Frameworks for Dealing with IT Governance Issues

Robert Shedden, Principal
Proteus Systems IT – Advisors & Consultants
http://www.proteussystemsit.com/

“There is nothing so practical as a good theory” – Kurt Lewin
IT Questions for the Board

A review of recent research, applied as practical frameworks to address major IT issues
## IT Issues - Self-assessment

**IT Questions for the Board:**

Are you sure that you have...

1. Adequate IT governance?
2. Appropriate IT investment levels?
3. IT risks covered?
4. Sufficient visibility of IT-related projects?
5. Senior executive understanding of IT?

**What Business Impact?**

<table>
<thead>
<tr>
<th>Your Response?</th>
<th>Don't know</th>
<th>Yes</th>
<th>Maybe</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Questions for the Board</td>
<td>1. Adequate IT governance?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Appropriate IT investment levels?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. IT risks covered?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Sufficient visibility of IT-related projects?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Senior executive understanding of IT?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assess the adequacy of IT governance in your organisation
1. Adequate IT governance?

- Do your IT governance processes enforce formal decision-making authority and responsibilities, and support IT alignment with business aims?
  
  - Implement a proven decision rights and accountability framework to encourage desirable behaviour in the use of IT
  - Approve management recommendations for
    - the role of IT in the organisation
    - IT investment levels and priorities (appropriate to business goals)
  - Ensure appropriate organisational responsibilities and clear exception-handling processes

- References: Weill et al  http://mitsloan.mit.edu/cisr/
### IT Governance Arrangements - IT Domains & Decision-making Styles:

<table>
<thead>
<tr>
<th>Domain:</th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure</th>
<th>Business Application Needs</th>
<th>IT Investment, Prioritisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Style:</td>
<td>Role for IT: High-level statements about how IT is used in the business, developed into themes for action</td>
<td>Technical choices, and policies: Migration path for integration, compatibility and sustainability</td>
<td>Technology fabric underlay: Base foundation of shared, reliable IT services, centrally coordinated</td>
<td>Required IT systems: specifying business needs for IT applications (purchased or developed)</td>
<td>How much, where and when to invest: Decisions include project approvals, priorities and justification techniques</td>
</tr>
<tr>
<td>Business Monarchy</td>
<td>Individual or group of business executives (sometimes includes CIO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Monarchy</td>
<td>Individual or group of IT executives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td>Shared by CxOs and one or more business groups (may include IT executives)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duopoly</td>
<td>IT executives and one other business group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feudal</td>
<td>Business unit leaders, key process owners or their delegates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anarchy</td>
<td>Individual user or small group (<em>not considered to be governance</em>)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Input and Decision rights matrix to be specified  
Adapted from Weill et al, 2004
### IT Governance Arrangements - most common vs best-performed patterns:

<table>
<thead>
<tr>
<th>Domain Style</th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure</th>
<th>Business Application Needs</th>
<th>IT Investment, Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Monarchy</td>
<td>Profit, Growth</td>
<td>Profit</td>
<td>Profit</td>
<td>Growth</td>
<td>Profit, Growth</td>
</tr>
<tr>
<td>IT Monarchy</td>
<td></td>
<td></td>
<td>Profit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td>ROA</td>
<td></td>
<td></td>
<td>Profit</td>
<td></td>
</tr>
<tr>
<td>Duopoly</td>
<td>ROA</td>
<td>ROA</td>
<td>ROA</td>
<td>ROA</td>
<td>ROA</td>
</tr>
<tr>
<td>Feudal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Growth</td>
</tr>
</tbody>
</table>

- Shaded cells = Most common pattern
- Adapted from Weill et al, 2004

+ clear exception-handling processes
IT Governance Arrangements - example of organisational structures:

<table>
<thead>
<tr>
<th>Domain Style</th>
<th>IT Principles*</th>
<th>IT Architecture</th>
<th>IT Infrastructure</th>
<th>Business Application Needs</th>
<th>IT Investment, Priorities*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Monarchy</td>
<td>D: Senior Executive</td>
<td>I: Senior Executive</td>
<td></td>
<td>D: Senior Executive</td>
<td></td>
</tr>
<tr>
<td>IT Monarchy</td>
<td></td>
<td>D: IT Executive</td>
<td>D: IT Executive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td>I: IT Steering Committee</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duopoly</td>
<td>I: Business + IT</td>
<td>I: Business + IT</td>
<td></td>
<td>I: Business + IT</td>
<td></td>
</tr>
<tr>
<td>Feudal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* = subject to Board approval, appropriate to business goals  
I = Input required, D = Decision rights  
Adapted from Weill et al, 2004
## IT Governance Arrangements - Self-assessment

<table>
<thead>
<tr>
<th>Domain</th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure</th>
<th>Business Application Needs</th>
<th>IT Investment, Priorities</th>
<th>Overall score 0...5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questions:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who has input?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who decides?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arrangements understood?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arrangements effective?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enter the executive groups and the levels of understanding / effectiveness, then assess an overall score for each row, summing all rows to get a total.
2. Appropriate IT investment levels?

