IT GOVERNANCE IN AN E-BUSINESS WORLD

Vernon Poole
Agenda

1. e-Business Challenges
2. Business Threats
3. Business Opportunities
4. International Standards Update
5. IT Governance Framework
6. e-Business Conclusions
1. The e-Business Challenges

- organisations are embracing new business models to leverage the Internet
- organisations are connecting customers, partners and suppliers to IT resources or e-commerce and e-business
- in the new electronic environment there are new opportunities, but also new risks and responsibilities
- How do organisations conduct e-commerce and e-business safely?
The e-Security Challenge

• how secure is the enterprise?
• can you assess security vulnerabilities and measure the effectiveness of your corporate security policy?
• is the enterprise appropriately protected from unauthorised and unwanted entities?
• can you enable remote users, suppliers, partners and customers to access your network securely?
• can you manage and administer every user and resource across your organisation?
2. Business Threats

• Need for global awareness of increased security threats/vulnerabilities - information warfare, cyberthreats, denial of service attacks etc

• Need for improved controls - currently a patchwork of measures, developed in an uncoordinated, unstructured manner

• Need for internationally accepted best practice standards guidance - IT7799, COBIT, ITCG, IBAG???
3. Business Opportunities

- e Business - need for organisations to demonstrate effective control of IT/information to trading partners/customers/stakeholders

- Corporate Governance - need for better stewardship
Need for better stewardship

- Influence of corporate governance initiatives like ‘Turnbull Report’

- Call for ‘sound assessment of internal controls’ through a process of:
  - control environment
  - risk assessment
  - information & communication
  - monitoring
Control Environment

- Commitment to competence and integrity
- Communication of appropriate agreed standards and control consciousness
- Appropriate organisational structure to meet business objectives
- Sufficient time/resources allocated
- Create environment for risk/control learning
- Appropriate delegation of authority
Risk Assessment

• Identify key business, operational, financial and compliance risks

• Likelihood of ‘risks crystallising’ and significance of business impact

• Priorities for resource allocation

• Use of performance indicators to monitor activities/risks

• Relevant, reliable, up to date information systems

• Communication to right people, right time ……….
Information & Communication

- Complete and accurate accounting
- Appropriate authorisation limits
- Reliable processing and integrity
- Controls that limit exposure (loss or fraud)
- Checks re: supervision of control activities
- Compliance with laws and regulation
- Policy/operational manuals
Monitoring

- Ongoing monitoring process embedded in operations (reasonable assurance - appropriate controls)
- Identify changes which impact on ‘internal control system’
- Formal/timely procedures for reporting weaknesses and appropriate corrective action
- Adequate high level support on internal controls in public statements
4. International Standards Update

- CICA : ITCG
- ISACA : COBIT2 (under review)
- IIA : IS Management & Assurance
- BSI : BS7799/I7799
- EU : IBAG
ITCG : Background

• **ITCG** - *Information Technology Control Guidelines (third edition) - November 1998*

• **Author** - *Canadian Institute of Chartered Accountants*

• **Aim** - *Practical means of identifying, assessing and implementing IT controls based on risks:*
  - technology independent
  - applicable to all types of organisation

• **Focus** - *Control Areas (7)*
  - Control Objectives (31)
  - Minimum Control Standards (162)
  - Control Techniques
ITCG : Control Areas

1. Risk Management and Control
2. IT Planning
3. Acquisition, Development and Maintenance of Information Systems
4. Computer Operations and Information Systems
5. IT Security
6. Business Continuity and Disaster Recovery Planning
7. Application Based Controls
COBIT: Background

- Attention on Corporate Governance
- Management Accountability for Resources
- Specific Need for Control of IT Resources
- Business Orientated Solutions
- Framework for Risk Assessment
- Authoritative Basis
- Improved Communication Among Management, Users and Auditors
One of the most challenging tasks will be getting top management’s attention. Two tools for getting management’s attention and raising management’s awareness are:

**IT Governance Self-Assessment**

**Management’s IT Concerns Diagnostic**
COBIT: Scope and Objectives

- Generally Applicable and Accepted Standard for Good Practice for Information and Information Technology (IT) Control
- For Application to Enterprise-Wide IT
- Starting from a Framework for Control in IT
- Based on ISACF’s Control Objectives
- Management Orientated
- Aligned with De Jure and De Facto Standards and Regulations
- Based on Critical Review of Tasks and Activities Regarding Business Re-Engineering
COBIT : Standards and Regulations

- Technical standards from ISO, EDIFACT, etc
- Codes of Conduct issued by Council of Europe, OECD, ISACA etc
- Qualification criteria for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc
- Professional standards in internal control and auditing: COSO report, IFAC, IIA, AICPA, GAO, PCIE, ISACA standards etc
- Industry practices and requirements from industry forums (ESF, 14) and government-sponsored platforms (IBAG, NIST, DTI), etc
- Emerging industry specific requirements such as from banking, electronic commerce and IT manufacturing
COBIT Framework
COBIT : Product Family

4 major elements

- COBIT as an open standard for increased world-wide adoption covering summary, framework and detailed control objectives;

- Three proprietary guideline products
  - Implementation Tool Set : how to introduce the COBIT standard in the enterprise
  - Audit Guidelines : how to audit against the standard
  - Management Guidelines : how to benchmark, implement and self-assess
IIA : IS Management & Assurance
- A Call to Action for Corporate Governance (April 2000)

- Launched at Critical Infrastructure Assurance Summit Conference - Washington DC to address IS threats

- Organisers - IIA, AICPA, ISACA

- Need for action - US Federal Government call, for both improved IS practices and meaningful assurance that IS risks are being effectively managed
IIA - IS Management & Assurance Report

**Background**  -  written by team of 5 experts (advisory board of 100)

**Content**  -  Key responsibilities including audit

- Process for managing IS risks

- Major guidance documents (AICPA, BS7799, COBIT, OECD)

- List of selected references
BS7799: Imperative

- Authoritative surveys show that security risks to information systems are increasing e.g. ISBS 2000

- Organisations are becoming vulnerable to security threats from greater dependence on IT systems and services especially with the e-business/e-government growth
BS7799 Part 1 : 10 Guiding Principles

1. **IS policy document**
2. **Allocation of security responsibilities**
3. **IS education and training**
4. **Reporting of security incidents**
5. **Virus controls**
6. **Business continuity planning process**
7. **Safeguarding of organisation’s records**
8. **Control of proprietary copying**
9. **Legal compliance**
10. **Compliance with IS policy**

*Basis for the Code of Practice - hopefully will become an ISO standard in August 2000*
BS7799 Part 2 : 10 Baseline Controls

1. IS Policy
2. Security Organisation
3. Asset Classification/Control
4. Personnel Security
5. Physical/Environmental Security
6. Computer and Network Management
7. System Access Control
8. Systems Development/Maintenance
10. Compliance

Basis for an ISMS Assessment (Information Security Management System)
EU : IBAG Background

- IBAG = Infosec Business Advisory Group of the European Community

- Members
  - European Security Forum (ESF)
  - Comité Européen des Assurances (CEA)
  - International Chamber of Commerce (ICC)
  - International Information Integrity Institute (I4)
  - Associated Banks of Europe Corporation (ABECOR)
  - Information Systems Audit and Control Association (ISACA)
  - European Confederation of Institutes of Internal Auditing (ECIIA)
  - X/Open, OSITOP, EWOS, ECMA, EUROBIT,...
EU : IBAG Framework

“Creating the Information Security Management System”

Policy
- Security Policy
- Organisation
- Ownership
- Awareness

Practice
- Areas/Topics
- Baseline Controls
- Specific Controls

Procedures
- Installation/Operation
- Monitoring/Review
5. **IT Governance Framework**

- **Creation of ‘IT Governance Institute’ by ISACA in late 1999**

- **Mission** - to assist enterprise leadership in ensuring long-term, sustainable success and increased stakeholder value by expanding awareness of the need for and benefits of effective IT Governance

- **Role** - develop and advance ‘awareness of the vital link between IT and Enterprise Governance - offer best practice guidance on the management of IT-related risks.'
IT Governance: Governance Family

