What Auditors Want

14th February 2008

John Mitchell
PhD, MBA, CEng, CITP, FBCS, FIIA, MIIA, CISA, QiCA, CFE

LHS Business Control
47 Grangewood
Potters Bar
Herts EN6 1SL
England

Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Cell: +44 (0)7774 145638
john@lhscontrol.com
www.lhscontrol.com
Themes

- What we are
- What we do
- What we need
- Why we need it
- What you get in exchange
- A better way?
About IRMA

• Information Risk Management & Assurance SG
• The oldest specialist group in the BCS
• Officially recognised in 1965, but in existence since 1962
• Previously the Information Risk Management & Audit SG
• Before that we were the Auditing By Computer SG
Some Views of Audit
Our View!
What We Do

• Primary
  – Provide *assurance* that IT is well controlled, is adequately performing and is providing value for money

• Secondary
  – *Assist* in developing well controlled business solutions
Governance v Assurance

• IT Governance
  – The leadership, structure, relationships, processes and monitoring that ensure IT sustains & extends the enterprise's strategies & objectives by adding value while managing associated risk

• Assurance
  – The provision of a statement that inspires confidence:
    • A guarantee or pledge
    • Freedom from doubt
    • Certainty
The APG

- Deals with developments in programming languages, environments and techniques

- New stuff

- New risks

- New assurance requirements
Assurance Frameworks

COSO

CobiT

ISO 9126

ISO 27001

ISO 20001

ITIL
ISO 9126 Components

- Functionality
- Reliability
- Usability
- Efficiency
- Portability
- Maintainability

Are the required functions available in the software?
How easy is to transfer the software to another environment?
How easy is to modify the software?
How reliable is the software?
Is the software easy to use?
How efficient is the software?
SEI Process Maturity Concept

Non-Existent

Initial

Repeatable

Defined

Managed

Optimised

0

1

2

3

4

5

© John Mitchell
How Assurance Works
IT Processes

IT ASSURANCE PROGRAMME

Plan & Organise
- Strategic Planning
- Information Architecture
- Technological Direction
- IT Organisation & Relationships
- Manage the IT Investment
- Communicate Aims & Direction
- Manage IT human resources
- Manage quality
- Assess & manage IT Risks
- Manage Projects

Acquire & Implement
- Identify Solutions
- Acquire & Maintain applications
- Acquire & Maintain infrastructure
- Enable operations
- Procure IT resources
- Manage changes
- Install & Accredit Solutions

Deliver & Support
- Define Service Levels
- Manage third-party services
- Manage performance and capacity
- Ensure continuous service
- Ensure systems security
- Identify and allocate costs
- Educate and train users
- Manage service desk
- Manage the configuration
- Manage problems
- Manage data
- Manage the physical environment
- Manage operations

Monitor & Evaluate
- Monitor & evaluate performance
- Monitor & evaluate internal control
- Ensure regulatory compliance
- Provide IT governance

© John Mitchell
Development Assurance Underpinning

- ISO 9126 (Software Product Evaluation)
- ISO 12207 (Software Life Cycle)
- ISO 15504 (Software Process Assessment)
- ISO 90001 – (Quality within the SDLC)
- ISO 20001 – (Service Delivery)
- ISO 27001 (Information Security)
- Control Objectives for IT (CobiT)
Where We Fit In

Corporate Governance

IT Governance

Finance Governance

Marketing Governance

IT Assurance

Risk Management

ISO 27001
Security

ISO 20001
Delivery

ISO 9126
Development

ITIL

TickIT
We Have The Tools

- International standards
- Assurance processes (CobiT)
- Professionalism
  - BCS
  - ISACA
- Qualifications
  - CISA, QiCA, MIIA, PIIA, MBA, MBCS, etc.
- Computer Assisted Audit Techniques (CAATs)
Assurance Roadmap

- **Prepare Strategic Plan**
  - Process Maturity Assessment
  - Risk Identification
  - Gap Analysis between CobiT processes & inherent risks
  - Gap Analysis between processes maturity & residual risks
  - Prepare strategic plan
  - Select processes for assurance