• Do you consider that your company is under- or over-investing in IT relative to your business strategy and the value generated by IT?
  
  – Distinguish between defensive and offensive strategies for IT
  – Ensure that the scope and scale of IT investment are consistent with both the company's dependence on IT and the opportunities for competitive advantage through IT
  – Recognise the risks inherent in a major business transformation project involving IT, and ensure oversight of staged investment and benefits delivery

  – References: Nolan & McFarlan, 2005 IT and the Board of Directors *HBR Oct 2005*
  McFarlan et al, Corporate Information Strategy and Management *HBS 1999*
DEFENSIVE

Factory Mode
System failures / delays serious
Core business activity on-line
IT maintenance focus
"Don't cut corners"

Support Mode
System failures / delays tolerated
Systems deployed internally only
Manual process fall-back feasible
"Don't waste money"

OFFENSIVE

Strategic Mode
System failures / delays serious
New systems promise major gains:
cost, service or process benefits
"Spend up, monitor closely"

Turnaround Mode
New systems promise major gains:
cost, service or process benefits
Major IT expenditure / investment
"Don't mess it up"

(adapted from McFarlan et al 1999)
Appropriate Risk / Reward Relationship

(Adapted from McFarlan et al. 1999)
IT Investment Levels - Self-assessment

1. Where are you currently on the IT strategic grid, and is the scope and scale of IT investment appropriate?

2. Where must you move to in order to meet your business goals (and does this involve turnaround)?

3. Will your current and planned IT investment levels meet these strategic aims?

4. Are the risks of business transformation recognised, and matched by realisable business benefits from the investment?
3. IT risks covered?

- Are the risks of IT disaster proven to be adequately covered?
  - Assure security and reliability is appropriate to the firm's dependence on IT
  - Ensure existing IT risk mitigation matches baseline good practice in effectiveness of controls (external audit, Disaster Recovery...)
  - Require strategic IT assurance to balance the potential business impact of unusual but serious risks against the costs of improved controls

- References: AS17799, AS7799, HB231 Standards Australia; Nolan & McFarlan, 2005
## 1. IT Risk Mitigation

### Inherent Risk vs Consequences

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Med</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

### IT Strategic Impact Grid

**DEFENSIVE**
- Factory: Don't cut corners
- Support: Don't waste money

**OFFENSIVE**
- Strategic: Spend & Monitor
- Turnaround: Don’t mess it up

---

*Adapted from AS/NZS 4360, Nolan & McFarlan 2005*
2. IT Strategic Assurance

Control Effectiveness

<table>
<thead>
<tr>
<th>Residual Risk</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>Med</td>
<td>Med</td>
<td>High</td>
<td>High</td>
<td>?</td>
</tr>
<tr>
<td>Likely</td>
<td>Low</td>
<td>Med</td>
<td>Med</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
<td>Med</td>
</tr>
</tbody>
</table>

IT Dependency

Strategic Assurance

Consequences

GOOD PRACTICE

Factory System failures serious

BEST PRACTICE

Strategic Failures serious, Benefits important

Support Low system dependency

Turnaround Benefits important

Business Impact

Cost of Controls

Adapted from AS/NZS 4360, Nolan & McFarlan 2005
IT Risk Management - Self-assessment

1. How well are inherent IT risks understood in terms of likelihood and consequences?
2. Are risk mitigation controls appropriate to IT strategic impact across the business?
3. Has a high-level assurance review assessed controls in terms of strategic business impact?
4. Are these risk management processes clearly defined and reported for Board-level review?

![IT Strategic Impact Grid]

![Control Effectiveness]

![Inherent Risk]

![Consequences]

![Strategic Assurance]

![Risk Mitigation]

![IT Grow and Decay]

![Need for IT Relevancy]

![IT Opportunity]

![GOOD PRACTICE]

![BEST PRACTICE]

![Cost of Controls]

Adapted from ACFE 4561, Nelson & Idowu 2005

ACS - 10 May 2008
Proteus Systems IT
4. Visibility of major IT-related projects?

- Does the Board have visibility of major IT-related projects, and assurance that key business benefits are being delivered?

