our proof-of-concept.

2 Problem Statement

2.1 Problem Definition

Information is the lifeblood of a university. The emergence of a world-wide interconnected information biosphere known as the Internet has fundamentally changed the ways information is processed, managed, transmitted, stored, and access at academic institutions. University information systems are potentially accessible by over 20% of the population of the world that has access to the Internet.[1] Although the vast majority of Internet users do not engage in malicious activities, a network attack on university resources can originate from nearly anywhere in the world. UC Berkeley experiences thousands of network attacks every second.[2] And not all security incidents are network-based: the theft of a single laptop in 2005 cost the university hundreds of thousands of dollars. It is evident that there is a real and necessary need for effective IT security practices at UC Berkeley.

It is financially infeasible to protect every information system at the University from every possible attack. Determining which security measures to put in place for a given information resource should be based on the impact to the university and to those about whom information has been collected were the resource to be compromised. In addition, certain classes of sensitive information have legal or contractual requirements covering how to protect against or respond to data compromises. Mandates such the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), California's Security Breach Information Act, (SB1386), and the Payment Card Industry Data Security Standard (PCI DSS) impose IT security management requirements on organizations that store and process personal, financial, and other types of sensitive data. Institutions that are not in compliance may face the loss of funding or other penalties.

Selected mandates such as HIPAA, FISMA, and PCI specify security controls, some of which can be complex and expensive to put into place. Implementing common controls across multiple IT systems can result in significant cost savings due to economies of scale. But challenges arise when attempting to implement an IT security control regime intended for an operational environment with centralized management and funding upon a research institution comprised of autonomous organizational units with disparate funding sources and heterogeneous IT systems. At the University of California, these challenges include:

- The majority of information systems on campus are managed by academic units or by individuals and not by the office of the CIO (Chief Information Officer).
- A number of individual policies created by different university groups exist, but it is not clear what concrete steps should be taken to ensure compliance with them.
- Budgetary decision makers are not convinced that expending adequate resources on security provides sufficient ROI (Return On Investments) in current budgetary climate

[1] http://www.internetworldstats.com/stats.htm accessed May 3, 2008
[2] https://security.berkeley.edu/tutorial/

- Compliance at the departmental level among both faculty and staff is effectively voluntary due to lack of resources, incentives, and apparent consequences.
- Perception among some members of the campus community that IT security practices may interfere with research or threaten the freedom of academic discourse

Due to the decentralized nature of UC Berkeley, it is extremely difficult to promote awareness of IT security requirements, let alone compliance across the campus community. For example, campus policy requires that every system that contains sensitive data that could be used for identity theft be covered by a comprehensive security plan, yet no-one we met with within the CIO's office, the campus auditors office or departmental units had ever seen such a plan. Better compliance could be obtained through effective use of centralized campus IT resources. Absent the ability to inject IT security practices into mandatory campus processes, IT security proponents need to communicate clear benefits to campus units. Giving a clear understanding of the actions required for compliance would show the workload and associated costs campus units one could off-load by using IST (Information Services and Technology) resources. Were there a security plan template that described the actions that needed to be performed, the workload required for proper compliance would become obvious.

3 Project Background

Universities are decentralized by their nature. Modern universities are based on institutional forms that arose in the middle ages as scholars banded together to form scholarly guilds. One influential example is the University of Paris, whose structure evolved piecemeal over several centuries as the university faculty struggled with the Church and secular authorities over rights and entitlements. This resulted in a faculty dominated governance model, where the faculty chose the curriculum and degree requirements, chose the administration, approved new faculty members, and voted on the issues facing the university. As the university grew, internal groupings that would become schools and departments arose, often with severe disagreements between factions. Vicious and occasionally violent infighting within the university resulted in the evolution of intricate internal structures with strong internal walls separating highly autonomous groups, thereby protecting faculty from each other.[3] Features of these decentralized confederative internal structures included representative assemblies, bottom-up governance, and institutionalized forms of conflict resolution.[4] As a result, modern universities are highly decentralized organizations with organizational power rooted in the academic units rather than the university administration. University Of California, Berkeley is no exception.

3.1 The Researcher

As Western universities evolved, rights and cultural norms among scholars emerged that included the ability to move to the faculty of another institution, an ethos of free inquiry into academic subjects, and open discourse among members of an academic community.[5] In 19th Century Germany, the innovation arose of the discipline-specific professor who performs both instruction and research into a deeply specialized area of academic inquiry. This became the dominant model of the modern research university faculty member, whose research gains meaning when amalgamated with that of others investigating related questions within the larger discipline.[6] Thus participation within national and international scientific communities and organizations can be as or more important than the dictates of a home institution to a tenured professor. And in such professional societies, the prestige associated with well-received research is the coin of the realm.

3.2 Reward Structure for Researchers

In a university environment, faculty desire the autonomy to conduct their research programs, and dislikes encumbrances on that autonomy. IT security is a significant encumbrance as it requires faculties to deal with a great deal of procedures which are not

[3] *Darwinian Medicine for the University*, in Governing Academia p.74
[4] *Darwinian Medicine for the University*, in Governing Academia p.75
[5] *Darwinian Medicine for the University*, in Governing Academia p.75
[6] *Darwinian Medicine for the University*, in Governing Academia p.77

directly included in their reward structure. There is a clear lack of incentive for faculties and researchers to focus on security.

A well known framework in organizational behavior is as below:

Performance = Ability * Support * Effort[7]

Without the "support" of the university, the researcher will not be able to perform his security responsibilities in the maximum way possible. The equation articulates that even if the researcher has the adequate ability and is willing to work hard, without the appropriate motivation and reward structure, it is likely that his performance will be hindered.

A tenured researcher for instance is rewarded for the research he does, not the security measures he takes to protect his research data. His reward includes prestige and social capital of peers in specialized research communities, funding for research and sometime some prestige from affiliation in home department or even a place to perform funded research.

In the organizational behavior world, this will be considered as a case of rewarding "A" while hoping for "B". The university rewards researchers for doing research, but actually hopes that along with doing research, the researcher takes appropriate security measures.

Hence any supposed mandates from the university administration that do not directly affect the primary goal (research) or secondary goal (instruction) are below the radar of a tenured professor unless there are obvious ramifications for non-compliance (such as cases of gross misconduct).

We strongly feel that unless IT security is either embedded in mandatory processes relevant to faculty goals or is included as part of the reward structure directly in someway, researchers do not have enough incentive to perform tasks related to IT security, This combined with a systematic, standardized approach that makes it easier to comply will greatly increase compliance. Some funding organizations such as NASA are making compliance with US government standards, which introduces compliance into the reward system

3.3 Information Security in the University Context

For hundreds of years universities and research institutions were "ivory towers" and relatively isolated repositories of information. Although there was an ethos of free discourse and open information, dissemination of information was limited by the cost of reproduction, and access often involved traveling to the library achieves or scriptoriums that contained it.

[7] MBA209F – Fundamentals of Business class notes

The advent of the printing press allowed mass copying of information that was of interest to sufficient individuals to justify printing costs. It was not economical to reproduce items that only appealed to small niche groups, unless those groups had sufficient financial resources to privately fund printing. Individuals who owned information could to some extent still chose what was reproduced, and could limit access to "sensitive information" and raw research data by physically isolating it in locked cabinets or secured archives. With the ubiquitous use of personal computers connected to the global Internet, the information handling procedures that were historically used to protect sensitive information are no longer sufficient to do so. The emergence of the Internet and powerful search engines has effectively ended the era of "security through obscurity.

The modern Internet has its origins in exclusively academic research networks that linked universities and research institutions. For nearly twenty years access to these networks was generally not available to the general public and only available to select commercial entities. The underlying networking protocols were initially designed for use on research test bed– security was not a design criterion. As result key limitations and vulnerabilities exist in commonly used protocols. But the issues are not limited to communications protocols. Most modern operating systems are written using languages that do not prevent memory buffer overflows and are not type-safe. The majority of OS and application attacks exploit type casting errors and buffer overflows in installed programs.

Due to the inherent flaws in protocols, applications, and operating systems, new vulnerabilities are being discovered nearly every day.[8] There is an arms-race with one side being the attackers who find and exploit these vulnerabilities and the other being a combination of the vendors who release security patches and the system administrators who need to install them. This is why being up to date on installed patches and anti-virus software is critical. Equally important is proper configuration of a system. Effective authentication should be used, unnecessary services should be disabled, and host-based firewalls should be enabled. If these procedures are not performed, all the data within the system is at risk of being compromised or corrupted. If the information within a system is essential to the operation of an organization, additional security measures or controls should be put in place. Staff with access to the information and the system should undergo background checks. Critical information should be backed up to a location off site, and disaster recovery planning should be performed. Measures to protect the integrity of the information should be employed.

Equally important are the controls that should be put in place to protect confidential and privacy data. If a system containing information of this nature is compromised, the university can be subject to legal and financial penalties. Furthermore, the people whose information is compromised can find suffer significant negative consequences, among the most damaging being identity theft. Thus it is important that those who implement, manage, use, and are financially responsible for an information system need to be aware of their responsibilities under law and university policy.

[8] http://www.us-cert.gov/nav/t01/

3.4 Data Breaches

3.4.1 Overview of Identity Theft

Between 2003 and 2005, each year approximately nine million people, or 4% of the adult population of the United States fell victim to identity theft.[9] Identity theft is when someone makes use of the personally identifying information of another person without that person' knowledge in order to engage in fraud or other criminal activity. [10] Such activity can target the person whose identity has been stolen, can defraud financial institutions, or be used to obtain products and services fraudulently from businesses, organizations or government entities. Victims may not know that their identity has been stolen until they are notified by financial institutions of suspicious account activity.[11] The average identity theft victim will spend from 40 to 330 hours and $420 to $850 addressing the aftermath of an identity theft incident.[12] 85% of the incidents studied by the CA Office of Privacy Protection involved Social Security numbers. It can take thousands of dollars and hundreds of dollars to recover from identity theft resulting from the compromise of a social security number.[13] Information policy should provide disincentives to the collection of Social Security numbers unless they are absolutely necessary.[14]

One must keep in mind that not all identity thefts are the result of misuse of computerized information. Many identity thieves obtain sensitive personal information via stolen mail, lost or stolen wallets, or social engineering, such as claiming to be a system administrator to get a user to give their password .[15] And when electronic sources are compromised, often only a small percentage of disclosed identities are subject to identity theft. In the 2004 ChoicePoint incident, a notorious data breach that inspired many states to enact breach legislation, there were approximately 800 known incidents of identity theft resulting from the exposure of over 160,000 compromised records[16]. However, if one

---

[9] "Recommended Practices on Notice of Security Breach Involving Personal Information," *California Department of Consumer Affairs, Office of Privacy Protection,* (February 2006), http://privacyprotection.ca.gov/recommendations/secbreach.pdf (accessed April 26, 2007) at 5

[10] "About Identity Theft," *Federal Trade Commission,* (no date), http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (accessed May 2, 2007)

[11] David B. Reddick, "Security Breach Notification Laws: What Threats Do They Pose for Insurers?" National Association of Mutual Insurance Companies (July 2005), http://www.namic.org/insbriefs/050707SecurityBreach.pdf (accessed April 26, 2007) at 2

[12] Recommended Practices, supra note 2, at 5

[13] Id. at 6

[14] *Identity Theft: Innovative Solutions for an Evolving Problem: Hearings before the Senate Judiciary Committee Subcommittee on Terrorism, Technology and Homeland Security*, 110th Cong., 1d Sess. (2007) (testimony of Chris Jay Hoofnagle), http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6198 (accessed April 30, 2007) at 7

[15] Reddick, supra note 4, at 2

[16] Ragib Hasan and William Yurcik, "Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work," *National Center for Supercomputing Applications (NCSA), University of Illinois at Urbana-Champaign,* http://wesii.econinfosec.org/draft.php?paper_id=37 (accessed April 26, 2007), at 2

extrapolates this percentage to the 154.5 million records exposed between Jan 2005 and April 2007, one arrives at over 750,000 incidents.[17]

3.5 Data breaches at UC Berkeley

In the years immediately after the California state legislature passed SB1386, which mandated notification to individuals whose private data may have been compromised, UC Berkeley experienced several data breaches that required breach notification. All of these incidents resulted in significant cost to the university, as well as damage to the reputation of UC Berkeley as the incidents were publicized in the national media. We discuss the past data breaches at UC Berkeley because they illustrates the state of IT security at the time, the costs to the institution, and the potential damages to individuals.

3.5.1 Bancroft Library

In 2003, a hacker compromised a database at the Bancroft Library containing personal information of 17,000 visitors from around the world. There was no way to know whether the data was accessed, as there was no password system on the database. As a result of the incident, the stopped recording driver's license numbers[18]

This incident illustrates issues involved with:

- Risk of collecting sensitive data that isn't necessary
- Need for authentication and authorization
- Need for sufficient audit records to determine extent of compromise

3.5.2 2004 Visiting Researcher's Database

In August 2004, a hacker may have gained access to 1.4 million records containing social security numbers, birthdates, addresses and names of 600,000 participants in a California state in-home care program when they broke into a computer at UC Berkeley being used by a visiting researcher.[19] The hacker exploited a known vulnerability in commercial software for which a patch was available at the time but had not been installed.[20] The visiting researcher stated that to the best of her knowledge she had followed university policy.[21]

This incident illustrates the issues involved with:

- Not anonymizing or encrypting sensitive research data.

---

[17] "A Chronology of Data Breaches," *Privacy Rights Clearinghouse*, http://www.privacyrights.org/ar/ChronDataBreaches.htm (accessed May 3, 2007)
[18] http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/11/23/BUG5D37C7T1.DTL
[19] Poulsen, K., ''California Reports Massive DataBreach,'' SecurityFocus News, http://www.securityfocus.com/, October 19, 2004, http://www.securityfocus.com/news/9758
[20] http://www.eweek.com/c/a/Database/Hack-at-UC-Berkeley-Potentially-Nets-14-Million-SSNs/
[21] http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/10/23/BAGOL9EUFN1.DTL

- Proper awareness of IT security policies and best practices
- Need for timely installation of patches

3.5.3 2005 Stolen Graduate Division Laptop

On March 11, 2005, a laptop computer that contained social security numbers, addresses, birthdates of nearly 100,000 graduate students, applicants, and others was stolen from an unlocked office in the graduate division at UC Berkeley.[22] The laptop was later recovered, but there was no way of telling whether the sensitive information was ever accessed. Because the data had not been encrypted and there was not audit trail, the University had to notify the affected individuals as per SB1386. Some estimates place the cost of notification at hundreds of thousands of dollars, not including the cost of subsequently retaining PricewaterhouseCoopers to audit the way the school handles sensitive material.[23]

This incident illustrates the issues involved with:

- Why laptops with sensitive data should be encrypted.
- The importance of physical security
- The monetary costs of non-compliance

3.6 PricewaterhouseCoopers Report

Due to the highly publicized data breaches described above, in late April 2005 UC Berkeley engaged PricewarehouseCoopers (PWC) to conduct an audit of campus security practices. The resultant confidential report "UC Berkeley: Data Privacy & Security Review"[24] issued on July 19, 2005, describes the state of data privacy security and key challenges at the UC Berkeley campus. This report provides a baseline against which the current state of data privacy protection at UC Berkeley can be measured.

Some of its recommendations include:

- A data protection awareness and training program is required: This includes the need for training program(s) for system administrators and technical personnel across the campus.
- The information security architecture reference model should be defined: The model should provide the common baseline for the implementation of a consistent information security common infrastructure.
- Develop and communicate technology specific data protection standards: With no data protection standards, the security controls are implemented in an inconsistent manner. This increases the likelihood that the sensitivity data may be compromised.
- Incorporate data protection into systems development lifecycle (SDLC)

---

[22] http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/03/29/BAG3MBVSFH1.DTL
[23] http://www.pcworld.com/article/id,122576-page,1/article.html
[24] UC Berkeley: Data Privacy & Security Review, PricewaterhouseCoopers LLP, July 19, 2005.

- Establish a data (security) risk management program, especially on Personally Identifiable Information (PII) and restricted data.

3.6.1 UC Berkeley Response to the PricewaterhouseCoopers Analysis

A concerted effort has been made by UC Berkeley's office of the CIO to address the issues identified by PWC, and implement the recommendations to the extent permitted by available resources. Significant policy revision activities have been undertaken and the Restricted Data Management (RDM) system has been created to track restricted data on campus. However the decentralized federated nature of the University of California severely complicates the process.

An organization's supposed priorities are expressed in written policy, whereas actual organizational priorities are shown in allocation of resources.[25] Presently IT security efforts at UC Berkeley are funded out of temporary funding i.e. there is no permanent source of annual funding. There is insufficient funding for security infrastructure and services that would significantly reduce the risk to the university. There is no funding for security awareness and outreach.

Although the office of the CIO is aware of the situation and is working on remedying it, the reality of the state budget crisis is that even if a permanent source is found, sufficient additional investment to address key PWC recommendations will not be forthcoming, resulting in a "penny-wise, pound-foolish" situation.

3.7 Regulatory Regime

The regulatory regime covering information handling at a major research university such as UC Berkeley is varied and complex.

3.7.1 Laws and Regulations

Laws and regulations involving information in the United States are primarily sectoral, meaning that the mandates that apply in a particular situation are determined by the context the data was initially collected rather than any inherent nature of the data itself. The same sequence of bits collected for financial aid purposes will have a different set of conditions applied to it if it is collected as part of a research study. There are a number of regulatory regimes that may apply to sensitive information within the university environment. These include:

Family Educational Rights and Privacy Act (FERPA)

[25] "How Academic Ships Actually Navigate", in *Governing Academia* p. 165

FERPA governs the disclosure of student educational records and access to those records. Student records that contain personally identifiable information cannot be disclosed to third parties without the prior approval of the student. Student records are defined broadly. As instruction is a key business of UC Berkeley, FERPA applies to a majority of the units on campus, and could potentially apply to nearly every professor and graduate student instructor on campus. FERPA does not mandate specific information handling practices or security controls.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to protected health information collected by health care providers, health plans, and healthcare clearinghouses. These "covered entities" must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information.

