Corporate Governance of IT: ISO 38500 Case Study

Presented by:
Mark Toomey
This set of presentation slides was developed for, and delivered at the itSMF Australia 11th National Conference.

The slides are now available for download by participants in the conference and other interested parties, for their personal use in self-development, and for the purpose of facilitating conversations with their colleagues, including top level management and directors. Permission is hereby given for participants to print and copy this material for these purposes only.

The slides do not equip readers with the in-depth knowledge required to enable them to provide any form of instruction or consulting advice.

Consultants may provide a copy of these slides to their clients without royalty providing that they are in their original form and that they are accompanied by a recommendation that Infonomics be consulted if further guidance is required.

This material was prepared to provide general guidance and stimulate debate. It should not be construed as providing professional advice and services for any particular or specific situation. As such, it should not be used as a substitute for consultation with expert advisers. Before making any decision or taking any action you should consult with Infonomics Pty Ltd or other competent professionals.
# Top 5 management priorities of local CIOs
(Courtesy Peter Hind)

<table>
<thead>
<tr>
<th>Priority</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aligning IT and business goals</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Improving internal user satisfaction</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Business continuity/risk management</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>IT-enabled process improvement</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>IT staff development</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Controlling IT costs</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Measuring &amp; communicating IT value</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td><strong>IT governance</strong></td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Improving project management discipline</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>Revenue generating services/products</td>
<td>N/A</td>
<td>11</td>
</tr>
<tr>
<td>Internal IT knowledge management</td>
<td>7</td>
<td>12</td>
</tr>
</tbody>
</table>

The Midco Case Study

As presented at the CEO’s briefing
IT is changing the rules of the game in delivery of education – how do we adapt and lead?
We worked through a structured process to build understanding and prepare for change.

1a Logistics
1b Assertions
1c Briefings

2a Interviews
2b Artefacts

3 Executive Workshop

4a Develop Charter
4b Develop Policy

5 Develop Process

6a Signoff
6b Communication
6c Meeting

Four-draft Review Cycle

Prepare
Collect
Design
Implement
We measured ourselves against the standard for corporate governance of IT
ISO 35000 Framework
A Model, and Six Principles

- Responsibility;
- Strategy;
- Acquisition;
- Performance;
- Conformance;
- Human Behaviour.
# Using ISO 38500
Guide for assessment and improvement

<table>
<thead>
<tr>
<th>Principles</th>
<th>Evaluate</th>
<th>Direct</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquisition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conformance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Behaviour</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What does each cell mean?

How do you perform?

What should you seek to improve?

What consequences of improvement should you seek?

Do our management systems meet the needs of effective governance?

vs

Do our management systems meet the requirements of formal frameworks?
The measurement showed where we had scope for improvement.

AS8015 Principles

A = Financial Institution
B = Listed Industrial
C = Local Government Body

2006 Research with RMIT
Industry November 2006
Midco, May 2007
We considered key issues regarding assignment of responsibility for IT

- Things Midco needs to change
  - Clearly define responsibility / Clear alignment of role to responsibility
  - Assign executive responsibility
  - Provide staff with the skills and tools associated with their assigned responsibilities
  - Clarify the role of business owners
  - Develop and monitor performance indicators
  - Implement KPI’s & reporting
  - Promote responsibility (in all directions) to all staff

- Barriers to change
  - Lack of vision
  - Role clarity
  - Acknowledgement and acceptance of business imperative to change
  - Acceptance of new approach and roles
  - Shared understanding of issues
  - Capability
  - Internal expertise in operational management
  - Executive ownership
We considered key issues regarding planning for IT

• Things Midco needs to change
  – Develop a business structure and process to plan
  – Plan process improvement first and include IT as a tool to achieve outcome
  – Link strategic and business planning with IT planning
  – Develop an IT plan
  – Define/clarify responsibilities
  – Assign responsibility
  – Monitor performance

• Barriers to change:
  – Willingness to own
  – Current workloads
  – IT not seen as integral to company planning
  – Understanding the business
  – Competence
  – Internal expertise at all levels
We considered key issues regarding decisions to invest (spend) on IT

• Things Midco needs to change
  – We need to plan to know what to acquire
  – Ownership / Sponsorship at senior & exec levels of products
  – Business case methodology / formal business case process
  – Stakeholder consultation
  – Integrated planning process
  – Return on investment evaluation

• Barriers to change
  – Lack of adherence to process
  – Lack of resources / time to fully develop business case
  – Culture
  – Skills / competence, time & inclination
  – No formal steering committee
  – Lack of business ownership
We designed a new way of controlling our use of IT

Performance Measure:
We can target and assess our improvement.

