LHS

What Auditors Want

14th February 2008

John Mitchell

PhD, MBA, CEng, CITP, FBCS, MBCS, 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

LHS

Themes

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

LHS

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

LHS

Some Views of Audit

LHS

Our View!

LHS

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

LHS

Governance v Assurance

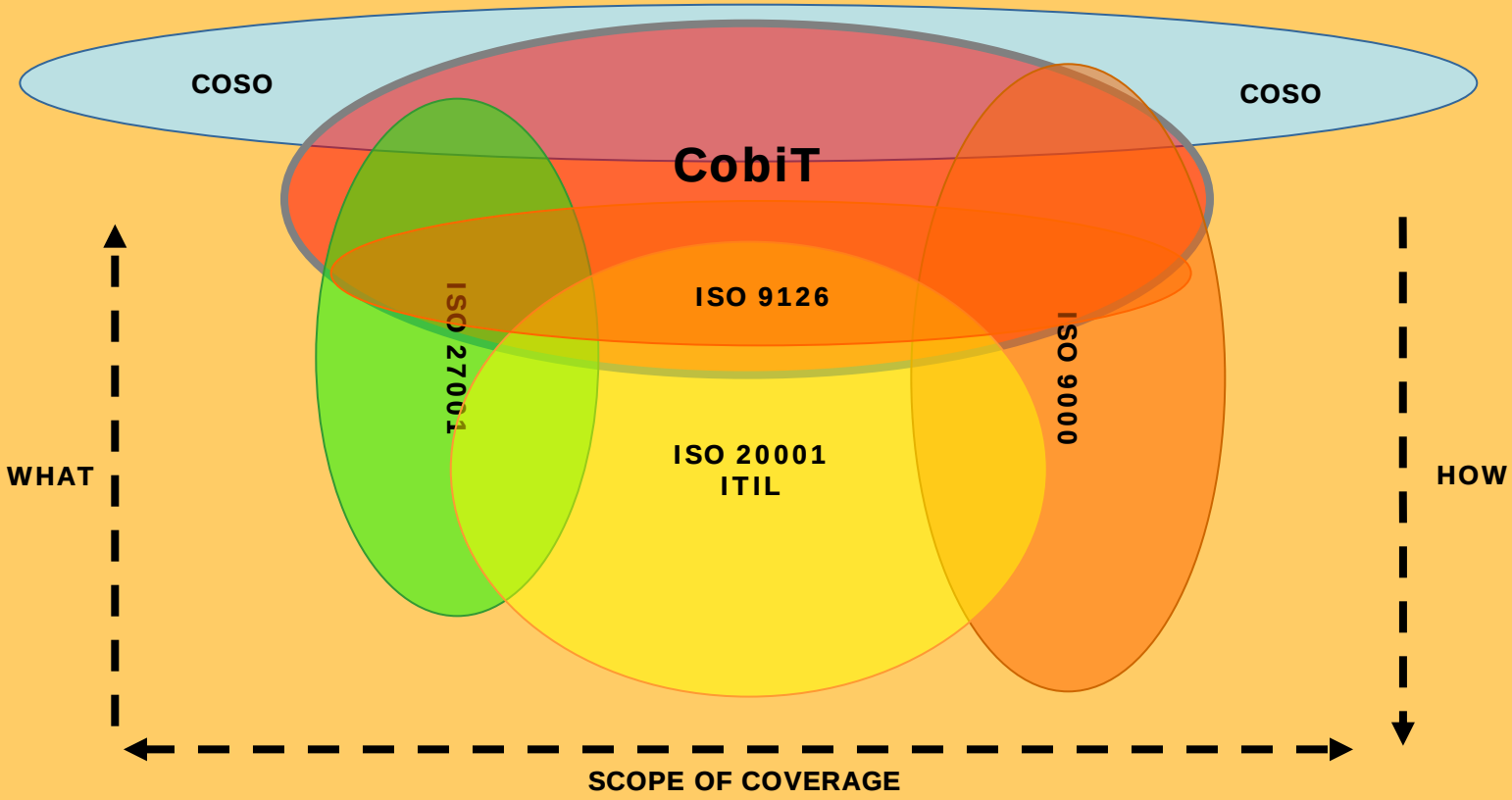
- IT Governance
  - The leadership, structure, relationships, processes and monitoring that ensure IT sustains & extends the enterprise's strategies & objectives by adding value while managing associated risk
- Assurance
  - The provision of a statement that inspires confidence:
    - A guarantee or pledge
    - Freedom from doubt
    - Certainty