At Berkeley, HIPAA directly applies to work functions performed within the following campus units: Human Resources, Intercollegiate Athletics, Optometry Clinic, Psychology Clinic, and University Health Services. Researchers who obtain protected health information from a "covered entity" are required to comply with HIPAA privacy and security regulations.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions, including certain functions of educational institutions. GLBA mandates that financial institutions have a comprehensive written information security program with administrative, technical, and physical safeguards. It requires that financial institution security programs do risk assessments, control risks, and both apply employee sanctions and disclose when breaches occur.[26]

Security Breach Information Act, (SB1386)

The first data breach in the United States notification law was passed in California in 2003. Commonly known as SB1386, it came about in the aftermath of a hacker breach of the state payroll database in April 2002. The breach was not discovered for more than a month, and state employees were not notified until two weeks after that.[27] The resultant outcry from state employees led to the passage of the California Civil Code Sections 1798.29 & 1798.82. It is a sunshine law, based on the concept that awareness of an incident allows a person whose information has been compromised sufficient knowledge to take actions to mitigate the risks resultant from the unauthorized disclosure. It also makes use of the concept that entities, aware of the damage to their reputation caused by disclosure of a data breach, will take steps to improve their institutional data security.

---

[26] Schwartz & Janger, supra note 12, at 7
[27] Reddick, supra note 4, at 2

The California law is solely a notification mechanism, and it doesn't require that agencies or business engage in any security practices, although it does provide an exemption from notification if the disclosed information is encrypted. Additionally, it doesn't mandate breach disclosure to any entity other than the affected consumer. It does not require notifying law enforcement or credit reporting agencies.[28] The California law does not impose any fines on entities that violate the notification law, but individuals injured by such violation can bring a civil action against violators to recover damages.[29]

Data breach reporting mandated by SB1836 has resulted in significant monetary and reputational damage to UC Berkeley. (See above)

3.7.2 Policies

Laws are interpreted by the university administration, which issues policies that describe how members of the university community are supposed to comply with the regulatory regime. The intent here is to have a common interpretation of legal requirements and to shield members of the campus community from having to interpret numerous Federal and state legislation. There are multiple levels of policy that apply to activities at UC Berkeley. At the top level there are University system-wide policies issued by the UC office of the president. These apply to all UC campus. Then there are campus-wide policies, which are issued by the administrative unit, council, body, or entity responsible for the activity covered by the policy. Finally, there may be policies that apply within a department or campus unit.

3.7.2.1 System wide Policies

IS-2 Inventory, Classification, and Release of University Electronic Information

IS-2 is a University of California system-wide policy that establishes guidelines on the classification of university information assets and describes obligations related to disclosure of various classes of electronic information. The detail description of IS-2 can be found at http://www.ucop.edu/ucophome/policies/bfb/is2.pdf.

IS-3 Electronic Information Security

The purpose of IS-3 is to establish guidelines for achieving appropriate protection of University electronic information resources and to identify roles and responsibilities. It provides mandates for risk assessment, workforce controls, operational & technical controls, and physical & environmental controls that should be applied to information systems owned or maintained by the university community. The detail description of IS-3 can be found at

---

[28] Paul M. Schwartz & Edward J. Janger, "Notification of Data Security Breaches", *available at:* http://ssrn.com/abstract=908709 at 19
[29] Reddick, supra note 4, at 3

http://www.ucop.edu/ucophome/policies/bfb/is3.pdf.

3.7.2.2 UC Berkeley Campus Policies

Campus policies are intended to describe how an individual campus will implement university-wide policy requirements. Local policy at UC Berkeley is very fragmented, with different committees and organizations within the campus having policy-making authority. Policies can be issued by administrative units, academic bodies, committees composed of combinations of faculty, staff, and students, or proclamation by senior campus officials. Although often based on interpretations of system-wide policies, there can be a lag between when a system-wide policy is updated and changes filter down to campus policies.

Data Management, Use, and Protection (DMUP) Policy

The "Data Management, Use, and Protection" (DMUP) Policy is a UC Berkeley campus policy that defines roles such as data proprietors, data custodians, data integrators, data users, and delineates the responsibilities of each. It also defines key concepts such as System of Record, Essential System (more descriptions available in a later section), and provides high-level policy requirements. It is maintained by the UC Berkeley Data Stewardship Council.

Minimum Standards for Security of Berkeley Campus Networked Devices

The minimum standards for the security of Berkeley Campus Networked Devices describe the minimal security controls that must be applied to any computer that connects to the UC Berkeley campus network. Computers are verified to have these in place before they are allowed to attach to the network. The standards can be found at https://security.berkeley.edu/MinStds/AppA.min.htm

4 Framework Analysis

This section describes different frameworks that we analyzed for the use in the context of IT security plan project. It includes NIST, and OCTAVE framework.

4.1 NIST Framework

The National Institute of Standards and Technology is the source of standards that govern a wide variety of activities. With the passage of the Federal Information Security Management Act (FISMA), the NIST Special Publication 800 series of standards has become mandatory for Federal information systems, and de facto best practices for private industry. Several of the UC system wide policies have been revised to be compliant to NIST standards. Although the FISMA framework is extensive enough that as currently mandated it can be burdensome in an academic environment, adoption of key aspects provides a standards-based approach to security management. Key relevant NIST documents include:

SP 800-18 Guide for Developing Security Plans for Federal Information Systems[30]

This document describes what sort of information should be included in a security plan. We used this document as the basis for our security plan template, customizing it to fit the UC policy landscape.

SP 800-27 Engineering Principles for Information Technology Security31

NIST compiled a set of security engineering principles to assist with the design of information systems. These principles provide the foundation for a consistent and structured approach to the design, development, and implementation of IT security capabilities .

SP 800-30 Risk Management Guide for Information Technology Systems

This document describes the NIST risk assessment methodology, which includes identifying threats and vulnerabilities of an information resource, a simple quantitative method for determining the likelihood and impact were a particular vulnerability to be exercised, and a way of assigning a value to risk.

SP 800-53 Recommended Security Controls for Federal Information Systems32

This publication provides a catalog and taxonomy of security controls. Although 800-53 also provides for minimum baselines, these baselines are intended for US government systems and should be considered advisory: only the subset of these controls that are required

[30] http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
[31] http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
[32] http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

by UC policy should be mandated for campus systems. We mapped individual UC controls to their SP 800-53 equivalent.

SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems

Currently in final public draft, SP 800-53A establishes common methods and procedures to assess the effectiveness of the security controls described in SP 800-53.

4.1.1 The use of the framework in the project

Mapping UC policies to NIST FISMA requirements provides value by allowing the campus to make use of procedures and tools developed to meet government requirements. It provides a common vocabulary and methodologies to design, implement, and assess security controls. As certain government agencies such as the Veterans Administration and NASA are mandating FISMA compliance for contracts and research grants, there is value in mapping UC requirements to this framework. However, we recommend a subtractive approach to the use of NIST FISMA, only implementing those aspects that are relevant or feasible within a large academic institution.

4.2 Risk Assessment Guideline/Octave Allegro Framework

4.2.1 OCTAVE Allegro Overview

The OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation – Allegro method provides the standard framework to perform an organization's information security risk assessment. It focuses primarily on information assets in the context of how they are used, stored, and transported, and processed. In addition, it aims at how information assets are exposed to threats, vulnerabilities, and disruption. The framework provides the best-practices-guidelines, worksheets, and questionnaires to conduct risk assessment. Figure 1 illustrates the OCTAVE framework. The framework takes into consideration not only the IT security technology perspective, but also IT security practices and its operational risk to the organization.

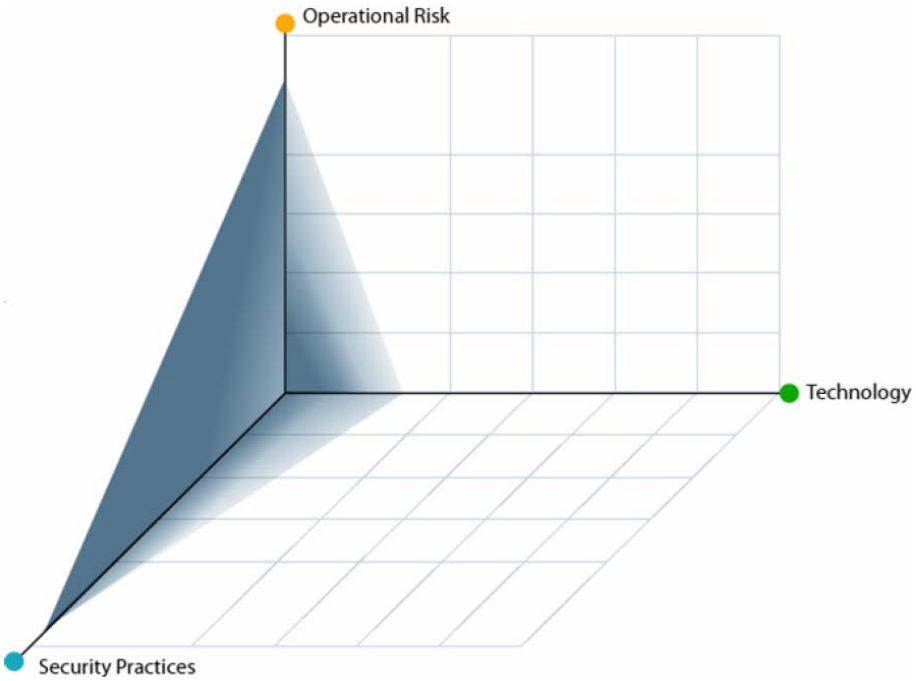

Figure 1: OCTAVE Framework Conceptual View

Based on the same OCTAVE framework's three phases as shown in Figure 2, the OCTAVE Allegro framework simplifies the process to have four phases with eight steps as illustrated in Figure 3.

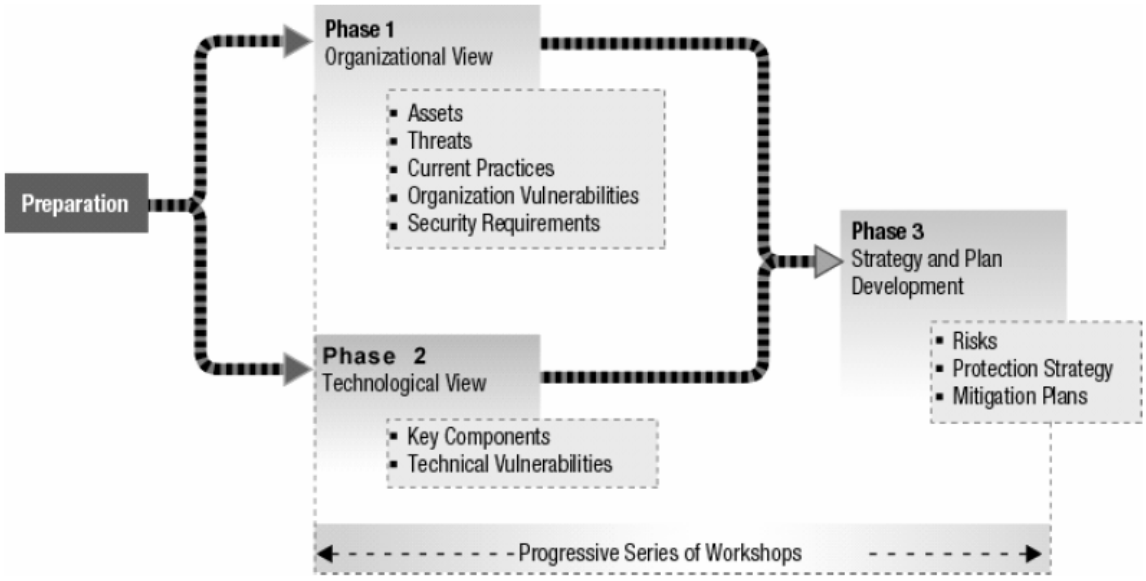

Figure 2: Three OCTAVE Method Phases

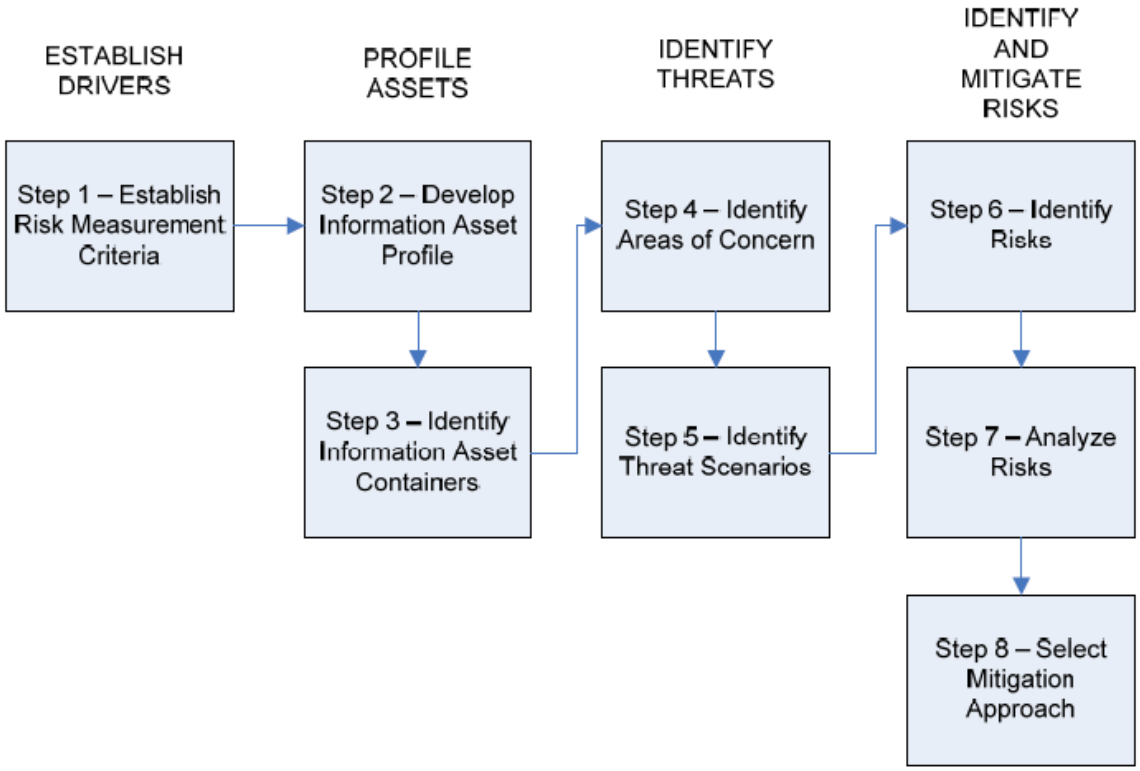

Figure 3: OCTAVE Allegro Roadmap

4.2.2 OCTAVE Allegro Benefits

- Identifies information security risks that could prevent an organization from achieving organization's strategic mission.
- Enables the management of information security risk assessments.
- Creates a protection strategy designed to reduce the organization's highest priority information security risks.
- Prepares the organization for compliance with data security requirements or regulations.

4.2.3 Findings and the use of the framework in the project

The project team studied and analyzed the use of the OCTAVE framework in the university information security context. However, in order to implement this framework, the IT assets should be built/captured in place. This step requires a work-shop based approach which requires resource commitment and very time consuming. Given the time constraints of our project and the urgency of IST needs, the team decided not to use this framework.

Going forward, the project team recommends the use of this framework. It can be the reference guideline to perform campus and unit level information security risk assessments regularly, i.e. once a year. The assessment should focus on its information assets, vulnerabilities, and risk mitigation plan in the context of aligning them with its organization's operational and strategic goals. Using this framework together with IST risk-based assessment will help IST to better prioritize its information security risks, and thus plan its resources (including staff and budgets) accordingly to mitigate those risks. Moreover based on the discussion with the IT policy department, IST is now in the process of developing the risk-based assessment model to enhance its IT security controls/requirements guideline.

5 Security Requirements

5.1 Security as Risk Tradeoff

It is not possible to protect absolutely against every potential IT security threat. If an attacker is sufficiently skilled, heavily motivated, and has significant resources at their disposal, they will probably find a way to exploit information system vulnerabilities of even the most secure system. And trying to protect against every eventuality can be extremely expensive. . So a tradeoff needs to be done between the cost of protection and the risks of non-protection. In an environment of limited resources, one needs to determine the most cost effective place to apply resources. In the works of Daniel Greer, "what you want is a 'minimax' solution - the maximum good for the minimum evil."[33] Security is about effective risk mitigation: understanding what risks are acceptable and investing sufficient resources to mitigate the majority of the most common and most dangerous vulnerabilities. Recent university policies require a risk-based analysis and that is why efforts have been made to develop electronic data classification based on risks.

5.2 Risk to Person Vs Risk to Organization

5.2.1 Definition

Risk to organization: is the risk to the university in terms of reputation, source of funding, and the compliance to law and regulations.

Risk to person: is defined as any risk related to each individual whose data was kept in the system, and could be impacted in the case that their information is compromised.

5.2.2 The Shift from "Risk to Organization" to "Risk to Person" Focus

Previously, the university focused on the risk to the organization. This was shown in the original IS-2 and IS-3 definition of the data classification; restricted or unrestricted, essential, required, or deferrable, data of record or unofficial data (refer to the following section for the detail definition). However, since identity theft has become a big concern lately (See the previous section of "data breaches"), the latest version of the IS-2 policy defined the new data classification to focus more on the risk to the individual person: confidentiality, integrity, and availability. Going forward, the DMUP together with Boalt School of Law's IT security department are working on defining the set of criteria to identify the three levels impact for each data classification: low, medium, and high.

[33] http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=478

5.3 Data Classification

This section describes the important data classification as defined by the campus' Data Management, Use, and Protection (DMUP) policy. Note that for the official source of data type definition; please refer to DMUP's official website (http://dataintegration.vcbf.berkeley.edu/DMUP.htm). Figure 4, illustrates how the data classification is derived by several federal and state laws, and university's policies.