Responsibility Policy:
Everybody can understand and be effective in their role.

Governance Organisation:
Revised committee structures focus on business issues and executive responsibility.

Process Model:
Twenty-four key processes to be detailed, showing how we translate strategy into plans, plans into projects and projects into appropriate operational capability.
Midco Developed Policy for control of IT based on the ISO 38500 principles

Usage policies
- Rules for how people use the business systems and technology resources
- Board role: part of user community.

Operating policies
- Specify how projects and operations are conducted
- Board role: awareness

Strategic Policies
- Your posture relative to Principles
- Board role: consultation and approval

Your ISO 38500 Framework
Midco’s structure for governing IT is firmly based on clear responsibility for Demand and Supply

Business Domain: How IT is used to enable and operate the business

IT Domain: How IT is managed and delivered.

Strategic Business Future

Ongoing business operations

Effective IT enabled change

Reliable IT Service

ITIL, ISO 20000, ISO 27000, CoBiT etc
Midco’s system for governing IT fully integrates board oversight and management tasks.
Midco’s Overarching Policy: Responsibility for IT

- IT is an essential enabling resource for current and future administration of Midco and for service Delivery. Responsibility for effective, efficient and acceptable use of IT is broadly based and not confined to the Information Systems Department.

- All procedures relating to the use of IT in Midco shall contain clear and specific statements of responsibility regarding:
  - monitoring performance of the procedure, and maintenance and improvement of the procedure;
  - conduct of roles defined in the procedure.

- The IT Governance Committee is responsible for monitoring performance of, and acting to resolve problems with, the company’s ongoing operational use of IT and with the company’s IT related investment projects.

- The IT Governance Committee is responsible for establishing and maintaining an effective system of governance within which the responsibilities defined in this policy are implemented.
  - Realisation of the value of IT investments is the direct responsibility of the Chief Executive Officer and the Executive Management Team. This responsibility may not be delegated.
  - Capability of the company to conduct its normal administrative and service operations insofar as they are dependent on IT is the direct responsibility of the Chief Executive Officer and the Executive Management Team. This responsibility may not be delegated.
  - The Chief Executive Officer and the Executive Management Team are all members of the IT Governance Committee and are collectively responsible for implementing the decisions of the Committee.
The Responsibility Policy is specific about executive and management responsibility

- **Responsibility for Strategy**
  - for the ongoing and future use of IT ... is integral to business strategies and is the direct responsibility of the Chief Executive Officer and the Executive Management Team.
  - Allocation of resources for IT ... is the responsibility of board, acting on the advice of the Chief Executive Officer. The IT budget is a responsibility of the IT Governance Committee with the support of the Business Systems Steering Committees and the IT Infrastructure Steering Committee.

- **Responsibility for Planning**
  - Preparation of proposals for investment in IT is the responsibility of the Steering Committees ...
  - Steering Committees ... are responsible for ensuring that the full intended benefits of the investment are realised.
  - Preparation of technical plans for IT infrastructure and software systems aspects of business initiatives is the responsibility of the Senior Manager Information Systems, working collaboratively with the corresponding Business System Steering Committee.
It establishes clear expectations of the new IT Governance committees

• **Responsibility for Delivery**
  - Projects ... are the responsibility of the Steering Committee which was responsible for preparing the business case.
  - This responsibility includes ensuring that the project is properly managed and has sufficient, appropriately skilled resources to deliver the intended business outcome and continues until acceptance by the IT Governance Committee that all attainable benefits have been delivered.

• **Responsibility for Operation.**
  - Day to day operation, control and maintenance of Midco’s operational business systems and infrastructure is the joint responsibility of the Information Systems Department and the designated Business System Owners and Administrators.
  - This responsibility is subject to ... procedures for .. change management, problem management, data protection and security, performance and availability management and so on.
  - It requires clearly defined Service Level Specifications for each business system and for the IT infrastructure.
There five further overarching policies

• **IT Innovation Posture (Strategy)**
  - Defines Midco’s intentions in respect of technology leadership:
    • how and where innovation is encouraged
    • how much innovation risk is acceptable.