LHS

The APG

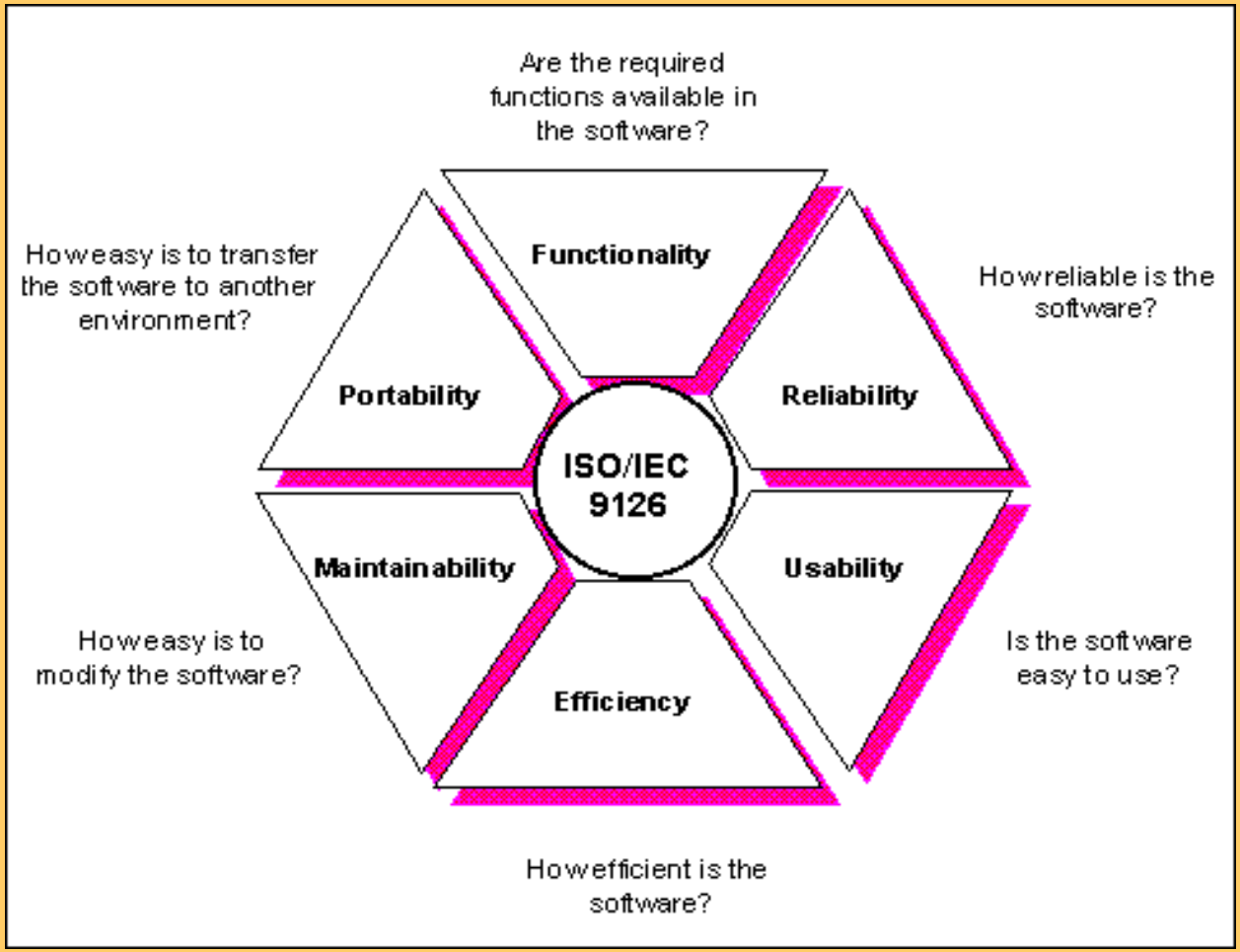
- Deals with developments in programming languages, environments and techniques
- New stuff
- New risks
- New assurance requirements

