UTech Services
Compliance, Auditing, Risk, and Security (CARS)
Team Charter

Version [1.0]
1/29/2013
Revision History

This document is controlled and tracked through the use of the following table. Versioning is updated in accordance with amount of change being made: for small modifications, a point increase is made (ex: version 1.0 to 1.1); for a significant content update, a whole number increase is made (ex: version 1.1 to 2.0).

<table>
<thead>
<tr>
<th>Version #</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>10/12/2012</td>
<td>DMC</td>
<td>Draft</td>
</tr>
<tr>
<td>1.0</td>
<td>1/29/2013</td>
<td>DMC</td>
<td>Approved by Cabinet</td>
</tr>
</tbody>
</table>
# Table of Contents

Purpose ................................................................................................................................................................. 4  
Stakeholders ......................................................................................................................................................... 4  
Charter Owner ...................................................................................................................................................... 4  
Charter Description ............................................................................................................................................... 4  
  Vision ................................................................................................................................................................ 4  
  Mission .............................................................................................................................................................. 4  
  Motivation ........................................................................................................................................................ 5  
  Goals ................................................................................................................................................................. 5  
  Objectives ....................................................................................................................................................... 5  
  Scope ............................................................................................................................................................... 5  
Proposed Strategy ................................................................................................................................................. 6  
Operating Procedures ........................................................................................................................................... 6  
  Team Composition ............................................................................................................................................ 6  
  Team Leader ..................................................................................................................................................... 6  
  Meetings ........................................................................................................................................................... 6  
  Communication Plan ......................................................................................................................................... 7  
  Decision Making ............................................................................................................................................... 7  
  Conflict Resolution .......................................................................................................................................... 7  
  Closeout Criteria .............................................................................................................................................. 7  
  Performance Evaluation ................................................................................................................................... 7  
Approved by: ......................................................................................................................................................... 7  
Appendices [optional] ........................................................................................................................................... 8  
  Timeline ............................................................................................................................................................ 8  
  Supporting Documentation ............................................................................................................................... 8  
  Acronyms/Definitions ...................................................................................................................................... 8
Purpose
This document presents the philosophy of Compliance, Auditing, Risk, and Security (CARS) within California University of Pennsylvania and represents the endorsement of California University of Pennsylvania’s executive management team. It identifies the motivation for CARS, describes information security principles and terms, and defines the scope of policies and responsibilities of the various CARS functions.

Stakeholders

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>All users including faculty, staff, students, contractors and guest users of California University of Pennsylvania.</td>
<td>Every computer user is responsible for securing and protecting the information technology resources and data over which he or she has control. In addition, you are to comply with all California University of Pennsylvania Policies and Procedures.</td>
</tr>
<tr>
<td>Cabinet</td>
<td>Cabinet is accountable for compliance, risk, and security and must ensure compliance with policies, standards, procedures and practices within their respective areas of responsibility.</td>
</tr>
<tr>
<td>Information Security Leadership (Vice President of Information Technology and CARS)</td>
<td>Information Security Leadership is responsible for determining methods of implementing and enforcing security policies and for advising the enterprise on security-related issues. The leader ensures, in particular, that information security awareness is increased, and audits are performed and reported regularly. The leader appoints and manages suitably skilled people to staff information security teams as deemed appropriate, and the leader has the authority to request the appointment of security representatives in business units.</td>
</tr>
</tbody>
</table>

Charter Owner
UTech CARS Team

Charter Description
Vision
The CARS Office coordinates and supports the University community’s efforts to mitigate risk associated with the security of Information and Information Systems from unauthorized access, disclosure and disruption.

Mission
California University of Pennsylvania recognizes that information and IT assets are critical business assets. It is the responsibility of all users to ensure the safe-guarding of business assets. California
University of Pennsylvania implemented, maintains and monitors a comprehensive enterprise Compliance, Auditing, Risk, and Security program in order to:

i. Ensure the ability of California University of Pennsylvania to grow and fulfill its mission in the face of an ever changing risk environment.
ii. Enhance the University experience for students, faculty and staff by facilitating a more secure computing environment.
iii. Ensure that all applicable regulations regarding the privacy and security of data are followed.
iv. Collaborate with University data owners and leadership to understand current and emerging needs regarding information security, licensing, and IT asset management.
v. Educate the Cal U community concerning IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies in order to support leadership decisions.

