Secure Application Development

Governance of Information Technology:
Talking to Senior Management

March 6\textsuperscript{th}, 2008

Georges Ataya
Georges Ataya  MSCS, PBA, CISA, CISM, CISSP

- Professor and Academic Director at Solvay Business School (www.solvay.edu/it)
  - Postgraduate in ICT Audit & Security
  - Executive Master in IT Governance
- International Vice President of the IT Governance Institute (ITGI.org)
- Member of the Belgian association for Board Directors teaching the accreditation program
- Participated in the research and development of various publications.
- Managing Partner at ICT Control NV (www.ictcontrol.eu)
- Georges@ataya.net – www.ataya.info
The Information Paradox

The value of IT is being increasingly questioned......
...yet organizations continue to spend more and more on IT

The Fundamental Question

Management concerned whether we are we managing our investments in IT such that:
- we are getting optimal value;
- at an affordable cost; and
- with an acceptable level of risk?
The Reality

- Gartner – more than 600 billion $ thrown away annually on ill-conceived or ill executed IT projects
- Standish Group – about 20% of projects fail outright, 50% are challenged and only 30% are successful
- ITGI 2005 Survey early findings confirm concerns

- Low return from high-cost IT investments, and transparency of IT’s performance are two of the top issues
- More than 30% claim negative return from IT investments targeting efficiency gains
- 40% do not have good alignment between IT plans and business strategy
- Interest in and use of active management of the return on IT investment has doubled in 2 years (28 to 58%)
Delivery of Value is a key focus area

- Realization of value depends on sound IT investment decisions, and the processes and responsibilities governing those decisions

- Senior management increasingly recognizes the need to:
  - Look at the lifecycle of IT-enabled business investments from the investment decision to full benefits realisation
  - Manage them as portfolio of programmes, including the full range of activities that are required to achieve risk-adjusted business value

The current focus on IT governance
Communication with Senior Management

CEO concerns in relation with IT:

* Costs and values
* Responsiveness to Business
* Risks and compliance
IT Management Focus Areas

IT management have moved from the technology-related arenas to the management-related arenas:

- **Strategic alignment**, with focus on aligning with the business and collaborative solutions
- **Value delivery**, concentrating on optimising expenses and proving the value of IT
- **Risk management**, addressing the safeguarding of IT assets, disaster recovery and continuity of operations
- **Resource management**, optimising knowledge and IT infrastructure

Furthermore, none of these factors can be managed appropriately without:

- **Performance measurement**, tracking project delivery and monitoring IT services

Source: predictions of reputable market analysts such as Gartner, Compass, Giga and CSC
Results from a Global Survey

Figure 16—IT-related Problems in Last 12 Months

<table>
<thead>
<tr>
<th>Problem</th>
<th>2003</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>7%</td>
<td>21%</td>
</tr>
<tr>
<td>No view on IT performance</td>
<td>15%</td>
<td>38%</td>
</tr>
<tr>
<td>IT not meeting compliance requirements</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>IT staffing problems</td>
<td>23%</td>
<td>27%</td>
</tr>
<tr>
<td>Outsourcing problems</td>
<td>24%</td>
<td>30%</td>
</tr>
<tr>
<td>Disconnect between business/IT strategies</td>
<td>28%</td>
<td>35%</td>
</tr>
<tr>
<td>Security/privacy incidents</td>
<td>21%</td>
<td>30%</td>
</tr>
<tr>
<td>Operational IT incidents</td>
<td>35%</td>
<td>30%</td>
</tr>
<tr>
<td>High cost/low ROI</td>
<td>41%</td>
<td>40%</td>
</tr>
</tbody>
</table>

(Based on 688 respondents of the overall sample)

Source: IT Governance Global Status Report—2006 (itgi.org)
ValIT Approach

Start here

1. Are we doing the right things?
2. Are we doing them the right way?
3. Are we getting the benefits?
4. Are we getting them done well?
ValIT Developments

The **strategic** question. Is the investment:
- In line with our vision?
- Consistent with our business principles?
- Contributing to our strategic objectives?
- Providing optimal value, at affordable cost, at an acceptable level of risk?

