

# LEVERAGING WITH INFORMATION TECHNOLOGY: WHAT IS IS RISK MANAGEMENT\*

## Global Text Project

This work is produced by OpenStax-CNX and licensed under the  
Creative Commons Attribution License 3.0<sup>†</sup>

### Abstract

Business Fundamentals was developed by the Global Text Project, which is working to create open-content electronic textbooks that are freely available on the website <http://globaltext.terry.uga.edu>. Distribution is also possible via paper, CD, DVD, and via this collaboration, through Connexions. The goal is to make textbooks available to the many who cannot afford them. For more information on getting involved with the Global Text Project or Connexions email us at [drexel@uga.edu](mailto:drexel@uga.edu) and [dcwill@cnx.org](mailto:dcwill@cnx.org).

**Editors:** Donald J McCubbrey (Daniels College of Business, University of Denver, USA) and Garry Woods (CommerceNext LLC, USA)

**Reviewer:** Richard A Scudder (Daniels College of Business, University of Denver, USA)

The IS risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of information/technology solutions (Application, Hardware, Network and People) within an organization. IS risk consists of IS-related events that could potentially impact the business. It is also the management of uncertainty within the functions of IS so as to provide the organization with assurance that:

- the possibility of a threat occurring is reduced or minimized, and
- the impact, direct and consequential, is reduced or minimized.

To provide this assurance, threats must be identified and their impact on the organization evaluated so that appropriate control measures can be effected to reduce the possibility or frequency of a threat occurring and to reduce or minimize the impact on the business.

Information is a key business resource which, in order to be of value, must be correct, relevant and applicable to the business process and delivered in a timely, consistent and usable manner; it must be complete and accurate and provided through via the best use of resources (planned or unplanned), and if sensitive it must have its confidentiality preserved. Information is the result of the combined application of data, application systems, technology, facilities and people. IS Risk Management ensures that the threats to these resources are identified and controlled so that the requirements for information are met.

---

\*Version 1.4: Oct 6, 2010 4:22 pm -0500

<sup>†</sup><http://creativecommons.org/licenses/by/3.0/>

## 1 Project management risks

Despite the fact that sound system design and installation methodologies have been well known for decades, the IT profession is still plagued by troubled or failed projects, colloquially called “an Ox in the ditch.” Studies like the Chaos Reports published by the Standish Group over the years have documented the extent of IT project successes and failures. For example, the latest publicly available report, “CHAOS Summary 2009,” states:

*“This year’s results show a marked decrease in project success rates, with 32% of all projects succeeding which are delivered on time, on budget, with required features and functions” says Jim Johnson, chairman of The Standish Group, “44% were challenged which are late, over budget, and/or with less than the required features and functions and 24% failed which are cancelled prior to completion or delivered and never used.”*

“These numbers represent a downtick in the success rates from the previous study, as well as a significant increase in the number of failures”, says Jim Crear, Standish Group CIO, “They are low point in the last five study periods. This year’s results represent the highest failure rate in over a decade” (Standish 2009). So, you have to be aware of figure like these before you give the go-ahead for an IT project. Failed IT projects can be disastrous to an organization, even forcing them to go out of business.

Some of the reasons IT projects fail are:

- An inadequate understanding of what functions and features (i.e. requirements) the organization needs in the new system. It would be like trying to build a building before its design has been completed.
- Poor project planning, task identification, and task estimation. Usually this means that essential tasks have been overlooked or under-estimated meaning the project’s time and cost estimates are too optimistic.
- Lack of proper skills on the project team. This would be like assigning carpentry tasks to an electrician. Some IT professionals think they can do anything and this is almost always not true.
- Failure to address problems and/or no project champion. Just about every IT project has problems. If they are not dealt with on a timely basis they don’t go away by themselves, they just get worse. It is helpful in addressing problems if a highly-placed executive is a “champion” of the project and can step in and get problems solved if the project team is struggling.
- Inadequate testing. All too often, a new system is put into operation before it has been adequately tested to be sure it handles all conditions it is likely to encounter. A system failure after conversion can cause normal business processes (like accepting customer orders, for example) to fail.
- No fall-back plan. Before converting to a new system, the project team should have a tested fall-back plan they can revert to in order to keep business processes working while the new system is adjusted.
- Executive champions should be aware that IT project risks are all too often known to the IT professionals but are not always shared with others. Therefore, you should always ask that a formal project risk assessment be done at the beginning of a project and that plans are in place to keep risks at a minimum.

## 2 Security risks

The biggest challenge companies’ face in tackling IS security risks is the growing sophistication of hackers and other cyber-criminals. Organizations must now contend with a range of hi-tech attacks orchestrated by well-organized, financially-motivated criminals. While large organizations often have independent IS security staffs, it is likely that your start-up can focus on just a couple of basic items, such as:

- Identifying the value of information stored on your computer(s) and making sure that access to such information is restricted to employees who need to use for legitimate business purposes. For example, your customer database and customer profitability analyses should be protected as you would not

want such information to fall into the hands of a competitor as the result of actions taken by a disloyal employee.

- Computers sometimes break down (“crash”). This is why it is important to have a procedure of backing up critical files on a daily basis, and have written, tested procedures to recover needed information from backup files quickly. Organizations have gone out of business as a result of failed computer systems that were not properly backed-up.

If you have a website, you will need to be sure that it is adequately protected from both internal and external threats. We discuss Internet risks in the next section.

### 3 Internet risks

Companies considering a web site or Internet-based services need to be aware of the various risks and regulations that may apply to these services. Over the past few decades, the Internet has become critical to businesses, both as a tool for communicating with other businesses and employees as well as a means for reaching customers. Each day of the week and every month, there are new internet threats. These threats range from attacks on networks to the simple passing of offensive materials sent or received via the internet. The risks and particular regulations that apply may vary depending on the types of services offered. For example, Institutions offering informational websites need to be aware of the various consumer compliance regulations that may apply to the products and services advertised online. Information needs to be accurate and complete to avoid potential liability. Security of the website is also an important consideration. Companies and some individuals traditionally have relied on physical security such as locks and safes to protect their vital business information now face a more insidious virtual threat from cyber-criminals who use the Internet to carry out their attacks without ever setting foot in an establishment or someone’s home. More often than not, these crimes are conducted from outside the United States. Security measures should protect the site from defacement and malicious code.

It is clear that no single risk management strategy can completely eliminate the risks associated with Internet use and access. There is no one special technology that can make an enterprise completely secure. No matter how much money companies spend on cyber-security, they may not be able to prevent disruptions caused by organized attackers. Some businesses whose products or services directly or indirectly impact the economy or the health, welfare or safety of the public have begun to use cyber risk insurance programs as a means of transferring risk and providing for business continuity.

### 4 Summary of IS risk management

Managing IS Risk is a daily decision making process aimed at reducing the amount of losses and threats to a company. It is a pro-active approach to reducing ones exposure to data/information loss and ensuring the integrity of the applications used day-to-day. An IS security plan should include at minimum a description of the various security processes for specified applications, procedural and technical requirements, and the organizational structure to support the security processes. A risk assessment should be performed first. Identifying risks provides guidance on where to focus the security requirements. Security requirements and controls should reflect the business value of the information assets involved and the consequence from failure of security. Security mechanisms should be ‘cost beneficial’, i.e., not exceed the costs of risk. It should also include what is expectable for risk within the overall IS security plan