Motivation

California University of Pennsylvania values the ability to openly communicate and share information. California University of Pennsylvania information (whether belonging to California University of Pennsylvania or held in trust on behalf of its clients and business partners) is an important asset that shall be protected according to its value and the degree of damage that could result from its misuse, unavailability, destruction, unauthorized disclosure or modification. Improper disclosure or destruction of these assets may result in harm to the business. Information assets are identified, valued, assessed for risk and protected as appropriate to the needs and risks of the business. Users are required to abide by this Compliance, Auditing, Risk and Security (CARS) Charter and subsequent policies and procedures.

Goals

Information security is a risk management discipline addressing the preservation of information confidentiality, integrity and availability. The information security effort is established via a hierarchical set of policies and procedures that help users and administrators to define and mitigate risks, maintaining a trade-off between information value and cost of risk mitigation. Policies are high-level documents used to put information security principles into practice. Procedures are a series of related activities aimed at achieving a set of objectives in a measurable and repeatable manner.

Objectives

I. Risk Management activities provide a structured process of identifying, assessing, and taking steps to reduce risk to what the organization deems to be an acceptable level in a cost-effective manner.
II. Information security policies, standards, guidelines and procedures are developed to communicate security requirements and guide the selection and implementation of security control measures.
III. Personal accountability and responsibility for information security are incorporated in roles and responsibilities that ensure that every individual applies the applicable information security policies, principles, procedures and practices in their daily work-related activities.
IV. Information security education, training and awareness programs ensure that users are aware of security threats and concerns and are equipped to apply organizational security policies and principles.

V. Incident response ensures that proper methods for handling IT Security incidents are followed.

VI. Legal, regulatory and contractual requirements are identified, documented and followed.

Scope

It is intended that information is protected in whatever form, including, but not limited to, paper documents, electronic data and the spoken word. Information should be protected while at rest and when it is handled, transmitted or conveyed. IT assets include all devices and hardware/software components of the IT infrastructure, applications and data stores.

Proposed Strategy

Every user of California University of Pennsylvania’s information systems resources is responsible for protecting the confidentiality, availability and integrity of the University's information assets. The Information Security Strategy supports and coordinates our University community's efforts to secure Information and Information Systems from unauthorized access, disclosure and disruption by providing the following services:

I. Policy/Standard/Procedure/Guideline Development – ensures that the University community has a standard methodology for IT security.

II. Risk Management - is the process of identifying, assessing, and taking steps to reduce risk to what the organization deems to be an acceptable level in a cost-effective manner.

III. Compliance - assists the University in maintaining a compliant reputation with regulatory bodies.

IV. Security Awareness and Education - recognizes the importance of the human aspect of IT security.

V. Incident Response - ensures that the proper methods for handling IT security incidents are followed.

VI. IT Security Consulting - ensures that the University user community has access to the information it needs to establish a secure IT environment.

Operating Procedures

Team Composition

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Area of Expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charles Mance</td>
<td>Vice President of Information Technology</td>
</tr>
<tr>
<td>Dennis Carson</td>
<td>Auditing, Risk, Security, Policies</td>
</tr>
<tr>
<td>Kerry Clipper</td>
<td>Compliance, Contracts, Licensing, Asset Management, Auditing</td>
</tr>
</tbody>
</table>

Team Leader

Dennis Carson

Meetings

Formal Meetings will be held once a month in the UTech Services Conference Room.
Communication Plan
Email will be used to communicate developments. Updates will be provided quarterly in UTech Department Meetings. Communication to the campus community will be provided as needed.

Decision Making
Consultative input gathering will be used for decision making. This is when you ask for input from the group but make the final decision yourself. If CARS is unable to make a decision, it will be escalated to the Vice President of Information Technology.

Conflict Resolution
Collaborating will be the conflict resolution style. This is an attempt to find a solution that satisfies the needs of both parties. If CARS is unable to resolve conflict, it will be escalated to the Vice President of Information Technology.

Closeout Criteria
This is a permanent team.

Performance Evaluation
Metrics will be developed and used to evaluate performance annually.

Approved by: Cabinet 1-29-2013
Appendices \textit{optional}

**Timeline**
Not Applicable

**Supporting Documentation**
Not Applicable

**Acronyms/Definitions**
CARS – Compliance, Auditing, Risk, and Security