
Chapter 4: Information Architecture & Security

The fundamental question that this chapter seeks to answer is “How do we create a secure IT environment that also ensures the availability of resources in an effective and efficient manner?” Any IT system must still be built with specific business and academic needs in mind. In addition to understanding business needs, it is imperative that risk must be addressed as part of the planning and deployment of any IT system. Without a consistent and unified approach to identifying risk, it will be impossible to achieve adequate safeguards. An accurate inventory which captures both the business criticality of the system and the sensitivity of the data is a prerequisite for the development of both technical and non-technical safeguards and ensure that there are not gaps in implemented controls. To provide appropriate safeguards that are cost effective to reduce risk often means centralizing services, especially if certain components such as services that handle either sensitive data or authentication are in place.

Additionally, this chapter outlines the initiative to develop a unified, IT architecture though building a central data and application service. This would mature the campus’ IT infrastructure and allow for real-time secure data to be accessed by campus departments rather than departments accessing and distributing sensitive data with few downstream controls and accountability. It would also significantly increase security by storing data centrally rather than perpetuating the need for departments to often store information locally on “shadow” systems. Duplication of both personnel and hardware/software by providing central data and application services that includes responsive support services for departments would decrease.

Another aspect to this chapter is ensuring the availability of critical assets, especially in the event of a natural or man made disaster. CU-Boulder needs to develop processes that ensure disaster recovery and business continuity plans are developed, maintained, and routinely tested. The campus must also continue to conduct risk assessment of all departments to determine our areas of greatest exposure.

4.1 Information Architecture and Security

Major Issue: CU-Boulder must develop an information architecture and accompanying set of services that provide for the need of departmental applications to access and create sensitive data, yet enforce much greater controls over how such data is stored and used. Without an enforced architecture and supporting services, there is no relief to the current practice of widely distributing sensitive data with few controls and little accountability with respect to how data is used and handled.

A. Background/Rationale

Many campus applications depend on access to electronic records which contain personally identifiable or otherwise sensitive information. Some of this data is generated and maintained locally by the application or elsewhere within the department, but most business applications on campus also require data from a University primary system, such as the Student Information System (SIS), the PeopleSoft Human Resources System (HR) or the Computer Information Warehouse (CIW). The typical use of this data involves establishing a feed from a primary system, populating “shadow” databases that are maintained locally within the department.

The need for data is genuine, as many applications that best suit a business need are rigid in how they access and manage data. Applications tend to assume an autonomous, application database that stores a mix of data specific to the application and sensitive personal or financial information derived from a source system. For the most part, departments who a data feeds from a source system and maintain data locally understand the sensitive nature of the data and take measures to secure it. In some cases, the department would gladly not own responsibility for a copy of sensitive data if there were a viable alternative. In other cases, the departments express a need for flexibility in organizing and using the data that can only come from keeping a local copy.

There are two significant security concerns in having multiple, autonomously managed stores of sensitive data on campus:

1. There is increased direct risk of a security incident that inadvertently exposes sensitive data. Without better controls, this risk increases in proportion to the number of local databases that are maintained on campus.
2. System-wide data owners establish access permissions and controls for the data that are maintained by the source systems, SIS, HR, and the CIW. When data is exported from these systems to another database, the access controls on the data are not maintained or even known. This leads to a great deal of inconsistency on data access, where it is up to many individual applications to assert their own type of access controls on the data.

In addition to the security implications of managing multiple, application-centric data stores, there are the campus inefficiencies of needing numerous robust and secure database servers distributed across campus to house the data and a large number of highly distributed, skilled staff to maintain these servers.

A new information architecture must be established with the following goals:

- a. Sensitive data should be transmitted over the network as infrequently and as securely as possible,
- b. The number of copies of any data should be minimized,
- c. The infrastructure for housing data and the staff skilled in managing database systems should be more centralized,
- d. The access controls for data should be retained outside the source systems for the data. That is, Jane Doe accessing SIS sourced data through a departmental application should have the same access rights that Jane Doe would have using SIS. This should be enforced at the data access level and not necessarily by the application.

B. Accomplishments to Date

The System wide security policy initiative is establishing data classification standards and policies and procedures for managing data classified as critical or sensitive¹. This will require that regular risk assessments be performed on systems that house or access data and will place a larger burden on those that manage these systems.

Additionally, the data itself has been “cleaned”, removing unnecessary SSNs from copies of the data where it isn’t explicitly needed.

