

## **Managing IT Risk University-Wide**

Ian Waters

*University Of Technology*

### **Abstract:**

The University of Technology, Sydney has assessed the risk of all its major IT systems and resources. The presentation will describe experience with performing this institutionally inclusive risk assessment, the limited resources employed and their sourcing, the outcome, the lessons learnt from the exercise and the work that still remains.

### Description of Presentation:

The University of Technology, Sydney (UTS) has been developing and refining its IT security policy and procedures for over seven years. These procedures include a formal methodology for assessing the risk of IT systems.

The University's IT Security Program requires that a risk assessment be performed on all major IT systems. The UTS approach to IT risk assessment is to perform first a high-level risk assessment of all systems, and then to use the results to rank the systems in order of criticality for a detailed risk assessment.

This presentation will cover the steps that were involved in an environment constrained by severely limited budgets. First was the challenging task of identifying all major systems University-wide, followed by the conduct of a high-level risk assessment on each. The results of this exercise allowed the prioritising of systems for detailed risk assessment. The detailed risk assessment stage involved the division of each high priority system or resource into its core components, the conduct of risk assessment workshops on each of these components, the development of risk mitigation strategies, and then preparation of risk management plans. This process involved IT Managers and key technical and administrative staff, facilitated by the University's IT Security Office. The final stage for each system involves documentation of the process followed together with its results in IT system security plans.

The presentation will describe UTS experience with performing this institutionally inclusive risk assessment, the resources used and their sourcing, the successful outcome, the lessons learnt from the exercise and the work that remains for the future. The approach adopted and its results were subsequently validated by an internal audit review of IT security management at the University.

### Audience:

IT Directors, IT managers, academic and administrative managers, IT technical staff