
**Monash University
Information Technology Services**

IT Security Process Review

July - August 2003

Contents

| | |
|--|-----------|
| 1. Executive Summary | 3 |
| Background | 3 |
| Approach | 3 |
| Scope of Work | 3 |
| Summary of Key Findings | 4 |
| 2. Capability Maturity Model Ratings | 8 |
| ITS Security & Risk | 8 |
| Shared Systems - Unix | 8 |
| Network Infrastructure Services | 9 |
| 3. Detailed Findings | 10 |
| ITS Security & Risk | 10 |
| Shared Systems - Unix | 12 |
| Network Infrastructure Services | 13 |
| 4. Other Considerations | 14 |
| Appendix 1 – Working Papers | 15 |
| Appendix 2 – Organisational Security at Monash University | 46 |
| Appendix 3 – Detailed CMM Rankings | 47 |
| Appendix 4 – Capability Maturity Model | 49 |
| Appendix 5 – High Level Security Performance Indicators | 51 |
| Appendix 6 – CobiT | 52 |
| Appendix 7 – Statement of Responsibility | 53 |

1. Executive Summary

Background

Monash University (“Monash”) Information Technology Services (“ITS”) has established a Service Level Agreement (“SLA”) regarding the provision of IT security services to the Faculties. The University IT Security Steering Committee has agreed that an annual independent review of the ITS security services provided could be used as one measure of the adequacy of the service provision.

This report is the first evaluation of the IT security services provided by ITS and has been performed using the AS NZ ISO/IEC 17799 Information Technology – Code of Practice for Information Security Management as a basis for evaluation. The Code of Practice is an extension of the SLA’s currently in place and provides a more detailed framework to perform an assessment against.

Approach

As agreed with Monash, the current IT security processes as adopted by ITS, were compared against ISO 17799 and complemented with interviews of key personnel.

In order to assist Monash compare the annual reviews, the current IT security processes are rated using the Capability Maturity Model (“CMM”) as detailed in Section 2. This will allow Monash to assess if the IT security processes mature over time.

Deloitte Touche Tohmatsu’s (“Deloitte”) reporting is in accordance with Australian Auditing Standards AUS810 and AUS902. By reporting in accordance with the above mentioned standards, we have provided you with a moderate level of assurance in relation to the areas included within the scope outlined below.

Scope of Work

Our review included the following IT security processes as adopted by:

The Shared Systems (Unix) and Network Infrastructure Services (NIS or Networks) groups for the SAP and Callista application systems; and

The IT Security & Risk Section.

The ISO 17799 standard has 10 domains relating to Information Security Management. As detailed in our engagement letter, Deloitte has only reviewed Monash’s security processes against six of the ten domains. The six domains are listed below:

3. Security policy*;
4. Organisational security*;
7. Physical and environmental security*;
8. Communications and operations management;
9. Access control; and
10. Systems development and maintenance.

* For sections 3, 4 and 7 the application of the ISO 17799 standard has been addressed only once as it universally applies across the three groups (IT Security and Risk, Shared Systems (Unix)

and Network Infrastructure Services (Networks)). Section 7, which addresses physical and environmental security, has been assessed at a high level only.

Sections 8, 9 and 10 have been addressed separately for each of the three groups as the security process adopted may differ between each group.

Scope limitations meant we have not covered the IT security processes for the database and application groups.

Summary of Key Findings

Better Practices Observed

Monash have made, and continue to make significant progress in terms of creating a security conscious environment across the University whilst not sacrificing students and staff usability of IT systems. Implementing an effective security management framework, including the development of policies and procedures, improving technical security configurations, increasing security awareness and developing mechanisms for ensuring compliance with policies, is made possible through three important elements: People, Process and Technology. One element alone, will not contribute to a more secure environment, it is the combination of all three that will have the greatest benefit to an organisation such as Monash.