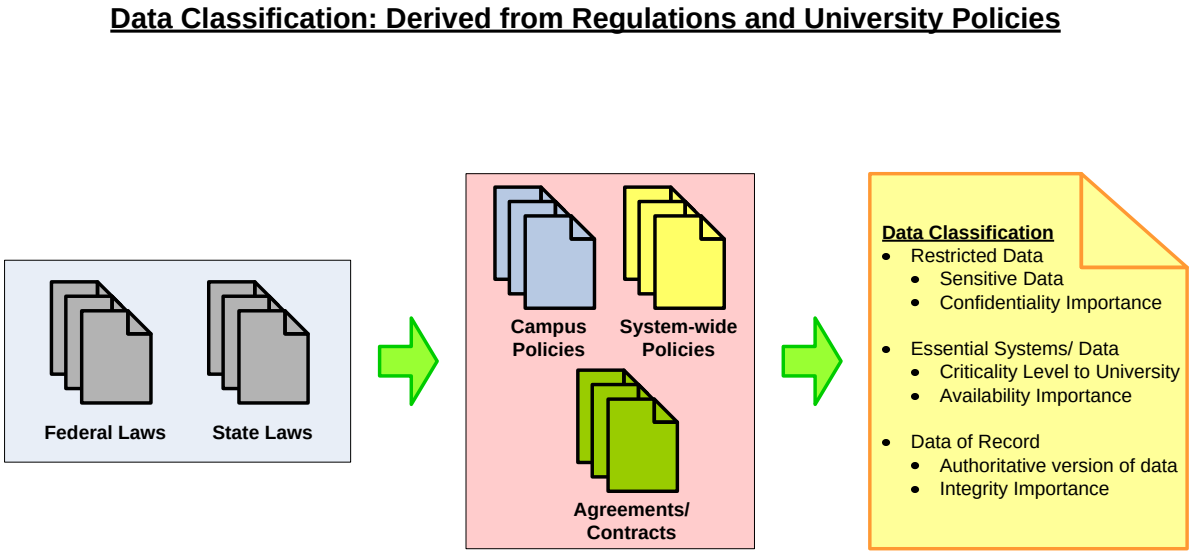

Figure 4: Data Classification – Derived from Regulations and University Policies

5.3.1 Existing Data Classification

The policy classifies the "Campus Data" into the following classifications:

- Restricted or Unrestricted
  - Restricted data is defined as the data that identifies or describes an individual and data to which unauthorized access, modification, or loss could seriously or adversely affect UC Berkeley, its partners, or the public. Examples of restricted data include
    - Social security number
    - Employee home address, date of birth, Financial information such as credit card number or bank account number
    - Student grades and financial aid records, etc.
  - Unrestricted Data is defined as the data to which access or modification is not restricted by federal or state law or University or campus policy and to which access is permitted by the Data Proprietor.
- Essential, Required, or Deferrable

- Essential data is defined as the data resource whose failure to function correctly and on schedule could result in either a major failure to perform critical business functions, a significant loss of funds, or a significant liability or legal exposure.
- Required data is defined as the data resource that performs an important function, but the operation of the campus could continue for some designated period of time without it.
- Deferrable data resource is defined as the data resource that the campus could operate without; it need not be performed correctly or on schedule and would not affect mission-critical business functions.

- Data of Record and Unofficial data
  - Data of record is defined as a certain data type to which data users must reconcile when producing official or external to the department reports. Data of record normally resides within a System of Record, which may or may not be the place in which the data originated. Data of Record should be modified only with the consent of the Data Proprietor and only within the System of Record where the data officially resides. Data of record is required to be accurate, timely and needs to be maintained,
  - Unofficial data is defined as all campus data that *are not* data of record. Unofficial data typically resides in data warehouses, locally administered data systems, or workgroup level applications that have been created to administer additional data not found in Systems of Record or data of record. Unofficial data should never be distributed as data of record

The purpose of these classifications is to determine what sets of security controls need to be put in place to protect an information resource and the information within. Both campus and system-wide policies require that certain controls be put in place for each classification. The classifications are inclusive rather than exclusive: that is an information system can be essential, contain restricted data, and be a system of record.

Note: Refer to *Appendix A – Data Classification Definition* for the detail definition of each data classification.

5.3.2 Electronic Information Classification and Risk Assessment

Recent revisions to IS-2 and IS-3 establish risk-based criteria for determining the security measures, or controls that should be used to protect an information resource. The IS-2 policy defined information security as the practice to achieve three main objectives: confidentiality, integrity, and availability. The failure to meet each of the information security objectives could effect in university operations, and reputation. Thus, IS-2 and IS-3 have defined the three possible impact levels criteria – low, medium, and high – for electronic information classification and risk assessment.

IS-2's information security objectives:

- Confidentiality: Preserving authorized restrictions on access and disclosure including means for protecting personal privacy and proprietary information.

- Integrity: guarding against improper information modification or destruction and may include ensuring accuracy and authenticity.

- Availability: ensuring timely and reliable access to and use of information.

Impact levels criteria definition for electronic information classification and risk assessment

- **Low:** The event could be expected to have a limited adverse effect or negative outcome to the University, or result in limited damage to University operations or assets, requiring minor corrective actions or repairs.
- **Medium:** The event could be expected to have a significant adverse effect on the University or cause a significant degradation in its mission capability, place the University at a significant disadvantage, or result in limited damage to University assets, or reputation requiring extensive corrective actions or repairs.
- **High:** The event could be expected to have a severe or catastrophic effect on University operations, assets, or individual and could be expected to cause a loss to mission capability for a period that pose threat to human life, results in a loss of major assets, or would result in severe financial **important** impact to the reputation of the University.

Note that for the detail description of information security objectives please refer to *Appendix B – Risk-based assessment Data Classification Definition.*

6 Security Program

6.1 Security Controls

As defined by National Institute of Standards and Technology (NIST), Security controls are management, operational and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information.[34] Controls can be implemented at various levels within the organization. For example, some controls might be implemented for an individual system, while some others might be implemented at a unit, sub-unit or even campus-wide level

There are a set of controls which are mandated by the campus policies known as "Minimum Security Standards". They apply to for each system and device that needs to be connected to the campus network. For example, Access control measures, Host-based Firewall, Patch Management etc. are considered as minimum security controls. If a system does not comply with any of these minimum security standards, the system is not allowed to connect to the campus network.

Different Controls can be mandated for different data categories. Previously, there were just two broad data categories – Restricted and Essential – and appropriate controls were applied based on which of these two buckets the data fell into.

Recently, efforts have been made to move to a risk-based model. Even through the risk assessment procedure has not been identified or standardized yet, the appropriate controls for different levels of Confidentiality, Integrity and Availability are identified and documented. The controls roll up as the level Confidentiality, Integrity and Availability increases. For example, a system with a high level of Confidentiality should also implement the controls for the "medium" confidentiality level and so forth.

Controls can be also mandated based of platform types, i.e. – based on whether a system is a Database Server, Web Server or a portable device, it might have to implement different security controls specific to each platform category.

Controls implementation and maintenance responsibility might belong to various roles based on the information sensitivity and the scope of the system as well as the scope of the control itself. For example – the "Security Awareness and Training" control must be performed by Administrative officials.

[34] NIST Recommended Security Controls for Federal information systems
http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

6.2 Data Stewardship Roles

Data Management, Use, and Protection (DMUP) Policy, a University Of California, Berkeley campus policy strives to broadly educate campus on their specific responsibilities for data resources under their control by articulating data stewardship roles and the practices necessary to achieve the campus' goal. An individual may perform any or all of the roles depending on their relationship to a specific data resource. However, there are lot of policies within the campus, with differing terminologies and definitions for these roles. For example, the DMUP role "Data Custodian" is called as "Provider" in a separate campus policy even though both are essentially the same.

To overcome the issue of name conflicts and to make sure that role definitions cover all the responsibilities mentioned in various policies, Jeremy Lapidus, Principal IT Auditor, Audit & Advisory Service on campus has created consolidated definitions for each of these roles. Through the use of these consolidated roles, we can map requirements across policies, determine who is responsible for what tasks, and ease some of the confusion created by terminology mismatches.

Consolidated definitions for the various data stewardship roles:

6.2.1 Data proprietor

The person or group that is responsible for determining how an information system and its data are to be used and who has access to these resources, such as the Office of Human Resources with regard to HRMS, or the Office of the Registrar with regard to various student information systems.

6.2.2 Data custodian

The person or group that physically or logically controls an information system, such as a central IT unit or a system administrator.

6.2.3 Administrative Official

The person with administrative and/or financial management responsibility, such as a control unit head, dean, department chair, principal investigator, director, or manager.

6.2.4 Information System Security Officer

Information System Security Officer is a designated official responsible for the security program of the campus. He/she is responsible for facilitating the compliance with the IS3 bulletin through collaborative relationships with academia and administrative officials.

6.2.5 Data user

Berkeley employees, students, or other individuals affiliated with UC Berkeley granted authorization to access or create campus data and who invoke or access data for the purpose of performing their job duties or other functions directly related to their affiliation with UC Berkeley.

6.3 Security Plan

Multiple regulations and policies mandate that all systems containing sensitive information should be under a comprehensive, written security plan that captures the details about the measures taken to protect the system and the information residing within. The security plan should describe cost-effective strategies that or will be implemented for mitigating potential security vulnerabilities. The security plan should account for the management, use, and protection of information that has some level of confidentiality, and identify the procedures and controls that will be implemented to enhance security for information assets. Ideally, an inventory should be maintained for these security plans and periodic reviews/audits should be conducted to assess the appropriateness of the security measures taken at individual and department levels. Although multiple policy documents call for the creation of security plans for systems that contain sensitive data, there does not appear to be guidance as to the specific elements that a security plan should contain, let alone a template that could be used by someone needing to compose a security plan.

6.4 Existing Tools and Services

The University of California, Berkeley campus offers different tools and services to help departments and individuals meet security standards, while attempting to establish an overall secure information technology environment. Most of these tools and services are offered by the Information and Services Technology (IST) division. If these tools can be mapped to controls and requirements in a central control catalog, those individuals needing to protect systems can easily discover their existence.

6.4.1 Existing Tools

Restricted Data Management System (RDM)

RDM is a free service offered by IS&T which is used by the campus to inform System and Network Security (SNS) about systems throughout the University that collect or use restricted data. RDM was designed with an aim to keep an inventory of hosts which hold sensitive information and these hosts are tracked by their IP addresses.

As a part of the RDM registration process, users are required to fill out a set of forms through which they let the system know about the different restricted data they have in their system and their machine IP addresses. Based on the information provided, SNS tries to prioritize the machine according to their sensitivity levels and schedule periodic automated scanning. Apart from scanning, systems registered in RDM also benefit from automated monitoring, enhanced vulnerability detection services and rapid IDS alert response.

Restricted Data Identification and Registry (RDIR)

The Restricted Data Identification & Registry (RDIR) was an iSchool final year project completed in 2005. It was envisioned to assist developing a more active communication channel between campus database, application administrators and restricted data policy experts.

RDIR was intended to be used by campus policy experts to describe the legislation or policies that affect UC Berkeley systems, such as SB1386, HIPAA and FERPA. After policy experts had described these rules, RDIR used those to create a questionnaire/wizard through which system administrators and/or application managers on campus could identify their systems' sensitive data and register those systems. RDIR tried to take the decision making of policies away from system administrators and also aimed to categorize UC Berkeley's restricted data by system.

The RDIR project completed with a proof-of-concept web application and, it did not include many of the necessary elements for a production system. Even through its categorizing aspect is covered by the RDM application, the campus can greatly benefit from having a system for policy experts to describe and encode policies.

6.4.2 Existing Services

Outsourcing of system administrator for small departments

For many departments that cannot afford to have an individual IT division or do not need extensive IT infrastructure, IST has been serving all their IT needs (such as servers, databases, and networking) as the system administrator.

Intrusion Detection

IST provides intrusion detection services at the campus border to detect several types of malicious behavior that can compromise the security of the computer system. If the Intrusion Detection discovers any potential threats, the security contacts at different departments are contacted for corrective action

Audit for Policy Compliance

IST also conducts periodic audits at different levels to gauge the level of policy compliance. These audits are generally done by picking up random IP addresses and assessing the measures taken to protect restricted data on that system.

7 Needs and Requirement Gathering Process

Our team performed an intensive needs analysis for this project. We began our needs gathering process in November 2007 and the process continued till March 2008. This process included numerous meetings with different units on the UC Berkeley campus. Navigating the university bureaucracy was an interesting process, and we learned a lot about how things function in the academic landscape. During this process, our team brainstormed several approaches and directions since every meeting changed our perspective about the IT security issues on campus. The silo based architecture of the university made our process challenging, but an interesting and knowledgeable one nevertheless. Below is a short description of all the people/units whom our team spoke to during to gather requirements for our project.

7.1 IST IT Policy Team

7.1.1 Overview of Organization

Our project sponsors, Bill Allison and Karen Eft from UC Berkeley's Information Services and Technology division were an integral part of our requirements gathering process. They helped us understand how the university functioned, and explained the political as well as organizational layout of the campus.

Bill Allison, Senior Manager in IST is a technical expert. He runs the Web Applications unit that has over 60 projects in development and 100 applications in the production system. He is also active on the campus information security governing committee. He helped us immensely to understand what could be implemented practically, with existing systems in mind. He shared a previous PricewaterhouseCooper UCB security assessment with our team for reference and he was the one pointed us to important contacts such as Karen Eft, Jeremy Lapidus and the RDM team.

Karen Eft, IT Policy Manager analyzes emerging information technology policy issues for UC Berkeley. She proposes policy positions to take and procedures to implement; publicizes IT policies and related issues; and advises campus departments and staff on correct handling of sensitive and precedent-setting situations. Recently she led the effort to produce the campus IT Security Policy, as well as leading discussions to clarify the campus' positions with respect to data privacy and issues. She helped us understand the IT policy landscape on campus.

7.1.2 Discussion Topic

We discussed several issues and some of them included:

- Investigating whether it makes sense to implement selected controls at the campus, department, laboratory, or individual system level.
- How to implement identified controls in a cost-effective light weight manner that is in compliance with the spirit and the letter of the regulation.
- Mechanisms and methodologies for minimizing duplicative information collection and maximizing effective re-use of information collected as part of the compliance process.

7.1.3 Findings

- Compliance is effectively unenforceable on campus since department technical staffs are already overloaded and may not have cycles or incentive to ensure compliance. Professors may see security requirements as interference with their researches. Policies are sent by university to unit heads: the extent to which they trickle down to staff and professors is unknown. Unfortunately there are no apparent consequences for willful violation of security policies.
- The CIO wants economy of scale through effective use of centralized resources and security controls where politically feasible.
- Privacy is the biggest driver for security for several reasons. These include high public visibility when privacy breaches happen and the high cost of breach reporting/notification which is borne by individual departments. Privacy security has a clear economic ROI, fits within the academic ethos of Berkeley and is the current area of academic and political discourse.

We met with both Bill and Karen on a frequent basis. In the initial phase, they were the ones who suggested that we work with privacy since it was a priority for IST at this time. They pointed us to people we needed to meet, which was extremely helpful, and something that we would have been unable to do on our own. We kept them informed about any significant findings and progress made throughout. Every time we needed to make a critical decision, we met with them to get feedback. We presented all options we were considering, and paid a lot of attention to their inputs and suggestions.

In the later stages of our project we also met with Jeremy Lapidus, Principal IT Auditor, Audit & Advisory Service on campus. IST conducts periodic audits at different levels to gauge the level of policy compliance. These audits are generally done by picking up random IP addresses and assessing the measures taken to protect restricted data on that machine Jeremy explained his needs and how he could potentially use our system for audit purposes. After speaking to him, we consolidated roles into our list of controls since it would help him in the audit process. Our team's effort in fact inspired him to create a similar database he could use for auditing. We spent time trying to integrate his list with ours, and he mentioned that he would use our system for auditing purposes once the integration was complete

7.2 Chris Hoofnagle (Samuelson Clinic)

7.2.1 Overview of Organization

The IST team suggested that our project should provide some level of academic credibility for security. This was seen as necessary to get buy in from the campus academic community, We approached the Samuelson Clinic and and intended on getting guidance from Chris Hoofnagle, senior staff attorney to the Samuelson Law, Technology & Public Policy Clinic and senior fellow with the Berkeley Center for Law & Technology. His focus is consumer privacy law.

7.2.2 Discussion Topic

Chris explained the privacy landscape and the laws applicable to our team. He discussed how multiple federal and state laws may apply to the campus, also mentioning that Cal may need to be in compliance with the Gramm-Leach-Bliley Act (Financial Aid office, credit union) along with HIPAA, FERPA and other laws.

7.2.3 Findings

He explained that there were two levels of consideration, compliance and other policy decisions (i.e. to protect students). He mentioned that in the US, privacy law is sectoral i.e. privacy requirements depend upon the context under which data is collected.

He mentioned that there is currently no central inventory of mandates which apply to different types of data. He also exposed us to what other what other universities were doing in this space and gave us a privacy audit template which was very valuable.

7.3 Restricted Data Management (RDM)

7.3.1 Overview of Organization

We meet with the RDM team since they were involved with data privacy and security on campus. RDM is a free service offered by IST that is used by the campus to inform System and Network Security (SNS) about systems throughout the University that collect or use restricted data. RDM was designed with an aim to keep an inventory of hosts that hold sensitive information and these hosts are tracked by their IP addresses. The RDM system is in existence for last two years and it was built in-house at the UC Berkeley. Recently the code has been shared with UCSB, UCLA and few other branches of University of California are also considering the use of this system.

7.3.2 Discussion Topic

We met with Karl Grose, Allison Henry and Vahid Nadi from the RDM team within IST-Infrastructure Services. They showed us how the system works, running through the whole process. As a part of the RDM registration process, users are required to fill out a set of forms through which they let the RDM know about the different restricted data they have in their system and their machine IP addresses. Based on the information provided, SNS tries to prioritize the machine according to their sensitivity levels and schedule periodic automated scanning. Apart from scanning, systems registered in RDM also benefit from automated monitoring, enhanced vulnerability detection services and rapid IDS alert responses. While there is no strict enforcement for registering systems into RDM, initiatives have been undertaken at different levels to publicize the importance of this service.

7.3.3 Findings

The RDM team gave us access to the QA site of RDM along with providing us the data schema so that we could understand the system better. Before we met with the RDM team, our project was heading in the direction of doing something similar to what RDM does ie. a way to categorize sensitive data. We wanted to understand what constitutes restricted data, and when we saw the RDM system, we realized that this functionality already existed on campus.

We decided to change tracks, and fill in the missing pieces. We realized that the RDM system asked security questions but didn't save it or generate any security plan which could be valuable and is in fact required for all systems having restricted data. Hence in a way we were inspired by the RDM team and built additional functionality on top of their system.