Assurance Frameworks



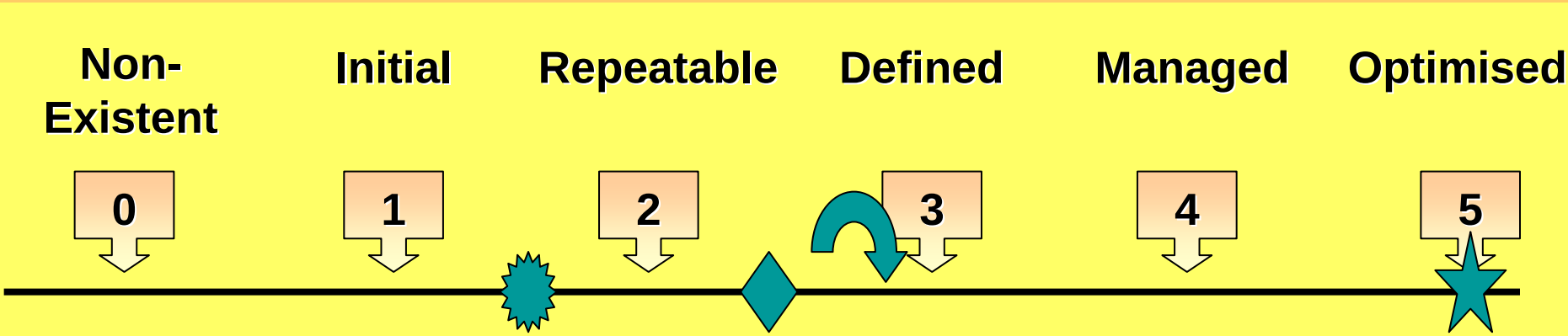
LHS

ISO 9126 Components



LHS

SEI Process Maturity Concept

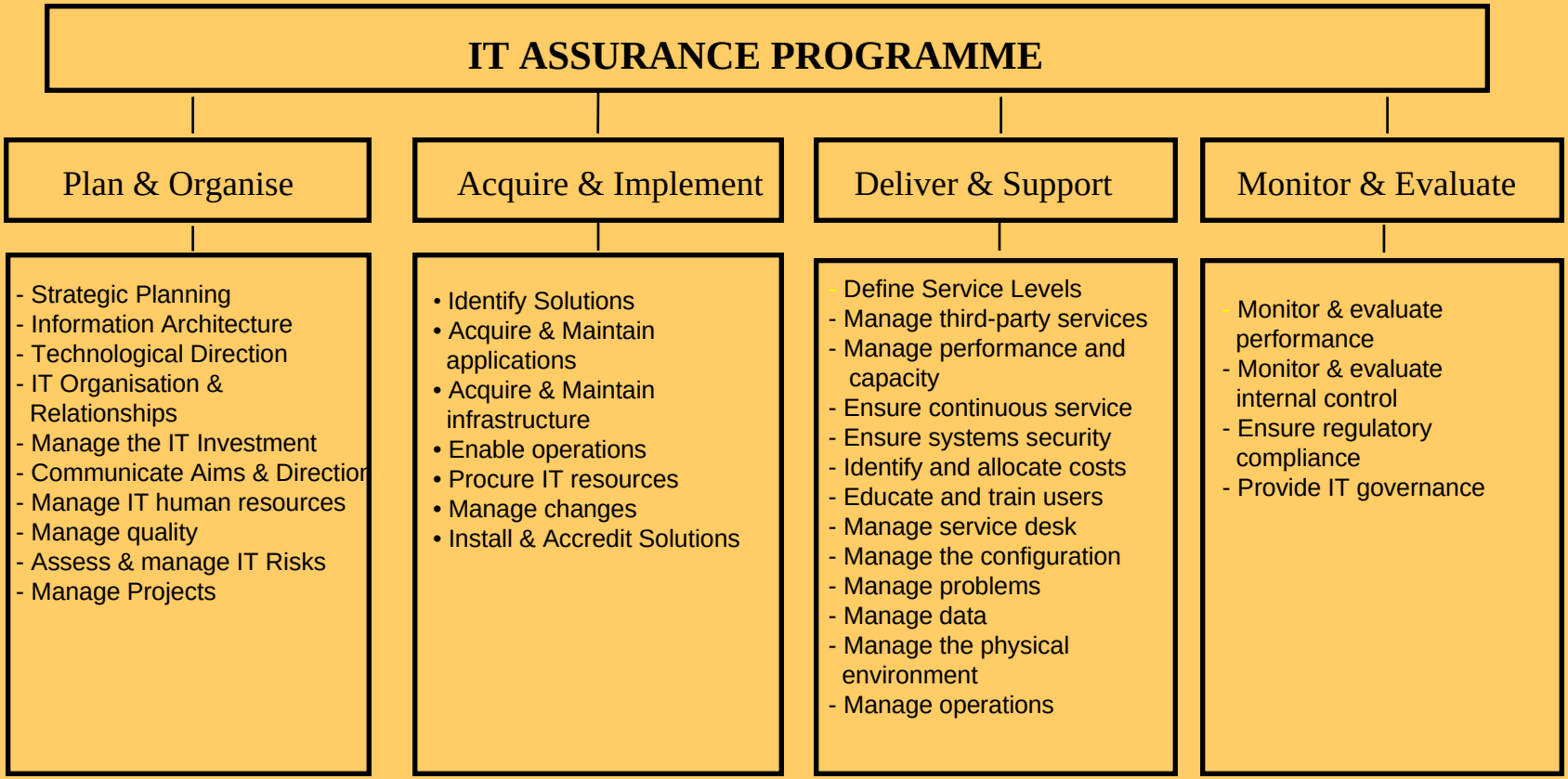