• **IT Investment Controls (Acquisition)**
  - rules for expenditure on IT (including allocation of staff resources).
  - business cases for new initiatives, and oversight of initiatives through to realisation of results.
  - controls for selection and engagement of external organisations for all classes of IT supplies.

• **IT Capability (Performance)**
  - IT capabilities that are to be maintained within Midco
  - limits for the amount of concurrent change the organisation undertakes
  - level of dedicated resources available for IT and other aspects of change
  - benchmark targets for performance, capacity, availability, reliability, integrity and security

• **IT Controls (Conformance)**
  - which controls are to be established
  - delegation of authority to design, implement and enforce the controls
  - baseline identification of the external controls (legislation, regulation, code of practice etc.) that affect planning, delivering and operating IT capabilities.

• **IT Human Factors (Human Behaviour)**
  - Identify the “people in the process”
    • involved in providing the IT capabilities
    • who use the business systems
    • business partner organisations (both upstream and downstream),
    • individual “customers”,
    • people seeking information.
  - attitude to preparing for change, and supporting people as change is delivered.
Midco’s system for governing IT recognises that IT is the enabler, not the driver

- Operating context of the organisation
  - External
  - Internal.

- Four key elements of operating organisations
  - People – who participate in business events
  - Process – what business events take place
  - Structure – where business events happen
  - Technology – enabling and recording events

- IT intrinsic to day to day operations
  - Business process specific - Transactions, Customers, Etc
  - Generic - Email, Telephony, Information

This model is a variant on H.J. Leavitt’s Model of organisational change, published in 1965.
The Fundamental Equations: Changing The Business System

- IT is now a fundamental enabler of change and is leading to new business models and new business practices
  - Eg e-Government
- Implementing IT enabled change involves attention to every facet of business models and practices
  - Internal and external factors

"Traditional" IT Change Project
The Fundamental Equations: Changing The Business System

• IT is now a fundamental enabler of change and is leading to new business models and new business practices
  - Eg e-Government

• Governing IT Enabled Change involves much more than governing technology activities.

• Implementing IT enabled change involves attention to every facet of business models and practices
  - Internal and external factors

- Traditional IT Change Project
- Business System
- Process
- Technology
- Structure
- People

- Business Context
- Process
- Technology
- Structure
- People

- Change Program
  - Business System
    • Process
    • Technology
    • Structure
    • People
  - Business Context
    • Process
    • Technology
    • Structure
    • People

- Changed Business Context
- Changed Business System
- Changed Structure
- Changed Technology
- Changed People
The Executive has overall responsibility for IT

• Three organisation elements:
  - IT Governance Committee
  - Business System Steering Committees
  - IT Infrastructure Steering Committee
The IT Governance Committee is the focus for key decisions about the use of IT

• Purpose:
  – **strategy** for future use of (and investment in) IT is integral to and driven by the company’s business strategy;
  – all **investments** in IT produce their intended outcomes;
  – the company’s IT **assets** are managed and used appropriately; and
  – the operational **performance** of the company’s IT resources meets reasonable expectations in an efficient, effective and acceptable manner.

• Duties:
  – Establish and manage conformance with top level policies governing the use of IT
  – **Set responsibility for IT**, planning, acquiring, performance and conformance
  – **Define strategy for the use of IT** in service and administration, prioritise initiatives and allocate resources
  – Ensure appropriate business cases and plans for investment in IT
  – Monitor IT investments through to realisation of business outcomes.
  – Approve or recommend proposed investments in IT to CEO and board.
  – Direct and monitor appropriate Key Performance Indicators for use and delivery of IT, **initiating corrective action as and when required**.
  – Establish and monitor conformance with additional detailed policies as required to ensure that use of IT at Midco is appropriate and that Midco’s assets are properly managed and protected.
  – Ensure that use of IT conforms with legal and regulatory requirements
  – Ensure that the people involved in and impacted by IT are given due consideration.
  – Continue development of a system of governance for IT to ensure effective, efficient and acceptable use of IT in both administration and service delivery.
The IT Governance Committee is an Executive Committee, which engages the organisation.

