REFLECTIONS ON RISK AND VALUE IN ENTERPRISE GOVERNANCE OF IT

A story of risk, value, uncertainty, aircraft carriers, racing cars and sailing trips.

Erik Guldentops, Antwerp Management School, Belgium
Positioning risk and value within enterprise governance of IT
Enterprise Governance of IT

Top management needs to know that IT is:

- Likely to achieve its objectives
- Resilient enough to learn and adapt
- Judiciously managing its resources
- Appropriately recognising opportunities
- Obtain enterprise value from IT enabled business initiatives
- Applying “due care” about IT related risks

From “The IT Governance Briefing”, ITGI. [www.isaca.org](http://www.isaca.org)
Essentially two things

Risk and Value

Enterprise Governance of IT

- Essentially two things
- Risk and Value
- Entirely intertwined

Value = (Benefits – Costs) adjusted for Risk

Risk and Value

From “ValIT Governance of IT Investments, www.isaca.org
Translate strategy into action
- Increase automation (make the business effective)
- Decrease cost (make the enterprise efficient)
- Manage risks (security, reliability & compliance)

Set Objectives
- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT-related risks are managed appropriately

Evaluate performance

Provide direction

Measure and report performance

Translate direction into strategy

IT GOVERNANCE

IT MANAGEMENT

www.isaca.org
IMPLEMENTING IT GOVERNANCE

Considers the major IT processes

1. Strategic Planning
2. Business/IT Alignment
3. Portfolio Management
4. Programme Management
5. Enterprise Architecture
6. Resource Management
7. Solution Delivery
8. Service Delivery
9. Enterprise Change Management
10. Cost Optimisation
11. Innovation
12. Risk Mitigation

Monitor
Direct
Evaluate
IMPLEMENTING IT GOVERNANCE

Responds to 5 fundamental questions

- Are we doing the right things?
- Are we doing them the right way?
- Are we governing things properly?
- Are we getting the benefits?
- Are we doing them well?
IMPLEMENTING IT GOVERNANCE

The Board providing high level direction and control.

Executive Management translating direction into plans, focusing on the bottom-line results.

Line Management translating plans into action and ensuring adequate performance.

How do we govern IT?

- Monitor
- Direct
- Evaluate

Are we doing the right things?
1. Strategic Planning
2. Business/IT Alignment
3. Portfolio Management

Are we getting the benefits?
10. Cost Optimisation
11. Innovation
12. Risk Mitigation

Are we doing them in the right way?
4. Programme Management
5. Enterprise Architecture
6. Resource Management

Are we doing them well?
7. Solution Delivery
8. Service Delivery
9. Enterprise Change Management

Performance Drivers
Outcome Measures
Where do we want to be?

Objectives

IT Strategy

How do we know we are progressing?

IT Scorecards

• Delivery Performance
• Service Quality
• Resource Utilisation
• Benefits Realisation
• Risk Reduction

What are we doing to achieve them?

IT Business Cases

Portfolio
• Programmes
• Projects
• Services
• Resources

The engines of IT Governance
Implementing IT Governance

Why invest in better governance of IT Risk and IT Value?

McKinsey & London School of Economics surveying 100 companies – Oct 2005
How well are we doing in respect of minimising risk and optimising value of IT?

RISK AND VALUE
Enterprise Governance of IT

How are we dealing with Risk and Value?

A medium-sized international bank has to decide to make a loan of 500,000,000$ several points above premium interest, for three years but ‘callable’ after two, to a country about which it has the following facts:

- weak currency
- more than 20% inflation
- industrial potential used at only 60%
- unemployment at over 12%
- international conflict verging on war
- heavy racial riots
- weak leadership, i.e. leadership vacuum
- heavy internal and international debt
<table>
<thead>
<tr>
<th></th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do I accept the loan? Before I decide, what extra question would I ask?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>2. Do I consider myself a better than average driver?</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>3. Traffic accidents cause more deaths than stomach cancer</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>4. Do I take the 1000€ check offered to me or do I flip a coin to receive 4000€ if it is ‘heads’ and nothing if it is ‘tails’?</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Enterprise Governance of IT

How are we dealing with Risk and Value?
Risk and Value Management – A survey

▶ Is there personal bias?
▶ Are we objective?
▶ Have we asked the right questions?
▶ Are we influenced by “sensational” data?
▶ Do we estimate our capabilities correctly?
How well is the industry doing in respect of minimising risk and optimising value of IT?

RISK AND VALUE
Enterprise Governance of IT

How are we dealing with Risk and Value?

- Process maturity
- Portfolio approach
- Financial transparency of projects
- IT Intensity
- Percentage of new developments
- etc

ITGI, ING and IBM – 2006 – in support of VaIT
# Enterprise Governance of IT

**How are we dealing with Risk and Value?**

## IT Value Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Results CIO Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT-enabled investments will be managed as</strong> a portfolio of investments.</td>
<td></td>
</tr>
<tr>
<td><strong>IT-enabled investments will include the</strong> full scope of activities that are required to achieve business value.</td>
<td></td>
</tr>
<tr>
<td><strong>IT-enabled investments will be managed through their</strong> full economic life cycle.</td>
<td></td>
</tr>
<tr>
<td><strong>Value delivery practices will recognize that there are</strong> different categories of investments that will be evaluated and managed differently.</td>
<td></td>
</tr>
<tr>
<td><strong>Value delivery practices will define and monitor</strong> key metrics and will respond quickly to any changes or deviations.</td>
<td></td>
</tr>
<tr>
<td><strong>Value delivery practices will engage all stakeholders and assign appropriate accountability for the delivery of capabilities and the realization of business benefits.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Value delivery practices will be</strong> continually monitored, evaluated and improved.</td>
<td></td>
</tr>
</tbody>
</table>

*ITGI, ING and IBM – 2006 – in support of ValIT*
Enterprise Governance of IT

How are we dealing with Risk and Value?