LHS

How Assurance Works

LHS

IT Processes



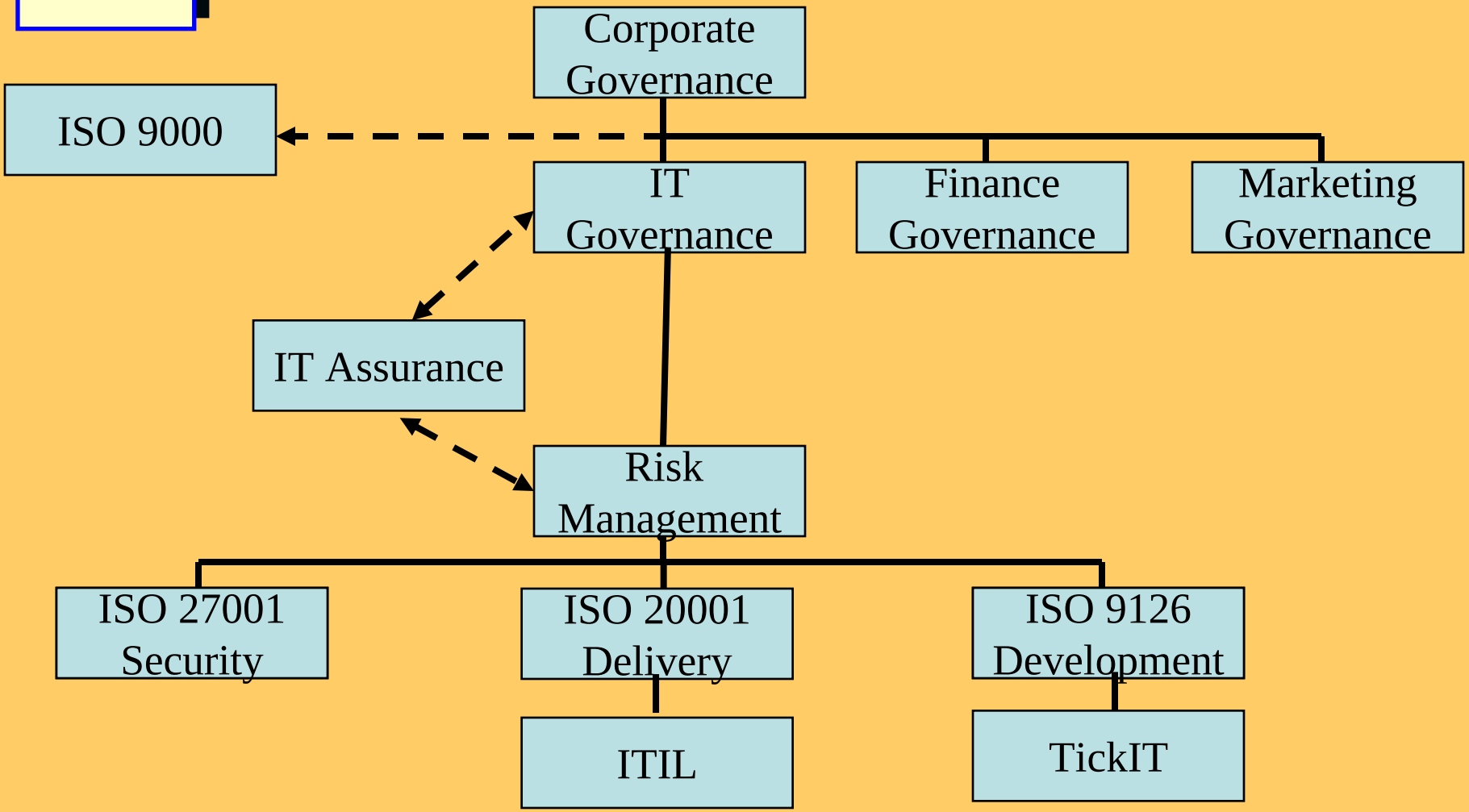
LHS

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)

