

2ND BOARD RISK MANAGEMENT COURSE

The Board's Role in Technology Investment Oversight

Federated Press

November 16-17, 2009

Calgary, Alberta

Robert Matheson, *B.Com., J.D.*

CEO, Glenbriar Technologies Inc. ©2009

What's Coming

- Director's role
- Board's role
- TSX Guidelines
- NI 52-109
- Limitations to these standards
- Additional tests for non-TSX entities
- Problems for the non-technical director
- Leaving technology to the “experts”
- 20 questions for board oversight of IT
- US General Accounting Office
- FedEx – a simpler approach
- Conclusions
- Appendix – IT Oversight Committee Charter

Director's role

- A director must act in good faith with a view to the best interests of the corporation.
 - A director must be reasonably informed and act prudently.
 - A director must not act for a “collateral purpose” (e.g., conflict or personal gain).
 - This duty is owed to the corporation, not the shareholders.
 - This is not the same as “maximizing shareholders’ value”.
 - A director’s exercise of reasonable business judgment is not subject to review by the Court.
 - A director must not interfere with the daily management of the corporation.

Board's role

- The board governs. The CEO and officers manage.
 - The board sets strategic directions and policies.
 - The board hires, reviews and replaces the CEO.
 - The board oversees performance and trends.
 - The board asks the “right questions” of management.
 - The board must not micromanage the CEO or otherwise attempt to manage the corporation.
 - The board must focus on the long-term success of the corporation.

TSX Corporate Governance Guidelines

- The board has “stewardship” of the corporation.
 - Adopt a strategic planning process
 - Identify business risks and implement systems to manage them
 - Succession planning – appoint, train and monitor senior management
 - Establish a corporate communications policy
 - *Assume responsibility for the integrity of the corporation’s internal control and management information systems.*

NI 52-109 – Certification of Disclosure

- CEO & CFO certify quarterly and annually that they have:
 - Designed or supervised the design of disclosure controls and procedures and internal controls over financial reporting
 - Evaluated and reported on the effectiveness of controls
 - Disclosed relevant changes in controls procedures
- These certifications are loosely based on US Sarbanes-Oxley disclosures.
- The board's role in this area is to monitor management's efforts.
- Board relies strongly on the auditors in this area.

Limitations to these standards

- The TSX Guidelines are meant for the largest public companies in Canada. They don't apply to venture issuers.
- NI 52-109 is watered down for venture issuers.
- Neither standard applies to private, non-profit or public sector organizations, and may be inappropriate in certain areas.

Additional tests for non-TSX entities

- Entity's "IT comfort zone" (culture/needs/resources)

Survival

Status
quo

Leading
edge

Bleeding
edge

receivership

conservative

progressive

tech junkies

- Entity's degree of reliance on technology
 - Is technology critical to the entity's long-term success?
 - Is technology a key contributor to results?
 - Is IT oversight a "missing link" in entity governance?
 - Is there excessive reliance on in-house expertise?
 - Are IT decisions being made for the entity or the techies?

Problems for the non-technical director

- Technology is a “black box” to many non-technical persons
- Most board members are not technology experts.
- Some board members think they know more than they do.
- How does a non-techie keep up with rapid technology change?
- What is the downside to leaving technology investment decisions to the experts?
- What inquiries can a non-techie make to address IT issues?

Leaving technology to the “experts”

- Some blue chip boards have been bamboozled by “experts”:
 - AT&T Canada – purchased MetroNet in 2000 for \$4.25 billion. MetroNet was building dark fibre networks in downtown Calgary, Vancouver, Toronto and Montreal. Rogers AT&T was a 50/50 wireless venture in Canada. Five years later, when AT&T wanted out of Canada, they sold to Rogers, but took a \$4.25 billion writedown.
 - Time Warner – purchased AOL in 2001 for \$112 billion, leading to a \$98 billion writedown the next period. AOL had millions of dialup Internet subscribers. According to an A&E documentary, Steve Chase (AOL) and Gerald Lavigne (TW) reached the deal on the back of a napkin in a Las Vegas lounge, and the deal was approved by the board the following Monday.
 - Y2K – Peter de Jager made a career out of scaring the world into believing in the Y2K monster. Large and small companies spent thousands to billions on compliance. Banks, insurance companies, auditors and technology companies joined in. 8 hours on the Internet confirmed it was a house of cards for most businesses.
 - Nortel/WorldCom/Enron – all relied upon some degree of technology obfuscation to achieve their ends.