C. Specific Recommendations

The recommendation is to embrace the direction of the System wide IT Security Office (ITSO) with regard to policies and procedures for data access and management. These will be supported by creating central data services that enforce the policies and procedures through a managed information architecture.

Specifically:

- a. The System ITSO must follow through on data classification policies and procedures and effectively communicate them to the campus,
- b. The System ITSO, in cooperation with the Boulder Campus IT Security Office (within ITS), must enforce policies by assigning accountability for managing data according to policy,
- c. The policies must include not only data owner consent to use data, but data owner specification on access roles and rules regardless of how the data is accessed,
- d. CU-Boulder, working with UMS, should design and document an information architecture that:
- e. Identifies authoritative sources of data,
- f. Establishes acceptable methods and conditions for exporting or otherwise making data available to applications that require it,
- g. Establishes methods for ensuring that access rights established in the source systems are retained even if the data resides external to the source system.

¹ Draft APS 131 requires classification of all information assets. Critical data is defined as being essential to the mission of the university or having life/safety implications, sensitive data is defined as being either protected by state or federal statute or data the university places access restrictions upon.

ITS, in cooperation with UMS, must vastly improve the data services available to CU-Boulder departments. Centrally provided data services should include:

- h. Support and consulting knowledgeable on the data, who owns it, what policies apply, and what options are available to accessing it,
- i. Development and operations of secure data services that implement the information architecture and allow for greater central management and control over sensitive data in order to mitigate security risks. Access to this data will be provided in an efficient and secure manner that supports legitimate downstream business functions.
- j. Continual improvements to central reporting and analytics services so that demand for raw data for these purposes is reduced (along with concern over misinterpretation of data).
- k. Continual improvements to real-time access of data from source systems via Web Services, SQL Queries or a service bus architecture.

A critical success factor is that an inventory of current consumers of data must be taken and we must understand the business processes that result in a need for the data. This is necessary input for the design of the information architecture.

D. Resource Allocation

The resource allocation requirement of the proposed plan is **high**.

The policy and procedure recommendations are underway and require no additional investment.

Developing an information architecture is a significant undertaking that can be done with existing personnel, but only with prioritization that will certainly impact other important campus and system-wide initiatives. It is imperative that UMS assume a leadership role in establishing a scaleable information architecture.

Implementing the architecture through centrally provided data services will require a substantial investment in both infrastructure and skilled personnel.

There will be efficiencies realized by the campus in being able to consolidate database infrastructure and personnel.

It may be that certain tailored data services should be provided under a cost-recovery model.

E. Action Plan (short-term: 12 months; long term: 12-36 months)

Short Term:

- Work with System ITSO to ensure policies and procedures adequately address accountability for data managers and compliance with source system access policies,
- Inventory “shadow” data stores and understand the business need behind them,
- ITS deploy secure managed data services per ITSP section 4.8

Long Term:

- Design, document, and communicate an information architecture,
- Develop a comprehensive set of central data services that incorporates ITS managed data services

Timeline

Summer 2006 – Work with system office on policy and procedure recommendations

Fall/Winter 2006 – Inventory campus data stores

Early 2007 – Design information architecture

Summer/Fall 2007 – Communicate and refine information architecture and implications for central data services.

Summer/Fall 2007 – Specification of central data services

2008 – Development and deployment of central data services

2009 - 2010 – Redesign and update services as necessary for new SIS deployment architecture

On-going – Refinement and update of the information architecture to account for new technologies and changing application needs. Subsequent modifications to central data services.

Primary Person Responsible for Action

Dennis Maloney, Executive Director for ITS

Evaluation of Achievement

Periodic inventory of data usage by campus applications and audit against University policies and procedures and adherence to the information architecture.

Annual audit/assessment of central data services for adherence to policy and architecture.

Customer satisfaction reviews of central data services.

4.1.1 IT Infrastructures for New Applications

Major Issue: Departmental application systems are currently developed and operated in an ad hoc manner, using a variety of technologies and development environments. Students, faculty, staff, and other end users are confronted with a variety of interfaces and differing authentication requirements. Functional, performance, and security testing are typically not part of the software development lifecycle.

