

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2008, Issue 6

March 18, 2008

Managing IT Risk in Higher Education: A Methodology

Ian Waters, University of Technology, Sydney



Overview

Sometimes it seems as if information technology (IT) in higher education is all about risk and security. This is because risk-taking is involved in everything we do, and also often in what we decide not to do. One of America's most successful military leaders, General George S. Patton, once gave this advice: "Take calculated risks. That is quite different from being rash."¹ The qualification "calculated" provides the key to his recommendation.

What is security? The Wikipedia definition is "the condition of being protected against danger or loss." That absolute state is often unattainable, or at least impractical even with unlimited resources, and security must often represent some compromise. Security can be more realistically defined as "the state of being free from unacceptable risk."

What is risk? A good higher education definition comes from Texas A&M University: "Any event or action that adversely impacts the university's ability to achieve its objectives."² It is noted that this risk definition is very broad in scope.

By what means do we reach our secure state, free of unacceptable risk? One solution is to employ a risk assessment methodology. The University of Technology, Sydney (UTS) in Australia assessed the risk of all its major business applications and IT infrastructure resources. This research bulletin describes the background, the methodology, the implementation, and the outcomes of this institutionally inclusive risk assessment, which, despite limited resources, yielded valuable results that can be applied in other higher education institutions.

Highlights of Managing IT Risk

Information is an asset that has considerable value to an institution. The objective of IT security is to protect information by maintaining its confidentiality, integrity, availability, accountability, authenticity, and reliability.

An IT security program serves to protect this information asset from a wide range of threats in order to ensure the continuity of the key business processes of the institution. The core processes of an IT security program as identified by Proctor and Byrnes³ and adopted at UTS are

- Policy definition—the policies required and the contents of those policies;
- Risk assessment and data classification—how risk assessments are to be performed and how data are to be classified for security;
- User administration—the procedures required for registering users and giving them access to services; and
- Technical planning, design, and implementation—the level of security oversight for IT projects.

The Proctor and Byrnes core processes, as practiced at UTS, may be interpreted as described below.

Security policies are defined in response to an identified business need. Any new or changed security policy may generate a requirement that becomes a security project to achieve compliance with the new policy.

UTS has been developing and refining its IT security policies and procedures for over seven years. There are two major directives related solely to IT security: IT security policy, and IT security standards and guidelines. The IT security policy sets the context for IT security within the university. It provides a set of principles that gives guidance for the security of information and a high-level statement of controls to protect institutional information. The IT security standards and guidelines are derived from these principles. They provide the detailed procedures, measures, and controls to assist users and system custodians in meeting their IT security responsibilities.

The security standards and guidelines are based on the Australian and International Standard for information security management AS/NZS ISO/IEC 17799⁴ (Standards Australia 2006) and the *Australian Government Information and Communications Technology Security Manual*⁵ tailored for the environment at UTS.

Risk Management and Assessment Methodology

Risk management refers to a systematic method of identifying, analyzing, evaluating, mitigating, monitoring, and communicating risks associated with activities, functions, or processes in order to minimize losses. The purpose of risk management is analysis of the business risks of a process, application, system, or other asset to determine the most prudent method for its safe operation. Risk assessment and management are intended to provide an assurance that the security measures selected are commensurate with the security risks involved.

Risk assessment is the process of identifying risks to mission, functions, image, reputation, operations, assets, or individuals by determining the likelihood of occurrence, the expected impact, and the appropriate security controls to mitigate that impact. The risk assessment process determines the appropriate level of security. It identifies current threats and vulnerabilities, the current level of risk, the desired risk level, and the action required to progress towards this desired level.

A risk assessment may be undertaken

- to determine effective security policy and controls;
- when new systems or applications are introduced;
- as part of change-control procedures to reassess the risk associated with the change; or
- periodically to ascertain whether the risk environment has changed.

The UTS methodology has been adapted from one previously used by the Australian government and documented in a former edition of the *Australian Government Information and Communications Technology Security Manual*.

Identify Assets. The first step in the risk assessment process is to identify assets. An asset is anything that requires protection. It can be a tangible quantity (such as hardware), a service, staff, or information.

Identify Threats. The next step involves identifying the nature of individual threats, their sources, and the probabilities of occurrence. There can be multiple threats associated with one asset. A threat source is any circumstance or event with the potential to cause harm. The three main categories of threat sources are natural (such as a flood), human (such as hacking), and environmental (air conditioning, for example).

