Insights into Security Policies and the University Sector

Kent Adams
Franz Eilert
Gary Gaskell
Dianna Madden
Adrian Tarca

3 July 2013
© Infosec Services
Overview

- Introduction – Kent Adams
- Project drivers
- Approach
- Outcomes
- Key Success Factors
Support for Controlling Security Risks

Impact

Likelihood

Difficult

No Arguments 😊

Low priority

Usually controlled 😊

3 July 2013

© Infosec Services
Drivers

- A%$*^%(&* --- Auditors
  - 😊

- Executive Management
  - Demonstrate sound risk management
  - “No more surprises”

- Operations Management
  - Enhance consistent application of security
    - i.e. - move to a defined level of Control Maturity
# Capability Maturity Model

<table>
<thead>
<tr>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimised</td>
</tr>
<tr>
<td>Managed</td>
</tr>
<tr>
<td>Defined</td>
</tr>
<tr>
<td>Repeatable</td>
</tr>
<tr>
<td>Initial/Adhoc</td>
</tr>
</tbody>
</table>
The Mandate

Fix the “Security Policy”
The Approach

- Not just update IT security policies
  - Implement a framework
- Consult all stakeholders
  - Avoid the perception of a ‘power grab’
- Team approach
  - JCU staff & consultants
- Principles
  - Policy approved by an accountable person
  - Threats change – so must the response
  - Security controls are at different levels
    - “policy should match this”
Solution – Part 1 (decomposition)

<table>
<thead>
<tr>
<th>Level</th>
<th>Policy type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive</td>
<td>Overarching information security policy</td>
<td>Univ Policy Library</td>
</tr>
<tr>
<td>Managerial</td>
<td>Corporate management policies</td>
<td>Univ Policy Library</td>
</tr>
<tr>
<td>Technical</td>
<td>Information Technology specifics</td>
<td>IT wiki</td>
</tr>
<tr>
<td>Operational</td>
<td>Procedures and “How-To” documents</td>
<td>IT wiki</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procedure Manuals in other Business Units</td>
</tr>
</tbody>
</table>
JCU Information Security Framework –
Policy Lifecycle

Inputs
- Information Standards (IS 18)
- Audits (JCU AA and QAC)
- Legislative
- Overall JCU policies
- ICT Strategic Plan

New Policy Development

Director & ITR MAC
- Discuss planned strategy
- Discuss proposed policy
- Appoint policy owner
- Grant/Deny approval

CAB
- Develop concept for new policy
- Discuss with shareholders
- Draft policy
- Recommend new policy to ITRMAC

Information Security Policies
(JCU Policy Library)

Middle Management Policies
- Based on IS 18
- Strategic planning policies

IT&R Level policies
(held in ITR wiki)
- Govern internal activities
- Evaluated yearly
- Supports ICT Strategic plan
- Supported by underlying procedures

IT&R Procedures
(held in ITR wiki)
- Supports policies developed by team leaders

Policy Review

Director & ITR MAC
- Review policies annually
- Discuss changes to policy
- Grant/Deny approval
- Send to DVC for final approval

CAB
- Policy owner reviews policy annually
- Discuss with stakeholders
- Draft changes to policy with CAB
- Recommend changes to policy to ITRMAC

3 July 2013
Solution Part 3 – (A lifecycle)
Mandate and Commitment (4.2)

Design of framework (4.3)

Continual improvement of the Framework (4.6)

Implementing risk Management (4.4)

Monitoring and review of the Framework (4.5)

Principles (Clause 3)

Framework (Clause 4)

Process (Clause 5)

ISO 31000:2009 Figure 1 – Relationship between the principles, framework and process

- Mandate and Commitment
- Design of framework
- Continual improvement of the Framework
- Implementing risk Management
- Monitoring and review of the Framework

- Creating value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on the best available information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement and enhancement of the organization
Project Steps

- Know the context
- Build support (exec and IT)
- Build a good team
- Policy “gap analysis”
- Deliver the framework
- Test the framework
  - Deliver ‘high priority’ policies (see gap analysis)
Standards and Guides

- ISO 27001, & 2
- Qld Govt Info Standard 18 – Information Security
- ISO 31000 and 31010
  - Formerly AS 4360
- ISO 27005
  - ISO 31000 interpreted for security
Key Success Factors

△ The framework – not just a “security policy”
  ▪ Stratified policy architecture
  ▪ Diversified policy stakeholders and approvers

△ Executive support
  ▪ Incl – Business support

△ 80 – 20 rule

△ A team with ‘we’re here to help you’ message
  ▪ Rather than . . . .
Risk Management Decisions

Level of Risk

- Catastrophic
- Insignificant

Cost of Treatment

- No Brainer
- Open for debate!
- Forget it!