IT Solution Delivery
IT Operational Implementation

Business changes
Business integration

IT Service Delivery
Benefit Realisation

Programme design and initiation

Asset Lifecycle & Configuration Management

Effective ITSM
To ITIL and beyond!
www.effectiveitsm.com
Enterprise Governance of IT

How are we dealing with Risk and Value?

Project failures and budget overruns have a weak correlation with:

- Fit with strategy
- Reuse of the resources
- Commitment of top management

High-risk IT-projects do well and have a strong correlation with:

- Internal Rate of Return is high
- Business demand is high
- The solution is innovative
- Strategic impact is high
Enterprise Governance of IT

How are we dealing with Risk and Value?

We don’t learn from our past

ROI as expected in the Business Case

Expected Benefits

Budgeted ROI = \( \frac{\text{€114 m} - \text{€100 m}}{\text{€100 m}} \times 100\% = +14\% \)

Expected Budget

Actual ROI allowing for typical solution delivery performance

Functionality achieved -16%  

Approximately 6 months delay, so benefits discounted at 12% After - Tax Rate

Budget Overrun +24%

Actual ROI = \( \frac{\text{€114 m} \times 84\% \times \frac{1}{1.12} - \text{€100 m} \times 124\%}{\text{€100 m} \times 124\%} \times 100\% = -38\% + 14\% \)

Cumulative cash flow (€)
Enterprise Governance of IT

How are we dealing with Risk and Value?

We don’t learn from our past

Correction in the business case vs. Solution Delivery Performance

Theoretical curve

Good fit

Empirical curve
Enterprise Governance of IT

How are we dealing with Risk and Value?

- Technical
- Supervisory
- Middle Management
- Executive

Senior Management

Assess Respond Follow up

Report

React to events

- Articulate Risk
- Maintain Risk Profile
- Analyse Risk
- Collect Risk related Data
- Supply Info for Business Decisions
- Integrate with ERM
- Establish & Maintain a Common Risk View

Other

Perform Compliance
Enterprise Governance of IT

How are we dealing with Risk and Value?

Accountability for IT risk management

Risk domains addressed

Risk management reporting line

IT risk related activities
Enterprise Governance of IT

How are we dealing with Risk and Value?

CIO/CEO Discussion topics by priority – CIONet and ISACA Survey Aug 2012 of 90 CIO’s
# Enterprise Governance of IT

How are we dealing with Risk and Value?

<table>
<thead>
<tr>
<th></th>
<th>Depth</th>
<th>Frequency</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Effectiveness</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agile/Innovation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CIO/CEO Discussion topics by priority – CLONet and ISACA Survey Aug 2012 of 90 CIO’s
Enterprise Governance of IT

How are we dealing with Risk and Value?

List of IT Outsourcing Risks from one of the most important academic sources on the subject:

- Backlash from internal IT staff
- Biased portrayal by vendors
- Breach of contract by the vendor
- Cultural differences between client and supplier
- Difficulty in managing remote teams
- Excessive transaction costs
- Hidden costs
- Inability to manage supplier relationship
- Inflexible contracts
- Infringement of IP rights
- Lack of trust
- Loss of autonomy and control over IT decisions
- Loss of control over data
- Loss of control over vendor

- Loss of in-house capability
- No overall cost savings
- Perceived as unpatriotic (offshore)
- Poor supplier capability, service, financial stability, cultural fit
- Security/privacy breach
- Supplier employee turnover/burnout
- Supplier employees are inexperienced
- Supplier employees have poor communication skills
- Supplier goes out of business
- Supplier has too much power over the customer
- Transition failure
- Treating IT as an undifferentiated commodity
- Uncontrollable contract growth
- Vendor lock-in (high switching costs)
How are we dealing with Risk and Value?

RISK = a important threat that applied to an applicable vulnerability, results in an significant business impact

An important mechanism for risk management and especially to debate and decide on risk relevance and mitigation
Enterprise Governance of IT

How are we dealing with Risk and Value?

The right terminology?

I. Threat
   a. Unintentional
      5. Acts of Gods
      6. Accidents
      7. Errors of Omission
      8. Errors of Commission
   b. Intentional
      9. Fraud
      10. Damage
      11. Sabotage
Enterprise Governance of IT

How are we dealing with Risk and Value?

The right terminology?

II. Vulnerability

a. Inherent Susceptibility
   1. Type of Business (internal)
   2. Environment (external)

b. Control Deficiency
   3. Absence of Controls
   4. Ineffectiveness of Controls
Enterprise Governance of IT

How are we dealing with Risk and Value?

The right terminology?

III. Impact
   a. Tangible
      12. Financial
      13. People
   b. Intangible
      14. Reputation
      15. Business Continuity
      16. Competitiveness
Enterprise Governance of IT

How are we dealing with Risk and Value?