- **Prepare Tactical Plan**
  - Understand process operation
  - Identify value drivers
  - Identify risk drivers
  - Select control objectives
  - Select control practices
  - Identify process owners

- **Prepare Assurance Plan**
  - Interview process owners
  - Select control tests
  - Prepare assurance documentation

- **Test for Assurance**
  - Test control design
  - Test control effectiveness
  - Document impact of control weakness

- **Report Opinion**
  - Prepare draft report
  - Obtain agreement & commitment
  - Issue final report

© John Mitchell
We Are Interested In

• The SDLC process
• Development risk management
• Meeting customer requirements
• Providing functionality
• Ensuring performance
• Security
  – Confidentiality
  – Integrity
  – Availability
• Change management
• Testing (not just the logic)
• Quality Assurance
• Conformance with internal & external policies and standards
Reaching The Desired Solution

Constraints (Technology)

Current Situation

Constraints (Time)

Desired Solution

Constraints (Legislation)

Constraints (Resource)
Technology Developments 1970 to Present

- Single batch program
- Batch Multi-tasking
- On-line retrieval
- Real-time update
- Stand alone PCs
- Networking
- File servers & distributed processing
- Internet, Intranet & Extranet
- Palm Devices
- Phone devices
- Implants
Sources of Development Risk

- Poor Project Management
- Bad Design
- Inferior Build
- Bad Implementation
Traditional ‘Waterfall’ SDLC

Terms of Reference
Feasibility Study
Systems Analysis
Systems Design
Program Design
Program Coding
Testing (program/system/user)
Implementation
Maintenance
Real Development Life Cycle

- Enthusiasm
- Disillusionment
- Search for the Guilty
- Punishment of the Innocent
- Rewards for New Participants
"It must be remembered that there is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage, than the creation of a new institution. For the initiator has the enmity of all would profit by the preservation of the old institution and merely lukewarm defenders in those who would gain by the new one"

Machiavelli 1532
Why Rewards For New Participants?

Start → T0 → T1 → T2 → T3 → TIME

- Original Request
  - Original Authorised

- Revised Request
  - New Goal Authorised

- Project Leader
  - Sacked

New Project Leader
Building Quality Systems Requires Achievement of ….

- Functionality
- Performance
- Timescale
- Cost
- Maintainability
Development Constraints

Functionality

Quality

Time

Cost
# New British Aircraft Carriers

<table>
<thead>
<tr>
<th>Year</th>
<th>Tonnage</th>
<th>Est. Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>35,000</td>
<td>£2.8 Billion</td>
</tr>
<tr>
<td>2003</td>
<td>50,000</td>
<td>£2.8 Billion</td>
</tr>
<tr>
<td>2008</td>
<td>65,000</td>
<td>£2.8 Billion</td>
</tr>
</tbody>
</table>
Conformance & Performance

Business

IT Processes

requirements information

Control Objectives

Controlled by

Made effective and efficient with

Audited by

Activity Goals

Assurance Guidelines

Control Practices

Measured by

For performance

For outcome

For maturity

Key Performance Indicators

Key Goal Indicators

Maturity Models

For conformance
What We Want  
(Co-active Auditing)

• Audit & IT work together  
• “Open book” approach  
• IT understand the risks (hopefully)  
• Audit understand the controls (hopefully)  
• Working together provides a synergy  
• Problems are identified and IT propose any required solutions
Summary

• We want evidence that the software will:
  – Do only what it is required to do
  – Be reliable in operation
  – Be robust and handle all error conditions
  – Be suitably documented
  – Be easy to maintain

• We look at the integrity of the development process, from requirement to implementation & subsequent maintenance

• We prefer to work with developers

• Getting it right in the first place is more important than finding that it is wrong subsequently
Questions?

John Mitchell
PhD, MBA, CEng, CITP, FBCS, MBCS, FIIA, MIIA, CISA, QiCA, CFE

LHS Business Control
47 Grangewood
Potters Bar
Hertfordshire  EN6 1SL
England

Tel: +44 (0)1707 851454
Fax: + 44 (0)1707 851455
Cell: +44 (0)7774 145638

john@lhscontrol.com
www.lhscontrol.com