7.4 System and Network Security (SNS)

7.4.1 Overview of Organization

We met with Kate Riley from IST-ASD who is involved with application scanning on campus.

7.4.2 Discussion Topic

She gave us a better idea of security controls available at the campus level.

7.4.3 Findings

We learnt that the security infrastructure and IT management at the network level is very solid at UC Berkeley. By using the information registered in the Restricted Data Management System (RDM), the System and Network Security (SNS) team identifies the

systems to be scanned by the type of data stored in users' system and its IP addresses. The team is mainly responsible for routinely scanning the campus network for threats and vulnerabilities and notifying security contacts so that corrective action can be taken before vulnerabilities are exploited Proactive scanning is done regularly across the network. Current reporting from vulnerability scans is sub-optimal due to difficulties in mapping systems to responsible parties

Another thing we learned was that IST provides intrusion detection service at the campus border to detect several types of malicious behaviors that can compromise the security and trust of the computer system. If the Intrusion Detection discovers any potential threats, the security contacts at different departments are contacted for corrective action.

7.5 Identity Management Team

7.5.1 Overview of Organization

As part of our needs analysis for data privacy on campus, we met with Dedra Chamberlin, Security Applications Manager within IST-Infrastructure Services.

7.5.2 Discussion Topic

She gave us an insight about the various identity management resources available centrally on the campus

7.5.3 Findings

We discussed the CalNet Authentication Web Server (AWS) service, which is the common authentication and directory service provided by IST for all UC Berkeley's on-line web applications to verify their users' credentials. Currently, the system uses Kerberos technology for its authentication service, and LDAP technology for its directory service[6].

Dedra discussed how IST is in the process of migrating "CalNet AWS service" to the new platform called "CalNet Central Authentication Service (CAS)". Unlike the CalNet AWS, the new system will also provide the single sign-on functionality[7.] She also provided us with system architectures of which were very valuable to understand the domain better.

7.6 Kevin Heard (School of Information)

7.6.1 Overview of Organization

Kevin Heard is the Director of Computing & Information Services for the School of Information. He is responsible for overseeing the design, implementation, management, and support of the departmental information resources of the School of Information. Due to the

nature of the school, several of these resources are used by students and faculty to develop software and websites for academic projects.

7.6.2 Discussion Topic

We met with Kevin to obtain an understanding of the perspective of a data custodian, his understanding of required security controls, desired services available from the campus, and perceptions about compliance with campus security policy.

7.6.3 Findings

Although Kevin and his staff are quite technically adept and follow industry best practices, they were somewhat frustrated with the complexity of the campus security planning process. Because the requirements are so opaque, they have made the decision to ban restricted data from departmental systems. A desire was expressed for guidance on how to meet requirements, with checklist or procedures to direct efforts. Kevin would like to be able request additional campus services, such as additional scanning reports, intrusion detection at the point where the department connects to the campus network, guidelines for performing an internal IT audit, and to be able to request external audits.

7.7 Campus Information Security and Privacy Committee (CISPC)

7.7.1 Overview of Organization

The Campus Information Security and Privacy Committee (CISPC) is a standing committee providing oversight and prioritization of UC Berkeley campus information security and privacy-related policies, procedures and initiatives. The Committee recommends strategic direction on campus information security and privacy-related work to ensure that it supports the University mission, improves the overall security posture of the University, and is appropriately supported, funded and implemented within the campus community.

7.7.2 Discussion Topic

Our team was fortunate to get the opportunity to attend a CISPC meeting The Committee is charged with broad oversight of the campus information security operations (System and Network Security group) and advises SNS on budget and project priorities. The Committee reviews requests for exception to campus security policies and determines whether and with what constraints exceptions will be granted. CISPC also functions as an advisory group for the Deputy CIO Technology Council on matters of information security and privacy. [35]

[35] https://security.berkeley.edu/cispc/charter.html

7.7.3 Findings

During the CISPC meeting, we saw a campus policy decisions in action, and better understood campus priorities around security and privacy

It was at this meeting we met with Michael Greens, Infrastructure Applications Manager, IST-Infrastructure Services and Ryan Means from the Law School who helped us further in our project in consequent meetings.

7.8 Ryan Means (Boalt School of Law)

7.8.1 Overview of Organization

We met Ryan Means, Chief Technical Officer at University of California, Berkeley - School of Law after the CISPC meeting since he was involved in compiling controls for different data sensitivity levels. Ryan is a reputable figure in the security space on campus and is known for developing and executing innovative policies and procedures.

7.8.2 Discussion Topic

We discussed the Electronic Information Classification and Impact Analysis (EICIA) draft policy, which he had developed. It incorporates the concept of specific controls being invoked based on risk levels related to confidentiality, integrity, and availability. Although these controls are not extracted directly from any policy, Ryan is in the process of getting these signed of by the Data Stewardship Council on campus.

7.8.3 Findings

We got the permission to use his controls list, and our system is partly based on his compilation of controls being invoked according to certain risk levels. We met with him a few times to show him how we had integrated his controls in our data schema and he gave us valuable feedback, at the same time appreciating and validating our work.

7.9 Committee for the Protection of Human Subjects (CPHS)

7.9.1 Overview of Organization

Within the University of California, all proposed research involving interactions with or identifiable private information about living individuals must be approved by the Committee for the Protection of Human Subjects (CPHS). Researchers who do not comply with CPHS are not allowed to perform research.

A researcher wanting to perform human subjects research submits a document set that describes the research protocol they propose to use. Among other things, this protocol describes the purpose of the research, the subject population, the study procedures, and the risks & benefits of the research. In section 11 of the current UC Berkeley "CPHS Protocol Narrative Form", the researcher is required to "explain how subject privacy will be protected and how confidentiality of subject information will be maintained." The protocol should include a "detailed plan for data security." There appears to be minimal guidance beyond reference to various campus, UC, & federal policy documents

7.9.2 Discussion Topic

We met with Jonathan Banda, Senior Administrative Analyst at the Office for the Protection of Human Subjects, and he described the whole CPHS process to our team. Part of the submitted protocol describes the steps the researcher will take to secure personally identifiable privacy data collected as part of the proposed study. . In the current protocol system, this information is provided in narrative form using paper documents. IS&T is implementing "eProtocol," an electronic version of the process, for CPHS.

7.9.3 Findings

After detailed analysis of the CPHS process, our team concluded that it would be useful for the researcher to get some guidance before they fill out the CPHS protocol about whether they have restricted data, and if yes, do they truly need this data, since several different laws have many rules and regulations around restricted data. Depending on what kind of data types the researcher has, recommendations should be made about how this data should be protected based on the laws which apply. We were considering building a decision logic which would guide the researcher even before he/she starts the CPHS protocol, and hence add a lot of value to the process. A researcher cannot publish research based on studies that are not approved by CPHS. Thus the CPHS process is directly integrated into the reward structure of researchers studying humans, and could get us buy in for our system.

We also analyzed that since this process is mandatory, it should tie in with the Restricted Data Management (RDM) service offered on the campus by IST. Since all PII is restricted, it should ideally be part of the RDM, and hence be offered greater security services.

Our project sponsors, Karen and Bill supported our decision, and thought this step would be valuable at the campus level. We met with the Director of OPHS, Rebecca Armstrong to discuss this. Unfortunately things did not work out as planned and we had to completely change directions due to resistance we were offered from OPHS upper management. Part of this may have been because they were in the midst of porting the paper-based CPHS protocol to an electronic system, and may have been concerned about introducing changes into a process that was already behind schedule. Part of it may have been because management did not see the value to them of integrating their collection of

privacy protection information with resources managed by other campus units. And lastly, there was a stated distaste to being the subject of an academic inquiry, even if it may have benefits to their organization.

8 Needs/Requirements Analysis

8.1 Key Findings

Several key issues emerged from our interviews with members of the campus community.

8.1.1 Lack of Visibility of the Overall IT Systems

The first was the lack of visibility at the campus security, privacy, and policy (SPP) department into what systems existed within campus units; let alone what security measures were being put into place. SPP is required to periodically report to the Berkeley and UC-wide administration on the status of IT security compliance on campus. Without accurate information, it is difficult for upper management to understand the true state of compliance, or justify expending resources on IT security.

8.1.2 No IT Security Control Guidance

The second, related issue was that for those charged with maintaining unit information systems; it was difficult to find guidance on what security controls were required, as mandates were spread across multiple UC-wide and campus policies. Finding out which controls were applicable to a system involved reviewing a number of policies. Different policies use different terminology for the same role or control, and sometimes the multiple policies that govern a given situation may be out of sync with what is required.

8.1.3 Detail Recommended Procedures are not Available

Third, the policies often describe controls at a very high level, leaving the concrete steps that should be put into place up to the interpretation of the reader. Recommendations for individual security best practices are available at various campus websites, but there is no overall list of recommended practices, nor of centralized campus resources that can be used to fulfill specific requirements.

8.1.4 Lack of Understanding of the Overall IT Security Requirement

Fourth, even though many unit technical staffs are aware of good security practices, the unit heads, researchers, and other decision makers internal to a campus unit may not understand the extent of security controls mandated by policy or law. Without a list of mandated requirements, a member of the technical staff may not be easily able to explain why certain technology or procedures need to be put in place to protect a unit resource.

Similarly, without being able to reference explicit restrictions, a member of the technical staff may be reluctant to refuse an insistent request to bypass a control or procedure from someone higher in the unit hierarchy.

8.1.5 No Security Plan Template

Fifth, even though multiple policies mandate the development of comprehensive security plans that describe the controls used to protect sensitive data and resources, there was no template or form that a unit could use to create a security plan. In fact, the Campus IT Policy Manager, The CTO of the Law School, the Director of Computing and Information Services for the School of Information, nor the primary campus IT auditor had ever seen a completed security plan. There have been several attempts to create a security plan template for the university in the past, but as of the time of writing, none of them have been successful. The controls that need to be put in place for a particular system depend on the sensitivity of the data and nature of the information resource, so a single security plan template that covers all possible requirements would be confusing and overwhelming.

8.2 AS-IS Security Plan Report Generation Process

The existing system security plan process is ad hoc, and to the best of the knowledge of the people we interviewed as part of our needs analysis, had never been successfully completed, with the possible exception of those campus units whose funding organizations required one as a condition of contracts or grants. Privacy protection procedures are documented in narrative text by researchers submitting human subject, these are not comprehensive, there is limited guidance on campus requirements, and the information within the documents is not shared outside of CHPS.

8.2.1 Existing security plan requirements on Campus

The university, IS-3:III.D.4.b, requires that an acceptable level of data security protection must be established for systems processing “personal information”.

> *[IS-3:III.D.4.b]*
>
> *Campuses shall establish a process or processes to identify where “personal information,” as defined above, is used and stored, the primary employee positions that have access to and use of the data, the Resource Proprietor and Custodian of the data, and an acceptable level of security protection for the data. Where is personal information defined in our report?*

The information related to the security plan is solicited in different campus resources as followed.

- **Security Plan as a part of the CPHS process:** Section 11 of the CPHS protocol requirement states that the research entity must submit its data security plan to the

CPHS committee. The objective is ensure that personal identity of any subjects involved in the research is confidential and protected appropriately. If the researchers fail to address this issue, the protocol will not be approved and thus, they cannot continue their research. Refer to CPHS' policy on the Security of Research Subjects' Personally Identifiable Data Held by Researchers[36]

- **Security Plan as a part of Restricted Data Management (RDM) system:** RDM is a free UC Berkeley service provided by IST. It scans for the vulnerability of registered systems. Any system which contains restricted data as defined by IS-2 policy should register themselves in the RDM system or establish their own data security procedures to ensure that the confidentiality, integrity, and availability of the system is maintained.

8.2.2 Existing Security Plan Generation Process

There is no formal guidance on how to create a security plan. Although a security plan is required in many processes within the university information security context (i.e. the CPHS process and the RDM system, as mentioned above), there are no formal guidelines on how to create a security plan. Each entity is responsible to come up with its own standard and guideline for data protection. The approval process is carried out on a case-by-case basis with different standards used by different organizations. Moreover, they could be different than the one used by the campus policy audit process.

8.2.3 How does this create problems?

The lack of common process and guidance to create a security plan creates the following problems.

- **Unnecessary additional effort to create and submit security plan**: The information of the security plan in kept within each organization. There is no information flow between the OPHS department, RDM system, and the IST policy auditor. This adds unnecessary additional effort for the research entity, since the plan has to be submitted at least twice: once to CPHS committee, and again to the RDM system.

- **Inconsistency of security plans**: The security plan submitted to the CPHS committee might not be in-sync with what has been submitted and registered in the RDM system. In addition, it might not actually be implemented by the research entity.

- **No common references for what is the minimum requirement to satisfy the campus' standard of data security requirement**. As mentioned in the previous subsection, the approval criteria vary from department to department, including the auditing process.

[36] (http://cphs.berkeley.edu/content/datasecurity.htm).

- **No common references between university information security policy and the government/industry information security standard**. This leads to the lack of the overall understanding of the importance of how the university policy addresses/apply industry's standard/best practices. Moreover, it leads to the lack of visibility to the management level and thus impacts the level of support and funding to improve the university information security initiatives.

8.3 Improving the Security Plan Creation Process

A standardized campus security plan template would address several of the issues described above. By giving a comprehensive list of the requirements for a system, it removes the need for a unit or researcher to review all the requisite policies in order to determine what they need to put in place. A well-designed security plan template that is part of an automated system could provide senior management visibility into the current state of IT resources on campus.

Such an automated system could use conditional logic to ensure that only the controls that are relevant to the data sensitivity of a given system appear on the security plan template.

8.3.1 PWC Report Drivers for our Project

One of the primary documents for our project is the confidential PWC audit report "UC Berkeley: Data Privacy & Security Review" issued on July 19, 2005. This report describes the state of data privacy security and key challenges at UC Berkeley campus in the aftermath of several highly publicized breaches. No other documents of this nature are known to be publically available. This report provides a baseline against which the current state of data privacy protection at UC Berkeley can be measured. Several of the PWC recommendations were instrumental in our decision to investigate the security plan process at UC Berkeley:

PWC Recommendation #3: Define an Information Security Architecture that allows for the implementation of security policy

> *"Each information owner is expected to do their own research and determine a [security] solution that will work within their environment. While this approach provides flexibility, groups often don't have the time or technical proficiency to perform this assessment effectively"*[37]

PWC Recommendation #7: Develop a policy compliance and enforcement program

[37] PricewaterhouseCoopers Report, page 27

"The program should provide easy access to policies and standards….An exception process should be developed for unique instances of non-compliance."[38]

PWC Recommendation #8: Establish a regulatory compliance program

"Establish an initiative to develop strategies for automating compliance requirements across the campus."[39]

8.4 Cataloging Requirements

The first step to build a system that applies conditional logic to determine which set of controls that are pertinent to a particular system is to create a catalog of controls that includes the conditions to which it applies. To do this, we first had to decompose the various policies into individual controls, each with a set of attributes that described the controls, the source of the requirement, the criteria that invoked the control, and information sources and suggested implementations of the controls. This was an iterative process whereby we would extract all the controls from a particular policy document, and then we would consolidate controls that appeared in multiple policies.

In the course of our interviews, we became aware of additional policies and tools that were under development by members of the campus community. As practicable, we incorporated both the contents and additional control-attribute-types into our analysis. The most important of these tools were the Electronic Information Classification and Impact Analysis (EICIA) draft policy, being developed by Ryan Means, and the IT Risk Management database, being developed by Jeremy Lapidus. From the EICIA we incorporated the concept of specific controls being invoked based on risk levels related to confidentiality, integrity, and availability. From the IT Risk management database we adopted the concept of controls being tied to roles, and made use of Jeremy's consolidated role definitions, which rationalized the different names for specific roles used by different policies. We also extracted a number of controls from each system.

As various policies had different terminology and names for the controls, we decided to map each control to the National Institute of Standards and Technology (NIST) security control taxonomy as described in NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems.

We chose to do this for several reasons:

- Having a standard taxonomy makes reconciling controls across policies easier
- NIST SP 800-53 provides a stable catalog and taxonomy for specifying security controls
- Future assessment of controls can use standards-based methods

[38] See above, page 30
[39] See above, page 33

- NIST is developing a set of methods and criteria for assessing the efficacy of SP 800-53 controls for use in the federal government
- SP800-53 doesn't mandate the use of a particular vendor technology

8.5 Building a Control Catalog

For each control, we captured the attributes listed in Table 1 below. The attributes fell into three categories:

- *Control Details*
  These attributes describe the control itself, such as the name, source(s), control description, NIST SP800-53 mappings, and role(s) responsible for implementation.

- *Recommendations and Resources*
  These attributes provide those responsible for implementing control information about tools or procedures to implement the control, if there are relevant centralized available and informational resources about the control.

- Criteria that invoke the control
  These attributes serve as the heart of the decision logic. They describe whether the control is invoked when the information resource matches risk-based control classifications, university defined classifications, externally mandated classifications, or platform specific control requirements.

Table 1: List of attributes extracted from campus policy for each control

Control Details	
CR No.	Unique Control ID (determined by our team).
Name	Name of Control.
Control Requirement Detail	Detailed description of control requirements.
Requirement Source(s)	Policies and sections from which control is derived.
Role	The role(s) that that perform the control. These are: o Data Proprietor o Data Custodian o Security Officer o Administrative Official o Data Users
Waivable?	Can the control be waived, and if so, the waiver process.
Periodic Review?	Is periodic review of control required?
Family	Logical grouping of controls into a family. Primarily based on NIST SP 800-53 references.
(NIST SP800-53)	Identifiers and names of applicable NIST SP 800-53 controls.
Recommendations, IST Services, and Information Resources	
Potential Remedy	Potential mechanisms, procedures, or tools that can be used to meet the control requirements.
Relevant IST Services	IT Services provided by IS&T or other campus units that can be used to meet control requirements.
Information Resources	One or more URLs that describe the control requirements.
Criteria that invoke control	
Confidentiality	Impact of a loss of confidentiality. Rated on a scale of high, moderate, or low for EICIA controls.
Integrity	Impact of a loss of integrity. Rated on a scale of high, moderate, or low for EICIA controls.
Availability	Impact of a loss of availability. Rated on a scale of high, moderate, or low for EICIA controls.
Internal Data Class	Relevant data classes that are defined by university policy. These include Restricted, Essential.
External Data Class	Data classes defined by sources outside the university. These are generally legislative mandates such as HIPAA, FERPA, GLBA, SB1386, etc.
Platform	Platform specific controls for things such as portable systems, web servers, database servers, etc. Currently system lifecycle phases such as “systems under development” are in this column-it may make sense to create a separate SDLC column.