IT Risk Analysis

I. Vulnerability
   a. Inherent Susceptibility
      1. Type of Business (internal)
      2. Environment (external)
   b. Control Deficiency
      3. Absence of Controls
      4. Ineffectiveness of Controls

II. Threat
   a. Unintentional
      5. Acts of Gods
      6. Accidents
      7. Errors of Omission
      8. Errors of Commission
   b. Intentional
      9. Fraud
     10. Damage
     11. Sabotage

III. Impact
   a. Tangible
      12. Financial
      13. People
   b. Intangible
      14. Reputation
      15. Business Continuity
      16. Competitiveness
Enterprise Governance of IT

How are we dealing with Risk and Value?

The right focus?

Based on combined sources from 2006
• ISF, E&Y, CSI etc

Note: Within the largest group ‘Internal Errors & Omissions’ there are significantly more errors of commission than omission.
Enterprised Governance of IT

How are we dealing with Risk and Value?

The right focus?

1. Just over one third is **theft** either
   - in collusion with outsiders (22%)
   - by insiders (10%)
   - by outsiders (3%)

2. Just under one third is **errors by commission**
   - no or bad instructions
   - wrong instructions
   - wrong examples

3. Well under one third is **errors by omission**
   - awareness, training & education
   - discipline & motivation
   - remuneration & enforcement
How are we dealing with Risk and Value?

Enterprise Governance of IT

Customers moving to the competition or need to adjust the price plan resulting in margins erosion caused by marketing and pricing info disclosure to competitors by disgruntled employee.

Financial loss and reputational damage resulting from fraudulent attempts going undetected because auditing was inadvertently logged off.
How are we dealing with Risk and Value?

**Scenario** = an important business impact caused by a significant threat exploiting an applicable vulnerability

<table>
<thead>
<tr>
<th>Nr</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Customers moving to the competition or need to modify erosion caused by marketing and pricing info disclosed to employee.</td>
</tr>
<tr>
<td>2</td>
<td>Severe violation of Privacy Regulations leading in large use because client financial or health information has been in operator error requiring extensive recovery.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent susceptibility</td>
</tr>
<tr>
<td>- Type of business (internal)</td>
</tr>
<tr>
<td>- Environment (internal)</td>
</tr>
<tr>
<td>Control Deficiency</td>
</tr>
<tr>
<td>- Absence of control</td>
</tr>
<tr>
<td>- Ineffectiveness of existing controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unintentional</td>
</tr>
<tr>
<td>- Acts of God</td>
</tr>
<tr>
<td>- Accidents</td>
</tr>
<tr>
<td>- Errors of Omission</td>
</tr>
<tr>
<td>- Errors of Commission</td>
</tr>
<tr>
<td>Intentional</td>
</tr>
<tr>
<td>- Fraud</td>
</tr>
<tr>
<td>- Damage</td>
</tr>
<tr>
<td>- Sabotage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tangible</td>
</tr>
<tr>
<td>- Financial</td>
</tr>
<tr>
<td>- People</td>
</tr>
<tr>
<td>- Infrastructure</td>
</tr>
<tr>
<td>Intangible</td>
</tr>
<tr>
<td>- Reputation</td>
</tr>
<tr>
<td>- Business continuity</td>
</tr>
<tr>
<td>- Competitiveness</td>
</tr>
</tbody>
</table>
Another thing they have in common: CHAINS

• **Cost**
  - Human resources
  - Infrastructure
  - Tools, licences etc.
  - ....

• **Intermediate benefits**
  - Capabilities (tech., operational, business)
  - Financial
  - Competitiveness
  - Risk mitigation
  - ....

• **Assumptions**
• **Dependencies**
• **Risks**
• **Timeframe**

**BUSINESS CASE**
- Overall Cost
- End Benefits
- Key Assumptions
- Key Dependencies
- Major Risks
- High Level Timeline

**Summarise**

**Alternatives**
Degree of Alignment
- Strategy
- Architecture
Enabling Opportunities
Another thing they have in common: CHAINS

How are we dealing with Risk and Value?

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
<th>Probability of Occurrence</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lost competitive edge and loss of planned earnings because new product disclosed in unprotected e-media</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Vandalism to the production chain (V) by disgruntled employees (T) results in delivery of faulty products (I)</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Faulty products delivered to customers (T) is followed by litigation (V) resulting in fines and lawyer fees (I)</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

<an important business impact caused by a significant threat exploiting an applicable vulnerability>
Another thing they have in common: CHAINS

- Especially true in Information security
- Very hard to put information risks in business context
- Two step approach
  - Threat/vulnerability leads to loss of Confidentiality, Integrity and/or Availability
  - Loss of CIA becomes a vulnerability that combined with business related threats (errors, fraud, theft etc.) results in a business impact
- Business impact?
<table>
<thead>
<tr>
<th>People resources</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>P 1</td>
<td>1</td>
</tr>
<tr>
<td>P 2</td>
<td>2</td>
</tr>
<tr>
<td>P 3</td>
<td>3</td>
</tr>
<tr>
<td>P 4</td>
<td>4</td>
</tr>
<tr>
<td>P 5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial resources</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>F 1</td>
<td>1</td>
</tr>
<tr>
<td>F 2</td>
<td>2</td>
</tr>
<tr>
<td>F 3</td>
<td>3</td>
</tr>
<tr>
<td>F 4</td>
<td>4</td>
</tr>
<tr>
<td>F 5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reputation</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>R 1</td>
<td>1</td>
</tr>
<tr>
<td>R 2</td>
<td>2</td>
</tr>
<tr>
<td>R 3</td>
<td>3</td>
</tr>
<tr>
<td>R 4</td>
<td>4</td>
</tr>
<tr>
<td>R 5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business continuity</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>B 1</td>
<td>1</td>
</tr>
<tr>
<td>B 2</td>
<td>2</td>
</tr>
<tr>
<td>B 3</td>
<td>3</td>
</tr>
<tr>
<td>B 4</td>
<td>4</td>
</tr>
<tr>
<td>B 5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Competitiveness</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>C 1</td>
<td>1</td>
</tr>
<tr>
<td>C 2</td>
<td>2</td>
</tr>
<tr>
<td>C 3</td>
<td>3</td>
</tr>
<tr>
<td>C 4</td>
<td>4</td>
</tr>
<tr>
<td>C 5</td>
<td>5</td>
</tr>
</tbody>
</table>
IDENTIFY INITIAL CAUSES

