MetriCon 3.0

Workshop Presentation

Plans for a Balanced Scorecard Approach to Information Security Metrics

Kevin Peuhkurinen

The Great-West Life Assurance Company

Background

The Information Security Office (ISO):

Ø Provides information security governance services for an Enterprise consisting of 3 insurance companies and 3 investment fund companies, operating in Canada, Europe, and the USA.

Information Security

Ø Internally, the ISO has structured itself according to 8 functional practices:

- Policy and Standards Development and Maintenance
- Risk Analysis
- Vulnerability Assessments
- Alert Monitoring and Incident Response
- Compliance
- Awareness, Training, and Communication
- Professional Services
- Planning and Strategy
  - § includes the Information Security Metrics program

Information Security

- The I.S. organization, of which the ISO is a part, is an enthusiastic proponent of the use of the Balanced Scorecard for measuring and reporting on I.T. Governance.
  - The I.S. organization's experiences with their IT BSC program have been included in two books:
    - "IMPLEMENTING THE IT BALANCED SCORECARD: Aligning IT with Corporate Strategy" by Keyes
    - "Strategies For Information Technology Governance" by Van Grembergen

- The IT BSC used by the I.S. organization does provide some reporting on IT risk in general. However, currently our information security-specific measurements are reported through a variety of channels rather than the IT BSC.
- We are developing a new Information Security BSC to harmonize with the IT BSC already in use.

A Generic Maturity Model for an Information Security Balanced Scorecard Program

Level 1 Initial There is evidence that the organization has recognized there is a need for a measurement system for its information security. There are ad hoc approaches to measure information security (e.g. virus counts, number of incidents). This measurement process is often an individual effort in response to specific issues.

Level 2 Repeatable Management is aware of the concept of the balanced scorecard and has communicated its intent to define appropriate measures. Measures are collected and presented to management in a scorecard. Linkages between outcome measures and performance drivers are generally defined but are not yet precise, documented or integrated into strategic and operational planning processes. Processes for scorecard training and review are informal and there is no compliance process in place.

Level 3 Defined Management has standardized, documented and communicated the BSC through formal training. The scorecard process has been structured and linked to business planning cycle. The need for compliance has been communicated but compliance is inconsistent. Management understands and accepts the need to integrate the BSC within the alignment process of business, IT, and information security. Efforts are underway to change the alignment process accordingly.

Level 4 Managed The BSC is fully integrated into the strategic and operational planning and review systems of the business, IT, and information security. Linkages between outcome measures and performance drivers are systematically reviewed and revised based upon the analysis of results. There is a full understanding of the issues at all levels of the organization which is supported by formal training. Long term stretch targets and priorities for information security investment projects are set and linked to the scorecard. Individual objectives of ISO employees are connected with the scorecards and incentive systems are linked to the BSC measures. The compliance process is well established and levels of compliance are high.

Level 5 Optimized The BSC is fully aligned with the business and IT strategic management frameworks and vision is frequently reviewed, updated and improved. Internal and external experts are engaged to ensure industry best practices are developed and adopted. The measurements and results are part of management reporting and are systematically acted upon by senior and ISO management. Monitoring, self-assessment and communication are pervasive within the organization and there is optimal use of technology to support measurement, analysis, communication and training.

Based on “Aligning Business and Information Technology through the Balanced Scorecard at a Major Canadian Financial Group: its Status Measured with an IT BSC Maturity Model (http://www.performance-measurement.net/news-detail.asp?nID=35) by Ron Saull and Wim Van Grembergen

Our Plans

Objectives of the ISO metrics program:

- Ø Show value for investment
  - Display linkage between business and I.S. goals and the information security program
  - Demonstrate where additional investment may be warranted
- Ø Provide input into the strategic planning process for the information security program and track progress towards goals
- Ø Provide visibility into risk
  - Show trends in risk posture
  - Measure residual risk in our control framework
- Ø Support the continuous improvement requirements of the functional practices of the ISO

"Metrics That Matter"

Information Security Balanced Scorecard

Corporate Contribution	Customer Orientation
How should information security appear to business and I.S. senior leadership in order to be considered a significant contributor to Enterprise success?	How should the Information Security Office appear to its clients in order to be considered a trusted advisor?
Internal Processes	**Future Orientation**
What services and processes must the Information Security Office excel at in order to satisfy stakeholders and clients?	How will we develop the information security skills and knowledge both within the ISO internally and the entire Enterprise necessary to achieve our goal of good governance?

Information Security

Corporate Contribution:

Mission

- Ø Contribute to the achievement of the goals of our businesses through effective delivery of value-based information security services.

Objectives

- Ø Management of information security expenses
- Ø Benefit realization on information security investments
- Ø Provide insight into risk profiles

Potential Measures

- Ø New and retained business where information security was a significant concern
- Ø Visible risk reduction through closure of exceptions to information security standards
- Ø Clean regulatory audits and assessments

Customer Orientation:

Mission

- Be the supplier of choice for all information security consulting and other services to the Enterprise.

Objectives

- Client satisfaction
- High quality, timely, deliverables (e.g. accurate, relevant risk assessments)

Potential Measures

- Hours spent consulting
- Feedback from internal clients

Internal Process:

Mission

- Deliver timely and effective information security services at targeted service levels and costs.

Objectives

- Practice maturity
- Process improvement

Potential Measures

- Functional practice maturity levels
- Internal process effectiveness

Information Security

Future Orientation:

Mission

- Develop the internal capabilities to learn, innovate, and adapt, and raise information security awareness throughout the Enterprise.

Objectives

- Knowledge management
- Emerging risks research
- Heightened information security awareness

Potential Measures

- Information security-related certifications
- Information security awareness activities

Issues and Concerns

- Can a single BSC satisfy the needs of multiple stakeholders?
  - Is some sort of dashboard also required?

- What sort of metrics can be used to measure the cost (and benefits) of all information security technology and processes across a large Enterprise?

Thank You!

Kevin.Peuhkurinen@LondonLife.com