LHS

Where We Fit In



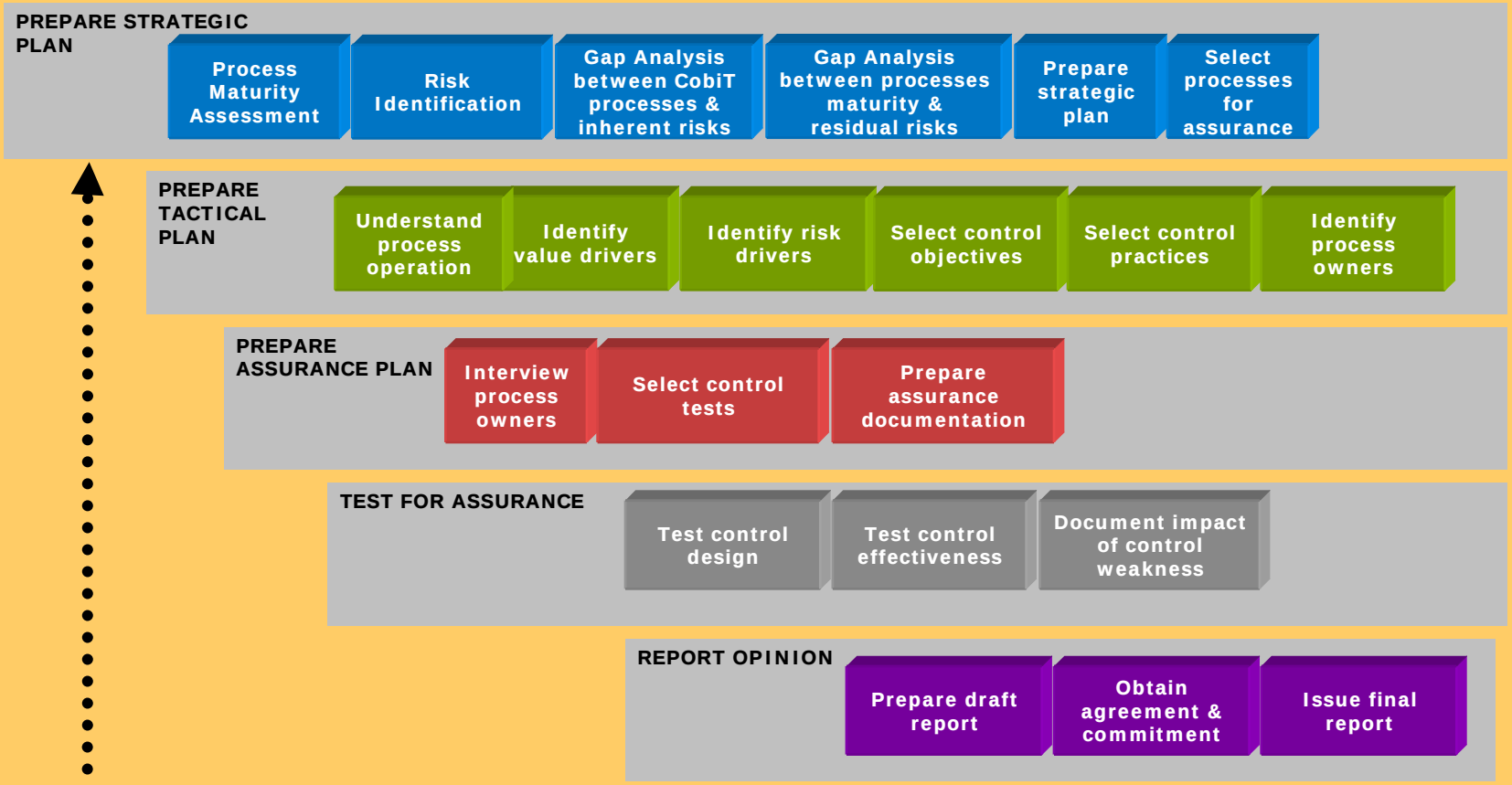
LHS

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)