DISCOVER PREDISPOSING CONDITIONS

CONSIDER SUSTAINING CAUSES

DOCUMENT NEGATIVE IMPACT

USING THE TECHNIQUES OF ACCIDENT CHAIN ANALYSIS

IDENTIFY REQUIRED CAPABILITIES AND PRACTICES TO BREAK THE ACCIDENT CHAIN
For both risk and value, accept uncertainty and deal with it!
Enterprise Governance of IT

How should we be dealing with Risk and Value?

Governance

- Simple model
- Clear responsibilities and accountabilities
- Monitor, direct and evaluate
- Tools: Scorecards and Business Cases
- Structured interactions
Enterprise Governance of IT

How should we be dealing with Risk and Value?

Value

● Manage uncertainty

● Portfolio management of all major initiatives

● Business cases take into account past history, all activities to achieve the benefits and the full economic lifecycle of the initiative

● Business cases assign clear accountabilities and are continuously kept up-to-date

● Focus on initiatives that fit with strategy, reuse resources and have top management’s support
Enterprise Governance of IT

How should we be dealing with Risk and Value?

**Risk**

- Accept and manage uncertainty
- Define risk tolerance at the top
- Continuous pragmatic approach
- Identification, awareness, responsiveness
- Less focus on big risks and more on day-to-day value preservation
- Clarity of definitions and concepts and the use of risk scenarios
- Awareness of bias (capability, subjectivity, sensational)
What should we be doing further to minimise risk and optimise value of IT?

RISK AND VALUE
The underlying practices

- Learn from High Reliability organisations
- Learn from McKinsey
- Learn from Frameworks
1. High Reliability Organisations

- In high reliability organisations (HRO’s)
- Lessons from the operation of an aircraft carrier
1. High Reliability Organisations
1. High Reliability Organisations

FAILURE IS NOT AN OPTION
1. High Reliability Organisations

- Delegation
- Team work
- Constant coaching
- Continuous communication

“If there is one principle that explains why some consistently and dramatically outperform their rivals, it is that every person in the organization, regardless of job title or function, understands what makes the organization tick and why - what the organization does - matters.”

Bill Taylor in Harvard Business Review Blog, 20 April 2012, on the reasons why Apple, Southwest Airlines, USAA, Cirque du Soleil, the Marine Corps, Pixar — consistently and dramatically outperform their rivals.
The McKinsey team analysed 100,000+ questionnaires to uncover the practices of hundreds of business units and companies around the world and eventually arrived at one winning combination:

- Clear roles for employees (accountability)
- A compelling vision of change (direction) and
- An environment that encourages openness, trust and challenge (culture)

Nothing else came close in improving organisational performance

from “Management Practices that Work”
The McKinsey Quarterly Newsletter, Sep 2007
3. What about frameworks?

What do 70 CIO’s say about Frameworks?

**CIONet Survey, Sep 2011**

<table>
<thead>
<tr>
<th>Framework</th>
<th>CIO</th>
<th>IT Governance</th>
<th>Service Delivery</th>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>CobiT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO27001</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Not used at all**
- **Just influenced by its concepts**
- **To obtain guidance from it in decision making**
- **In addition used regularly as reference material**
- **Basis for IT policy but not for practices**
- **Extensively used for practices but compliance not verified**
- **Extracted practices applied and compliance verified**
3. What about frameworks?

For management, follow the lead of the CIO’s: governance and security guidance, operational implementation

For compliance, performance improvement and audit

- Start from the CobiT cascade of enterprise and IT goals
- Analyse your objectives and needs while keeping a balanced view of risk and value
- Extract what you need
- Compliment with ITIL and ISO27001 and others
- Track implementation rigourously
- Document the analysis and implementation process
3. What about frameworks?

**COBIT5** - Control objectives for IT

- De-facto standard
- 5 Governance Processes
- 29 IT Processes
  - Plan
  - Build
  - Run

**Content**
- Process descriptions
- Process objectives
- Inputs/Outputs
- Activities
- RACI Chart
- Metrics
- Management Practices

17 Enterprise goals for IT
17 IT goals
34 IT processes

www.isaca.org
3. What about frameworks?
3. What about frameworks?

- Metrics
- ?
- Goals
- Responsibility & Accountability
- Activities
- Performance
- Outputs
- WHAT
- HOW

Process Content
### 3. What about frameworks?