In the **value** question. Do we have:
- A clear and shared understanding of the expected benefits?
- Clear accountability for realising the benefits?
- Relevant metrics?
- An effective benefits realisation process?

The **architecture** question. Is the investment:
- In line with our architecture?
- Consistent with our architectural principles?
- Contributing to the population of our architecture?
- In line with other initiatives?

The **delivery** question. Do we have:
- Effective and disciplined delivery and change management processes?
- Competent and available technical and business resources to deliver:
  - the required capabilities; and
  - the organisational changes required to leverage the capabilities.

Some fundamental questions

Are we doing the right things?

Are we doing them the right way?

Are we getting the benefits?

Are we getting them done well?

about the value delivered by IT
The Reality

Only 38% of executives/senior management can describe their organizations IT Governance process.
In most cases, IT Governance has not been designed – it has just developed “piecemeal” in response to specific issues.

Source: Peter Weill and Jeannie W. Ross, *IT Governance*

85% of organisations demand business cases for change projects.
Only 40% of approved projects have valid (realistic) benefit statements.
Less than 10% of organisations ensure benefits are realised post-project.
Less than 5% of organisations hold project stakeholders responsible for benefit attainment.

Source: Meta Group July 2004
Without Effective Governance…

Situation
- Lack of Strategic Focus
- Projects are “sold” on emotional basis -- not selected
- Overemphasis on Financial ROI
- No strong review process
- Overemphasis on Financial ROI
- No clear strategic criteria for selection

Leads to..
- Can’t kill projects
- Reluctance to say no to projects
- Underestimation of risks and costs

Results in..
- Too many projects
- Quality of execution suffers
- Projects not aligned to strategy
- Benefits not received
- Business needs not met
- Over budget
- Projects Late
- Lack of confidence (in IT)

Source: Fujitsu
The Big Disconnect

- Filtered information*
- Selective hearing
- Wishful thinking
- Fear
- Emotional overinvestment
- Unrealistic stakeholder expectations

*Source: Larry Bossidy, Ram Charan – Confronting Reality
A Strategic Governance Framework

Management of Change

- Strategy Management
- Portfolio Management
- Programme Management
- Project Management
- Operations Management

Total Benefits - Total Costs

COBIT
Val IT
Future

Architecture

AM
ms
sm
et

The Business Case

- Same level of focus and rigor on Business Benefits as on Costs
- Full scope of effort (BPPTO), including managing the process of change
- Value contribution represented by three measures
  - Business worth - $ & non-$ contribution
  - Alignment - fit with business goals
  - Risk - chance of not realising benefits
- An Operational Tool
  - Pick the winners
  - Manage the realisation of value
Portfolio management
Moving Forward – The business challenge

To realize the true potential of investments in IT-enabled change

- Recognize we are implementing change not technology
- Continue to strengthen “core” IT competencies
- Take an integrated approach to IT and strategic governance
  - Establish portfolio management
  - Get business engagement and accountability
  - Manage the full economic life-cycle
  - Ensure clarity of the desired outcomes (strategy)
  - Enable understanding of the full scope of effort required (architecture)
  - Break down the “silos” and “connect the dots”
  - Sense and respond to changes and deviations along the way

This is a significant leadership opportunity for CIO's as a respected member of the CxO team!
CobiT - Research
Key is the delivery of IT Value

COBIT Financials -- VALIT

- Research, develop and promote a free internationally accepted set of good practices for optimising the value of IT enabled change through sound investment decisions, value transparency, cost optimisation and risk management, based on CobiT, supported with empirical data

- Principles
- Definitions
- Management Processes
  - IT Value Governance
  - Portfolio Management
  - Investment Management
- Control Objectives <> COBIT