Our review of the IT security processes adopted by ITS, identified areas where Monash displayed mature and well controlled security processes by embracing one, two or three of the above mentioned elements. Examples include:

- The establishment of an Information Technology Security Policy and IT Security Framework in line with commercially acceptable standards;
- The formulation of an effective structure for communicating security related issues and requirements throughout the ITS department and Faculties; and
- A good working knowledge of security related concepts, standards and technical configurations within the ITS division.

With respect to the IT Security policy and security framework, Monash have embraced the commercially acceptable standard on Security Management, ISO 17799, as a baseline for developing common practices across all areas of ITS and Monash.

In addition, Monash has established a number of committees and forums for the purposes of communicating security related issues and concepts to the broader Monash community and to raise the general level of user awareness (both staff and students) with regards to security and their obligations. An IT Security Steering Committee has been established to build awareness and set the “tone at the top” while a Security and Risk department including a dedicated Security Manager role, have been created to help implement the framework and enforce the standards as depicted in the various policy documents.

Overall, we observed that the security management processes operate at a satisfactory level. The definition of the Capability Maturity Level 3, which is the average score, states:

“...Procedures have been standardised, documented and implemented and have been communicated... The process is managed consistently with the defined procedures and standards...”

Areas for Improvement

Throughout our interviews with ITS staff, we noted a good working knowledge of the security framework and policies currently in place at Monash, including their requirements as depicted in

the framework and policy documents. At an operational level however, we noted varying levels of procedural documentation supporting the high-level framework and policies.

We also noted a number of other challenges currently facing Monash with regards to implementing effective, consistent and efficient security management processes across ITS and the wider Monash community:

- The Monash Faculties currently have the authority to administer their own systems that are outside the direct control of ITS;
- Communication between different sections within ITS can be improved to ensure better co-operation;
- Users do not formally signoff on acceptance of policies;
- Mechanisms for monitoring compliance with policies and a process for regularly updating policies have not been established;
- The SLA's that have been developed do not contain specific detail and have little or no measurable elements to them; and
- Data and information has not been classified according to importance, i.e. "Highly Restricted", "Confidential", "Internal" and "Public".

In summary, the procedures followed are not always documented. The end results are mostly satisfactory, however improvements cannot be easily achieved, as the procedures are not formalised. Only once this has occurred, can process improvement take place. This is a key requirement to achieve a higher level of process maturity.

Our findings did not highlight any high risk areas and would mostly be classified as medium or minor risks. High risk can be described as having a high impact on reliable processing and requiring immediate addressing of the issue. Whereas medium and low risks have varying levels of impact and require remedial activities within 3 – 12 months.

Key Recommendations

Our recommendations below are based on our observations across many organisations of better security management practices and how they may be applied to Monash. We would expect that should these recommendations be accepted and implemented, Monash would improve its Capability Maturity Model rankings.

- **Security must be approached as a "business process".**
Security is not only an IT matter, it is also a key process that concerns the wider Monash community. The establishment of different forums within Monash has put the organisation on the right path. Still, a significant challenge for Monash to overcome is the decentralised responsibility for security between the Faculties and ITS and also within the ITS department itself.

The Faculties are responsible for the maintenance and configurations of their own IT systems. However, they are not as timely or consistent in the application of security processes as are ITS. Although ITS have the authority to audit their systems and provide security advice, implementation and enforcement of common controls becomes increasingly difficult when a centralised body, in this case ITS, is not directly responsible. Further, given the way ITS is structured in functional areas, we have noted inconsistencies in security configurations and in the level of documentation supporting the processes adopted by the respective ITS groups, i.e. between networks and shared systems.

Monash should implement an ongoing training and awareness program for security particularly in the Faculties to demonstrate the importance of security and the importance of their role in maintaining appropriate security.

As security needs to be treated as a business process and not just the domain of ITS, we expect the Faculties to have a more active role in the management of security. This may be facilitated through the Faculties nominated security officers driving the acceptance and the implementation of Monash wide standards back into their own Faculty.