#### 3 Metrics and maturity models

#### 4 RACI, process linkages and control practices

#### 4.1 Assurance Guide

#### 5 Integration of Value and Risk governance and strong focus on enablers

<table>
<thead>
<tr>
<th>WHAT</th>
<th>WHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>A common language for IT activities and key management practices</td>
<td>To avoid misunderstandings, to have efficient dialogues and to enable synergy</td>
</tr>
<tr>
<td>A business focus and support for governance expectations</td>
<td>To enable alignment between business and IT and engage executives in the governance of IT</td>
</tr>
<tr>
<td>A structure of IT tasks and activities into discrete processes</td>
<td>To better define scope, responsibilities and extent of coverage</td>
</tr>
<tr>
<td>Consistency with generally accepted IT good practices and corporate governance standards</td>
<td>To be generally acceptable and to have a provably complete basis to select from</td>
</tr>
</tbody>
</table>
3. What about frameworks?

- Business Requirements
  - Enterprise Information
  - IT Processes
  - IT Resources

COBIT

- Requirements
  - Information Services
  - IT Processes
  - IT Resources

- IT Processes
  - IT Resources

- IT Resources

- Information Services

- Governance Objective: Value Creation
  - Benefits Realisation
  - Risk Optimisation
  - Resource Optimisation

- Governance Enablers
  - Governance Scope

- Owners and Stakeholders
  - Delegate
  - Accountable
  - Governing Body
  - Set Direction
  - Management
  - Instruct and Align
  - Operate and Execute
  - Monitor
  - Report

- Business Needs

- Governance
  - Evaluate
  - Direct
  - Management Feedback

- Management
  - Plan (APO)
  - Build (BAI)
  - Run (DSS)
  - Monitor (MEA)
3. What about frameworks?
3. What about frameworks?

- Process controls for maturity
- Process maturity a function of process attributes (ISO15404)
- Scales have to be applicable

<table>
<thead>
<tr>
<th>COBIT 4.1</th>
<th>Related ISO/IEC 15504 PA</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1 Process Goals and Objectives</td>
<td>PA 2.1 Performance management</td>
</tr>
<tr>
<td>PC2 Process Ownership</td>
<td>PA 2.1 Performance management</td>
</tr>
<tr>
<td>PC3 Process Repeatability</td>
<td>PA 3.1 Process definition attributes</td>
</tr>
<tr>
<td>PC4 Roles and Responsibilities</td>
<td>PA 2.1 Performance management</td>
</tr>
<tr>
<td>PC5 Policy, Plans and Procedures</td>
<td>PA 2.1 Performance management</td>
</tr>
<tr>
<td>PC6 Process Performance Improvement</td>
<td>PA 2.1 Process optimization attributes</td>
</tr>
</tbody>
</table>
3. What about frameworks?

- Get some of the complexity out
- Provide pragmatic maturity measurement
- Continue research in the value of good practices
- Revisit the concept of “Control”
- Leverage major management practices
Some tips for auditors, middle managers and executives

RISK AND VALUE
RISK AND VALUE TIPS

For IT Managers and Professionals
From a Bain survey, polling technology and business executives at 450 publicly-traded companies on IT Alignment and IT Effectiveness and what the effect is on Growth and IT Spend. (From CIO Insight, September 2007)

**Note:** growth is defined as 3-year compound annual growth rate.
From a Bain survey, polling technology and business executives at 450 publicly-traded companies on IT Alignment and IT Effectiveness and what the effect is on Growth and IT Spend. (From CIO Insight, September 2007)
Overcoming a bias against risk

Risk-averse midlevel managers making routine investment decisions can shift an entire company’s risk profile. An organization-wide stance toward risk can help.
RISK AND VALUE TIPS

For Auditors and Accountants
Why does a car have brakes?
...but when we do focus on the brakes

- Know the purpose of the control
- Know what you rely on
- Understand why you rely on it

Auditors, compliance officers and risk managers are often keen on pointing out there is no or insufficient documentation. While it may be necessary for compliance, we sometimes forget its true purpose which is to inform.
RISK AND VALUE TIPS

For Business Managers and Executives
Why does a car have breaks?

Which cars have the best brakes?
Sir Brian Pitman
Chairman Lloyds TSB

“Between 1983, when I was named chief executive of Lloyds Bank, and 2001, when I retired, Lloyds’s market capitalization grew from £1 billion to £40 billion.”

“Getting people to concentrate on things that really create value for the company demands something else: the transformation of their beliefs.”
RISK AND VALUE

Suggestions for Business Managers and Executives

- Invest in Enterprise Governance of IT
- Consider your breaking system if you want to move fast
- Understand the reluctance of middle managers to take risk
- Understand the tendency for short term gain at higher levels
- Instil the importance of enterprise value creation in all
IT AUDIT APPROACH?
IT Goals related to Value

Financial
01 Stakeholder value of business investments
02 Portfolio of competitive products and services
03 Managed business risk (safeguarding assets)
04 Compliance with external laws and regulations
05 Financial transparency

Customer
06 Customer-oriented service culture
07 Business service continuity and availability
08 Agile responses to changing business environments
09 Information-based strategic decision making
10 Optimisation of service delivery costs

Internal
11 Optimisation of business process functionality
12 Optimisation of business process costs
13 Managed business change programmes
14 Operational and staff productivity
15 Compliance with internal policies

Learning and Growth
16 Skilled and motivated people
17 Product and business innovation culture

Financial
01 Alignment of IT and business strategy
02 IT compliance and support for business compliance with external laws and regulations
03 Commitment of executive management to making IT-related decisions
04 Managed IT-related business risk
05 Realised benefits from IT-enabled products and services portfolio
06 Transparency of IT costs, benefits and risk