Measure Threat Likelihood. Information on the probability of external threats can be derived in quantitative form from crime reports, IT security surveys, and other means. The likelihood of internal threats may not be so readily ascertained, but it can be anticipated from previous experience, statistical information, or estimation. Using a semi-quantitative method, UTS uses the threat likelihood rating below as a basis for categorizing the threat probability or likelihood:

Negligible: Unlikely to occur

Very Low: Likely to occur two to three times every five years

Low: Likely to occur once every year

Medium: Likely to occur once every six months

High: Likely to occur once per month

Very High: Likely to occur multiple times per month

Extreme: Likely to occur multiple times per day

Define Consequence or Impact. The consequence or impact caused to the system as a result of the loss or compromise of an asset will vary with the nature of the asset. UTS uses the following consequence definitions in developing a security risk assessment:

Insignificant: Will have almost no impact if threat is realized.

Minor: Will have some minor effect on the asset value, but will not require any extra effort to repair or reconfigure the system.

Significant: Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals. Will require some expenditure of resources to repair.

Damaging: May cause damage to the reputation of system management and/or notable loss of confidence in the system's resources or services. Will require expenditure of significant resources to repair.

Serious: May cause extended system outage and/or loss of connected customers or business confidence. May result in compromise of large amounts of university information or services.

Grave: May cause system to be permanently closed and/or be subsumed by another (secure) environment. May result in complete compromise of university services.

Compare Current Risk and Required Risk. The current level of risk can be expressed mathematically as risk = threat likelihood x consequence.

The required risk is the desired risk level, as set by the owner of the system. It is the risk level that management is prepared to accept. Using the threat likelihood and consequence defined earlier, Table 1 illustrates how UTS derives the risk level.

Table 1. UTS Resultant Risk, by Likelihood and Consequence

		Consequence					
		Insignificant	Minor	Significant	Damaging	Serious	Grave
Likelihood	Negligible	Nil	Nil	Nil	Nil	Nil	Nil
	Very Low	Nil	Low	Low	Low	Medium	Medium
	Low	Nil	Low	Medium	Medium	High	High
	Medium	Nil	Low	Medium	High	High	Critical
	High	Nil	Medium	High	High	Critical	Extreme
	Very High	Nil	Medium	High	Critical	Extreme	Extreme
	Extreme	Nil	Medium	High	Critical	Extreme	Extreme

Risk Treatment Priority Rating. The outcomes of the risk assessment are used to provide guidance on the areas of highest risk. It is useful to determine a risk treatment *priority* rating. This rating is the gap between the required risk and the current risk. Priorities are assigned at UTS as follows:

- A. Where the required risk is less than the current risk by more than one risk level (e.g. low vs. high)
- B. Where the required risk is less than the current risk by one risk level (e.g. low vs. medium)
- C. Where the required risk is the same as the current risk
- D. Where the required risk is greater than the current risk (e.g. medium vs. low)

Treatments for Risk Mitigation. The final step in the process is to identify specific treatments for risk mitigation. The results of the risk assessment should be used to test the appropriateness of these measures and identify requirements for new treatments. A subsequent assessment of the residual risk following deployment of identified treatments forms the basis of management decision-making and endorsement. These decisions,

together with an implementation schedule, become the Risk Management Plan and are then documented in a System Security Plan.

The priority of the treatments may result in one of the following outcomes:

- Addition of security measures
- Reduction of security measures
- Risk avoidance through change of service and system specifications
- Acceptance of residual risk
- Minimization of harm through response mechanisms

A risk assessment is not a one-off process that is completed and forgotten. Rather, it is an iterative process that should be reviewed regularly to take into account changes in the value of assets, new threats, and changes to security measures.

UTS Approach to Enterprise-Wide Risk Analysis

The university has in place an enterprise-wide risk management process to identify and implement strategies to provide reasonable assurance that UTS is able to achieve its objectives. The management of risks is integrated and coordinated at the executive management level across the institution.

The UTS IT Security Program requires that a risk assessment be performed on all major IT systems and infrastructure resources. The approach is top-down, involving a high-level risk assessment of all systems, followed by identification of systems that require a more detailed risk assessment. This approach conforms to the “highly recommended risk analysis option for the majority of organizations” given in the Australian Standard AS 13335.2 Guidelines for the Management of IT Security.⁶

With the facilitation of the UTS IT Governance and Compliance Office, the methodology described above has been used across the university for high-level risk assessments. This process involved identification of the assets (that is, which major business applications, IT systems, and infrastructure resources need to be protected), an overall assessment of threats and the likelihood of these threats, and an assessment of the consequence or harm that would result from the loss or compromise of the system or resource. The standard definitions of threat likelihood and consequence were used in these assessments. Then a resultant risk for the system or resource was determined (again using the standardized measure), as well as an agreed required risk for the system/resource. A gap analysis of current versus required risk was then performed to determine the priority for a more detailed risk assessment, and then for the development of risk mitigation strategies.