A. Background/Rationale

Numerous campus departments, schools and colleges operate applications for use by their staff, faculty, students, and affiliates. These applications are purchased commercially or developed in-house. Typically these applications rely on system data, such as that from SIS and HR, that is stored local to the application. This data is delivered through periodic batch updates to the departmental system which then provides an interface to the user that gives the impression of being “real-time”, though the data may be one to several days old. The interfaces are developed independently and often have no common look-and-feel that would serve to reassure the end user that he/she is accessing a University rather than a departmental service. In addition, the method used to authenticate may differ from that used by central campus applications such as CUConnect, further leading to feeling of an uncoordinated set of online services.

Behind the scenes, the development tools and methods used vary from department to department as do the choice of server platform and the operating environment. Few departments use a structured methodology, using code review along with functional, performance, and security testing to ensure integrity before launching a service. Many put thought and funds into server redundancy but do not provide a secure data center environment protected by uninterruptible power supply and generator. A significant risk to continued operations in such a distributed environment comes from reliance on a single key individual who provides all layers of support necessary to sustain the application.

B. Accomplishments to Date

CUConnect, the portal for students, faculty, and staff, uses a single interface to deliver a variety of applications based on the role of the user. Identity data for CUConnect is retrieved from SIS, HR, and other authoritative sources and blended to create a single, unique identity for an individual; roles for the individual are assigned based on the individual's affiliation(s). The standard for authenticating to CUConnect is the Identikey, which is issued automatically to all students and is available to all faculty, staff, and authorized affiliates. CUAccess provides a unifying authentication service behind the scenes that grants access to web-based applications based on the individual's affiliation and role. ITS is redefining its data architecture and will move to eliminate batch datafeeds as soon as the source SIS and HR systems are capable of a service oriented architecture that will deliver on-demand, real-time data. The ITS development methodology includes attention to quality assurance, such as functional, performance, and security testing throughout the development cycle.

C. Specific Recommendations

The campus should provide access to campus-wide applications through an ITS-managed portal environment. ITS would have the responsibility to:

- a. develop and promote an enterprise architecture that specifies how data is stored and delivered and facilitates gaining permission for use of the data
- b. assess the suitability and supportability of selected applications
- c. serve the application through a common portal interface that grants access based on affiliation which is compliant with campus operating and security standards
- d. develop applications using common toolsets
- e. adopt testing methodologies to ensure systems meet functional, performance, and security requirements
- f. perform regular risk assessments to ensure data integrity and security

Departments that have applications that are specific to their unit and that serve a small number of users should be encouraged to investigate delivering access through the campus portal environment in order to benefit from the common means of authentication and authorization.

As the System office replaces & upgrades the SIS and HR systems, the current batch method of data transfer should be modernized to an on-demand, real-time delivery system using a Service Oriented Architecture (SOA) that can trigger downstream activities.

D. Resource Allocation

Cost of the project: low-to medium overall campus cost; the CUAccess infrastructure is in place and an enterprise architecture is under development. Requests for delivering applications through CUConnect should be evaluated and prioritized based on anticipated utilization and benefit. Additional developer resources may be needed if additional requests are received and/or current backlog continues.

E. Action Plan

Short Term: continue and expand usage of CUConnect and CUAccess

Medium to Long Term: continue campus participation in SIS replacement project; engage with central administration on data delivery enhancements to HR

Timeline:

- Summer 2006 – ITS to update its data, directory, and database architecture
- Ongoing – ITS to continue deployment of CUAccess for common authentication and authorization to web-based applications
- Ongoing – ITS to continue expanding usage of CUConnect by soliciting campus participation and evaluating feasibility for delivering access through CUConnect
- Summer to Fall 2006 – campus to participate in needs assessment for SIS replacement
- 2006-2007 – System office to develop service oriented architecture for Boulder campus that interacts with other data sources including central administration

Primary Persons Responsible

Bobby Schnabel, Vice Provost for Academic & Campus Technology;
Dennis Maloney, Executive Director, ITS; Steve McNally, Associate Vice President

Evaluation of Achievement

Annual review of CUConnect usage; annual survey of students, faculty, and staff regarding desired features.

Annual review by IT Council to determine the most significant, campus-critical applications leading to risk assessment by the IT Security Office.

4.1.2 Central Storage & Services for Sensitive Data

Major Issue: CU-Boulder needs to provide services which allow for the secure storage and provisioning of sensitive data. The availability of this data is critical to second tier business systems and functions. Data must be made available to support secondary business uses, ensure the data is used appropriately, and that the data remains secure at all times. While improving the security of sensitive data is the primary driver, providing centralized services can also result in improved overall efficiency.