Customer
07 Delivery of IT services in line with business requirements
08 Adequate use of applications, information and technology solutions

Internal
09 IT agility
10 Security of information, infrastructure and applications
11 Optimisation of assets, resources and capabilities
12 Integrating applications and technology into business processes
13 Delivering benefits on time and on budget
14 Availability of reliable and useful information for decision making
15 IT compliance with internal policies

Learning and Growth
16 Competent and motivated business and IT personnel
17 Knowledge, expertise and initiatives for business innovation
34 IT Processes

Processes for Governance of Enterprise IT

Align, Plan & Organise...
- APO1 - Define the Management Framework for IT
- APO2 - Define Strategy
- APO3 - Manage Enterprise Architecture
- APO4 - Manage Innovation
- APO5 - Manage Human Resources
- APO6 - Manage Relationships
- APO7 - Manage Service Agreements
- APO8 - Manage Quality
- APO9 - Manage Budget & Costs
- APO10 - Manage Risk

Build, Acquire & Implement...
- BAI1 - Manage Programmes And Projects
- BAI2 - Define Requirements
- BAI3 - Define Solutions
- BAI4 - Accept & Transition Changes
- BAI5 - Enable Organisational Change
- BAI6 - Create
- BAI7 - Accept & Transition Changes
- BAI8 - Knowledge Management

Deliver, Service & Support...
- DSS1 - Manage Operations
- DSS2 - Manage Assets
- DSS3 - Manage Configuration
- DSS4 - Manage Service Requests & Incidents
- DSS5 - Manage Problems
- DSS6 - Manage Continuity
- DSS7 - Manage Security
- DSS8 - Manage Business Process Controls

Monitor, Evaluate & Assess...
- MEA1 - Monitor & Evaluate Performance and Conformance
- MEA2 - Monitor System of Internal Control
- MEA3 - Monitor and Assess Compliance with External Requirements
## Enterprise Goals related to Value

<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>Enterprise Objectives</th>
<th>Governance Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EG2. Managed business risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EG3. Portfolio of competitive products and services</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td>Customer Perspective</td>
<td>EG6. Customer orientated service culture</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG7. Business service continuity and availability</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG8. Agile responses to a changing business environment</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG10. Optimisation of service delivery costs</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td>Internal Perspective</td>
<td>EG11. Optimisation of business process functionality</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG12. Optimisation of business processes costs</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG14. Operational and staff productivity</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG15. Compliance with internal policies</td>
<td>Value Optimisation: P</td>
</tr>
<tr>
<td></td>
<td>EG17. Product and business innovation culture</td>
<td>Value Optimisation: P</td>
</tr>
</tbody>
</table>
IT Goals related to Value

Removed 1, 3, 4, 6 and 13. Added 16.
## IT Processes Goals related to Value

<table>
<thead>
<tr>
<th>IT Related Goals</th>
<th>Corporate</th>
<th>Customer</th>
<th>Internal</th>
<th>Learning &amp; Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alignment of IT and business strategy</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>IT compliance with external laws and regulations</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Commitment of executive management for taking IT decisions</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Managed IT related business risks</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Realised benefits from IT enabled investments and services portfolio</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Transparency of IT costs, benefits and risk</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>IT services in line with business requirements</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Adequate use of applications, information and technology solutions</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>IT agility</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Security of information and processing infrastructure</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Optimisation of IT infrastructure, resources and capabilities</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Integration of applications and technology into business processes</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Delivery of programmes on time, on budget and meeting quality standards</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Availability of reliable and useful information</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>IT compliance with internal policies</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Competent and motivated IT people</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Knowledge, expertise and initiative for business innovation</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

### COBIT Processes

<table>
<thead>
<tr>
<th>Evaluation, Direct &amp; Monitor</th>
<th>Set and Maintain the Governance Framework</th>
<th>Ensure Value Optimisation</th>
<th>Ensure Risk Optimisation</th>
<th>Ensure Resource Optimisation</th>
<th>Ensure Stakeholder Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM1</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EDM2</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EDM3</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EDM4</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>EDM5</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

Legend:
- **P**: Priority
- **S**: Support
### IT Goals related to Value

<table>
<thead>
<tr>
<th>Enterprise Goals</th>
<th>03</th>
<th>04</th>
<th>08</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>14</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT Goals</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05 IT compliance with external</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>laws and regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07 Manage IT related business</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09 Transparency of IT costs,</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>benefits and risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Security of information and</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processing infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 Availability of reliable and</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>useful information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 IT compliance with internal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 Competent and motivated IT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>people</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## IT Processes related to Value

<table>
<thead>
<tr>
<th>IT Processes</th>
<th>05</th>
<th>07</th>
<th>09</th>
<th>11</th>
<th>12</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM02 Ensure benefits delivery</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>EDM04 Ensure resource optimisation</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>APO01 Manage the IT Management Framework</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO04 Manage innovation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO07 Manage human resources</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BAI01 Manage programmes and projects</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI02 Manage requirements definitions</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BAI04 Manage availability and capacity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI06 Manage changes</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI07 Manage change acceptance and transition</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI09 Manage assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS01 Manage operations</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS03 Manage problems</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA01 Monitor performance and conformance</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Enterprise Goals related to Risk