LHS

Assurance Roadmap

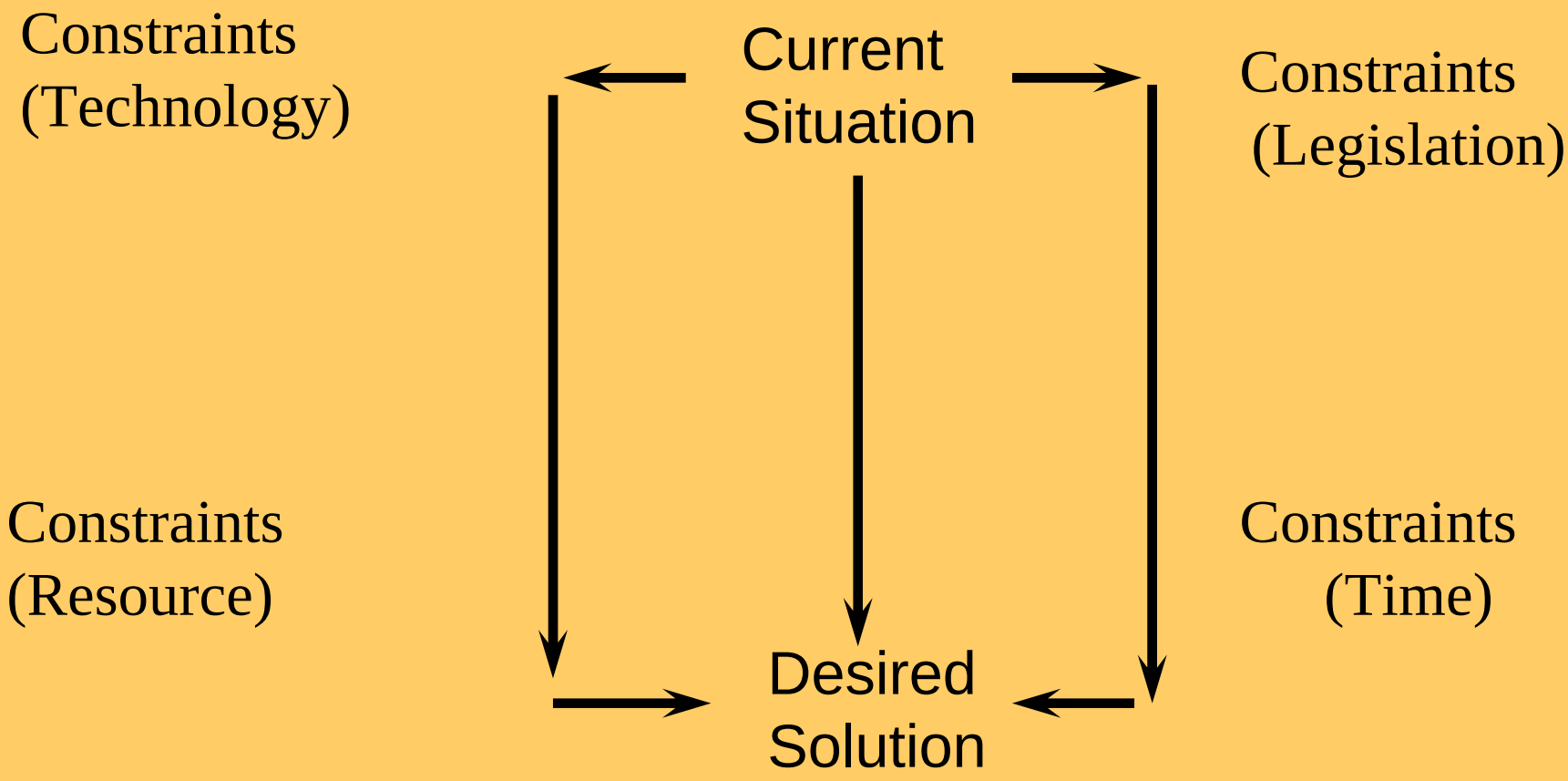


LHS

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



LHS

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

LHS

Sources of Development Risk

- Poor Project Management
- Bad Design
- Inferior Build
- Bad Implementation

LHS

Traditional ‘Waterfall’ SDLC

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

LHS

Real Development Life Cycle