A. Background/Rationale

Many departments on campus depend on access to electronic records which contain personally identifiable or otherwise sensitive information in order to provide services to their customers. This data may be generated and maintained locally or it may be pulled from a University primary system, such as SIS or the CIW. In some cases, this data is used to populate shadow databases that are maintained locally within the department, thereby creating additional instances and increasing security risk. Furthermore, at times the original data owner may not be aware of who is using their data or for what purpose, leading to a loss of control.

Departments depend on downstream feeds from SIS, CIW and other sources in order to support critical business functions. Without this data, their ability to provide services to their customers would be greatly impeded. The departments interviewed for this plan had a good understanding of the risk and responsibility that goes with managing sensitive data and were aware of the various policies pertaining to it. In general, they didn't store sensitive information locally unless it was absolutely necessary, and efforts were made to secure the systems on which it resides. Furthermore, most departments recognized that they are accountable for this information and that keeping it secure increased their costs. But since this information is critical to their operations, in the absence of an alternative solution, they had little choice but to maintain it locally.

To reiterate, the majority of the data being considered here is drawn from SIS and the CIW. While most discussion centers on the needs of downstream data users, it is also appropriate to consider the point of view of the data owners. Data owners, such as UMS, put significant effort into maintaining the security and integrity of data in core systems. Yet, they are often not aware or able to control how this data is used.

B. Accomplishments to Date

The SSN remediation project has reduced or eliminated the presence of social security numbers in student and personnel records. The ongoing security awareness campaigns have increased awareness of security concerns and the requirements for protecting personally identifiable information. Security audits initiated by the ITSO or Internal Audit have further raised awareness of the need to protect sensitive data and have exposed vulnerabilities so that they can be addressed.

C. Specific Recommendation

- i. Develop secure data services that allow for greater central management and control over sensitive data in order to mitigate security risks. Provide access to this data in an efficient and secure manner that supports legitimate downstream business functions. Analysis would be performed by the ITS Architecture group so that business data requirements are understood and appropriate services defined. Service would be maintained by ITS Operations.
- ii. Encourage the use of centralized services (database hosting) in order to reduce the occurrence of sensitive data on distributed systems and improve overall security policy compliance.
- iii. Involve data owners in decisions regarding downstream feeds where their data is concerned. Doing so allows for greater involvement and control over how the data is used.
- iv. Address specific business-driven data needs at the source system or as close to it as possible to improve overall data management effectiveness, reduce risk, and improve efficiency.
- v. Enforce standards and best practices for the storage and use of sensitive data in cases where it will be managed locally.

D. Resource Allocation

Cost of the project: The cost of this project would likely be high (in excess of \$80K). This is in effect developing a database hosting service, which requires analysis, development and some investment in hardware and software.

E. Action Plan

Short Term: Formalize the process for requesting and approving of the use of sensitive data to support second tier business functions and ensure ongoing oversight. Develop a service model that improves the campus' ability to secure and control access to sensitive data, while improving the efficiency of its provisioning for appropriate business functions. Long Term: Develop central database hosting service to provide storage for and access to sensitive data to support the University's business needs. To do this effectively will also require performing outreach and offering some form of business analysis service. Establish the funding requirements and determine if service will be supported through the GF or on a cost recovery basis.

Specific Steps:

- Draft a charter for a new service model that satisfies requirements of both downstream data users and the data owners.
- Develop central services to provide access to sensitive data.
- Formalize process for requesting and justifying the need to store or use data that contain personally identifiable or otherwise sensitive data.
- Determine appropriate level at which access/use will be authorized and define process for securing authorization.
 - Authorizations should be for a finite period of time and require renewed justification and authorization beyond that time.

Timeline:

- Spring 2007: draft charter and develop service definitions; define processes for justifying and authorizing access to data feeds.
- Fall 2007: develop services, such as database hosting.

Primary Person Responsible

Bobby Schnabel, Vice Provost for Academic & Campus Technology, for the enforcement of standards, best practices and policy compliance.

Dennis Maloney, Executive Director of Information Technology Services, for developing and maintaining secure data services.

Evaluation of Achievement

Review effectiveness of justification and authorization processes. Determine if the number of instances of sensitive data has been reduced and also if access for legitimate business needs has been preserved or enhanced. Evaluate adoption rate of centralized services and level of satisfaction of downstream data users and data owners. Gauge compliance with policies governing the use and storage of sensitive data as a result of centralizing services.