9 ITS a BeAR System – The Security Plan Generator

We see the lack of security plan template as a key issue preventing this requirement from being met. As part of our project, we have developed a proposed template based in large part on NIST standards, but modified to fit the requirements of the university. We also created a proof-of-concept system that walks users through a sequence of 5 steps, asks them a set of questions about their system, and then auto-generates security plan for users' system. Some of the key details that go into a security plan are the information about the system, details of each contact person, information sensitivity levels as well as the information about the scope and platform of the system. Purpose of the system, user categories and the approximated no of users in each category, system environment i.e. the hardware, software, IP address, physical location are some of the other important pieces of information that should be captured in the security plan. If a system shares information with any other system, then the name and owner of the system with which information is being shared should be captured. Finally, and most importantly, the security plan should capture implementation strategies for each of the controls that are applicable to the system. Please see Appendix G for our proposed template.

9.1 Overview of the System

The proof-of-concept that we implemented, is a web-based application which guides the user through the process of security plan generation. It captures all the key details that should go into a security plan. A point to note is that our system is based on the assumption that the user is aware of the data sensitivity levels. Based on the responses from the user, the system executes complex decision logic for extracting the appropriate controls for that particular system. User is then required to fill-in implementation details for each control and guidance is provided as how to implement those. Once all implementation details are entered, the user submits the form and the final security plan is generated, saved and can be printed for future reference.

Currently the decision logic of our system is based solely on the data sensitivity levels, but can be extended on other criteria's in the future. Since the system implementation and data model is xml based, the system can be extended without much effort.

9.1.1 Design Consideration

While designing the system, we had to make some important design decisions. One of the key decisions was whether to use XML or Database as a repository for the controls.

The "ITS A BeAR" is a system which we envision to get finally integrated with campus systems like RDM rather than existing as an independent system. Also, there is a high probability that this system might exchange data with other campus systems like the CPHS information system. XML being the de-facto standard for data sharing, using XML

makes our system more flexible to share information. Extensibility is another key reason why XML makes a better alternative over databases.

The data structure for the controls is very flat and simple. We don't need any advanced database functionalities like referential integrities as most of the data could be just saved in one or maximum two tables. Thus using a database would have introduced needless complexities in the system. Usage of database will slow down the system and also the network calls will be expensive.

XML is a very popular and widely supported technology. There is also lots of open-source IDEs that support editing of XML files. If we use databases, then we need specific UI or scripts to add, modify or delete controls. However, since XML files are just text, we could just use text editors to create/modify our control repository.

Finally, ease-of-use and expertise was another reason why we decided to use XML. Our group members have high expertise in XML and related technologies like XSD and XSL which made XML a better alternative for our system.

9.1.2 Project management approach: Waterfall Model

Our project followed the Waterfall project management approach, which is linear and sequential. Waterfall development has distinct goals for each phase of development.

The advantage of waterfall model is that it allows for departmentalization and managerial control. A schedule can be set with deadlines for each stage of development and a product can proceed through the development process smoothly and theoretically, be delivered on time. Development moves from concept, through design, implementation, testing, installation, troubleshooting, and ends up at operation and maintenance. Each phase of development proceeds in strict order, without any overlapping or iterative steps.

The disadvantage of waterfall model is that it does not allow for much reflection or revision. Once an application is in the testing stage, it is very difficult to go back and change something that was not well-thought out in the concept stage. Alternatives to the waterfall model include joint application development (JAD), rapid application development (RAD), synch and stabilize, build and fix, and the spiral model.

Despite known disadvantages, Waterfall model appeared to be well-suited for our project given the time and resource constraints that we had. Since we were working within UC Berkeley's organizational context, where more continuous development and testing were not feasible, Waterfall methodology was a better choice as it did not require continuous commitment from all the stakeholders.

9.2 TO-BE Process of Security Plan

Following personas and scenarios can help better understand the use of the Security Plan Generator. The characters represented by the personas are fictitious and they are being used as more of a communication tool for the purpose of explanation. The personas along with the respective scenarios clearly depicts the problems that the security plan generator is trying to solve and also at the same time it gives a sense of the target audience for this system.

9.2.1 Persona 1 – Larry Wu

Larry Wu is the director of computing and information services of the anthropology department at UC Berkeley. His responsibilities include maintaining security of the all the departmental level systems. He is in charge of implementation, management and technical support of all systems in the anthropology department.

Larry often feels that there is a lack of resources for security compliance and wishes there was an easy description of what needs to be done. He is the only person responsible for overall security in the anthropology department and his responsibilities leave him overburdened on many days. The faculty members in the anthropology department often want administrator rights to their system, and Larry finds it challenging to explain their exact responsibilities to them. He wishes that there was some kind of framework or checklist that would point him to security best practices and make his work less complicated.

9.2.2 Scenario 1

Larry got a phone call from his friend Thomas, CTO in the physics department. Thomas told him about a new service provided by the campus to generate security plan in a quick and efficient manner. Thomas mentioned that the system generated a list of controls based on the information you enter, and ensured that you are in compliance with campus policy. “Great! This is what I needed!” thought Larry as he hung up the phone with Thomas. He quickly logged on to the “ITS a BeAR” system and started filling in the information. He was responsible for all the department level systems including the servers of the anthropology department, and entered information about each system he was responsible for. After about forty minutes, he was glad to see that the system returns a list of controls. He entered details on how he was planning to implement the controls, and voila!...his security plan was generated and saved in a centralized database.

9.2.3 Persona 2 – Mark Deely

Mark Deely is a senior researcher at the anthropology department at UC Berkeley. His area of research is Social Cultural Anthropology. He studies European and Latin American ethnography. His research projects include peasant society and culture, demographic anthropology, folklore, the life course, symbolism, ritual and religion, food and drink of people in these cultures. While abroad, he lives and works in both rural and urban

settings and his work is grounded in direct observations of a given people and reflects a sensitivity to regional, ethnic, class, and gender diversity. Inevitably, he collects personally identifiable data, which is restricted and needs to be protected. He stores all this data on his personal laptop. He often thinks of having a security plan, but is not very fluent with the policies and laws that apply. He has some kind of a security plan and puts certain controls like encryption in place, but really is not sure of whether these satisfy policy and laws.

He wishes there was some guidance about how to write a security plan, and implementation of controls that need to be in place.

9.2.4 Scenario 2

Mark heard about the "ITS a BeAR" system from Larry, the chief technical officer of the anthropology department. He was told that this was any easy way to generate a security plan for the sensitive data he had stored on his laptop, along with understanding which controls need to be in place according to policy.

Mark clicks on the link that his CTO provided in his email and starts using the IT'S a BeAR system. He enters the information he is asked for, often times asking the system for definitions if he isn't sure of the terms that are used. He finds the system is easy to use and doesn't take him more than twenty minutes to submit the information solicited. On submission, the system returns a set of 50 controls which he needs to implement in order to be in compliance with policy. He finds this extremely useful since now he doesn't need to interpret the policy on his own and be afraid of making mistakes.

He enters how he will implement each of the controls he needs to. He is not sure of how to implement one of the controls and clicks on the option "Don't know how to implement" for that particular control. He submits the form and is happy to see that his security plan is generated, along with guidance on how to implement the control he was not sure how to implement. He is thrilled to see how convenient this procedure was. He sips his coffee, smiles and prints his security plan.

9.3 System Design

9.3.1 Technologies Used

To implement the "ITS a BeAR" system, we employed a combination of XML, XSL, PHP, JavaScript, HTML and CSS technologies. We used XML to store the list of controls and the security plans created by users. XSD has been used to create and describe the data model for the controls. PHP delivered our server-side scripting, interacting with our backend XML-based control repositories to display dynamic content to our user interface. JavaScript was used to improve the usability of our. Lastly, CSS was used to style our interface, giving it a completely customized and consistent look and feel.

9.3.2 High-Level User Interaction

The following diagram depicts the user interactions with the ITS a BeAR system at a very high-level.

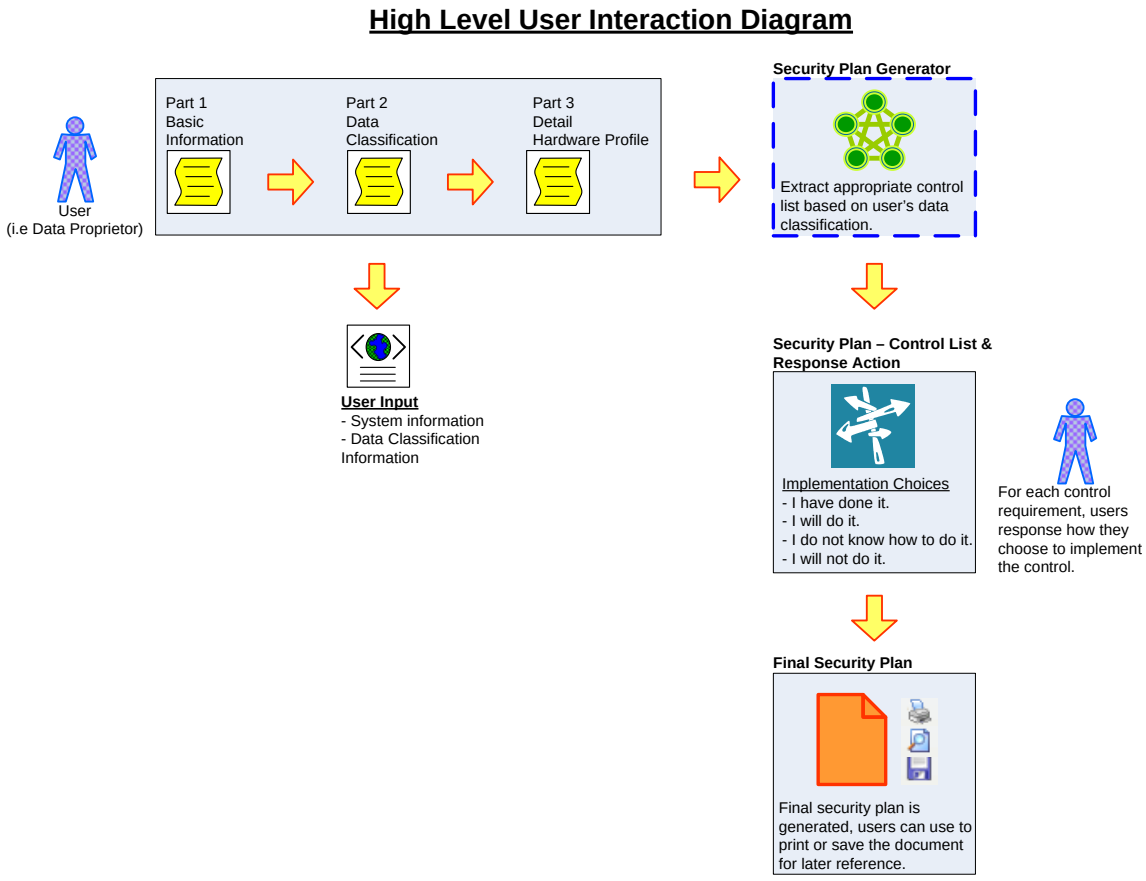

Figure 5: High-level user Interaction

The system takes the user through a five-step process, where information is captured from the user at the first four steps and the final security plan is generated at the fifth step.

At Step 1, user is asked to provide basic information about the system – the system name and the responsible organization. User is also required to give details of the key contact persons who have some responsibility for the system. The key contact persons are – Data Proprietor, Data Custodian, Administrative Official and Information System Security Contact. The interface gives user the option to select if one person serves more than one role, thereby preventing the user from having to enter the same details again and again.

At Step 2, user is required to provide the information sensitivity level of the system as well as the information about its scope and type. Information sensitivity levels have several pieces of information; whether the system houses restricted or essential data, the severity of Confidentiality, Integrity and Availability, the laws that apply to the system and

whether or not the system is a "System of Record". Questions are asked about the scope of the system, whether it is a Web of DB server, if it is portable and if it contains vital records. The answers captured at step 2 are very crucial for the decision logic behind the Security Plan Generator to be able to extract appropriate controls for the system.

At Step 3, the user needs to provide information about the purpose and environment of the system. Different user types and the corresponding numbers for each category of users are being asked. The system environment section asks the user to provide information about the physical location, the network location, the hardware and software being installed on the system. If the system shares information with any other system, user is required to provide details about what information is being shared and the name and owner of the target system(s).

At Step 4, the information being captured at the previous three stages is being fed as input to the Security Plan Generator and it spits out all the required controls for the system. At this stage, user is required to provide the implementation choice and implementation details for each of the controls. In case, user is unsure as how to implement a particular control, and select the implementation choice as "I do not know", the appropriate procedure for that control gets filled in automatically which the user can then edit as necessary.

At every stage, the information captured from the user gets saved to intermediate XML file for the purpose of preventing data loss in the face of network failure.

Once, user submits their control implementation details at step 4, the system generates a final "Security Plan" for the system. This plan contains all the data captured at every stage and user is given the option to either save the security plan or print for their future reference.

9.3.3 Detailed System design

The following diagram depicts the detailed system design and shows the processing that take place at various stages inside the ITS a BeAR system.

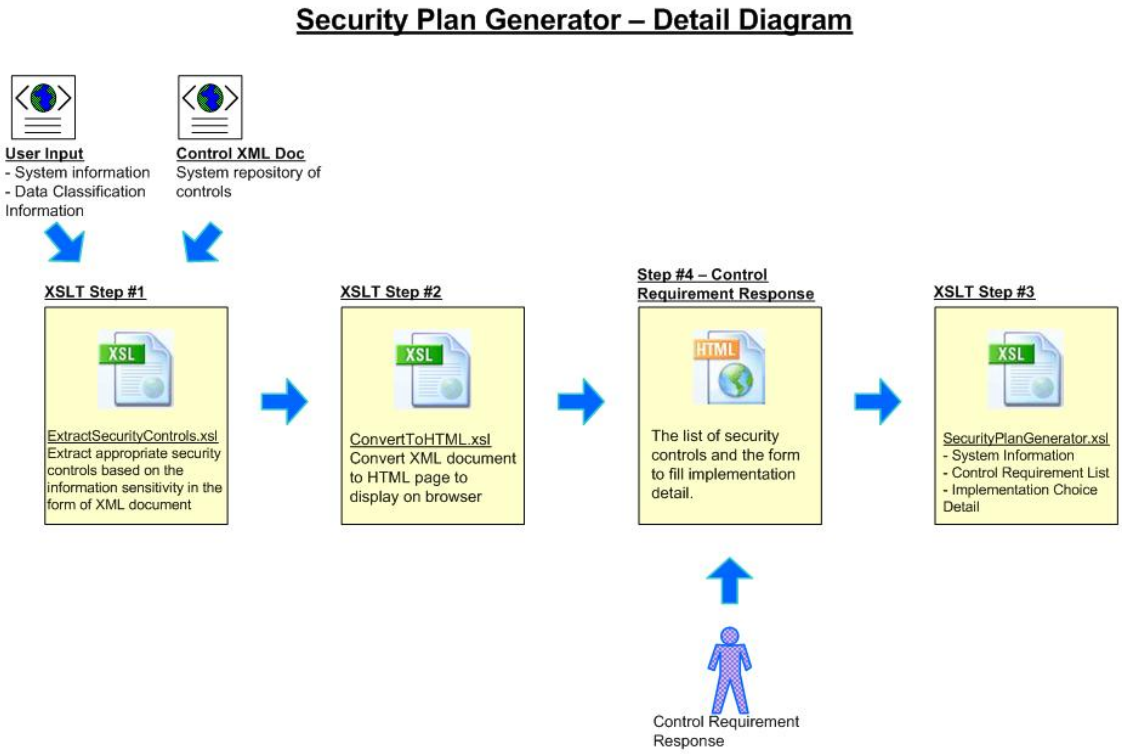

Figure 6: Detailed Flow diagram

All the security controls pertaining to the UC Berkeley campus environment are modeled and stored in a control repository in the form of an xml file – "**Controls.xml**". This is the master list of 76 controls which are applicable to the security landscape of Berkeley campus. For extensibility and maintainability, the repository xml file is being governed by a schema definition – "**Controls.xsd"**. The detailed data model of the controls can be seen in the *Appendix F – ITS a BeAR Detail Data Model*.

As described in the preceding section, Security Plan Generation system captures user inputs at four different stages. At every stage, the input gathered from the user gets stored in an intermediate XML file for every user. This is done to make sure that data is not lost in case of a network failure on the client side.

After gathering all relevant user inputs, the system uses a XSL file "ExtractSecurityControls.xsl" to extract the pertinent controls from the repository based on the information sensitivity of the user's system. This XSL file essentially has a decision logic which uses the sensitivity levels of Confidentiality, Integrity and Availability as well as the data categories "Restricted" and "Essential" as parameters for the extraction process. The resulted list of security controls are then fed to another XSL file "ConvertToHTML.xsl" which then generates and renders a HTML form for the user to enter the implementation details for each of these controls.

Once user completes entering implementation details for all the controls, a final XSL - "SecurityPlanGenerator.xsl" - is used to generate the final security plan for the system.

At this point, user is given the option to either print the plan or to save it to the file system for future reference.

9.4 Benefits of the System

- The system gives users guidance on how to write a security plan, which currently doesn't exist
- Based on data sensitivity levels, it tells the users which controls should be in placed based on specific policies. The user doesn't need to interpret various complex policies to figure what needs to be done anymore
- If the user doesn't know how to implement the control, our system shows the users to implementation procedures.
- Intuitive User Interface including definitions and help options ensures a smooth user experience.
- The ability to save and print the security plans in a centralized database would facilitate the local/internal review of those security plans in a periodic manner.
- This system will help the IT auditor speedup the audit process.
- The user can re-use the security plan in any other system which requires one. Hence the need to do duplicate work is addressed.