20 questions for board oversight of IT

- *Adapted from the CICA's IT Advisory Committee's list, which is used by the Institute of Corporate Directors (Canada)*

Strategic issues

- 1) **IT Plan** – Is there an IT Plan that is kept up to date? Is it used in budgeting and to prioritize projects?
- 2) **IT Trends** – Is there a procedure for tracking and assessing the effect of technology trends on the entity?
- 3) **Internal Performance** – Are indicators and drivers used to assess and benchmark internal IT performance?
- 4) **Third Party Performance** – Are indicators used to assess 3rd party service providers?
- 5) **Internal Personnel** – How are personnel needs identified and top talent recruited?
- 6) **Personnel Development** – Are procedures in place for turnover, training and project assignment?

20 questions for board *(cont'd)*

Internal control issues

- 7) **Governance** – Has the board assigned a director or committee to oversee investment in or use of IT?
- 8) **Managerial Responsibility** – Has IT governance been assigned to a high enough level? How are policies communicated?
- 9) **Compliance** – Are procedures adequate to ensure compliance with SOx/TSX/CSA rules?

Risk issues

- 10) **Risk Assessments** – Does management periodically conduct risk assessments of internal and external IT? Are they acted on?
- 11) **Data Integrity** – Does management ensure relevance, completeness, accuracy, timeliness and appropriate use of data?
- 12) **Audit** – Are IT systems reviewed and audited to test controls and support major business processes?