4.2 Information Technology Disaster Recovery and Business Continuity Planning

Major Issue: CU-Boulder needs consistent and pervasive disaster recovery and business continuity plans for Information Technology (IT) services. Additionally, IT services need to be prepared to facilitate campus-wide business continuity plans.

A. Background/Rationale

With the pervasiveness of information technology on campus, disaster recovery planning (DRP) and business continuity planning (BCP) for IT resources become critical to maintaining overall campus business functions during a disaster. Additionally, recent large-scale disasters at multiple institutions have underscored the role IT can play in enabling campus business continuity.

The UC Boulder campus has strengths in campus-wide disaster planning and business continuity planning for key IT services, but weaknesses in IT infrastructures designed to facilitate business continuity and the pervasiveness of department level disaster planning. The campus requires additional, and more consistent, IT disaster recovery and business continuity planning, and processes to properly handle moderate or major disasters.

B. Accomplishments to date

The UC Boulder campus has significant disaster planning and business continuity efforts headed by the Environment Health and Safety (EHS) department that bring together a number of campus constituents. This includes a standing emergency management operations group (EMOG), campus-wide disaster planning efforts on specific scenarios including large-scale floods and pandemic illness, and campus-wide table-top exercises for specific scenarios. Additionally, EHS provides BCP tools for campus departments.

For core campus IT services, ITS both participates in campus-wide planning efforts and internal planning for disaster recovery and business continuity. This internal work includes business continuity plans for services and annual table-top disaster exercises.

Individual departments have a variety of levels of disaster recovery and business continuity plans. Currently, there is a system-wide draft policy that would require each department to maintain business continuity plans.

C. Specific Recommendations

1. **The campus** will develop and utilize self assessment tools, both internally for ITS and for distribution to departments, including standardized checklists and templates to produce a clear map and census of critical systems, processes, and roles across campus. Plans will be stored both locally and in a central campus repository. Campus leadership will need to express that completing business continuity plans are of import and mandatory.
2. **The campus** will identify external dependencies and contact these entities to clarify expectations and procedures in a disaster or crisis situation.

3. **The campus** will identify additional technical resources which are available as for use during outages or disasters such as central storage services or potential partner institutions who may have usable facilities and services in the event that a CU Boulder building, office, or program is affected.
4. **The campus** will study ways to increase online availability of instructional resources such as classes, library materials, and instructor contact.
5. **The campus** will provide instructional material concerning standards and best practices for hardware, software, connectivity, and security to assist the setup and support of remote access. (telecommuting, distance learning). It is important to note that Telecommuting access must move with services (i.e., if a data store is moved to an offsite location during crisis accommodations must be made for remote access).
6. **The campus** will identify and test means to maintain communication in a crisis situation. Departments will be required to test plans in addition to the existing campus wide disaster planning exercises.

D. Resource Allocation

Recommendation	Existing Staff	New Staff	HW/SW	Vendor/3d Party
1 & 2 Assessment tools, determine external dependency	Training, Deployment, Local Staff (Tier 2)	Trainer	LBL Contingency Planner software, templates, and web site	No
3 Identify technical resources such as centralized storage or identify partner institutions.	Management support, with authority to enter into contractual relationships		HW/Software(?)	Explore third party contractors
4. Increase online instructional resources	Faculty time to plan and transition	Faculty assistance and training	Capacity - By 2007, individual departmental systems may not have backup	Explore vendor hosted services
5. Telecommuting support	Develop best practices	Support	Instructions VPN etc.	ISP
6. Crisis Communication	Website, info, email for parents, news releases, call center in ARC			Consider offsite/third party redundancies for onsite resources, esp. call center.

Cost of the project: TBD

E. Action Plan

Short Term (12 months):

- a. EH&S and the campus IT Security Office will determine specific tools, forms, guidance, and processes to be used by campus departments
- b. EH&S and the campus IT Security Office will develop communications and training
- c. Vice Provost for Academic and Campus Technology (VPACT) and/or Chancellor will encourage departments to evaluate third party services
- d. VPACT sponsors the effort to inventory critical IT resources which would need backup systems in the event of either an IT or physical disaster. The ITSO will provide assistance in this endeavor.
- e. ITS evaluates campus level resources and contracts
- f. VPACT beings discussions with other possible partner institutions to determine feasibility of solution
- g. VPACT documents departmental LMS systems which includes BC/DR posture
- h. ITS completes projects to increase capacity of WebCT
- i. VPACT forms committee to develop policies for Telecommuting and ITS providing supporting technical standards as appropriate.
- j. ITS develops campus-wide mechanisms for individuals to self-subscribe to crisis communication tools

