How Mature Is Your IT Risk Management?

George Westerman, Research Scientist, MIT Sloan Center for Information Systems Research
Brian Barnier, Strategy, Governance & Risk, CIO Office, IBM

Do your IT risk management activities just respond to today’s threats, or do they actually help you manage IT better? A joint MIT CISR/IBM survey of 258 IT and business executives shows that companies with mature IT risk management capabilities are more effective not only at risk management, but also at IT management in general. This is no accident; paying attention to risk helps to improve the culture of the IT unit and the way IT assets are structured. This briefing explains the concept of IT risk maturity and provides a self-assessment tool.

Maturity on Three IT Risk Disciplines

A mature IT risk management capability is built on three core disciplines:

- An effective risk governance
- A solid IT foundation
- A culture of risk awareness

The three disciplines work together to ensure that an organization understands the IT risks it is facing, makes good decisions about what to do about them, and creates conditions that reduce risk over time.

Risk governance is the set of policies, processes and roles that enable an organization to exercise oversight and make better decisions about IT risks in business processes. In most firms, a central group creates policies to help managers in each unit identify and manage their own IT risks. Local managers address their risks locally and notify the central group about their highest risks. An enterprise-wide committee then prioritizes how to invest centrally to mitigate the firm’s highest risks.

The self-assessment tool on page 3 lists practices associated with mature risk governance. Nearly half (48%) of firms have placed a single person in charge of all IT risk management, but only about a third have formal categories of risk or a formal exception process. An important issue is the 66% of firms that have not effectively integrated IT risk into enterprise risk management (ERM). General-purpose ERM frameworks such as AS/NZS 4360 or COSO’s framework do not explicitly address IT risk. To gain tighter integration, companies are increasingly mapping IT frameworks such as the IT Governance Institute’s COBIT® to the general purpose frameworks they are currently using.

While key risk indicators (KRIs) are an important way to assess level of risk and health of risk management, only 28% of respondents believe they use risk indicators effectively. A fully integrated real-time KRI dashboard is difficult to achieve, but firms can start with simpler measures. PFPC began by tracking trouble ticket volume and employee turnover, as warnings of availability risk and potential skill losses respectively. Other firms track indicators such as password resets, project completion rates, reconciliation failures, business process recovery times, and intrusion attempts.

The IT foundation is the set of infrastructure, applications, supporting technology, and people who enable business processes to run. An immature foundation—poorly managed or overly complex—is a recipe for risk. Inconsistent software updates and overly complex interdependencies cause it to fail often, to be difficult to recover, and even more difficult to change. A mature foundation, on the other hand, is statistically the most important element to reduce risk and improve IT performance.

While three-fifths of respondents reported they maintain infrastructure well and have a working Business Continuity Plan (BCP), it is important to stay vigilant. One firm experienced the same virus at three offices, six months apart, because IT staff did not inform other sites of the threat or the fix. IT staff in another firm routinely missed a set of servers when installing patches. Key to keeping the foundation well maintained are IT service management

---


2 On all of the self-assessment questions, we define a six or seven (on a seven-point scale) as indicating that the respondent believed a practice was being performed effectively.
processes such as those in the IT Infrastructure Library® (ITIL) and appropriate controls such as those in COBIT®.

Although the majority of firms are satisfied with their infrastructure maintenance, not as many are taking the more important step of improving the structure of the IT foundation. Only about 40% believe their foundations are no more complex than necessary, or that their executives understand the links between IT and business processes. BCP can be helpful here. Executives can use BCP-generated knowledge of links between IT and business process, and of issues in those links, to make the case for change. Then, leading firms use project-level IT governance mechanisms to gradually improve the IT foundation over time.

The third discipline is risk awareness. A risk aware culture is not risk averse; it is a culture where people understand what risks they face, can recognize activities that may lead to unnecessary risk, and can openly discuss how to manage their risks. A risk aware culture makes a firm both safer and more agile. The firm can take on bigger challenges because it is better able to both manage risks and to recognize when to change a risky activity.