10 Future work and Recommendations

10.1 Recommendations to ISD Clinic

Our recommendations to the ISD clinic fall into two categories: potential future work on the ITS a BeAR system, and potential areas of IT security collaboration with IS&T based on areas not covered by our project.

10.1.1 Additional functionalities

As mentioned earlier, our current implementation is a proof-of-concept system intended to illustrate key concepts, and is not intended for use in a production environment. Due to timeframe concerns, certain envisioned functionality is not part of our existing system.

Auditor Interface

Security plans should be reviewed internally at least once a year, and may be externally audited at any time. Having an interface whereby the results of such audits can be entered into a system provides a history of activity related to system security controls.

Periodic Review Scheduling and Reporting

University policy requires that certain controls undergo periodic review. Also, a system owner may want to define a review period for other controls. Being able to mark controls as subject to periodic review, and allow the person preparing the security plan to define a review period, could be used by the system to create review schedules and results reporting.

Incremental Entering of Information

Security plans are complex documents, and it probable that it will require multiple sessions to enter all the relevant information in the system. Being able to save a document before all information on a page is entered would be helpful.

Generation of Customized Guidance Reports For Units

It would be useful to print out reports that list all controls that will be waived, all controls that will be implemented in the future, and guidance documents that provide recommendations for all controls that are flagged as “I don’t know how to do this.” Reports could also be used by technical staff to explain controls that need to be implemented and justify resource expenditures

10.1.2 Potential Areas for Future Collaborations with IS&T

Risk Management Frameworks and Tools

Recent changes to system-wide policies are advocating a shift to using a risk-based approach to decide which controls should be put in place. But there isn't a clearly defined process to determine the risk. If each unit is using a different methodology, it is difficult to get a picture of accurate risk levels across the university. An analysis of risk assessment processes or frameworks for suitability in a campus environment and building of a proof of concept risk assessment tool would be a valuable project. The two risk management frameworks we reviewed, Octave and NIST SP 800-30, deserve further investigation as to suitability for implementation on at UC. There may be additional such frameworks and methodologies worth investigating as well. Once a suitable framework or combination of frameworks is identified for UC, there is opportunity for iSchool students to build proof-of concept tools to allow one to easily step through the risk assessment process.

Decision Tools to Help Identify Nature of Data on System

One of the major issues we identified as part of needs analysis was that requirements for data protection are based on laws that are sectoral in nature, so the circumstances under which the data was collected can matter as much as the nature of the data itself. For ITS a BeAR system, we assumed that the sensitivity level had already been categorized by the time the security plan is generated. There is an opportunity for ISD to assist with the creation of a sensitivity wizard that can help people classify their systems.

10.2 Recommendations to the CIO Office

Here are some recommendations that arose from our analysis of the campus security posture:

10.2.1 Advocate Inserting Security Activities Into Mandatory Processes

Our original project focus was exploring ways of inserting security activities into mandatory processes, such as CPHS protocols and mandatory training. Although we had to abandon this path due to resistance from OPHS, we still believe that tweaks to such processes would reap great benefits.

- With the conversion of the CPHS paper process to the electronic eProtocol system, it would be possible to:
  - Include guidance on what is required to protect restricted data, so that a researcher can make an informed decision on whether they actually need to collect personal information on subjects.
  - The CPHS process requires a security plan describing how personal data is to be protected. A standard template asking questions relevant to UC policy compliance could be inserted.

- Entry of location of sensitive information into RDM could be made part of the CPHS process.

10.2.2 Risk Management

With the shift within system-wide policy to a risk-based approach, standards and guidance are needed to properly implement this change.

- Define and adopt a standardized risk assessment methodology for the campus. Having a consistent risk assessment approach will reduce confusion and allow tracking/reporting of issues across multiple systems
- Consider having risk assessment POC in the CIO office that can perform risk assessments for campus units.

10.2.3 Consolidate security log auditing

Security audit review is a critical task when attempting to determine if an exploit has occurred, but it can be time consuming and error prone. The latest version of IS-3 recommends that campuses set up common log management infrastructures.

- Define a standard for audit log content so that centralized log auditing can be implemented IS-3 Appendix D can serve as a model
- Define a list of required events that would trigger audit log generation for operating system level, network, and applications.
- Add use of central campus Network Time Protocol (NTP) server as a control to either minimum standards or restricted/essential policies so that security events can be easily tracked across systems
- When funding permits, consider setting up a consolidated log server with analysis/reduction software such as Splunk or LogLogic

10.2.4 Improve Periodic Review of Controls

Periodic reviews are called for a number of security controls within various applicable policies, but not much guidance is provided, and one has to sort through multiple policies to determine which controls to review

- Define a list of candidate controls for periodic review and make this list available to the campus community
- For each control, define a recommended or required review period (ie every two years, annually, quarterly, etc)
- For each define and provide a set of review criteria, or at least a pointer to guidance
- Provide a form that can be used to schedule reviews and document the results thereof.

10.3 Advocate Granular Policy Gradations for Data Classifications:

Some of the data classifications that mandate controls are too broad, requiring controls be implemented that may not make sense from a risk based analysis. Consider advocating gradations within the restricted and essential data categories, specifically:

- The personal computer of nearly every faculty member contains FERPA data about students. Most FERPA data would not expose the student/subject to the threat of identity theft or other significant harm were it to be compromised. Creating a subset of the "restricted" data class that applies to FERPA data that only requires a subset of the controls mandated for "restricted" data, IT security will be less onerous to the faculty, and scarce resources can be allocated to address greater risks. This may require advocacy at the system-wide level to amend IS-2
- Similarly, a subset of "essential" resources that applies to systems that are not critical to the university as a whole but are important to individual units or departments should be given a subset with less required controls. This could be done at the campus level via changes to DMUP or successor policies.

10.3.1 Security as a Service

If designed to be scalable, security control services built for internal use within IS&T could be offered to the campus community, perhaps as part of security compliance bundle. This would be similar to typical managed security services are offered to small companies by outsourced security-as-a-service providers.

Specific services could include:

- Configuration management tools
- Integrity Checking tools such as tripwire
- Host-based firewall rule set management
- Patch distribution/updating
- Account management processes such as maintaining privileged access agreements, annual account reviews

Selected Bibliography

California Department of Consumer Affairs, Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information*, February 2006

Hammond, Thomas H, "Herding Cats in University Hierarchies: Structure and Policy Choice in American Research Universities," in *Governing Academia: Who Is in Charge at the Modern University?*, ed. Ehrenberg, R., Ithica: Cornell University Press, 2004

Geer, Daniel E, "The Evolution of Security", *ACM Queue* vol. 5, no. 3 - April 2007

Hasan, Ragib and Yurcik, William , "Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work," *National Center for Supercomputing Applications (NCSA), University of Illinois at Urbana-Champaign*, http://wesii.econinfosec.org/draft.php?paper_id=37 (accessed April 26, 2007)

Internet2 Security Guide: Compliance and Legal Issues
https://wiki.internet2.edu/confluence/display/secguide/Compliance+and+Legal+Issues

Identity Theft: Innovative Solutions for an Evolving Problem: Hearings before the Senate Judiciary Committee Subcommittee on Terrorism, Technology and Homeland Security, 110th Cong., 1d Sess. (2007) (testimony of Chris Jay Hoofnagle)

Kaplan, Gabriel E. "How Academic Ships Actually Navigate," in *Governing Academia: Who Is in Charge at the Modern University?*, ed. Ehrenberg, R, Ithica: Cornell University Press, 2004

Lohmann, Susanne, "Darwinian Medicine for the University," in Governing Academia: *Who Is in Charge at the Modern University?*, ed. Ehrenberg, R, Ithica: Cornell University Press, 2004

National Institute of Standards and Technology Special Publication 800-12, An *Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication *800-53, Revision 2, Recommended Security Controls for Federal Information Systems,* December 2007.

National Institute of Standards and Technology Special Publication 800-53A (Final Public Draft), *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, December 2007.

National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers, October 2006.

Petersen, Rodney J., *Insights on the Legal Landscape for Data Privacy in Higher Education* n.d. http://connect.educause.edu/Library/Abstract/InsightsontheLegalLandsca/46369

Reddick, David B. *Security Breach Notification Laws: What Threats Do They Pose for Insurers?*, National Association of Mutual Insurance Companies, July 2005).

Rezmierski, Virginia, *Final Report — NSF-Lamp Project: Identifying Where Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin*, American Association of Collegiate Registrars and Admissions Officers, 2001

Salomon, Kenneth and Cassat, Peter, *IT Security for Higher Education: A Legal Perspective, Prepared for EDUCAUSE/Internet2 Computer and Network Security Task Force,* issued March 2003

PricewaterhouseCoopers, *UC Berkeley: Data Privacy & Security Review*, Confidential Report prepared for UC Berkeley, issued July 2005

Samuelson Law, Technology & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers* issued December 2007

University of California Berkeley Data Stewardship Council, *Data Management, Use, and Protection Policy,* June 2004

University of California Berkeley Campus Information Security and Privacy Committee, *Minimum Security Standards for Networked Devices*, Jan 2004

University of California Berkeley Campus Technology Council, Campuswide Information Technology Strategic Plan: Critical Issue 4: Security, Reliability, Access

University of California Berkeley Campus Information Security and Privacy Committee, *Provisional Requirements for Restricted Data Security Plans*, August 2006

University of California Office of the President, *IS-2, Inventory, Classification, and Release of University Electronic Information* , University of California Business and Finance Bulletin

Series, December 2007

University of California Office of the President, *IS-3, Electronic Information Security* University of California I Business and Finance Bulletin Series, December 2007

University of California Office of the President, *IS-10, Systems and Development Standards,* University of California Business and Finance Bulletin Series, May 2001

University of California Office of the President, *IS-11, Identity and Access Management* University of California Business and Finance Bulletin Series, July 2007

University of California Office of the President, *IS-12, Continuity Planning and Disaster Recovery,* University of California Business and Finance Bulletin Series, July 2007

University of California Office of the President, RMP-8, *Legal Requirements on Privacy of and Access to Information,* July 1992

United States Computer Emergency Readiness Team (US-CERT) Technical Users Page http://www.us-cert.gov/nav/t01

Appendix

Appendix A – Data Classification Definition

Campus Data: All data owned by the University that are prepared, supplied, used, or retained by University employees, within the scope of their employment, or by agents or affiliates of the University, under a contractual agreement, except for data specifically excluded from University ownership by law, policy, or through special overriding ownership provisions. Some examples of types of campus data are payroll, personnel, faculty, student, alumni, development, financial, facilities-related, and sponsored research data. Campus data can be contained in any form, including but not limited to documents, spreadsheets, databases, email, and Web sites; represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof; communicated in any form, including but not limited to handwriting, typewriting, printing, photocopying, photographing, and Web publishing; and recorded upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks, and other devices. The term "data" as used in this policy is similar in definition and use to the term "records" in the policy of the University of California, Business and Finance Bulletin, Records Management Program (RMP-1).

Restricted Data: Data to which use is restricted by federal or state law or University or campus policy; or data that a Data Proprietor has designated as protected from general access or modification, even if such access may not be prohibited by federal or state law or University or campus policy. Types of restricted data include, but are not limited to, data that identifies or describes an individual and data to which unauthorized access, modification, or loss could seriously or adversely affect UC Berkeley, its partners, or the public. Examples of restricted data include social security number, employee home address, date of birth, financial information such as credit card number or bank account number, student grades and financial aid records, and responses to a Request for Proposal (RFP) before a decision has been reached. (See IS-3, Section IV, B)

Unrestricted Data: Data to which access or modification is not restricted by federal or state law or University or campus policy and to which access is permitted by the Data Proprietor. Examples of data that are unrestricted include data contained in annual campus financial reports, class catalogs, and campus general information handbooks. (See IS-3, Section IV, B)

Essential Data Resource: A data resource whose failure to function correctly and on schedule could result in either a major failure to perform critical business functions, a significant loss of funds, or a significant liability or legal exposure. (See IS-3, Section IV, B)

Required Data Resource: A data resource that performs an important function, but the operation of the campus could continue for some designated period of time without it. (See IS-3, Section IV, B)

Deferrable Data Resource: A data resource that the campus could operate without; it need not be performed correctly or on schedule and would not affect mission-critical business functions. (See IS-3, Section IV, B)

Data of Record: Data recognized by the campus as containing official information about a certain data type to which data users must reconcile when producing official or external to the department reports. Data of record normally reside within a System of Record, which may or may not be the place in which the data originated. Data of Record should be modified only with the consent of the Data Proprietor and only within the System of Record where the data officially resides. Data of record is required to be maintained, accurate, and timely. Campus systems should use data of record whenever possible and refresh data from the System of Record on a regular basis.

Unofficial or Reference Data: All campus data that *are not* data of record, including, but not limited to, data that are extracted, modified, extended, revised, or changed from data of record; data that duplicate data of record; and data created independently of data of record but not sanctioned by the campus as data of record. Unofficial data typically resides in data warehouses, locally administered data systems, or workgroup level applications that have been created to administer additional data not found in Systems of Record or data of record. Whenever possible, systems should use data of record rather than unofficial data. If using unofficial data for analytical and reporting purposes, analysts should note their use of unofficial data and be prepared to reconcile their findings back to the data of record. If any variances exist, they should be documented and explained by the analyst. Unofficial data should never be distributed as data of record.

Appendix B – Risk-based assessment Data Classification Definition

IS-2's information security objectives:

- Confidentiality: Preserving authorized restrictions on access and disclosure including means for protecting personal privacy and proprietary information.
  - Confidential information includes any information sensitive enough to require access controls, but this document is concerned only with restricted data: confidential or personal information that is protected by law or policy.

- Integrity: guarding against improper information modification or destruction and may include ensuring accuracy and authenticity.
  - Integrity is vital for "systems of record" and impact assessments should take into account potential loss of integrity in these systems, not in "client" systems.
  - Integrity is often confused with confidentiality because some security mechanisms are used to achieve both objectives; however, it is important to assess the impact of a loss of integrity separately from a loss of confidentiality in order to determine the most effective security measures.

- Availability: ensuring timely and reliable access to and use of information.
  - The overall importance of availability of data is based on its criticality to the functional operation of the campus or department or to the priority of that function in continuity plans and disaster recovery strategies.