- **Ongoing Security Risk Assessments.**

A successful security management framework is based on developing a risk profile that is aligned with both the Faculties and IT. The outcome of the risk profiling is to identify key risk areas that allow Monash to determine the level of effort and appropriate resources required to mitigate these exposures. A periodic review of the risks identified should occur together with a scoping process to recognise new risks.

We acknowledge that Monash has started this process, however we believe certain actions, such as data classification that should follow on from a risk assessment, have not been performed.

- **Data Classification.**

Data classification will provide a basis for Monash to safeguard its data. By classifying information according to importance, i.e. “Highly Restricted”, “Confidential”, “Internal” and “Public”, appropriate security measures can be put into place. “Definitions of use” and “data ownership” are essential components driving this process. We acknowledge that Monash currently has two levels of classification (“Public” and “Confidential”), however we believe a more granular level of classification would enable a more tailored security implementation.

An important step in this exercise is the identification of types of information within the Monash community and the associated current security levels. This will provide an overview of the different types of information, how it is secured and where it is stored. By implementing the data classification and its relevant security controls, Monash can address privacy and security concerns that currently exist. It would, for example, provide a framework for the Faculties to manage their own student and staff information in a consistent way in line with Monash security guidelines.

- **Monitoring of Compliance.**

Where acceptance of security policies and frameworks are not accompanied by a signature or formal acknowledgement by staff and students that they understand and will abide by Monash’s policies, enforcement may become difficult if a breach was to occur. In addition, where policies are not kept up to date and compliance mechanisms are not in place, there is the possibility that changes will not be adequately communicated to users increasingly the likelihood of breaches and non-compliance.

It is therefore recommended that Monash periodically require staff to acknowledge and accept the security policies. This will enforce the standards and provides an increased level of security awareness. Compliance monitoring in the form of security and policy audits should occur regularly. We acknowledge that technical compliance audits are performed regularly.

- **Measurable Service Agreements.**

It is also important that Monash consider revisiting the current SLA’s with the Faculties and modifying them to make them more specific and measurable such that ITS’ performance against them becomes more meaningful and quantifiable. We have provided you with some high level security performance indicators in Appendix 5.

Best Practice Security Management

To provide Monash with an overview of Best Practice Security Management, we have provided some key features observed from our world-wide experience in security management. As discussed in this Executive Summary, Monash displays some, however not all of these features.

- **Active Board and senior management oversight and direction.**
Monash currently has a well established security governance framework with clearly stated security policies. However, improvements can be made by applying the rigorous manner of security management as applied within ITS across the wider Monash community and its Faculties.
- **Security charter, policies, standards, and procedures.**
Monash displays best practice in the area of documenting its charter, policies and procedures, however we did notice varying levels of operational execution of the security standards within ITS and across the wider Monash community and its Faculties.
- **Technology and procedural controls to enforce policy.**
Monash has shown a better practice in applying technology to enforce security policy, such as the AuthCate solution and the Intellitactics project. We believe that the use of technology within Monash is supporting the People & Process components, however improvements can be made in the expansion to other applications and systems of these projects.
- **People in the right numbers, in the right places and with the right skills to efficiently implement the program.**
Monash has a strong Security & Risk team within the ITS department, however this group does not have enough resources to cover the wider Monash community. In addition, within the Faculties, an increase in security skills is required to effectively and efficiently deploy the security management framework.
- **Measurement systems to gauge the effectiveness of the program.**
Monash has taken a first step in implementing an SLA covering the security management processes provided by ITS. Monash needs to define specific measures of performance. Best practices shows that pro-active measurement of a service provided is key to the effective management of any program.
- **Process-based security that integrates people, technologies and policies.**
As outlined earlier in the Executive Summary, an effective framework involves the integration of people, technology and processes. The features mentioned in this section are all prerequisites for the successful implementation of Best Practice security management. Monash has taken its first steps towards process-based security, however will need to address our identified areas before the highest level of security management process maturity can be achieved. It is also a process that never ends; continuous improvement is the key to every successful process.

For more detail on the summary findings identified above, please refer to section 3, Detailed Findings.

Other considerations for Monash in comparing its practices to other industries are outlined in section 4.