Comparison of cost vs. duration
Correlation of delivery vs. capability
Value Governance Principles

- IT-enabled investments (programmes and projects) will
  - be managed as a portfolio of investments
  - include the full scope of activities (BPPTO) that are required to achieve business value
  - be governed through their full (economic) life-cycle from initial concept to the full realisation of value

- Value delivery practices will
  - define and monitor key metrics (lead and lag indicators) and will respond quickly to any changes or deviations
  - engage the business and assign appropriate accountability for the delivery of capabilities and realisation of business benefits
  - be continually monitored, evaluated and improved
Do we know the size and shape of our IT investment portfolio?

2004
- # of Projects: ..
- Budget: € .. mln
- Internal FTE
- External FTE

2005
- # of Projects: ..
- Budget: € .. mln
- Internal FTE
- External FTE

Awaiting Approval
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )
- Internal FTE
- External FTE

Continuity
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )

Discretionary
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )

Approved
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )
- Budget to be spent € .. mln
- Internal FTE
- External FTE

Mandatory
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )
- Internal FTE
- External FTE

Continuity
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )
- Internal FTE
- External FTE

Discretionary
- # of Projects: .. ( ..% )
- Budget: € .. mln ( ..% )
- Internal FTE
- External FTE

*the ‘to be spent’ total of .. mln Euros represents the maximum potential for future cost avoidance on the total projects portfolio

Mandatory = Compliance or regulatory
Continuity = ‘projects that maintain current service levels’
Discretionary = New revenue streams or innovative cost reduction

SeaQuation | Approach | IT Cost & Staff | IT Portfolio Management | Service Catalog
How good are we at delivering projects?

Solution Delivery Performance

2005: 13 projects (€ 22 mln)
2004: 33 projects (€ 11 mln)

% of Projects

- On time
- On budget
- 80% Functionality
- Benefits
- Meets all criteria

CMM Level 3

- 50%
- 66%
- 78%
- 83% 85%
- 94%
- 98%
- 66%
- 72%
- 85%
- 64%
- 72%
- 85%
- 28%
- 44%
- 94%

2004 2005 CMM Level 3

SeaQuation

Enterprise Portfolio Intelligence
Expected ROI Business Case

Budgeted ROI = €112 m / €100 m = 12%

Expected Benefits

Expected Budget

Actual ROI allowing for typical solution delivery performance

Projected ROI = (€112 m x 84% x 1 / 1.12) / €100 m x 124% = -32%

Functionality achieved -16%

Budget Overrun +24%

Approximately one year delay, so benefits discounted at ING 12% Rate

An Example
How do our projects contribute to value creation?

Cumulative NPV

- Max NPV: € 410 m
- Total NPV: € 313 m
- 70% of projects contribute to value creation

Cumulative NPV (€ m)

Discretionary Projects (sorted by NPV)
Are our projects outperforming the index? Efficient Frontier Analysis

Risk - Return Analysis Based on Investment Budget

Indication that project XYZ is an underperforming asset

- Return: 78.0% 10.71% Budget
- Return: 29.1% 23.33% Budget
- Return: 35.0% 4.56% Budget
- Return: 15% 59.40% Budget

Risk Exposure

- Fixed income
- Common Stock
- Emerging Countries
- Private Equity

Risk Rating

0: Zero Risk
1: Low Risk
2: Medium Risk
3: High Risk
4: Maximum Risk

ABC Project

XYZ Project

Efficient Frontier Analysis

Excess Return

Return Weighted by Budget

Hurdle Rate

Are our projects outperforming the index?
Risk Governance principles

- Management assurance on the risk position
- Cascading risk assessment and ownership
- Risk action plan promoted and controlled by management
- Software related risk is a black box for management
Risk Management process