The risk assessment methodology was first applied to all IT systems and resources for which the UTS central Information Technology Division (ITD) was the custodian. This process resulted in the identification of 33 major IT systems and resources and the application of the methodology to these. This pilot demonstrated that the methodology

could be employed relatively easily and was capable of prioritizing the systems and resources in preparation for a more detailed risk assessment.

A new student system was selected for the prototype of a detailed risk assessment using the same methodology. This assessment was initially performed on the system's components for which ITD was responsible. This was a significant test of the methodology, since the project involved replacement of a UTS-developed application with a package solution—a complex system with an even more complex technical architecture. The project involved many staff in the IT and registrar's divisions. Again, this prototype of the methodology was successful.

Following this, a high-level IT risk assessment was performed for the major systems and resources of all academic areas. Again facilitated by the IT Governance and Compliance Office, this process involved the departmental IT managers and technical staff, as well as department administrative managers whenever they wished to be involved.

Then all administrative unit directors were requested to nominate either themselves or a member of their staff as the liaison for the high-level risk assessment of their systems and resources. These risk assessments were performed in two stages, first for those units with service level agreements with ITD, and then for the remainder. Each academic department and administrative unit high-level risk assessment session occupied approximately one hour, with the IT Governance and Compliance Office responsible for facilitating the process and documenting the results.

The risk assessment process identified a total of 211 major systems and resources in use across the university. Of these, 48 were assessed at the highest priority—Priority A—which is where the current risk posed by the system or resource exceeds the required risk by two or more risk levels. Following the high-level risk assessment exercise, detailed risk assessments of the highest priority systems have been carried out. To date, over 28 of these have been completed.

The detailed risk assessment stage involves the division of each high-priority system or resource into its core components, conducting risk assessment workshops on each of these components, developing risk mitigation strategies, and then preparing risk management plans. This process involves IT managers and key technical and administrative staff, again facilitated by the IT Governance and Compliance Office. The final stage for each system involves documentation of the process followed, together with its results, in IT System Security Plans.

Resources Required for Risk Assessments

As a result of its risk management and risk assessment program, UTS identified that the following resources were required for risk assessments.

For high-level risk assessments: Total resources included one facilitator, one hour-long meeting, and two hours to document and confirm results—in 34 areas for a total of 102 hours for facilitator and 68 hours for participants (with an average attendance of two per area). Total: Approximately 170 person-hours or 24 person-days.

For detailed risk assessments: For forecasting purposes, systems were divided into three classes—simple, medium, and complex. From experience gained with the initial high-level and detailed risk assessments, an estimate of the number of personnel and their time involvement was derived as follows:

Simple system: 21 person-hours, or 3 person-days

Medium system: 83 person-hours, or 12 person-days

Complex system: 191 person-hours, or 27 person-days

The number of team members involved in the individual detailed risk assessment workshops varied from 1 to 6.

What It Means to Higher Education

The risk assessment process has two main objectives: to implement reasonable safeguards, and to document management's due diligence in mitigating risks. The inherent complexity of most systems, and in particular of large enterprise-wide applications, makes their risk assessment a time-consuming process.

Attention must be given to defining the scope of what is to be assessed and understanding its underlying architecture, to permit risks to be assessed thoroughly for all logical components. It is also important to determine precise boundaries and not to overlap components of systems being reviewed, so as to avoid duplication of effort. For example, the network, which is common to most systems, is only addressed in an individual system risk assessment with regard to those network components that are particular to the system.

It is also important to take time to precisely define what is meant by each threat that is identified. This understanding is required so that agreement can be more readily reached on its likelihood and consequence. Also, when the threat is revisited for determination of risk mitigation action and then later in reviews of the risk management plan, an exact definition is required to avoid erroneous reinterpretation.

There is theoretically an infinite set of possible risks. The risk assessment process permits prioritization of the potentially very large number of actions that could be taken to improve security. For a new system, it gives management (and the auditors) some confidence that the risks associated with introduction of the system have been considered and addressed before the system goes live.

As with many other IT activities, senior management buy-in is critical for success. High visibility and regular reporting of progress are essential. The university-wide IT risk assessment approach used at UTS, along with the results, have been validated by an internal audit review of IT security management at the university.

At UTS, the steps involved in the risk assessment process were constrained by severely limited budgets. Thus the depth of the detailed risk assessments was often defined by the resources available. In these cases, it is preferable to settle for a lower level of detail

so as to be able to conclude the exercise, rather than attempting something that is unrealistic and incapable of timely completion. It is also important that the risk assessment process be easy to describe and implement. The U.S. Government Accountability Office has found by way of a survey that organizations that were most satisfied with their risk management procedures used a relatively simple process.⁷

Key Questions to Ask

- Has our institution adopted a standardized approach to risk assessment?
- In what ways is executive-level support for this risk assessment approach expressed?
- Do we have an inventory of all critical systems and IT resources across the organization?
- To what degree is our risk assessment methodology based on metrics that can determine which of our multiple systems and IT resources present the greatest risk to the institution?
- What mechanisms are in place to prioritize the many actions that could be taken to mitigate risk?

