

ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*

Section I: Project Summary

| | |
|--|--|
| <p>Background and Problem Statement:</p> | <p>In order to protect campus assets, information and reputation, it is important to determine the overall picture of IT compliance with respect to existing laws, regulations and UC policy, as well as to identify existing areas of risk to campus IT assets. Currently, there is no coordinated campuswide program of IT risk assessment to obtain this information, resulting in an unknown level of overall risk and an incomplete understanding compliance. A campuswide program of risk assessment would enable ITS as a consolidated organization to facilitate and participate in the development of a coordinated, well-informed, effective campus security program that is responsive to needs across the campus.</p> |
| <p>Values/Principles:</p> | <p>It is important to protect the security and integrity of university assets and information, both from the perspective of legal compliance and in order to maintain confidentiality, integrity, and availability of information. A risk and compliance assessment of campus IT assets will provide the basis for a coherent campuswide security response that is responsive to identified needs, consistent with campus values and priorities, and balanced against campus resources.</p> |
| <p>Benefits and Return on Investment:</p> | <p>This project develops the tools, distinctions and processes necessary for campuswide risk assessment, including education and response to assessment outcomes. This project also acknowledges that risk assessment is an ongoing component of an overall campus security program and provides for the migration of this project to an ongoing program of campus risk assessment.</p> <p>The initial phase of this project provides the foundation for building an assessment toolkit that will enable the identification of areas of risk and non-compliance with respect to UCSC’s information resources. The benefit of this phase is appropriate planning for and understanding about campus risk and compliance assessment, leading to the creation of an effective assessment toolkit.</p> |
| <p>Approach and Deliverables:</p> | <p>The Risk Assessment Project will utilize a multi-phased approach. The initial phase and first deliverable of this project is to answer the question, “What is assessment and what is its purpose with respect to IT security in higher education?” This answer will explore assessment models, assessment scope options, and an overall statement of purpose for security assessment.</p> <p>Subsequent phases and deliverables include: Success of the overall Risk Assessment Project is defined by:</p> <ul style="list-style-type: none"> • Identification of necessary information, definitions and distinctions for risk assessment • Identification of roles and responsibilities with respect to risk assessment and reporting • Development of an assessment toolkit, including a basic assessment process, campuswide policies and practices as a reference, and identification of available IT services and solutions in support of compliance • Implementation of an assessment • Identification of gaps based on assessment • Development and presentation of recommendations to appropriate governance body for the development or evolution of policies, procedures, practices, and future projects in response to assessment outcomes • Migration to an ongoing campus program of risk assessment |

ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*

| | |
|--|---|
| Scope, Customers, System Users: | The scope of the overall Assessment Project ultimately includes all campus IT users and assets. All IT customers will have defined roles and responsibilities with respect to risk assessment and will be educated with respect to their roles and responsibilities. Campus management will also have additional defined roles and responsibilities with respect to reporting of assessment compliance and results for their units. |
| Sponsor: Project Leader: Project Manager: | Sponsor: Vice Provost of Information Technology, Larry Merkley Leader: Director IT Services, Janine Roeth Manager: Community and Compliance Service Manager, Julie Goldstein |
| Technical Features | The outputs of this project will not be technology, however they may lead to technology solutions in partnership with Security Architecture. |
| Cost/Budget for initial phase: | Approx. \$2600 for training/conferences, plus staff time |
| Completion Date for initial phase: | Start by June 15, 2005; completion by September 30, 2005. |

Approval:

This approval is an authorization to proceed with the project and concurrence with the terms of the project.

Project Leader **Date**

Project Sponsor **Date**

ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*

Section II: Project Detail:

| | |
|--|---|
| Governance Structure: | Initial approval by SMT as part of overall Campus Security Program: July 26, 2005 This project reports to IT Security Committee (ITSC). The ITSC recommends proposed policy to the ITC, which recommends to EVC Kliger for campus approval and mandate. |
| Status Reporting Method and Communication | A written report for the initial phase of this project will be submitted to the project leader on September 30, 2005. Regular progress reports will be presented to ITSC as part of Campus Security Program updates. These reports will include status, results, and budget status, as applicable. |
| Risks: | <p>The risk for the initial phase of this project is minimal since this is entirely a discovery phase. The risk could be considered to be equal to the estimated cost/budget for this phase.</p> <p>With respect to the overall Risk Assessment Project, it is possible that risk and compliance assessment practices will be viewed as a workload issue and as a burden, especially if the assessment is not perceived as having have a useful or supportive outcome. There could be negative consequences if this project results in (the perception of) additional requirements or workload without an associated allocation of resources. There could be negative consequences if this project results in the identification of compliance or security gaps that are not acted upon.</p> |
| Policy implication | <p>There are no policy implications for the initial phase of this project.</p> <p>The overall Risk Assessment Project depends on the existence of a top-level mandate and campuswide policy governing risk assessment, including associated roles and responsibilities for risk assessment and reporting. Policy defining IT customers' roles and responsibilities with respect to risk assessment, along with associated education requirements, will be required. Campus management will also have additional defined roles and responsibilities with respect to reporting of assessment compliance and results for their units. New policy could also be developed as a result of this project if gaps in existing policy are identified. This project will also lead to the development of campuswide security practices in support of risk mitigation and compliance with laws, regulations and UC policy.</p> |
| Performance Criteria: | <p>Success of the initial phase of this project will be an answer to the question, "What is assessment and what is its purpose with respect to IT security in higher education?" This answer will include assessment models, assessment scope options, and an overall statement of purpose for security assessment.</p> <p>Success of the overall Risk Assessment Project is defined by:</p> <ul style="list-style-type: none"> • Identification of necessary information, definitions and distinctions for risk assessment • Identification of roles and responsibilities with respect to risk assessment and reporting • Development of an assessment toolkit, including a basic assessment process, campuswide policies and practices as a reference, and identification of available IT services and solutions in support of compliance • Implementation of an assessment • Identification of gaps based on assessment • Development and presentation of recommendations to appropriate governance body for the development or evolution of policies, procedures, practices, and future projects in response to assessment outcomes |

ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*

| | |
|--|---|
| | <ul style="list-style-type: none">• Migration to an ongoing campus program of risk assessment |
| Dependencies / Key Relationships: | <p>No identified dependencies for the initial phase of this project.</p> <p>Successful completion of the overall Risk Assessment Project is dependent upon a top-town mandate for campuswide policy and procedures governing risk assessment, including responsibilities with respect to IT assets. Successful completion of this project is also dependent upon support from other ITS and campus units for the creation of project team, as necessary for each phase of this project. Other dependencies and key relationships TBD.</p> |
| Project Plan: | See below |
| Name Participants: | Julie Goldstein plus internal and external experts, to be determined. Long-term commitment for project team. |
| Budget: | Approx. \$2600 for training/conferences, plus staff time for the initial phase of this project. TBD for the overall Risk Assessment Project, including possibility of consultant services. |

ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*

PROJECT PLAN

| | |
|---|--|
| Phase 1: Answer the question, “What is assessment and what is its purpose with respect to IT security in higher education?” | |
| Resources: | \$2600 (conference attendance) plus staff time |
| Milestones & Tasks: | <ul style="list-style-type: none"> • Attend UC Davis IT Security Symposium, June 22-24, 2005 • Attend Burton Group Catalyst Conference, July 11-15, 2005 • Attend UCCSC Security Track, August 6-9, 2005 • Complete review of recommended resources on Burton Group website and other sources; Explore assessment models • Compile information from resources and conferences to answer Phase 1 question. • Develop an overall statement of purpose for risk and compliance assessment • Present report to Janine. |
| Timeline: | Report by Sept 30, 2005 |
| | |
| Phase 2: Identification of necessary information, definitions and distinctions for risk assessment | |
| Resources: | Commitment of project team, plus staff time Possibly hire a consultant for BIA or IPPA |
| Milestones: | <ul style="list-style-type: none"> • Assemble risk assessment project team • Verify executive mandate for risk assessment • Conduct BIA or IPPA to establish priorities for risk assessment <ul style="list-style-type: none"> ○ May involve a consultant • Identify scope models for risk assessment, including identification of classifications for campus IT assets, if appropriate |
| Timeline: | October 2005 – June 2006 |
| | |
| Phase 3: Identification of roles and responsibilities with respect to risk assessment and reporting | |
| Resources: | Project team, plus staff time |
| Milestones: | <ul style="list-style-type: none"> • Verify top-down mandate for roles and responsibilities with respect to risk assessment • Identify roles and responsibilities for risk assessment and reporting • Develop and provide associated communication and education for clients and management |
| Timeline: | October 2005 – June 2006 |
| | |
| Phase 4: Development of an assessment toolkit, including a basic assessment process, campuswide policies and practices as a reference, and identification of available IT services and solutions in support of compliance | |
| Resources: | Project team, plus staff time |
| Milestones: | <ul style="list-style-type: none"> • Develop a set of steps for a general assessment process • Compile campus policies and practices against which to measure compliance activities <p style="margin-left: 20px;">Note: This milestone is based on the output of two other Campus Security Program projects:</p> <ul style="list-style-type: none"> - Identify and document existing, generally-accepted UCSC IT security practices, and assess appropriateness/desirability; Compile recommended set of IT security practices for UCSC based on this assessment. - Map existing IT security practices to IS-3 and identify gaps; Identify projects to address gaps • Identify and package available IT services and solutions in support of compliance • Package risk assessment toolkit |
| Timeline: | June 2006 – December 2006 |

ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*



ITS Project Charter

Campus Security Program Project

Project Title: *Risk Assessment*

| | |
|---|---|
| Phase 5: Implementation of an assessment | |
| Resources: | Project team, OPM for communications, Staff time |
| Milestones: | <ul style="list-style-type: none"> • Determine scope and staging for risk assessment • Develop, get approval for and send out campus communications for risk assessment, including scope, process, assessment and reporting requirements, resources, timeline • Verify/document completion of risk assessment |
| Timeline: | January 2007 – June 2007 |
| Phase 6: Identification of gaps based on assessment | |
| Resources: | Project team, plus staff time |
| Milestones & Tasks: | <ul style="list-style-type: none"> • Compare assessment findings with campus practices • Create report of findings and recommendations <ul style="list-style-type: none"> ○ Identify and document gaps ○ Recommend compliance activities to address gaps |
| Timeline: | June 2007 – September 2007 |
| Phase 7: Development and presentation of recommendations to appropriate governance body for the development or evolution of policies, procedures, practices, and future projects in response to assessment outcomes | |
| Resources: | Project team, plus staff time |
| Milestones: | <ul style="list-style-type: none"> • Develop recommendations for the evolution of policies, procedures, practices in response to assessment outcomes • Develop recommendations for future projects in response to assessment outcomes <ul style="list-style-type: none"> ○ Including recommendations for IT services in support of compliance • Develop report for IT governance • Present recommendations to IT governance |
| Timeline: | September 2007 – March 30, 2007 |
| Phase 8: Migrate to an ongoing campus program of risk assessment | |
| Resources: | Project team, plus staff time |
| Milestones: | Establish and publish guidelines for regular updates of risk and compliance assessment |
| Timeline: | March 2008 – June 2008 |