Enthusiasm

Disillusionment

Search for the Guilty

Punishment of the Innocent

Rewards for New Participants

LHS

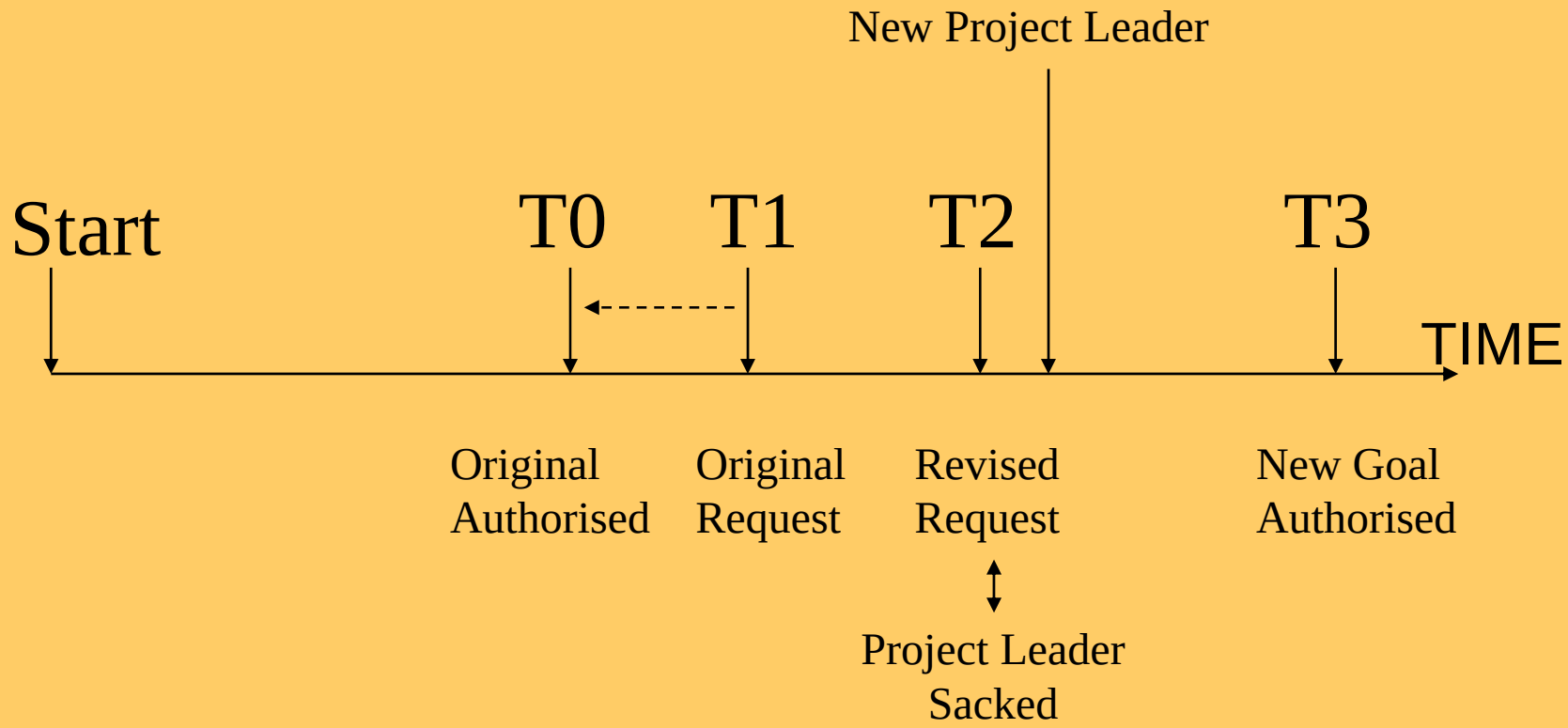
The Dangers

"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

LHS

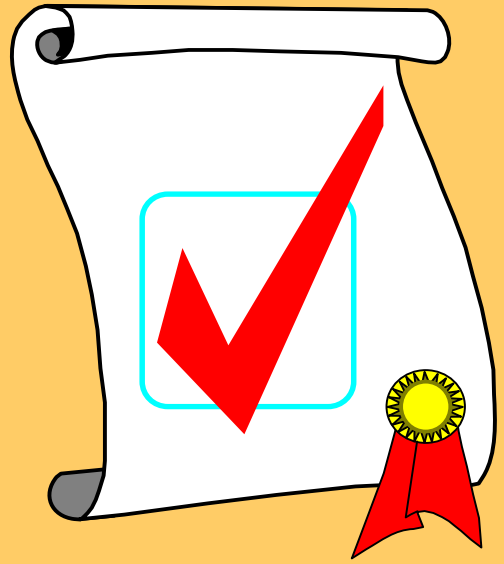
Why Rewards For New Participants?



LHS

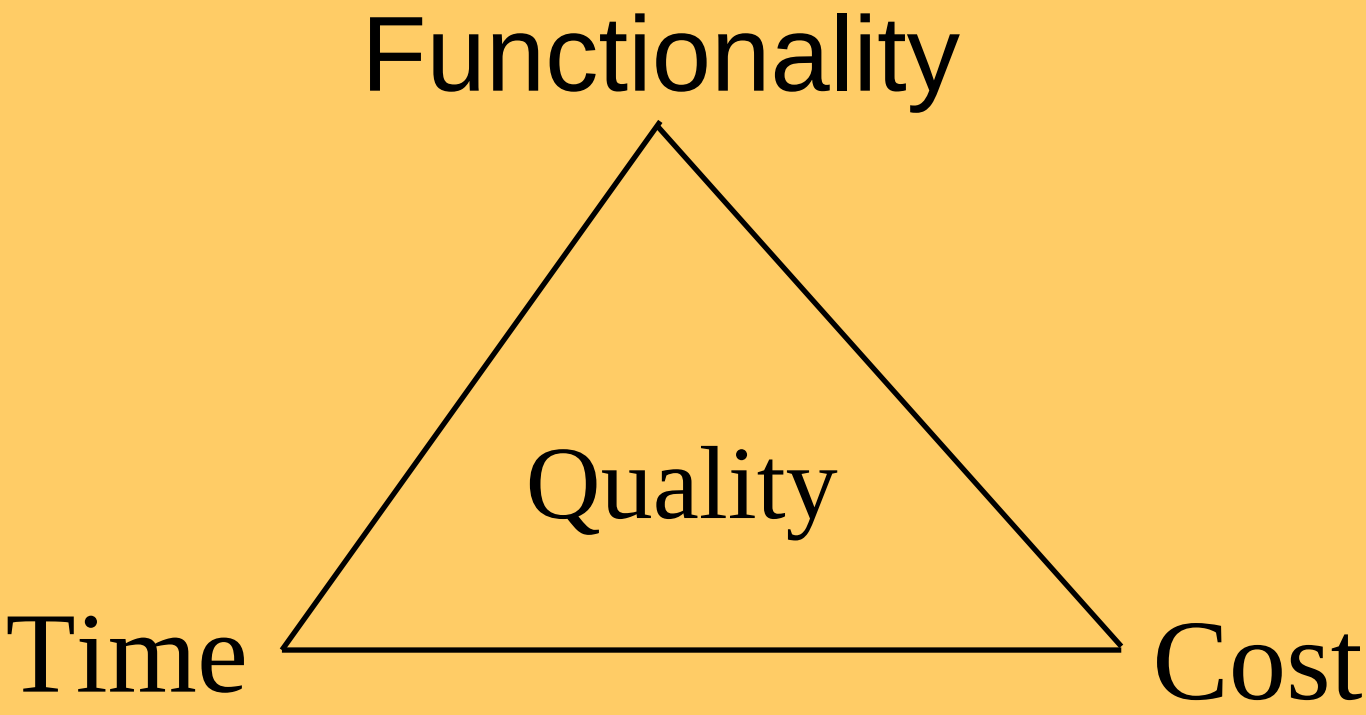
Building Quality Systems Requires Achievement of …..