  - Ensure sound project governance, with the separation of operational and technical change processes and responsibilities
  - Require measurable and appropriate business benefits to be identified, to justify detailed project costs and risks
  - Institute business executive accountability for the delivery of business benefits
  - Implement a monitoring and Board reporting regime for staged project cost, risk, & progress milestones and benefits delivery

- References: HB280, 2006 Standards Australia, *Case Studies … ICT Governance*
  Delone & McLean, 2003, *D&M Model of IS Success, Jnl MIS 19:4*
Different Definitions of Project Success

Technical Focus
- Information Quality
- System Quality
- Service Quality

User Focus
- Intention to use
- Actual Use
- User Satisfaction

Organisational Focus
- Business Benefits

Adapted from Delone & McLean 2003
ICT Project Governance Model

1. Initiate
   - Governance of ICT in projects

2. Evaluate
   - Top management
   - Direct & Monitor

3. Support
   - ICT operations
   - Projects
   - Business processes
   - Changed ICT operations
   - Changed business processes

4. Monitor
   - Disclose
   - ICT Project Governance Model
   - adapted from ASHB280 - 2006

AS HB280 - 2006

HB 280 ASX Governance

Initiate Benefits
1. What are the expected business benefits, and how will they be measured?

Evaluate Risk
2. How much organisational change and other risks are needed to realise the benefits?

Support Management
3. Who will sponsor the project and be accountable for the benefits?
4. How will the sponsor and other stakeholders be rewarded (or otherwise)?

Monitor Disclosure
5. Is there a well-considered project plan, and a process and culture for issues to be raised?
6. Are the benefits on target or being realised?
Large, complex project; High degrees of technology and organisational change - Are the strategic gains worth the high risk? → Contingency project management

(adapted from McFarlan 1999)

"Dolphins" not "Whales"

"Time-box" projects, deliver staged benefits

Feeny 1997

Mitigation of Risk of IT in Projects

Mcfarlan 1999, Feeny 1997

ACS - 10 May 2008

Proteus Systems IT
IT-related Projects - Self-assessment

1. Do you have sound project governance, with separation of technical, operational and project management processes?

2. Do projects have measurable and appropriate business benefits identified, justifying costs and risks?

3. Is a business sponsor responsible and accountable for benefits realisation?

4. Is a senior executive / Board reporting regime in place to ensure visibility of project progress stages and benefits delivery?
5. Senior executive understanding of IT?

- Are you sure that senior executives understand and are responsible for IT investment in their area?

  - Recognise the imperative for two-way strategic alignment between business and IT
  - Require executive focus on *strategic IT* – exploiting effective and flexible IT systems to enable effective and flexible business processes
  - Identify the challenge for effective *business systems thinking* – envisioning the improved business process that technology makes possible

  \[= \textit{shared understanding} \] (Lukaitis & Cybulski)

Strategic IT -
Enterprise architecture reflects business strategy, exploits enterprise assets, enables effective key business processes.

Strategic V Useful IT Investment
adapted from Feeny 1997
Organisational "Drag" (Blythe 1988) and Strategic IT (Feeny 1997)
IT / Business Alignment - Self-assessment

1. Does IT understand the strategic business aims in terms of reliability / opportunity and the role for IT to support these?

2. Do business executives understand how the IT principles can enable strategic business opportunities?

3. Do IT and business combine for effective business systems thinking about technology opportunities?

4. Is this two-way strategic alignment successful in improving business processes?
There are no simple answers to complex, dynamic questions - no ‘silver bullets’ - but there do exist frameworks for teasing apart the complexities, and thinking through the dynamics of each particular situation in a logical and repeatable manner.
e.g. 1. Align IT principles and priorities with the strategic positioning of IT reliability and opportunity  
2. Develop shared understanding of systems opportunities between business and IT  
3. Review the strategic assurance of IT risk in line with the IT reliability / opportunity position  
4. Ensure that IT-related projects have business benefits defined via shared systems understanding  
5. Assign business responsibility for delivering benefits appropriate to IT reliability / opportunity  
6. Assure project risk management and responsibility appropriate to the project benefits to be gained
### Your Response?

<table>
<thead>
<tr>
<th>Your Response?</th>
<th>Don't know</th>
<th>Yes</th>
<th>Maybe</th>
<th>No</th>
</tr>
</thead>
</table>

### IT Questions for the Board:

- Are you sure that you have...
  - 1. Adequate IT governance?
  - 2. Appropriate IT investment levels?
  - 3. IT risks covered?
  - 4. Sufficient visibility of IT-related projects?
  - 5. Senior executive understanding of IT?
  - 6. Appropriate IT consultancy support?

### What Business Impact?

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Don't know</th>
</tr>
</thead>
</table>

Contact PSI Consultants for a no-obligation discussion
IT Questions for the Board

http://www.proteussystemsit.com/