- Understand legal and regulatory requirements and business drivers and objectives
- Carry out a risk and threat analysis
- Define the company's acceptable risk level
- Outlined in security policies, standards, guidelines and procedures
- Identify the necessary countermeasures to mitigate the calculated risks
- Carry out cost/benefit analysis for these countermeasures and
- Report to senior management their findings

**Risk and threat analysis:**
- Identify company assets
- Assign a value to each asset
- Identify each asset's vulnerabilities and associated threats
- Calculate the risk for the identified assets

**Mitigate the risk by:**
- implementing the recommended countermeasure
- Accept the risk
- Avoid the risk
- Transfer the risk by purchasing insurance
The IT Governance Institute (ITGI)

- The IT Governance Institute (ITGI) ([www.itgi.org](http://www.itgi.org)) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise’s information technology.
- Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities.
- The IT Governance Institute offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.
- CobiT is the international de facto standard for IT governance.
- ValiT is a new publication designed to shed light on realising value from IT enabled business investments.
Suggested readings

- www.ITGI.org
- www.ISACA.org
- www.ISACA.be
- Board briefing on IT Governance, ITGI
- www.solvay.edu/ict
- www.solvay.edu/itgov
The Four “Ares”

Continually asking...

- Are we doing the right things?
- Are we doing them the right way?
- Are we getting them done well?
- Are we getting the benefits?
Conclusions
ValIT Project Status

**DONE**
- Framework
- Business Case
- Case Study

**PLANNED**
- Benchmarking
- Empirical Analysis
- Forum
ValIT Framework - Processes

**Value Governance (VG)**
- VG1: Ensure informed and committed leadership.
- VG2: Define and implement processes.
- VG3: Define roles and responsibilities.
- VG4: Ensure appropriate and accepted accountability.
- VG5: Define information requirements.
- VG6: Establish reporting requirements.
- VG7: Establish organisational structures.
- VG8: Establish strategic direction.
- VG9: Define investment categories.
- VG10: Determine a target portfolio mix.
- VG11: Define evaluation criteria by category.

**Investment Management (IM)**
- IM1: Develop a high-level definition of investment opportunity.
- IM2: Develop an initial programme concept business case.
- IM3: Develop a clear understanding of candidate programmes.
- IM4: Perform alternatives analysis.
- IM5: Develop a programme plan.
- IM6: Develop a benefits realisation plan.
- IM7: Identify full life cycle costs and benefits.
- IM8: Develop a detailed programme business case.
- IM9: Assign clear accountability and ownership.
- IM10: Initiate, plan and launch the programme.
- IM11: Manage the programme.
- IM12: Manage/track benefits.
- IM13: Update the business case.
- IM15: Retire the programme.

**Portfolio Management (PM)**
- PM1: Maintain a human resource inventory.
- PM2: Identify resource requirements.
- PM3: Perform a gap analysis.
- PM4: Develop a resourcing plan.
- PM5: Monitor resource requirements and utilisation.
- PM6: Establish an investment threshold.
- PM7: Evaluate the initial programme concept business case.
- PM8: Evaluate and assign a relative score to the programme business case.
- PM9: Create an overall portfolio view.
- PM10: Make and communicate the investment decision.
- PM11: Stage-gate (and fund) selected programmes.
- PM12: Optimise portfolio performance.
- PM13: Re-prioritise the portfolio.
- PM14: Monitor and report on portfolio performance.
CobiT Framework - Processes

**Monitor and Evaluate**
- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure regulatory compliance.
- ME4 Provide IT governance.

**Information**
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Security

**Plan and Organise**
- P01 Define a strategic IT plan.
- P02 Define the information architecture.
- P03 Define the IT processes, organisation and relationships.
- P04 Determine technological direction.
- P05 Manage the IT investment.
- P06 Communicate management aims and direction.
- P07 Manage IT human resources.
- P08 Manage quality.
- P09 Assess and manage IT risks.
- P010 Manage projects.