Long Term (12 to 36 months):

- ITS and EH&S to determine mechanism and requirements for campus BCP/DRP archive
- ITSO utilize BCP/DRP data as part of campus risk assessment activities
- EMOG monitor BCP/DRP efforts and assist in BCP/DRP process review.
- ITS implements backup solutions at partner institution or other third party
- Deans encourage faculty to develop on-line class materials
- ITS improves campus VPN services and evaluate VOIP to facilitate telecommuting
- Recognizing that providing IT support to the home is not feasible VPACT and Department Heads reinforce the need for individual accountability and improved technical knowledge for employees who telecommute. Individual campus departments provide more detailed documentation and coaching for employees to facilitate user independence.
- EMOG continue to evaluate campus level crisis communication mechanisms and tools.

Primary Person Responsible

Bobby Schnabel, Vice Provost for Academic & Campus Technology

Evaluation of Achievement

ITSO will prepare an annual evaluation report which will be presented to the VPACT, ITS Executive Director, EMOG, and IT Council. Success will be demonstrated by campus units competing business continuity plans.

4.3 Asset Management & Control for Data & Network

Major Issue: Security strategies must be appropriate to the type of asset to be protected. A "one size fits all" approach will result in security strategies which are either weak or too costly. A prerequisite for the development of both technical and non-technical controls must then be an accurate inventory which captures both the business criticality of the system and the sensitivity of the data.

A. Background/Rationale

Campus Information technology (IT) resources are valuable assets that the Campus has responsibility to manage, secure, protect, and control. IT resources are integral to teaching, research, and public service and must be provided and used efficiently and effectively to support those missions. Sensitive data or personally identifiable information is processed daily on a wide variety of systems by a wide variety of individuals. This means that security solutions will require both address system level controls and procedural controls. The University has established that it will establish a risk based approach as a foundation for security programs.

It is important to note that this section addresses asset management from a security and risk management perspective. Asset management has a broader technical context which is not addressed by this strategy.

B. Accomplishments to date

Campus has established minimum security standards both for networked devices and sensitive data systems since 2004. The data breaches from 2005 highlighted that implementation and enforcement of polices is a fundamental problem however.

Significant work has been completed at the system level, with a high level of involvement by the Campus, on development of a comprehensive suite of security policies based on ISO 17799. It is anticipated that the policies will be approved by Spring 2007.

ITS has completed a framework for completing risk assessments on campus and will be initially deployed with a small number of critical departments during the summer and fall of 2006.

C. Specific Recommendation

- a. Campus departments will inventory information and IT resources which catalogues the, location, and owner, criticality, and sensitivity of information assets. The process will follow guidelines established by the Campus IT Security Office (ITSO).
- b. The ITSO, working with the CU-System Information Security Officer, will establish campus specific processes and implementation guidelines for implementing security controls based on CU system-wide IT Security Policies.

D. Resource Allocation

There will be implications for ITSO staff currently charged with oversight of campus information risk management processes. There will also be significant implications for departments who may not currently have asset inventories and will need to reallocate staff time to complete inventories.

E. Action Plan

Short Term (12 months):

- The ITSO will develop and implement a training program to communicate requirements for asset inventories.
- The ITSO will work with the CU-System Information Security Officer to identify high priority process and implementation guides which need to be developed.
- Campus departments will complete initial inventory of information and IT resources.
- Long Term (12 to 36 months):
- The ITSO, through the risk assessment process, will work with campus departments to determine appropriate controls based on the criticality of the information or IT resource. Departmental level IT asset inventories will form the basis of this effort.
- The ITSO will evaluate options for providing a secure central repository for IT asset inventories.
- Working with the System Information Security Officer ITS will deploy training programs to communicate requirements, process, and guidelines for implementing security controls.

Primary Person Responsible

Bobby Schnabel, Vice Provost for Academic & Campus Technology

Evaluation of Achievement

ITSO will prepare an annual evaluation report which will be presented to the VPACT, ITS Executive Director, EMOG, and IT Council. Success will be demonstrated ability to complete asset inventories, ability to complete risk assessments, and policy compliance.