3 July 2013 © Infosec Services
Gap Analysis

Current controls

Baseline/checklist

Gap Analysis

Risk Assessment
Inherent Risk

Business Objectives & Environment

- Risk Assessment
  - Inherent Risk
  - Risk Assessment
  - Risk Register
  - Treatment Plan

Current Controls
### Executive level policy – Policy library

#### JCJ Information Security Policy

### Management level Policies – Policy library

<table>
<thead>
<tr>
<th>Policy, planning &amp; Governance</th>
<th>Asset mgmt</th>
<th>HR mgmt</th>
<th>Physical &amp; environmental</th>
<th>Communications &amp; operations mgmt</th>
<th>Access mgmt</th>
<th>System acquisition, dev &amp; maint</th>
<th>Incident mgmt</th>
<th>Business continuity mgmt</th>
<th>Compliance mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of comm &amp; computing facilities</td>
<td>Pubs by staff</td>
<td>Records mgmt</td>
<td>Cabling standards</td>
<td>AARNET use</td>
<td>AV funding</td>
<td>AV use</td>
<td>AARNET?</td>
<td>Cabling standards</td>
<td></td>
</tr>
<tr>
<td>Statement on use of computing facilities</td>
<td>Records mgmt</td>
<td>Student Info access</td>
<td>Use of comm &amp; computing facilities</td>
<td>Virus protection</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to archives</td>
<td>Retain email</td>
<td>AV funding</td>
<td>SPA email</td>
<td>Records mgmt</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web compliance</td>
<td>Wireless LAN use</td>
<td>Student Info access</td>
<td>Aura email</td>
<td>Retain email</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web security</td>
<td>Archive access</td>
<td>Student Info access</td>
<td>Aura email</td>
<td>Web security</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IT&R level policies - wiki

<table>
<thead>
<tr>
<th>Policy, planning &amp; Governance</th>
<th>Asset mgmt</th>
<th>HR mgmt</th>
<th>Physical &amp; environmental</th>
<th>Communications &amp; operations mgmt</th>
<th>Access mgmt</th>
<th>System acquisition, dev &amp; maint</th>
<th>Incident mgmt</th>
<th>Business continuity mgmt</th>
<th>Compliance mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support staff</td>
<td>Pubs by staff</td>
<td>Records mgmt</td>
<td>Cabling standards</td>
<td>AARNET use</td>
<td>AV funding</td>
<td>AV use</td>
<td>AARNET?</td>
<td>Cabling standards</td>
<td></td>
</tr>
<tr>
<td>home network</td>
<td>Records mgmt</td>
<td>Student Info access</td>
<td>Use of comm &amp; computing facilities</td>
<td>Virus protection</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>access</td>
<td>Retain email</td>
<td>SPA email</td>
<td>Aura email</td>
<td>Records mgmt</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile phone policy</td>
<td>Wireless LAN use</td>
<td>Student Info access</td>
<td>Aura email</td>
<td>Retain email</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Archive access</td>
<td>Student Info access</td>
<td>Aura email</td>
<td>Web security</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web security</td>
<td>Archive access</td>
<td>Aura email</td>
<td>Web security</td>
<td>AV funding</td>
<td>AV use</td>
<td>Cabling standards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IT&R Procedures - wiki

- Existing policies
- Proposed policies
- Might be policies
Contacts

Gary Gaskell, Infosec Services Pty Ltd
(CISSP, CISM, CISA, SBCI, MACS (Snr), CP, M App Sc, B Eng, B IT)
gary.gaskell at infosecservices.com.au
Ph 0438 603 307
You don’t have to manage risk