**Deliver and Support**
- D01 Define and manage service levels.
- D02 Manage third-party services.
- D03 Manage performance and capacity.
- D04 Ensure continuous service.
- D05 Ensure systems security.
- D06 Identity and allocate costs.
- D07 Educate and train users.
- D08 Manage service desk and incidents.
- D09 Manage the configuration.
- D10 Manage problems.
- D11 Manage data.
- D12 Manage the physical environment.
- D13 Manage operations.

**Acquire and implement**
- A01 Identify automated solutions.
- A02 Acquire and maintain application software.
- A03 Acquire and maintain technology infrastructure.
- A04 Enable operation and use.
- A05 Preserve IT resources.
- A06 Manage changes.
- A07 Install and accredit solutions and changes.
## ValIT Framework - Detail

<table>
<thead>
<tr>
<th>Domain: Value Governance (VG)</th>
<th>Control Objectives</th>
<th>CobiT Cross Ref.</th>
<th>RACI Chart</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Description</strong></td>
<td><strong>Control Objectives</strong></td>
<td></td>
<td><strong>Exec</strong></td>
</tr>
<tr>
<td>• Establish governance, monitoring and control framework</td>
<td><strong>VG1 Ensure informed and committed leadership</strong>&lt;br&gt;The reporting line of the CIO should be commensurate with the importance of IT within the enterprise. All executives should have a sound understanding of strategic IT issues such as dependence on IT, technology insights and capabilities, in order that there is a common and agreed understanding between the business and IT of the potential impact of IT on the business strategy. The business and IT strategy should be integrated clearly linking enterprise goals and IT goals and should be broadly communicated.</td>
<td>Primary: PO1.2, PO4.4, ME3.1, ME3.2</td>
<td>A, R</td>
</tr>
<tr>
<td>• Establish Strategic Direction</td>
<td><strong>VG2 Define and implement processes</strong>&lt;br&gt;Define, implement and consistently follow processes that provide for clear and active linkage between the enterprise strategy, the portfolio of IT-enabled investment programmes that execute the strategy, the individual investment programmes, and the business and IT projects that make up the programmes. The processes should include: planning and budgeting; prioritisation of planned and current work within the overall budget; resource allocation consistent with the priorities; stage-gating of investment programmes; monitoring and communicating performance; taking appropriate remedial action; and benefits management such that there is an optimal return on the portfolio and on all IT assets and services.</td>
<td>Primary: PO4.1, ME1.1, ME1.3, ME3.1 Secondary: PO5.2-5, PO10.2</td>
<td>A R C</td>
</tr>
<tr>
<td>• Establish portfolio characteristics</td>
<td><strong>VG3 Define roles &amp; responsibilities</strong>&lt;br&gt;Define and communicate roles and responsibilities for all personnel in the enterprise in relation to the portfolio of IT-enabled business investment programmes, individual investment programmes and other IT assets and services to allow sufficient authority to exercise the role and responsibility assigned to them. These roles should include, but not necessarily be limited to: an investment decision body; programme sponsorship; programme management; project management; and associated support roles. Provide business with procedures, techniques, and tools enabling them to address their responsibilities. Establish and maintain an optimal coordination, communication and liaison structure between the IT function and other stakeholders inside and outside the enterprise.</td>
<td>Primary: PO4.6, PO4.15 Secondary: PO4.8, PO4.9</td>
<td>A R C</td>
</tr>
<tr>
<td></td>
<td><strong>VG4 Ensure appropriate and accepted accountability</strong>&lt;br&gt;Establish a supporting and appropriate control framework that is consistent with the overall enterprise control environment, and generally accepted control principles. The framework should provide for unambiguous accountability and practices to avoid breakdown in internal control and oversight. Accountability for achieving the benefits, delivering required capabilities and controlling the costs should be clearly assigned and monitored.</td>
<td>Primary: PO1.1, ME3.1-3, ME3.3 Secondary: ME3.2</td>
<td>A R C</td>
</tr>
</tbody>
</table>