Integration of COBIT, Balanced Scorecard & SSE-CMM as a strategic Information Security Management (ISM) framework

James E. Goldman, Suchit Ahuja
Computer & Information Technology, Purdue University

Background / Issues
- Multiple frameworks for Information Security Management (ISM)
  - ISO 27001 Information Security Management System
  - ISO 27002 Information Security Controls
  - COBIT Processes for controls
- Multiple frameworks for Strategic Alignment of Business & IT
  - Balanced Scorecard
  - Project Portfolio Management
- Multiple frameworks for Metrics & Measurement
  - SEI CMM
  - SSE CMM
  - COBIT process area 4.0 - “Measure & Evaluate (ME)”

Problem
- Each framework addresses only a specific area within ISM domain
- Integration of two or more frameworks often consists of gaps
- Lack of alignment between Business + IT + InfoSec strategies
- Lack of TRACEABILITY

Proposed Solution
- Integration of COBIT, Balanced Scorecard & SSE-CMM for strategic ISM
  - ALIGN Business + IT + ISM Strategies
  - ESTABLISH clear TRACEABILITY + GOVERNANCE
  - USE of STANDARDIZED METRICS for Performance Management

Approach
- Integration is achieved by bridging the gaps or mitigating the weaknesses, that one framework inherently contains, using the methodology prescribed by the second framework and using SSE-CMM as an evaluation mechanism

Previous Work
  - Using ISO 27001 and SSE-CMM
  - Mapping of processes for effective integration of COBIT and SEI-CMM
  - IT Governance Institute, 2005
  - Mapping of COBIT with ITIL and ISO 27002 (IT Governance Institute, 2008)
  - For effective management and alignment of IT with business

<table>
<thead>
<tr>
<th>Proposed Solution</th>
<th>Balanced Scorecard (BSC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT Information Criteria can help classify information directly for audit purposes. This is similar to Information Classification Matrix developed by National Security Agency (NSA) for InfoSec Assessment Methodology (IAM)</td>
<td>Balanced Scorecard (BSC) can be used to set measurable business goals and objectives while providing a framework for evaluating the organization’s performance.</td>
</tr>
<tr>
<td>Key Goal Indicator (KGI) is used to measure the achievement of the organizational goals.</td>
<td>Balanced Scorecard (BSC) objectives are linked to measurable business goals and objectives.</td>
</tr>
<tr>
<td>KPI: Key Performance Indicator</td>
<td>Balanced Scorecard (BSC) is used to establish a metric for measuring the performance of the processes in the ISM framework.</td>
</tr>
<tr>
<td>Use metrics from cascading BSC to assess the performance of the information security strategy.</td>
<td>Balanced Scorecard (BSC) is used to establish a metric for measuring the performance of the processes in the ISM framework.</td>
</tr>
<tr>
<td>KGI: Key Goal Indicators and Critical Success Factors (CSFs) while measuring maturity vs COBIT procedures.</td>
<td>Balanced Scorecard (BSC) is used to establish a metric for measuring the performance of the processes in the ISM framework.</td>
</tr>
<tr>
<td>Use of COBIT control processes is used to evaluate the performance of the operational processes.</td>
<td>Balanced Scorecard (BSC) is used to establish a metric for measuring the performance of the processes in the ISM framework.</td>
</tr>
</tbody>
</table>

| Integration of COBIT, Balanced Scorecard & SSE-CMM as a strategic Information Security Management (ISM) framework | Using a cascading balanced approach would establish an information security reporting mechanism via KPIs, KGIs and CPs while measuring maturity via SSE-CMM. |