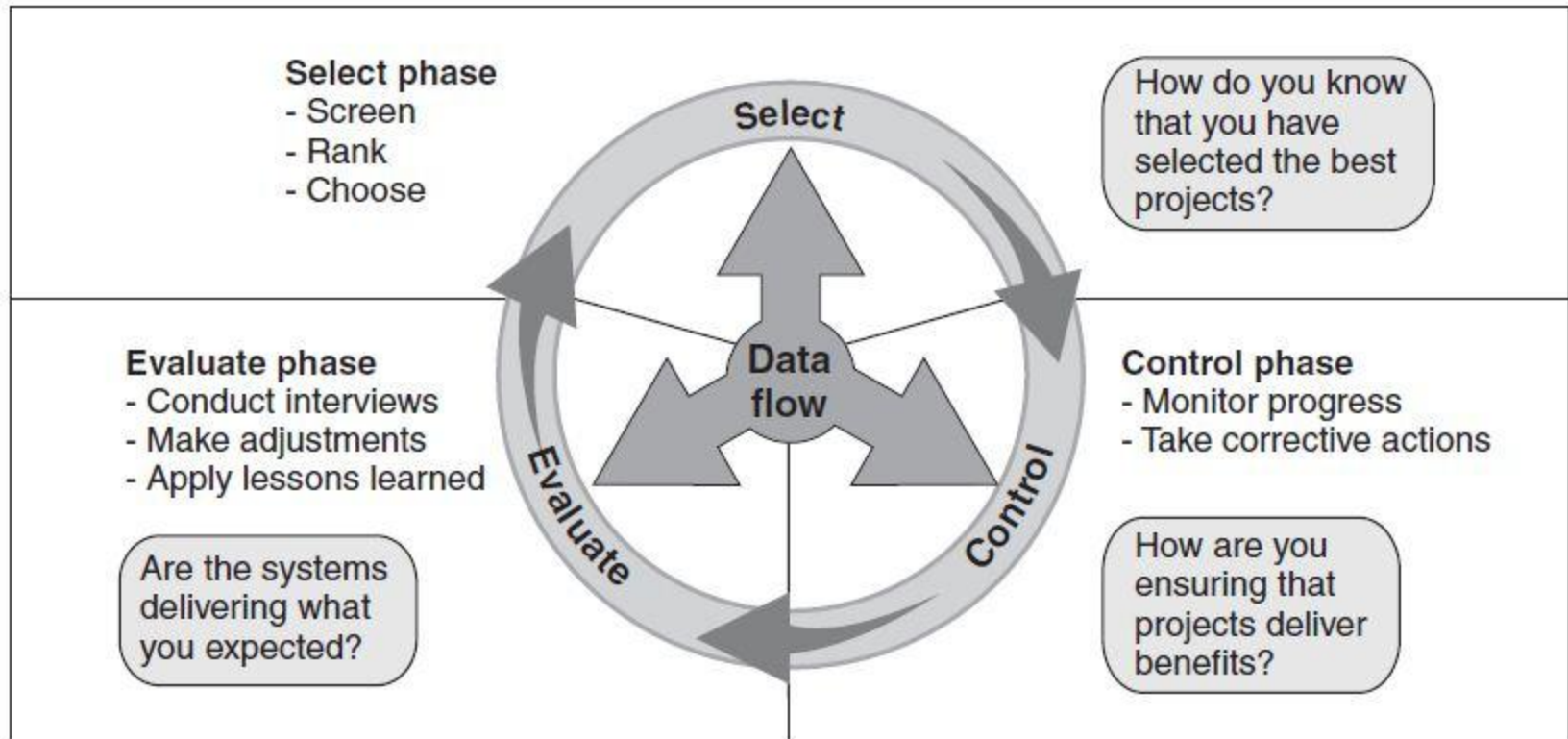
20 questions for board *(cont'd)*

Risk issues *(cont'd)*

- 13) **Privacy Legislation** – Has someone been given responsibility for this?
- 14) **Privacy Policies** – Are policies and monitoring in place for compliance?
- 15) **E-business Setup** – If used, have risks and controls been reviewed?
- 16) **E-business Security** – Is there appropriate security to protect entity and customers?
- 17) **Availability** – Are uptime policies set and being met?
- 18) **Continuity Plan** – Has a continuity plan been adopted? Is it regularly tested and improved?
- 19) **Intellectual Property** – Have the legal implications of use of software, hardware, service and copyright been addressed?
- 20) **Acceptable Use** – Are policies about licensing, agreements, copyright and acceptable use set up and being monitored?

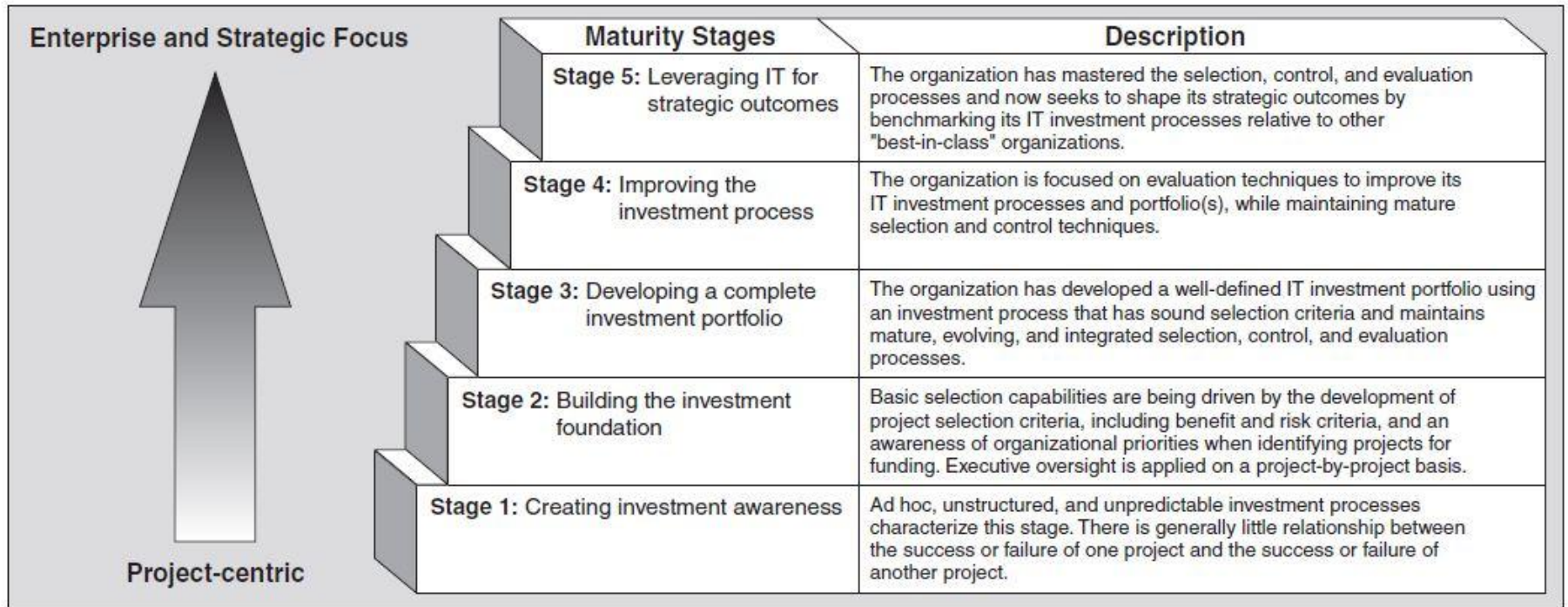
US General Accounting Office (GAO)