- **Members:**
  - Chief Executive Officer (Chair);
  - Deputy Chief Executive;
  - General Manager Corporate Services;
  - General Manager Front Line Programs;
  - General Manager, Production Operations.
  - Delegation of membership is not permitted.

- **Permanent attendees** (non-voting):
  - Secretary (EA to the General Manager, Corporate Services);
  - Senior Manager, Information Systems (also as chair of the IT Infrastructure Steering Committee);
  - Chair of each Business System Steering Committee.

- **As-required attendees** (non-voting):
  - Project managers (internal or external) of major business change and IT projects;
  - Representatives of stakeholder bodies (suppliers, customers, industry, government, IT vendors, consultants and auditors);
  - Additional personnel by invitation, to provide information in respect of an agenda item.
Steering committees are key to operation of the governance system

- Business System Steering Committees.
  - Evolution of existing committees;
  - **Focus on business** process or activity, and the use of the information systems in that context;
  - Prepare plans, recommend investment, deliver benefits and solve problems;
  - Chaired by a Senior Manager responsible for key business activities within the scope of the Steering Committee.

- IT Infrastructure steering committee.
  - Oversight of the company’s IT infrastructure;
  - Oversight of operational service delivery;
  - Chaired by the Senior Manager, Information Systems.
The Process Model involves four primary process groups

1. Vision
   - Generalised
   - Intended performance, capability, profile, behaviour

2. Strategy
   - Specific
   - Actions, Targets

3. Plan
   - Detailed
   - Business Change
   - Priority & Sequence
   - Business Case: Allocate Funds & Resources
   - Organise Systems & Infrastructure

4. Deliver
   - Activity
   - Business Projects
     - People
     - Process
     - Structure
     - Technology
   - Manage
     - Project Risk
     - Benefits

Operate
- Ongoing
- Set Targets
- Manage & report performance
- Ensure Service
- Support the business

Policy Foundation

3 Key Questions
- Do today’s IT systems meet ongoing needs?
- Does planned business affect IT systems?
- What does technology evolution mean for business?
Most of these things already happen, but we now have a different perspective

- New approach to responsibility
- Overarching policies to guide decisions
- All processes need to be reviewed and upgraded
It looks complicated, but experience will make it seem easy...

- The Magic Roundabout in Swindon, UK looks confusing but has a lower accident rate than “normal” intersections, with much higher traffic flows.
Process outlines provide initial understanding. Detailed process design is required.

Manage business/ICT investment budget & priorities

• **Purpose:**
  - Allocate available resources efficiently and to the most appropriate activities. Adjust allocation and priority in the light of experience.

• **Frequency:**
  - Annual establishment of budget overall, and determination of allocation for ongoing operation of IT, basic maintenance of business systems, and investment in new infrastructure and capability.

• **Responsibility:**
  - IT Governance Committee

• **Requires:**
  - Identification of the program of investment activities (derived from and aligned to strategy) with identification of likely benefits and priorities, in order to establish best sequence of activity. See Process “Develop business/ICT initiative change plan”.

• **Note:**
  - This process needs to be integrated to the company’s overall budget setting process, so that competing demands for funding from all activities (business development, infrastructure, IT etc) are properly managed.
Midco’s governance development program

Stage one
- Governance Committee
- Responsibility Policy
- Governance Process Model

Stage three
- Initiative Planning
- Initiative Delivery
- Continuing Operations

Business System & IT Infrastructure
- Steering Committees
- Governance Processes
- Detailed Policies
- Oversight

Governance Processes
- Guiding Policies
- Charters (including Membership)
- Training
- Strategic Assessments
- Strategic Plan

Continuing...
Midco’s situation today

• Continuing to evolve their system for governance of IT;
• Learnings from the project supported a major restructure of the organisation;
• Business is now fully engaged in setting the IT agenda and is fully responsible for deciding priority;
• IT department gets on with its job free of unfair criticism, and is able to devote resources to improving service delivery;
• New initiatives are getting off the ground as well defined, formal business projects for the first time in years;
• “Skunkworks” initiatives have disappeared;
• Suppliers are no longer driving the “Technocitement” agenda.
Information Technology allows us to change the way we do things.
Corporate Governance of IT enables us to direct and control the change with confidence.

- Responsibility;
- Strategy;
- Acquisition;
- Performance;
- Conformance;
- Human Behaviour.
ISO 38500 provides the missing link in building an effective system of governance.
Discussion and Questions