- Functionality
- Performance
- Timescale
- Cost
- Maintainability



LHS

Development Constraints

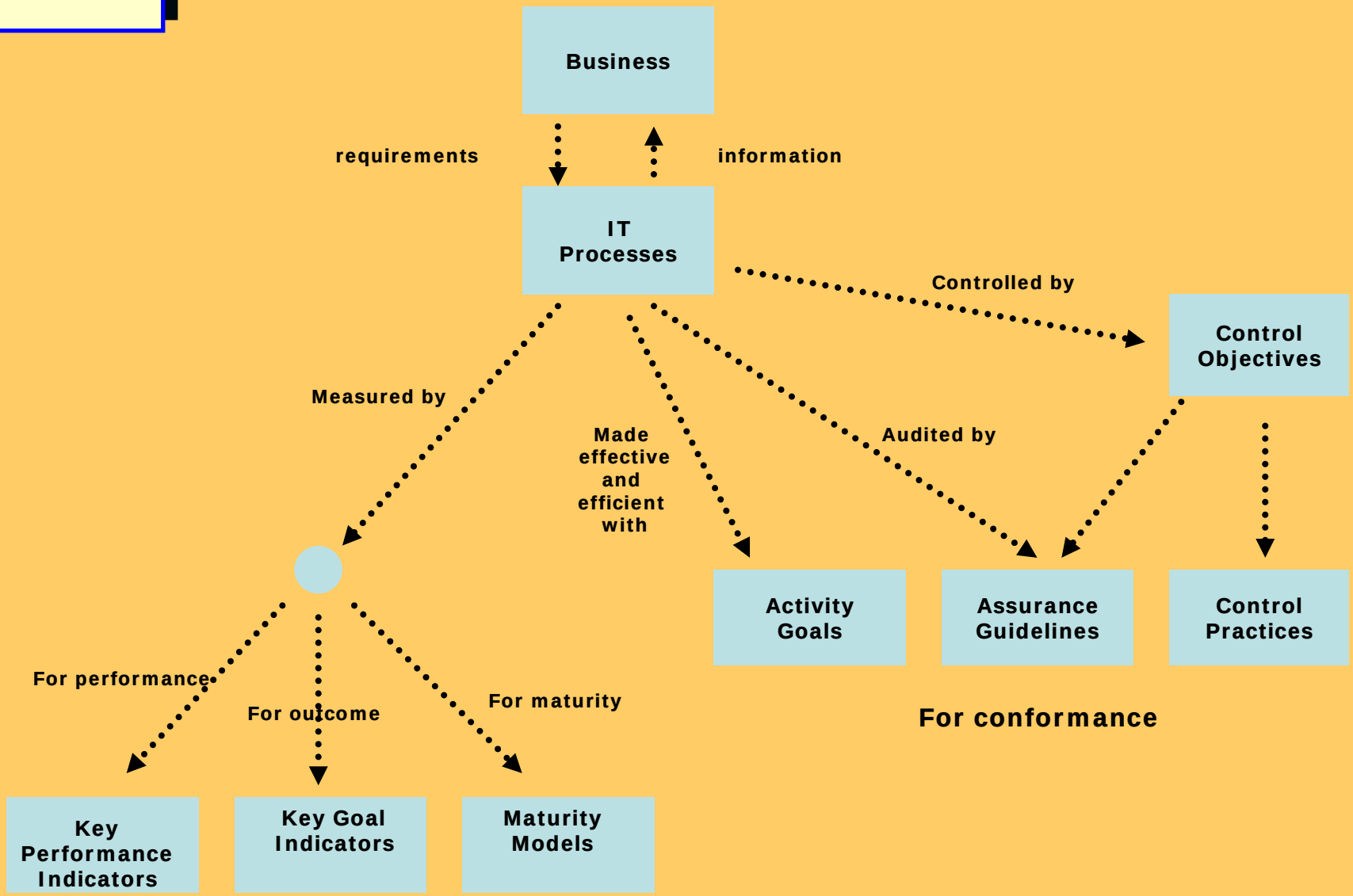


LHS

New British Aircraft Carriers

Year	Tonnage	Est. Cost
1996	35,000	£2.8 Billion
2003	50,000	£2.8 Billion
2008	65,000	£2.8 Billion

Conformance & Performance



LHS

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

LHS

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

LHS

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