Appendix C – Existing RDM Process Flow

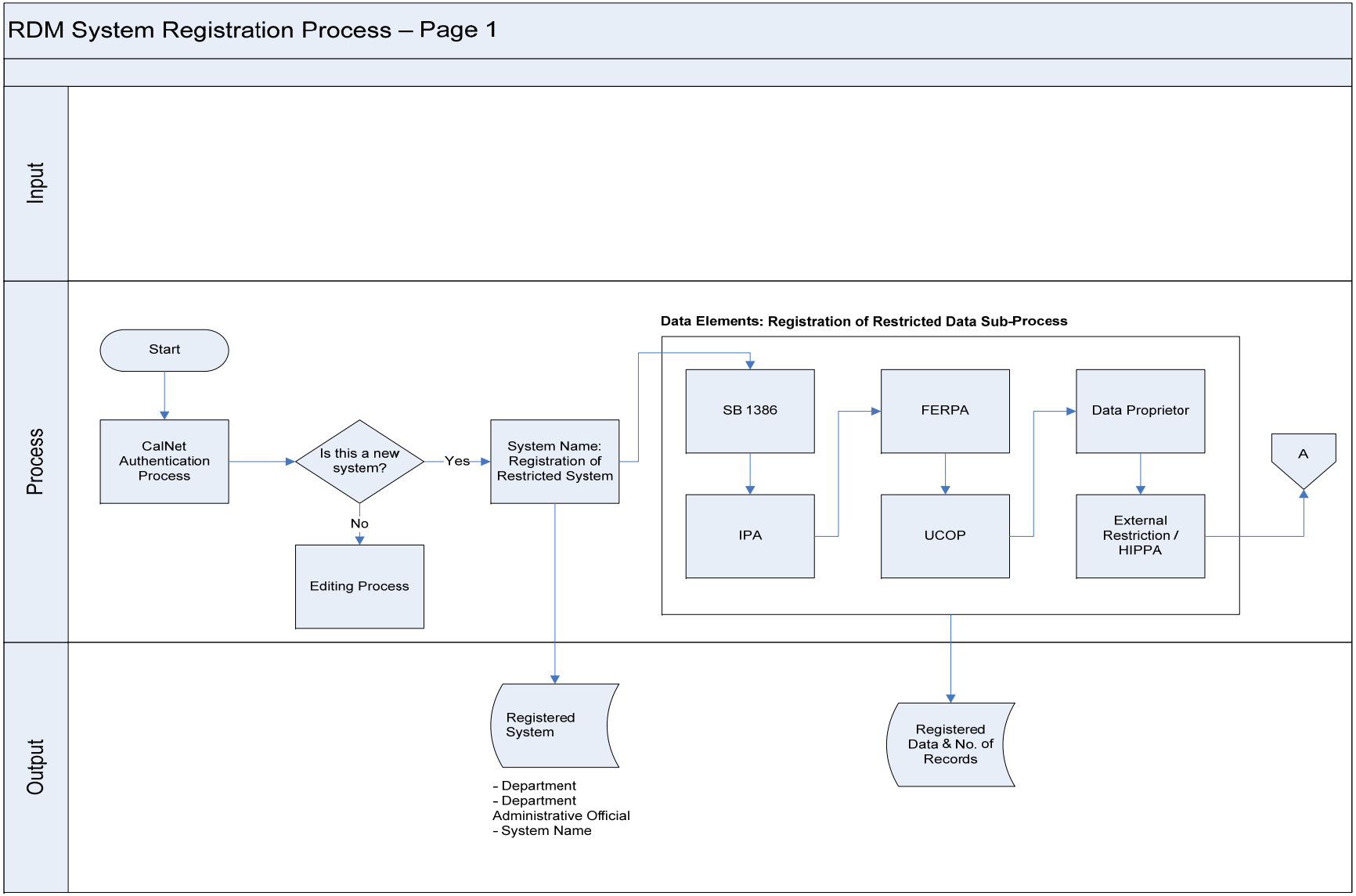

Figure 7: RDM System Registration Process – Page 1

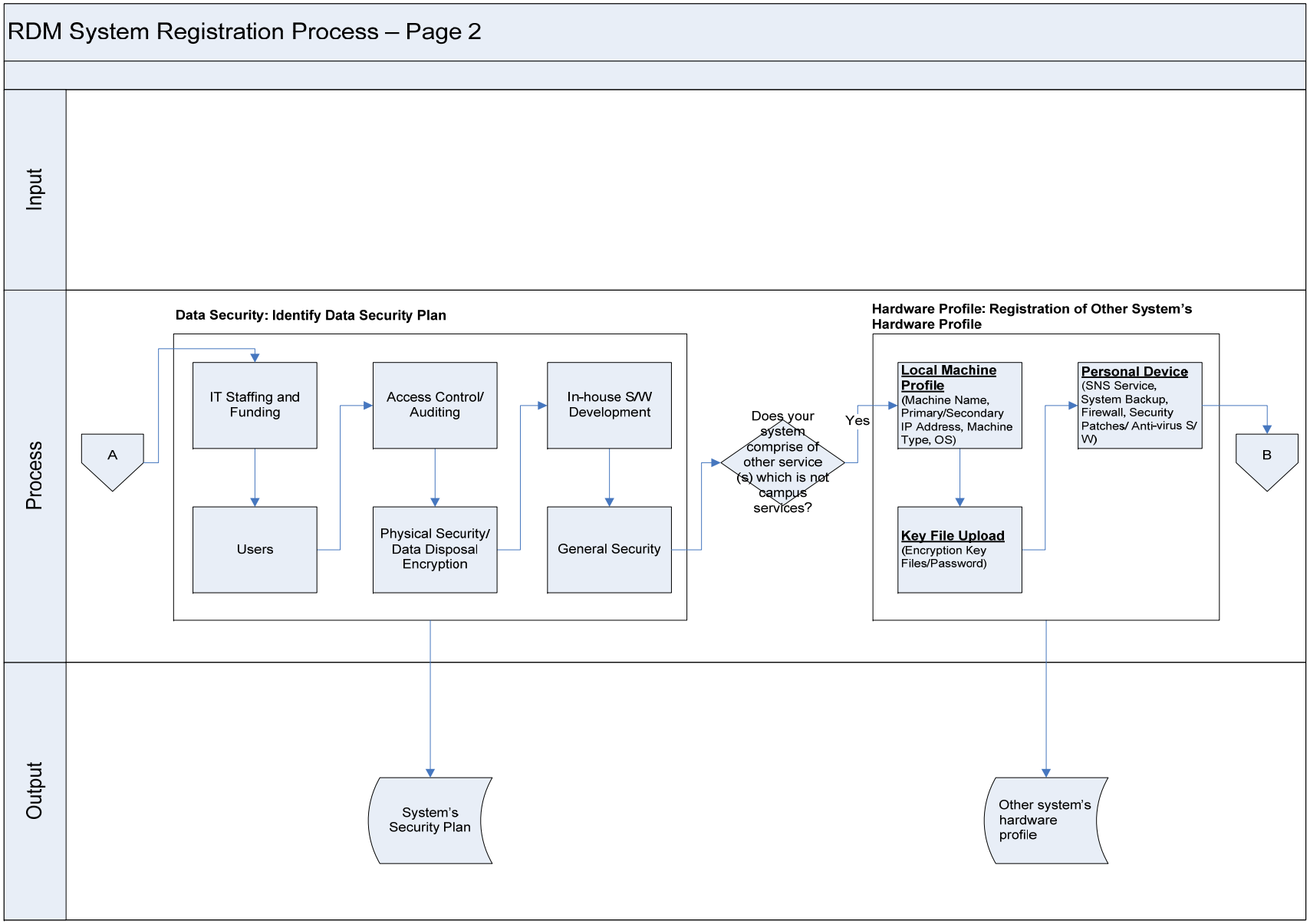

Figure 8: RDM System Registration Process – Page 2

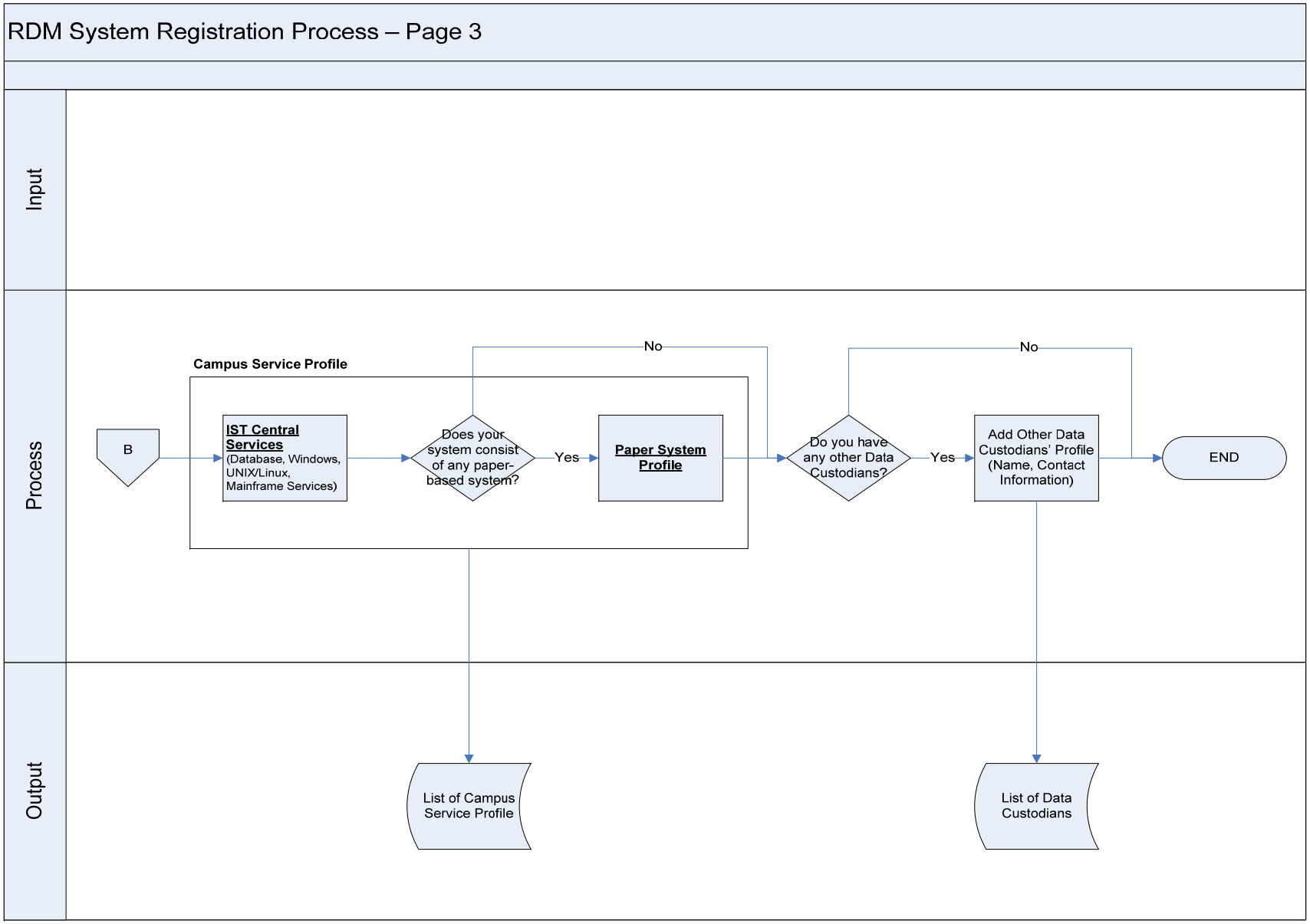

Figure 9: RDM System Registration Process – Page 3

Appendix D – ITS a BeAR Process Flow

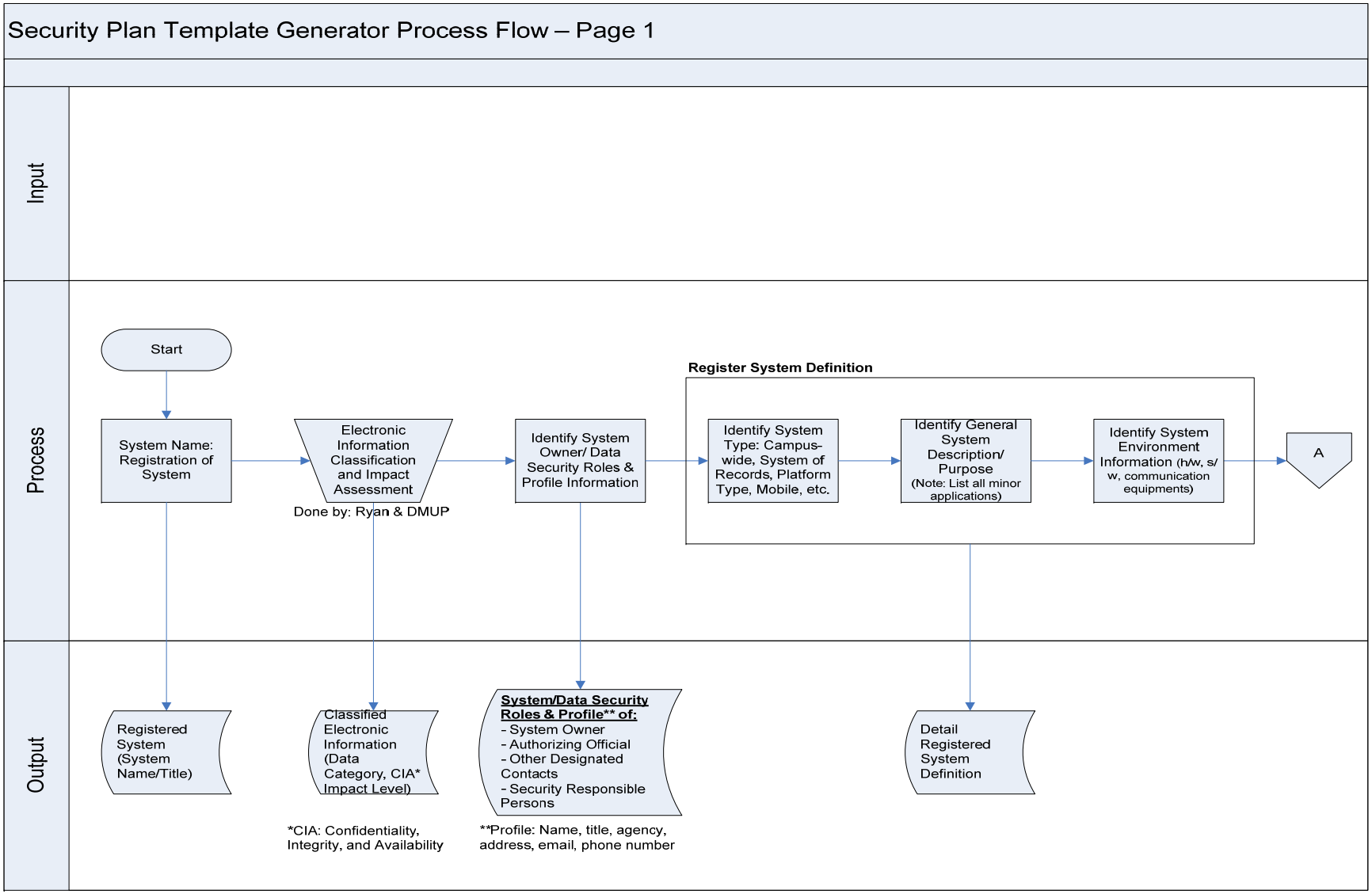

Figure 10: Security Plan Template Generator Process Flow – Page 1

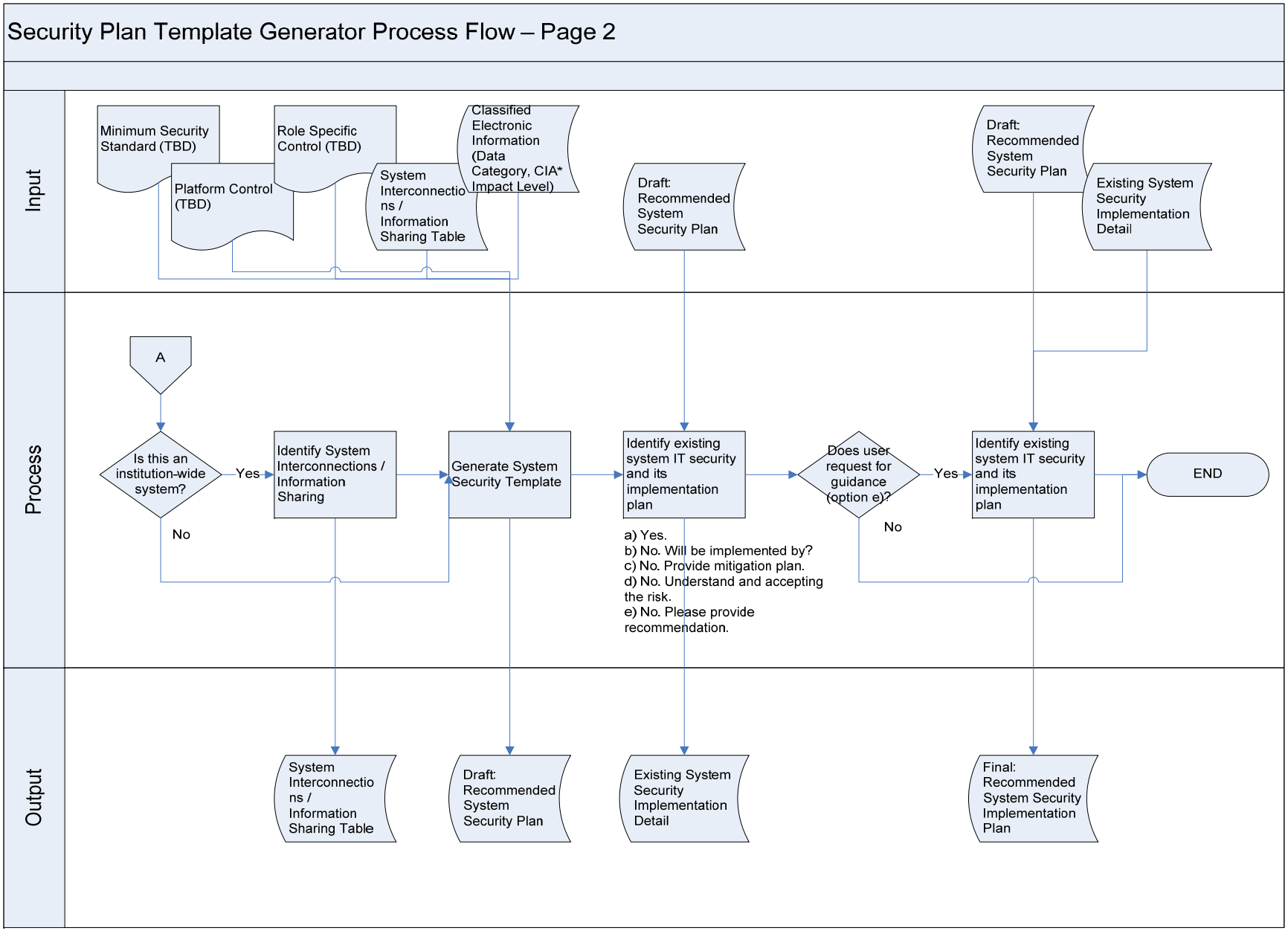

Figure 11: Security Plan Template Generator Process Flow – Page 2

Appendix E – IT Security Control Catalog

[Refer to *ITsaBeAR - IT Security Control Catalog.xls* for the IT Security Control Catalog Table]