A risk-aware culture does not happen accidentally. It must be consciously built and reinforced by the company’s leadership. Three-fifths of respondents said their employees are very comfortable talking openly about IT risks, but only about a third said they had effective risk training for employees or that awareness was reinforced effectively using reminders. Still fewer were using awareness to improve the way they make IT decisions, as only 27% said most IT/business discussions include risk. Discussing risk, such as whether to integrate an acquisition or whether to use a different set of technologies in a project, can be a useful way to improve decisions. For example, Intel’s project demand management process includes questions that raise awareness of architectural exceptions and other issues that may create operational risks later on.

The goal is to make the IT risk culture as prevalent as the safety culture in high-risk industries. Nearly every big oil company requires that meetings start with a short discussion on a safety topic of the meeting leader’s choosing. There are frequent safety reminders. Executives in these firms make a point of discussing risk and noting when people are being risk unaware. IT leaders can use similar practices to make their units’ cultures more risk-aware.

Assessing Your IT Risk Maturity

Figure 1 shows IT risk maturity for the 258 surveyed firms. LOB risk managers are a bit more optimistic about their firms’ IT risk maturity than IT managers are, with a mean of 70.3 versus 65.7. IT managers also had a higher variance in their self-assessments. The difference may be because LOB risk managers are focused on the general outcomes of the risk management effort while IT managers, being closer to the details, understand more of the difficulties in managing IT risks.

Take five minutes to complete the IT risk maturity self assessment on page 3. Then compare your answers with those of your peers in both IT and business management roles. This exercise will help everyone assess areas of agreement and disagreement, understand what it means to be mature, and jointly decide what to do next.

If your firm is at or above average, you are already reaping some of the benefits of effective risk management. Additional improvement, especially in the foundation and risk aware culture, will help all of IT—not just risk management—perform better. If your firm is below average, work to improve all three disciplines. A useful starting point is risk governance. Going through the governance process identifies weaknesses in the foundation and helps raise awareness. It is also the discipline that gets most attention and involvement from senior executives.

Firms with higher IT risk maturity report statistically significantly better control of their key risks and stronger alignment between IT and business managers. They also report statistically significantly lower IT costs and higher agility. So, in all of your risk management efforts, change the mindset from one of avoiding risks to one of risk-aware IT management. Then risk management pays off twice—in lower risk and a more effective IT unit.

Figure 1: IT risk maturity in a global sample of 258 companies
Self-Assessment: IT Risk Maturity
Please choose how much each statement describes your organization, using a scale of 1 to 7 where 1 means that it does not describe your organization at all, and 7 means that it describes your organization to a great extent.

Risk Governance Process
☐ We have clearly defined categories—such as availability, access, accuracy and agility—into which IT risks are grouped.
☐ We have guidelines to help individuals assess the magnitude of risks in a consistent way.
☐ We have a formal process for evaluating potential exceptions to IT policy.
☐ We have key indicators to monitor the effectiveness of our IT risk management activities on a regular basis.
☐ IT risk management is integrated into risk management for all other enterprise-level risks.
___ Total (out of 35)

Foundation
☐ A business continuity plan exists to help the organization recover in the event of an IT infrastructure failure.
☐ Our IT environment—including applications, middleware, servers, storage and networks—is well maintained.
☐ Our infrastructure and applications environment is no more complex than necessary for the business to run effectively.
☐ IT people understand how IT and infrastructure link to business processes.
☐ Applications and infrastructure follow a well-defined enterprise architecture.
___ Total (out of 35)

Risk-Aware Culture
☐ Employees can talk openly about IT risk.
☐ Employees are trained in risks and controls relevant to their roles and responsibilities.
☐ There are frequent reminders of IT risks and policies through a variety of communications approaches.
☐ Most discussions between IT and business include discussion of IT risk implications.
☐ Executives commend risk-aware behavior and criticize behavior that is not risk aware.
___ Total (out of 35)

IT Risk Maturity Score
To determine your IT risk maturity, copy your totals from above into the fields below, and then do the calculation.
Risk governance process _____
Foundation _____
Risk-aware culture _____
Subtract 5 - 5
TOTAL: IT risk maturity _____ (out of 100)
CISR MISSION

