Information Resources & Communications

About IR&C | Services | Resources | What's New | Search | Home

IT Risk Assessment

Departments whose units handle or manage information assets or electronic resources should conduct formal risk assessments. A risk assessment is a process by which **to determine what information resources exist that require protection**, and **to understand and document potential risks from IT security failures** that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is **to help management create appropriate strategies and controls for stewardship of information assets**.

Protect Information Assets

Protect Restricted Data

Report Security Incidents

Secure Your Computer

Unsafe Practices

UCOP Policies

Universitywide Policies

IR&C Security Initiative

Support Contacts

About This Site

Security Web Home

The Successful Risk Assessment

Successful risk assessments require full support of senior management and must be conducted by teams that include both functional managers and information technology administrators. As business operations, workflow, or technologies change, periodic reviews must be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes, and to determine the effectiveness of existing controls. (See ECAR, "Information Technology Security: Governance, Strategy, and Practice in Higher Education," vol. 5, 2003, p. 87.)

The risk assessment tool provided here may be used to identify assets as well as the risks to those assets, to estimate the likelihood of security failures, and to identify appropriate controls for protecting assets and resources. Management should evaluate the outcome of the risk assessment to prioritize solutions for potential problems, taking into account the severity of likely ramifications and the expense of implementing cost-effective and reasonable safeguards or controls.

Please note that the UC Information Security Program requires risk assessments of all functional areas that handle loan information, as described in the program.

Components of a Risk Assessment

Risk Assessment Methodology Overview

UCOP Risk Assessment

Risk Assessment Tool

Resources

Please submit your questions, comments, and suggestions at feedback.html
Last updated: January 31, 2005

Information Resources & Communications

About IR&C | Services | Resources | What's New | Search | Home

Components of a Risk Assessment

Administrative Safeguards

These include, but are not limited to, those control measures that ensure

classification of data handled by the unit and determination of controls to protect those assets;

documentation of procedures, standards, and recommended practices to ensure that applicable policies and controls are implemented appropriately for a given business process;

identification of personnel who are authorized to access systems;

assurance that appropriate authorization controls are implemented;

security awareness training and education for all personnel; and

background checks prior to the selection and hiring of new personnel into critical positions.

Logical Safeguards

These encompass the range of technical controls that

ensure access by only authorized users and session termination when finished;

enforce secure password management;

manage tracking of development, maintenance, and changes to application software and information systems;

manage access to the network; and

ensure event logging.

Physical Safeguards

These protect physical resources through controls that

allow access by only authorized individuals, through the use of physical means, such as locks, badge readers, or access cards;

ensure the prevention, detection, early warning of and recovery from emergency disruptions, such as flooding, power failures, or earthquakes; and

govern the receipt and removal of hardware and electronic media, including equipment reassignment, and final disposition of equipment.

Please submit your questions, comments, and suggestions at feedback.html
Last updated: August 18, 2004

Information Resources & Communications

About IR&C | Services | Resources | What's New | Search | Home

Risk Assessment Methodology Overview

Many different approaches to risk assessment have been developed. These following guidelines provide a simple step-by-step process. Additional resources and methodologies are linked under Resources to help you establish an approach appropriate to your business environment.

General Guidelines for a Risk Assessment

Establish the risk assessment team. The risk assessment team will be responsible for the collection, analysis, and reporting of the assessment results to management. It is important that all aspects of the activity work flow be represented on the team, including human resources, administrative processes, automated systems, and physical security.

Set the scope of the project . The assessment team should identify at the outset the objective of the assessment project, department, or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed, and operations to be observed.

Identify assets covered by the assessment. Assets may include, but are not limited to, personnel, hardware, software, data (including classification of sensitivity and criticality), facilities, and current controls that safeguard those assets. It is key to identify all assets associated with the assessment project determined in the scope.

Categorize potential losses. Identify the losses that could result from any type of damage to an asset. Losses may result from physical damage, denial of service, modification, unauthorized access, or disclosure. Losses may be intangible, such as the loss of the organizations' credibility.

Identify threats and vulnerabilities. A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Include natural threats, accidental threats, human accidental threats, and human malicious threats. These could include power failure, biological contamination or hazardous chemical spills, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism. A vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc.

Identify existing controls. Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

Analyze the data. In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to analyze data includes preparing a list of assets and showing corresponding threats, type of loss, and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

Determine cost-effective safeguards. Include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle of the safeguard.

Report. The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read, and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your organization. The report should include findings; a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

Please submit your questions, comments, and suggestions at feedback.html
Last updated: August 18, 2004

Information Resources & Communications

About IR&C | Services | Resources | What's New | Search | Home

UCOP Risk Assessment

The Office of the President conducted a risk assessment of the security controls for protected information subject to the Gramm-Leach-Bliley (G-L-B) Safeguarding Rule.* The analysis included evaluation of risks for both electronic and paper-based applications.

UCOP Risk Assessment Methodology

Identification of department/function to be reviewed

Determination of processes through which the assets pass

Identification of the procedure or storage action taken on each asset

Identification of the risks associated with the procedures or storage actions, or with the destruction of data prior to disposal of equipment

Identification of the control activities

Evaluation of the effectiveness of the controls

Identification of corrective actions

The risk assessment tool provided here may be adapted as required.

*For more information on this assessment, contact either Karl Heins, director of IT Audit Services, or Dan Sampson, director of Financial Control & Accountability.

Please submit your questions, comments, and suggestions at feedback.html
Last updated: August 18, 2004

University of California
Department or Function Under Review[1]
Risk Assessment Tool – Controls over Security of Protected Information

PROGRAM PROCESS OR ACTION[2]	*PROCEDURE AND/OR STORAGE ACTION[3]*	*RISKS[4]*	*EXAMPLE OF CURRENT CONTROL ACTIVITIES[5]*	*CONTROLS ADEQUATE, IN PLACE, EFFECTIVE?[6]*	*ACTION REQUIRED WHEN AND BY WHOM[7]*
General description of the program, process or business practice under review. Separate action steps that could expose the process to various types of risk should be described in individual rows.	Description of the types of information stored, level of sensitivity, how the information is stored (pc, laptop, paper, file cabinet, etc), who has access.	What could go wrong? What would be the impact to the University? Where is the University vulnerable? How could this information be compromised?	Description of control activities currently in place to mitigate the potential risks.	Assessment by people involved in the business process as to whether the business practice, procedures, risks and current control activities are accurately and completely described in this document. Typically a Yes or No answer.	If control improvements need to be made, document what will be accomplished, by whom and when.