Figure 1: Fundamental Phases of the IT Investment Approach



US General Accounting Office (GAO)

Figure 2: The Five Stages of Maturity Within ITIM



Source: GAO.

FedEx – a simpler approach

- FedEx has 4 board committees (12 person board):
Audit, Compensation, Governance & IT Oversight
- IT Oversight Committee's purpose:
 1. Appraise major IT related projects and technology architecture decisions
 2. Ensure IT programs effectively support business objectives & strategies
 3. Advise senior IT management team
 4. Advise board on IT-related matters
- Minimum of 3 members required, currently set at 4:
 - 3 CEOs of technology companies, plus Harrah's CEO
- Simple, effective 1.5 page Charter:
<http://ir.fedex.com/documentdisplay.cfm?DocumentID=120>

Conclusions

- Most entities rely heavily on IT. This dependence is expected to increase over time.
- Failure of IT systems can put an entity, its customer base, and its intellectual property at risk.
- IT systems have grown increasingly complex and pervasive, making it difficult for a non-technical director to stay informed.
- IT investments should be judged on their merits, just like any one of many critical business components, such as marketing, service or product development.
- In most entities, the board of directors has a necessary and positive role to play in the review of technology investment decisions.
- The board can meet its obligations in this area without undue complexity or interference with management's role.
- Directors should avoid following a herd mentality by asking questions until they are sufficiently informed to make reasonable decisions.

Appendix – IT Oversight Committee Charter

1. **Purpose.** The purpose of the Information Technology Oversight Committee is to:
 - a) Appraise major IT related projects and technology architecture decisions.
 - b) Ensure that IT programs effectively support business objectives and strategies.
 - c) Advise the senior IT management team.
 - d) Advise the board of directors on IT related matters.

2. **Membership and Subcommittees.** The IT Oversight Committee shall consist of at least 3 or more members of the board of directors as shall be appointed by the board from time to time. The board shall designate the Chairperson of the Committee. The Committee may delegate authority to any subcommittee as it deems appropriate or advisable.

3. **Functions, Powers and Responsibilities.** The Committee shall:
 - a) **IT Projects**
 - i. Appraise and critically review the financial, tactical and strategic benefits of proposed major IT related projects and technology architecture alternatives.
 - ii. Appraise and critically review the progress of major IT related projects and technology architecture decisions.
 - iii. Make recommendations to the board of directors with respect to IT related projects and investments that require board approval.

Appendix – IT Oversight Comm Charter (*cont'd*)

b) IT Security

- i. Monitor the quality and effectiveness of IT security.
- ii. Periodically review and appraise IT disaster recovery capabilities.

c) Internal Controls

- i. Monitor the quality and effectiveness of IT systems and processes that relate to or affect internal control systems.
- ii. Periodically report to and consult with the Audit Committee regarding IT systems and processes that relate to or affect internal control systems.

d) Advisory Role

- i. Advise the senior IT management team.
- ii. Stay informed of, assess and advise the senior IT management team with respect to new technologies, applications and systems that relate to or affect IT strategy or programs.

Appendix – IT Oversight Comm Charter *(cont'd)*

e) Other

- i. Annually review the Committee's performance, and report the results of such review to the board.
- ii. Annually review and reassess the adequacy of this charter and recommend any proposed changes to the board for approval.
- iii. Report regularly to the board on matters within the scope of the Committee, as well as any special issues that merit the attention of the board.
- iv. Perform such other duties as are necessary or appropriate to ensure that the IT programs effectively support business objectives and strategies, or as the board may from time to time assign to the Committee.