CISR was founded in 1974 and has a strong track record of practice based research on the management of information technology. As we enter the twenty-first century, CISR’s mission is to perform practical empirical research on how firms generate business value from IT. CISR disseminates this research via electronic research briefings, working papers, research workshops and executive education. Our research portfolio includes:

- Achieving Superior Business Value from IT — A Single Framework of What Matters
- Managing IT for Efficiency and Growth
- Benchmarking and Building Risk Management Capabilities
- Business Models
- Distributed Collaboration
- Building Innovative Capabilities Through IT
- Building a Platform for Agility
- Enterprise Architecture as Strategy
- IT-Enabled Business Change
- Maturing and Globalizing IT Governance
- Redefining the CIO; Introducing the SEO
- Enhancing Engagement
- IT Portfolio Investment Benchmarks, IT Savvy and Links to Firm Performance
- Strategic Outsourcing

In July of 2008, Jeanne W. Ross succeeded Peter Weill as the new director of CISR. Peter Weill became chairman of CISR, with a focus on globalizing CISR research and delivery. Drs. George Westerman and Stephanie L. Woerner are full time CISR research scientists. CISR is co-located with MIT Sloan’s Center for Digital Business and Center for Collective Intelligence to facilitate collaboration between faculty and researchers.

CISR is funded in part by Research Patrons and Sponsors and we gratefully acknowledge the support and contributions of its current Research Patrons and Sponsors.

CONTACT INFORMATION

Center for Information Systems Research
MIT Sloan School of Management
5 Cambridge Center, NE25-777
Cambridge, MA 02142
Telephone: 617-253-2348
Facsimile: 617-253-4424
http://mitsloan.mit.edu/cisr/

Jeanne Ross, Director jross@mit.edu
Peter Weill, Chairman pweill@mit.edu
Chris Foglia, Associate Director cfoglia@mit.edu
George Westerman, Res. Scientist georgew@mit.edu
Stephanie Woerner, Res. Scientist woerner@mit.edu
Jack Rockart, Sr. Lecturer Emeritus jrockart@mit.edu
Chuck Gibson, Sr. Lecturer cgibson@mit.edu
Tea Huot, Sr. Administrative Assistant thuot@mit.edu

CISR RESEARCH PATRONS
The Boston Consulting Group, Inc.
BT Group
Diamond Management & Technology Consultants
Gartner
IBM Corp.
Microsoft Corporation
Tata Consultancy Services Limited

CISR SPONSORS
Aetna, Inc.
Allstate Insurance Company
ANZ Banking Group (Australia)
AstraZeneca Pharmaceuticals, LP
Banco Itaú S.A. (Brazil)
Banco Real (Brazil)
BP
Campbell Soup Company
Canadian Imperial Bank of Commerce
CareFirst Blue Cross Blue Shield
Caterpillar, Inc.
Celanese
Chevron Corporation
CHRISTUS Health
Chubb & Sons
Commonwealth Bank of Australia
Credit Suisse (Switzerland)
Det Norske Veritas (Norway)
DHL Global Management GmbH (Germany)
Direct Energy
Embraer – Empresa Brasileira de Aeronautica S.A. (Brazil)
EMC Corporation
ExxonMobil Global Services Co.
Fidelity Investments
Guardian Life Insurance Company of America
Hartford Life, Inc.
HBOS Australia
ING Groep N.V. (Netherlands)
Intel Corporation
International Finance Corp.
Johnson & Johnson
Liberty Mutual Group
Marathon Oil Corp.
Mars, Incorporated
Merrill Lynch & Co., Inc.
Mohegan Sun
MetLife
Mohegan Sun
NASA
News Corporation
Nissan North America, Inc.
Nomura Research Institute, Ltd.
Parsons Brinckerhoff
PepsiAmericas, Inc.
PepsiCo International
Pfizer, Inc.
PNC Global Investment Servicing
Procter & Gamble Co.
Quest Diagnostics
Raytheon Company
Renault (France)
Standard & Poor’s
State Street Corporation
Sunoco, Inc.
TD Bank
Time Warner Cable
Trinity Health
TRW Automotive, Inc.
Unibanco S.A. (Brazil)
VF Corporation
Wal-Mart, Inc.
World Bank