Appendix F – ITS a BeAR Detail Data Model

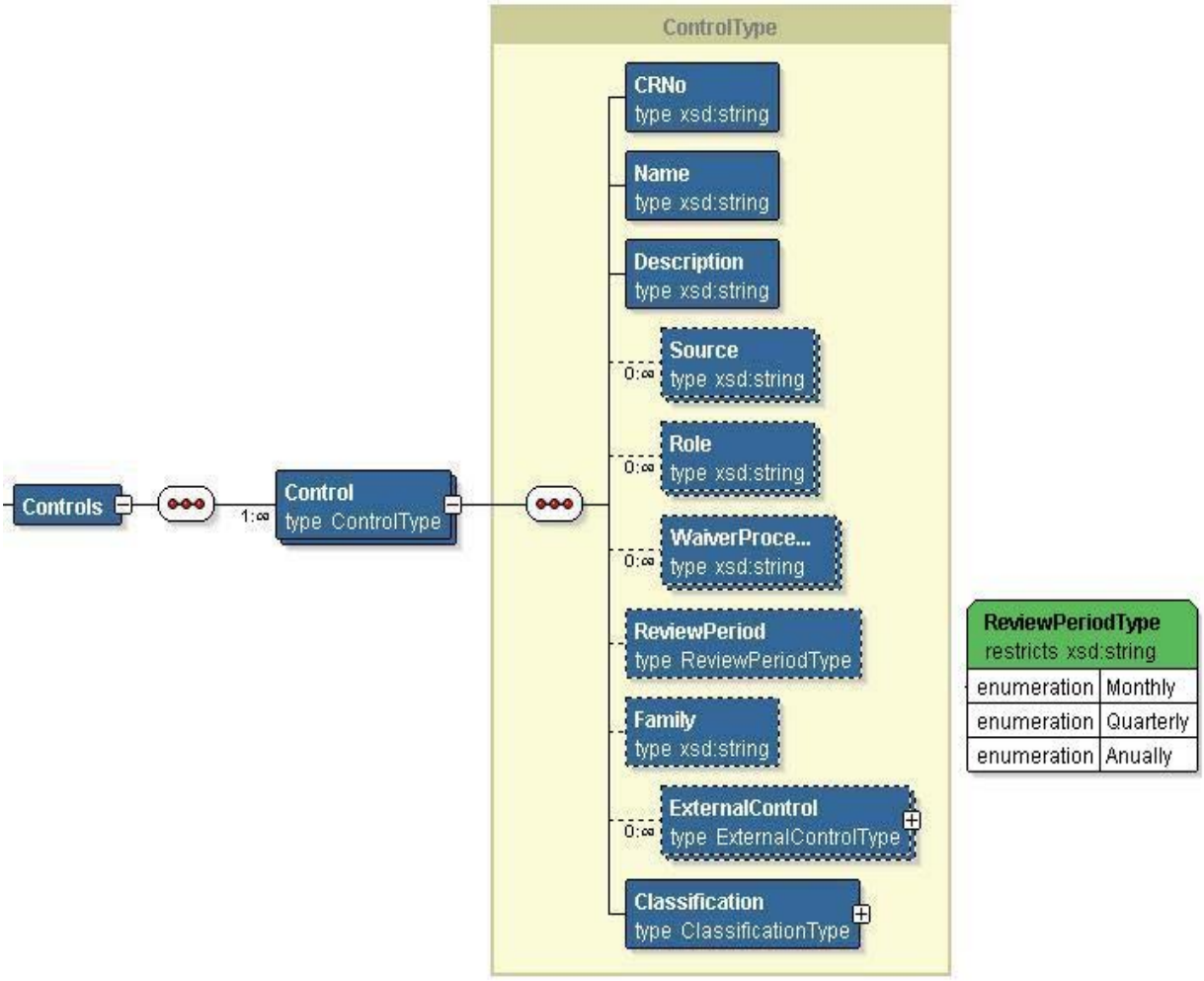

Figure 12: Data Model for each Control and the Review Period Type

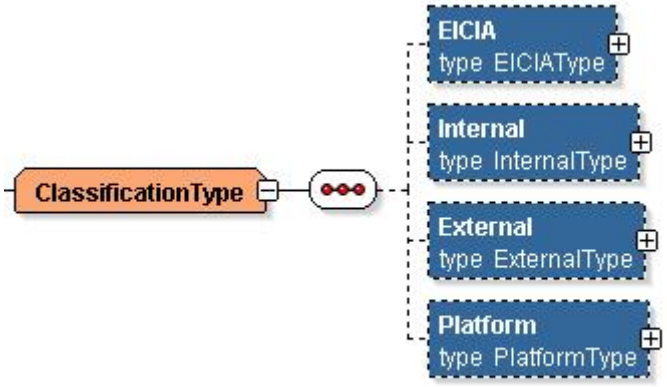

Figure 13: Data Model for Classification Type used by the Classification Element

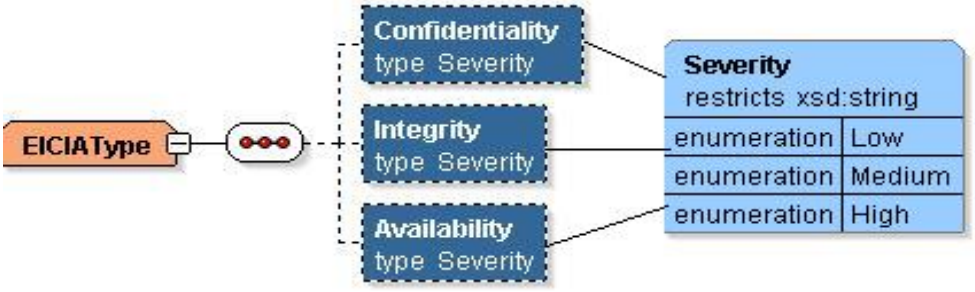

Figure 14: Data Model for EICIA Type – a child element of Classification

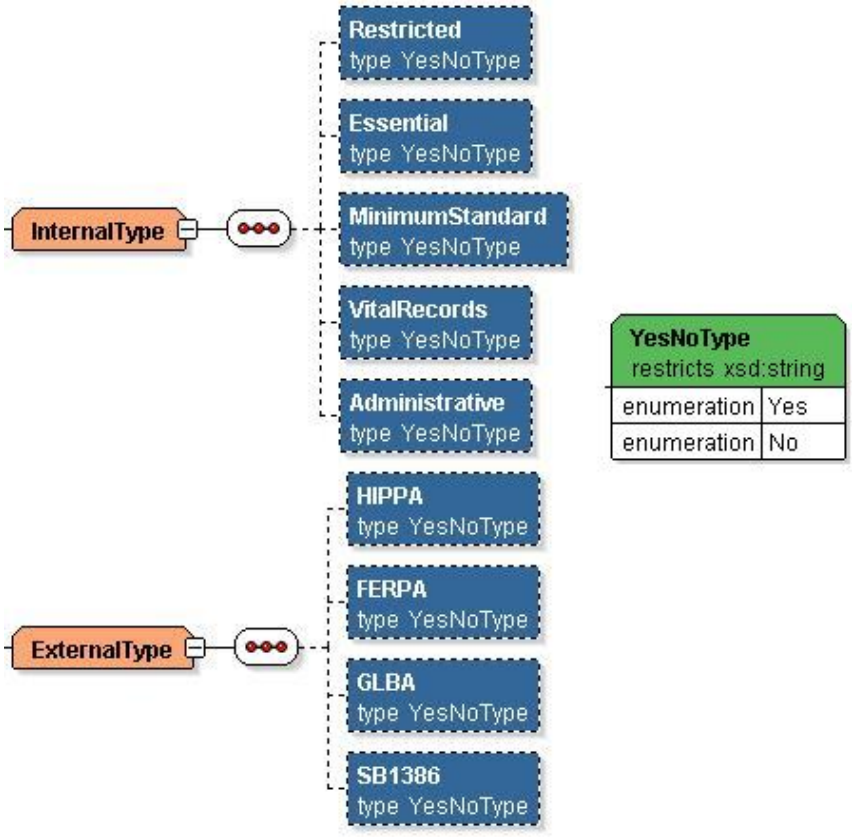

Figure 15: Data Model for Internal and External Type – child elements of Classification

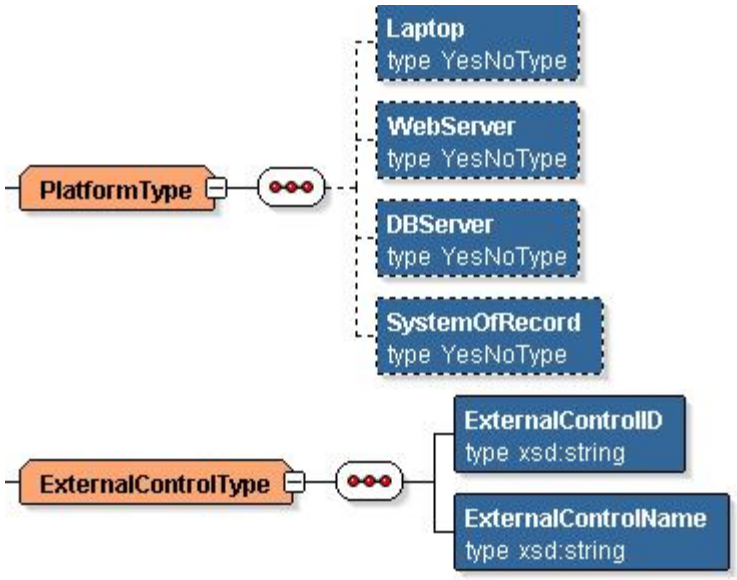

Figure 16: Data Model for Platform Type and External Control Type

Appendix G – Sample Security Plan Document

System Security Plan

Submit application to:
Information Services and Technology
University of California, Berkeley

This form must be filled out completely. After completion, please submit the form to the department of Information Services and Technology.

System Information:

System Name _____

Responsible Organization _____

System Contact Persons:

Data Proprietor

Name _____ Organization _____

Address _____

Email _____ Phone _____

Data Custodian

Name _____ Organization _____

Address _____

Email _____ Phone _____

Administrative Official

Name _____ Organization _____

Address _____

Email _____ Phone _____

System Security Contact

Name _____ Organization _____

Address_____

Email_____Phone_____

Information Sensitivity:

Restricted Yes ☐ No ☐

Essential Yes ☐ No ☐

System of Record Yes ☐ No ☐

Confidentiality High ☐ Medium ☐ Low ☐

Integrity High ☐ Medium ☐ Low ☐

Availability High ☐ Medium ☐ Low ☐

Applicable Laws HIPAA ☐ FERPA ☐ GLBA ☐

Information System Type:

Scope Single User System ☐ Unit-wide ☐ Campus-wide ☐

Web Server Yes ☐ No ☐

Database Server Yes ☐ No ☐

Portable Systems included in the system? Yes ☐ No ☐

System contains Vital Records? Yes ☐ No ☐

Purpose of the System:

Purpose

User Types and Number:

Privileged User Estimated Number _____

User Type _____ Estimated Number _____

User Type _____ Estimated Number _____

User Type _____ Estimated Number _____

System Environment:

Physical Location: _____

Network Location: _____

Hardware(s) _____

_____

Software (s)_____

_____

Information Sharing:

Does this system share information with other systems? Yes ☐ No ☐
If **Yes**,

- What Information _____

  System Name _____System Owner _____

- What Information _____

  System Name _____System Owner _____

- What Information _____

  System Name _____System Owner _____

Required Controls

Family: **Awareness and Training**

Control No: CR063
Control Name: Security Awareness Training
Description: Security awareness training for all members of campus community
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: **Access Control**

Control No: CR012
Control Name: Session Lock
Description: Devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR029
Control Name: Privileged Access Agreement
Description: All users with privileged access to device must sign a Privileged Access agreement and file the agreement with the appropriate campus official
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR037
Control Name: Separation of duties
Description: The principle of separation of duties should be employed to ensure that responsibilities for critical functions are divided among different individuals.
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐

Will not do it ☐ Do not know How to do ☐

How:

Control No: CR041
Control Name: Privileged Access
Description: Audit Review Private Accounts shall be logged; logs should be reviewed by Independent person
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: **Acquisition and Development**

Control No: CR065
Control Name: Third Party Security
Description: Contracts with 3rd parties should protect restricted or essential data provided
Performed By: Data Proprietor
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: **Audit and Accountability**

Control No: CR007
Control Name: Privileged Access: Authentication
Description: Password: Users should initially authenticate with an unprivileged account rather than a privileged account; privileged access should occur through a privilege escalation mechanism which allows the log to show which user was granted additional privileges
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR054
Control Name: Audit Review
Description: Periodic review of logs
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR057
Control Name: Audit Protection
Description: Protect confidentiality and integrity of audit logs
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family Name: Authentication

Control No: CR004
Control Name: Default passwords
Description: All default passwords must be changed
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR005
Control Name: Password complexity
Description: Password: Must meet the "Minimum Password Complexity Standards"
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR006

Control Name: Privileged Accounts
Description: Passwords: devices should be configured with separate accounts for privileged and unprivileged access
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR008
Control Name: Privileged Access: Duration
Description: Password: privileged access should only be granted for as long as necessary to complete the task which requires additional privileges
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR009
Control Name: Encrypted Authentication
Description: All campus devices must only use encrypted authentication mechanisms unless authorized by CISPC
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR036
Control Name: Individual authentication
Description: Procedures for providing individual authenticated access to Resources should incorporate review and approval mechanisms to ensure that only Authorized Individuals are granted access.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR040
Control Name: Identity and Access management
Description: Establish an identity and access management strategy that ensures accurate identification of authorized users and that provides secure authenticated access to and use of network-based services
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR067
Control Name: Individual Responsibilities: Authenticators
Description: Individuals must protect passwords or authentication tokens
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: Configuration Management

Control No: CR010
Control Name: Email Relays
Description: No unauthenticated email relays: No active SMTP service is allowed on campus
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR011
Control Name: Proxy Services
Description: No unauthenticated proxy services is allowed on campus
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐

Will not do it ☐ Do not know How to do ☐

How:

Control No: CR013
Control Name: Least Functionality
Description: No unnecessary services should be run
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR052
Control Name: Configuration Change: Monitoring
Description: Monitoring and logging of all changes, including steps to detect unauthorized changes to system/ sec controls
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR053
Control Name: Hardware and Media Inventory
Description: Procedures that track the receipt, reuse, and removal of hardware and electronic media, including documentation of hardware reassignment.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR055
Control Name: Configuration Change: Testing
Description: Confirmation of testing of configuration changes
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR056
Control Name: Configuration Change: Roll Back Plans
Description: Back out plans for proposed configuration changes
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family Name: Incident Response

Control No: CR043
Control Name: Security Contacts
Description: Contacts must respond to security incident reports from central campus security staff and pass them on to responsible departmental or third party support personnel as appropriate
Performed By: Security Officer
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: Media Protection

Control No: CR025
Control Name: Equipment Sanitization
Description: Information must be securely and completely erased from all devices when equipment is retired / repurposed
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR046
Control Name: Encrypted Backups
Description: Restricted data backups shall be encrypted unless stored securely
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐

Will not do it ☐ Do not know How to do ☐

How:

Family: Personal Security

Control No: CR066
Control Name: Background Checks: Third Party
Description: Background checks for 3rd parties handling restricted or essential
Performed By: Data Proprietor
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR073
Control Name: Background Checks: Privacy
Description: Data People w/ access to detailed personally identifiable information about students, faculty, staff, or alumni which might enable identity theft must have criminal background check
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR074
Control Name: Security Planning
Description: A copy of the security plan must be retained by the Administrative Official's office, and a copy of the Plan must be submitted to SNS. Security Plans must be protected from unauthorized access
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: Personnel Security

Control No: CR038
Control Name: Account Mgmt: Transfer and Termination

Description: Accounts must be removed or disabled for terminated or transferred employees.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR039
Control Name: Sanctions for violations
Description: Depending on the nature of the violation and the likelihood of a recurrence, the Resource Proprietor or Custodian shall take prompt action to protect against future violations to the extent feasible, and/or remove the means by which the violation occurred. Depending on the nature of the violation, the Resource Proprietor or Custodian shall consult with other campus authorities in accordance with policies governing potential disciplinary action.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: Physical and Environmental Protection

Control No: CR059
Control Name: Environmental Risk mitigation
Description: Implement appropriate measures for the prevention, detection, early warning of, and recovery from emergency conditions, including, but not limited to, earthquake, fire, water leakage or flooding, disruption or disturbance of power, air conditioning failures, and environmental conditions exceeding equipment limits.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR060
Control Name: Physical Access controls
Description: Limiting physical access to locations housing restricted or essential Resources should be implemented through the use of combination locks, key locks, badge readers, manual sign in/out logs, verification of identification, etc. The ability to track both ingress and egress of all individuals should be maintained as appropriate. Records of access events should be maintained consistent with audit log guidelines
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR061
Control Name: Portable/ Removable Media Physical Protection
Description: Physical security of portable devices, Media, USB etc
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR068
Control Name: Individual Responsibilities: Physical Access
Description: Individuals must protect physical security of computers with restricted data.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: Security Assessment

Control No: CR075
Control Name: Internal Review
Description: Internal review of plans must happen at least annually and when significant changes are made to system
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR076
Control Name: External Review
Description: External Review may include, but are not limited to: proprietor(s), SNS, Audit and Advisory Services and/or outside experts as requested by the Proprietor or campus
Performed By: Data Proprietor, Administrative Officials

Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR070
Control Name: Access Control Testing
Description: Access control mechanisms must be tested periodically
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: Security Planning

Control No: CR042
Control Name: Security Responsibility
Description: Responsibility for systems and application security should be assigned to an individual knowledgeable about the information technology used in the system and in providing security for such technology. This individual should determine security plans as appropriate to the supported systems, applications, and data.
Performed By: Admin Official
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR069
Control Name: Data Proprietor Security Requirements
Description: Minimum security requirements of all Data proprietors must be met
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: System Integrity

Control No: CR001
Control Name: Patching
Description: Software patch updates
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR002
Control Name: Anti-virus
Description: Anti-virus software must be running at all level of devices; anti-virus software definitions must be up to date
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR048
Control Name: Malicious software protection
Description: Measures should be deployed to limit access to systems that host restricted or essential Resources and to protect systems from "malicious software" which includes programs, such as viruses, worms, Trojan horses, and spyware, usually installed on a device without an individual's knowledge or under false pretenses.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: System and Information Protection

Control No: CR003
Control Name: Host-based firewall
Description: Host-based firewall software must be running at all level of devices
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐

Will not do it ☐ Do not know How to do ☐

How:

Control No: CR022
Control Name: In-transit Encryption
Description: Information must be encrypted across all network segments, wired or wireless using a strong encryption algorithm
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR058
Control Name: Portable Device Protections
Description: Restricted information only on a laptop, a hand-held device, or other portable device if confidentiality and integrity safeguards to protect against theft or loss are in place, been reviewed and are authorized
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Family: System and Information Protection

Control No: CR034
Control Name: Encryption Key Management
Description: If encrypted, the authoritative copy of this information must be recoverable through the use of a central recovery agent
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR051

Control Name: Firewalls and IDS
Description: Firewalls and Intrusion Detection/Prevention Systems should be deployed as appropriate to limit access to systems that host restricted or essential resources.
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐
How:

Control No: CR062
Control Name: Restricted Data Inventory
Description: Restricted personal information entered into RDM
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Control No: CR071
Control Name: Information Sanitization
Description: Secure destruction of stored Restricted Data after retention period expired or completion of sharing agreements with 3rd parties
Performed By: Data Custodian
Implementation Choice: Have done it ☐ Will do it ☐
Will not do it ☐ Do not know How to do ☐

How:

Appendix H – Contact Information

Table 2: Project Contact Information

Name	Title	Department	Notes
Ryan L. Means	Chief Technical Officer	Law-Computer Services	
Dedra Chamberlin	Security Applications Manager	IST-Infrastructure Services	
Kate Riley	Scanning Services		75% IST, 25% SNS
Karl R Grose	Programmer/ Analyst IV	IST-Infrastructure Services	RDM
Allison Kay Henry	Programmer/ Analyst IV	IST-Infrastructure Services	RDM
Vahid Nadi	Programmer/ Analyst III	IST-Infrastructure Services	RDM
Michael Green	Infrastructure Applications Manager	IST-Infrastructure Services	RDM
Jeremy A. Lapidus	IT Audit Manager	Audit and Advisory Services	
Jonathan Banda	Senior Administrative Analyst	Office for the Protection of Human Subjects	
Rebecca Dianne Armstrong	Director	Office for the Protection of Human Subjects	
Clyde Valdez	Chief Security Officer, RSSP	Rsdn & Stu Svcs Prog	
Karen E. Eft	IT Policy Manager	Office of the CIO	
Kevin Heard	Director Computing & Information Services	School of Information	
Mr. Chris Hoofnagle, JD	Senior Staff Attorney, Samuelson Clinic	Law	
William Allison	Senior Manager	IST-Application Services	
Alice M. Agogino	Professor	Mech Engr	
Doug Tygar	Professor	CS/iSchool	