<table>
<thead>
<tr>
<th>BSC DIMENSION</th>
<th>ENTERPRISE OBJECTIVES</th>
<th>GOVERNANCE OBJECTIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>VALUE OPTIMISATION</td>
</tr>
<tr>
<td><strong>FINANCIAL PERSPECTIVE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EG1.</td>
<td>COMPLIANCE WITH EXTERNAL LAWS AND REGULATIONS</td>
<td></td>
</tr>
<tr>
<td>EG2.</td>
<td>MANAGED BUSINESS RISKS</td>
<td></td>
</tr>
<tr>
<td>EG3.</td>
<td>PORTFOLIO OF COMPETITIVE PRODUCTS AND SERVICES</td>
<td></td>
</tr>
<tr>
<td>EG4.</td>
<td>STAKEHOLDER VALUE OF BUSINESS INVESTMENTS</td>
<td></td>
</tr>
<tr>
<td>EG5.</td>
<td>FINANCIAL TRANSPARENCY</td>
<td></td>
</tr>
<tr>
<td>EG6.</td>
<td>CUSTOMER ORIENTATED SERVICE CULTURE</td>
<td></td>
</tr>
<tr>
<td>EG7.</td>
<td>BUSINESS SERVICE CONTINUITY AND AVAILABILITY</td>
<td></td>
</tr>
<tr>
<td>EG8.</td>
<td>AGILE RESPONSES TO A CHANGING BUSINESS ENVIRONMENT</td>
<td></td>
</tr>
<tr>
<td>EG9.</td>
<td>INFORMATION BASED STRATEGIC DECISION MAKING</td>
<td></td>
</tr>
<tr>
<td>EG10.</td>
<td>OPTIMISATION OF SERVICE DELIVERY COSTS</td>
<td></td>
</tr>
<tr>
<td><strong>CUSTOMER PERSPECTIVE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EG11.</td>
<td>OPTIMISATION OF BUSINESS PROCESS FUNCTIONALITY</td>
<td></td>
</tr>
<tr>
<td>EG12.</td>
<td>OPTIMISATION OF BUSINESS PROCESSES COSTS</td>
<td></td>
</tr>
<tr>
<td>EG13.</td>
<td>MANAGED BUSINESS CHANGE PROGRAMMES</td>
<td></td>
</tr>
<tr>
<td>EG14.</td>
<td>OPERATIONAL AND STAFF PRODUCTIVITY</td>
<td></td>
</tr>
<tr>
<td>EG15.</td>
<td>COMPLIANCE WITH INTERNAL POLICIES</td>
<td></td>
</tr>
<tr>
<td><strong>INTERNAL PERSPECTIVE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EG16.</td>
<td>SKILLED AND MOTIVATED PEOPLE</td>
<td></td>
</tr>
<tr>
<td>EG17.</td>
<td>PRODUCT AND BUSINESS INNOVATION CULTURE</td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
P: Priority, S: Strategic
## IT Goals related to Risk

### Corporate
1. Alignment of IT and business strategy
2. IT compliance with external laws and regulations
3. Commitment of executive management for taking IT decisions
4. Managed IT related business risks
5. Realised benefits from IT enabled investments and services portfolio
6. Transparency of IT costs, benefits and risk

### Customer
7. IT services in line with business requirements
8. Adequate use of applications, information and technology solutions
9. IT agility
10. Security of information and processing infrastructure
11. Optimisation of IT infrastructure, resources and capabilities
12. Integration of applications and technology into business processes
13. Delivery of programmes on time, on budget and meeting quality standards
14. Availability of reliable and useful information
15. IT compliance with internal policies

### Learning & Growth
16. Competent and motivated IT people
17. Knowledge, expertise and initiatives for business innovation

### Enterprise Goals
- Compliance with external laws and regulations
- Managed business risks
- Portfolio of competitive products and services
- Stakeholder value of business investments
- Financial transparency
- Customer-oriented service culture
- Business service continuity and availability
- Agile responses to a changing business environment
- Information-based decision making
- Strategic decision making
- Optimum service delivery costs
- Optimisation of business process functionality
- Optimisation of business process costs
- Managed business change programmes
- Operational and staff productivity
- Compliance with internal policies
- Competent and motivated people
- Product and business innovation culture

<table>
<thead>
<tr>
<th>IT Related Goals</th>
<th>Financial</th>
<th>Customer</th>
<th>Internal</th>
<th>Learning &amp; Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Alignment of IT and business strategy</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>2 - IT compliance with external laws and regulations</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>3 - Commitment of executive management for taking IT decisions</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>4 - Managed IT related business risks</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>5 - Realised benefits from IT enabled investments and services portfolio</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>6 - Transparency of IT costs, benefits and risk</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>7 - IT services in line with business requirements</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>8 - Adequate use of applications, information and technology solutions</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>9 - IT agility</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>10 - Security of information and processing infrastructure</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>11 - Optimisation of IT infrastructure, resources and capabilities</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>12 - Integration of applications and technology into business processes</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>13 - Delivery of programmes on time, on budget and meeting quality standards</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>14 - Availability of reliable and useful information</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>15 - IT compliance with internal policies</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>16 - Competent and motivated IT people</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>17 - Knowledge, expertise and initiatives for business innovation</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
</tr>
</tbody>
</table>
## IT Goals related to Risk