Where to Learn More

- Cassidy, Dale, Larry Goldstein, Sandra L. Johnson, John A. Mattie, and James E. Morley, Jr. "Developing a Strategy to Manage Enterprisewide Risk in Higher Education." NACUBO and PriceWaterhouseCoopers, 2003. http://www.pwc.com/gx/eng/about/ind/edu/risk_mgt_white_paper_2003.pdf.
- Davis, Brian. "U.Va.'s IT Security Risk Management Program." University of Virginia, 2004. http://www.itc.virginia.edu/security/riskmanagement/docs/ITS-RM_LSP_Apr2004.ppt.
- EDUCAUSE/Internet2 Security Task Force. "Risk Assessment Framework." 2006. <http://www.educause.edu/LibraryDetailPage/666?ID=CSD4380>.
- Jones, Andy, and Debi Ashenden. *Risk Management for Computer Security*. Jordan Hill: Elsevier Butterworth-Heinemann, 2005.
- Jopeck, Edward. "The Risk Assessment: Five Steps to Better Risk Management Decisions." *Security Awareness Bulletin*, no. 3-97. Richmond: Department of Defense Security Institute, 1997. <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=A330033&Location=U2&doc=GetTRDoc.pdf>.
- Knudsen, Kent, and Jeff McCabe. "Centralizing IT Risk Assessment and Measuring Security Policy Compliance." Paper presented at EDUCAUSE 2004, Denver, CO, October 20, 2004. <http://www.educause.edu/ir/library/powerpoint/EDU0460.pps>.

- Peltier, Thomas. *Information Security Risk Analysis*, 2nd ed. Boca Raton: Auerbach, 2005.
- Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *NIST SP 800-30 Risk Management Guide for Information Technology Systems*. Gaithersburg: National Institute of Standards and Technology, 2002.
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
- Waters, Ian. "How Secure is the Network? Assessing Network Risk Using a Formal Methodology." Paper presented at QUESTnet 2005, Coolum, Australia, July 6, 2005.
http://www.questnet.net.au/questnet2005/papers/ian_Waters.pdf.
- Waters, Ian. "How Secure is the University? Assessing Institutional IT Risk with Limited Resources." Paper presented at EDUCAUSE/Internet2 Security Professionals Conference, Denver, CO, April 11, 2006.
<http://www.educause.edu/ir/library/pdf/SPC0680.pdf>.

Acknowledgments

The author recognizes the patience, dedication, and enthusiasm of staff from the Information Technology Division and from all other areas throughout the university in collaborating to perform the risk assessments. The author also gratefully acknowledges the assistance of Standards Australia, the Defence Signals Directorate of the Australian Department of Defence, and Murdoch University in permitting reproduction of parts of their security documentation.

Endnotes

1. George S. Patton, from letter to Cadet George S. Patton IV, June 6, 1944.
2. Texas A&M University, University-wide Risk Management website,
<http://universityrisk.tamu.edu/default.aspx>.
3. Paul Proctor and F. Christian Byrnes, *The Secured Enterprise: Protecting Your Information Assets* (Upper Saddle River: Prentice Hall, 2002), 207.
4. Standards Australia, *AS/NZS ISO/IEC 17799 Information Technology—Security Techniques—Code of Practice for Information Security Management* (Sydney: Standards Australia, 2006).
5. Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual* (Barton: Defence Signals Directorate, 2007),
http://www.dsd.gov.au/lib/pdf_doc/acsi33/acsi33_u_0907.pdf.
6. Standards Australia, *AS 13335.2 Guidelines for the Management of IT Security Part 2: Managing and Planning IT Security* (Sydney: Standards Australia, 2003), 9.
7. GAO, *Executive Guide: Information Security Management* (Washington: Government Accountability Office, 1998), 24, <http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-98-68>.

About the Author

Ian Waters (ian.waters@uts.edu.au) is manager, IT Governance and Compliance, at the University of Technology, Sydney, Australia.

Copyright

Copyright 2008 EDUCAUSE and Ian Waters. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the author.

Citation for This Work

Waters, Ian. "Managing IT Risk in Higher Education: A Methodology" (Research Bulletin, Issue 3). Boulder, CO: EDUCAUSE Center for Applied Research, 2008, available from <http://www.educause.edu/ecar>.