Past/Present

CORPORATE GOVERNANCE
Finance
Business operations
Legal compliance
Ethics/Integrity
Director Responsibilities
Asset Management

Healthy/Sustainable

ENTERPRISE GOVERNANCE
Business Goals and Objectives
Knowledge Management
Business Communication
Customer Relations
Activities and Processes

Future

IT GOVERNANCE
IT Objectives
Information System
Technology/Networks
IT Knowledge Management
IT Asset Management
E-Business
IT Legal/Regulatory Compliance
IT Governance means:-

- IT is aligned with business, enables the business and maximises benefits

- IT resources are used responsibly

- IT related risks are managed appropriately

I.e. an inclusive term, which encompasses - information systems, technology and communication, business, legal and other issues, all concerned stakeholders
IT Governance - Alignment with Business

Risks
- strategic IT plan not based on business plan
- technological direction unclear
- business requirements unclear
- no common understanding of services

Challenges
- IT to keep pace with changing business objectives
- IT related risks growing especially with e-business
- business managers forced to manage adequacy of internal controls
IT Governance - IT Resources used Responsibly

Risks  -  IT project overruns (time budget)
        -  IT customer requirements not met
        -  user requirements not satisfied
        -  IT platform does not support business applications

Needs -  personal accountability of IT resources
         -  acquisition decisions business led
         -  demonstrate adequate stewardship
IT Governance - Risks managed Appropriately

Risks
- emerging technologies not managed
- non-compliance to legal/regulatory issues
- threats to IT services not recognised

Risk Management
- highlight most critical IT resources
- agree and communicate the level of protection required
- define and implement monitoring and incident handling
IT Standards : Technical References

COBIT / IT Governance : www.isaca.org

IIA : www.theiia.org

BS7799 : www.c-cure.org

ITCG : www.cica.ca

OECD : www.oecd.org
e-Business is still a brand new phenomenon

• Need to adopt best practices?

• Need to adopt a new way of thinking - from “traditional” (controlling) view to “new” (enabling) view
The Traditional View

- **Focus on employee access**
  - *identification implies authorisation*

- **Assets are centralised**
  - *databases are best protected in the IT centre*

- **Controls are predominately preventative**
  - *to stop inappropriate action*

- **Information Technology determines the requirements**
  - *“Nanny knows best”*
A Situation Report

- Today’s approach is flawed
- Security paranoia leads to:
  - lost opportunity
  - crippling complexity
  - imprudent investment
  - impossible expectations
- Implementors have difficulty handling:
  - wider access requirements
  - decentralised assets
  - threat proliferation
  - increasing requirements
Changing paradigms

- **Internal focus** - Access for employees only
- **Centralised assets** - ‘Bunker approach’
- **Prevention goals** - Stop loss
- **CIO controls** - Technology mandates

- **External focus** - Access for all business partners
- **Distributed assets** - ‘No boundaries’ philosophy
- **Generation goals** - Make money
- **COO controls** - Business mandates
### ‘New’ View - Movement To An Enabling Concept

<table>
<thead>
<tr>
<th></th>
<th>Traditional View</th>
<th>New View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Block threats</td>
<td>Enable access</td>
</tr>
<tr>
<td>Principle</td>
<td>Deny</td>
<td>Allow</td>
</tr>
<tr>
<td>Method</td>
<td>Prevent</td>
<td>Account</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Stick</td>
<td>Carrot</td>
</tr>
<tr>
<td>Approach</td>
<td>Reactive</td>
<td>Proactive</td>
</tr>
<tr>
<td>Control</td>
<td>Centralised</td>
<td>Distribute</td>
</tr>
<tr>
<td>Scalability</td>
<td>Poor</td>
<td>Good</td>
</tr>
</tbody>
</table>
Arguments For

• Risk management in action

• Puts money where the risk is

• Reduces impediments

• Increases effectiveness

• Improves response times

• Enables additional revenue generation
IT Governance : Contact Point

Vernon Poole
Deloitte & Touche
Gainsborough House
34-40 Grey Street
Newcastle upon Tyne
NE1 6AE

Telephone : 0191 202 5330

E-mail : vernon.poole@deloitte.co.uk