<table>
<thead>
<tr>
<th>IT GOALS</th>
<th>01</th>
<th>02</th>
<th>05</th>
<th>07</th>
<th>09</th>
<th>13</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT compliance with external laws and regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage IT related business risks</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Transparency of IT costs, benefits and risks</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security of information and processing infrastructure</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability of reliable and useful information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT compliance with internal policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Competent and motivated IT people</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT PROCESSES</td>
<td>02</td>
<td>04</td>
<td>06</td>
<td>10</td>
<td>14</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td>EDM03 Ensure risk optimisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO07 Manage human resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO10 Manage suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO12 Manage Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO13 Manage security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI01 Manage projects and programmes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI06 Manage Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS02 Manage service requests and incidents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS04 Manage continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS05 Manage security services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS06 Manage business process controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA2 Monitor system of internal controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA3 Monitor compliance with external requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IT GOALS
- IT compliance with external laws and regulations
- Manage IT related business risks
- Transparency of IT costs, benefits and risks
- Security of information and processing infrastructure
- Availability of reliable and useful information
- IT compliance with internal policies
- Competent and motivated IT people
High-impact COBIT Processes
- Define a strategic IT plan (P01).
- Manage the IT investment (P05).
- Communicate management aims and direction (P06).
- Assess and manage IT risks (P09).
- Identify automated solutions (AI1).
- Acquire and maintain application software (AI2).
- Acquire and maintain technology infrastructure (AI3).

High-impact IT Goals
- Align the IT strategy to the business strategy (IT_Corp6).
- Provide service offerings and service levels in line with business requirements (IT_User1).
- Acquire, develop and maintain IT skills that respond to the IT strategy (IT_Fut1).
- Ensure that IT demonstrates continuous improvement and readiness for future change (IT_Fut3).

High-impact Val IT Processes
- Define and implement processes (VG2).
- Establish effective governance monitoring (VG5).
- Continuously improve value management practices (VG6).
- Establish strategic direction and target investment mix (PM1).
- Update operational IT portfolios (IM7).

High-impact IT Goals
- Improve IT’s cost-efficiency (IT_Corp5).
- Align the IT strategy to the business strategy (IT_Corp6).
- Translate business functional and control requirements into effective and efficient automated solutions (IT_User3).
- Accomplish proper use of applications, information and technology solutions (IT_User4).
- Provide IT agility (in responding to changing business needs) (IT_Oper4).
- Seamlessly integrate applications and technology solutions into business processes (IT_Oper5).
- Acquire, develop and maintain IT skills that respond to the IT strategy (IT_Fut1).
- Ensure that IT demonstrates continuous improvement and readiness for future change (IT_Fut3).

High-impact Business Goals
- Achieve cost optimisation of service delivery (B_Cust4).
- Obtain reliable and useful information for strategic decision making (B_Cust6).
- Improve and maintain business process functionality (B_Int1).
- Improve and maintain operational and staff productivity (B_Int2).
- Enable and manage business change (B_Int3).
- Optimise business process costs (B_Int5).
• Define a strategic IT plan
• Manage the IT investment
• Communicate management aims and direction
• Assess and manage IT risks
• Identify automated solutions
• Acquire & maintain applications and infrastructure
• Portfolio and investment management

• Align the IT strategy to the business strategy
• Provide service offerings and levels in line with business requirements
• IT skills that respond to the IT strategy
• Continuous improvement and readiness for future change

• Cost optimisation of service delivery and business processes
• Obtain reliable and useful information for strategic decision-making
• Improve and maintain business process functionality and operational productivity
• Enable and manage business change
IT Goals

Refined and measurable IT Goals

Important IT Processes

**Governance Objective: Value Creation**

- Benefits Realisation
- Risk Optimisation
- Resource Optimisation

**Business Goals relative to IT**

**IT Goals**

**Important IT Processes**

**Generic process practices**

**Generic Practices**

C5 Enablers
C5 Maturity Model
C4 Process Controls

**LEVERAGING ISACA RESEARCH**

**Enterprise Objectives**

- EG1. Compliance with external laws and regulations
- EG2. Managed business risks
- EG3. Portfolio of competitive products and services
- EG4. Stakeholder value of business investment
- EG5. Financial transparency
- EG6. Customer-oriented service culture
- EG7. Business service continuity and availability
- EG8. Agile responses to changing business environments
- EG9. Information-based strategic decision making
- EG10. Optimisation of service delivery costs
- EG11. Optimisation of business process function
- EG12. Optimisation of business processes cost
- EG13. Managed business change programmes
- EG14. Operational and staff productivity
- EG15. Compliance with internal policies
- EG16. Skilled and motivated people
- EG17. Product and business innovation culture

**IT Related Goals**

1. Alignment of IT and business strategy
2. IT compliance with external laws and regulations
3. Commitment of executive management for taking IT initiatives
4. Managed IT-related business risks
5. Realised benefits from IT-enabled investments and initiatives
6. Transparency of IT costs, benefits and risk
7. IT services in line with business strategies
8. Adequate use of applications, information and technology
9. IT agility
10. Security of information and processing infrastructure
11. Optimisation of IT infrastructure, resources and services
12. Integration of applications and technology into business processes
13. Delivery of programmes on time, on budget and within scope
14. Availability of reliable and useful information
15. IT compliance with internal policies
16. Competent and motivated IT people
17. Knowledge, expertise and initiatives for business
CONCLUDING ON RISK AND VALUE

*Kubernán* (gr): to steer a ship – the process of continually orienting and adjusting

“Managing an uncertain journey to an uncertain destination”