

Megan Kasbohm
BADM 559
Term Paper

Enterprise Risk Management & IT Implications

All companies in all industries face risks to successfully running a business. A risk is any factor that can hinder the ability for a company to be successful. Companies have to be aware of both internal and external risks to effectively manage them. Enterprise risk management is an ongoing process that deals with handling the risks a particular company faces. It uses a combination of business processes and methods to better minimize risks and maximize potential opportunities. ERM provides a framework that companies can use within their own business internal control system and model to fit their individual needs. When a company is more aware of the risks it faces, potential losses can be prevented.

According to the COSO publication on Enterprise Risk Management¹, there are eight components that comprise ERM. A company can implement these eight steps to help minimize risks. The first is internal environment. This component takes into consideration the overall attitude of the firm towards risk, whether is it a risk adverse, neutral or seeking. This step requires the firm to define its risk seeking behavior to be able to apply it throughout all levels of the company.

The next component is the existence of objectives that align with the company's overall goals. Setting objectives helps management understand what the overall company needs to obtain from its risk management process. This step also helps management see if

they are pursuing the best type of risk management strategy based on how it fits in with the overall company's objectives.

The third component is event identification. This basically means that the management needs to recognize what set ups in the internal environments and factors in the external environment could cause failures or losses. The internal environment includes infrastructure, personnel, processes, and technologyⁱⁱ. The external environment includes economic, natural, political, social and technologyⁱⁱⁱ. Event identification identifies risks to the company and makes management aware of them. IT can help companies be aware of potential problems. For example, if a company is concerned with segregation of duties across employees, management could employ an IT process that automatically logs any changes to user privileges. Unauthorized changes would alert management to a possible event or risk.

Following event identification is risk assessment. In this component, management performs an analysis all the risks identified in the third component. They need to discuss the probability of a potential risk to occur and what the magnitude would be if it did occur. Magnitude is generally measured in dollar impact. The analysis shows companies which risk have higher likelihoods of occurrence and higher the magnitudes. Management can then pinpoint which risks to really focus in on and which risks are less of a threat. Grant Thornton^{iv} sees IT as an enabler to help identify events and assess risks. IT can assess risks through risk modeling tools, business intelligence, compliance and control systems and business process management.

The fifth component is risk response. In this stage, management chooses between the following responses to each identified risk^v:

1. Avoidance: exiting the activities giving rise to risk
2. Reduction: taking action to reduce the likelihood or impact related to the risk
3. Share or insure: transferring or sharing a portion of the risk, to reduce it
4. Accept: no action is taken, due to a cost/benefit decision.

Management can choose different responses for each individual risk based on the severity of the risk.

Once the risk response strategy is chosen, the company can begin implementing control activities. The control activities are put in place to make sure the chosen risk response strategy is carried out. Implemented controls span over all levels of the company and help prevent identified risks from occurring.

At this point, the communication stage comes into play. The entire organization is made aware of the time frame and responsibilities required to carry out the control activities. This phase involves broad communication of the strategic benefits of the controls and the changes that are involved in implementing some form of risk management.

Finally, the last component is monitoring. This phase allows managers to learn from the process and make changes where necessary to the process, strategies and controls in place. Monitoring is very important because it also helps ensure that the set objectives and controls are continuing to identify and prevent risks effectively and that no break

downs have occurred. All eight components work together to help the company avoid risks and maximize opportunities.

IT performs and supports many functions within a company. Successfully using IT can assist customer delivery, business strategy alignment and corporate efficiency.

Information technology can be a great opportunity for companies to effectively manage risks. Grant Thornton provided four profiles representing different types of companies and shows how IT can be an opportunity. The graph provided relates business risks and expected IT Role for the company. (Exhibit 1)^{vi}

Companies that are risk takers, or industry leaders, and tend to use IT for utility fall under The Butler category for IT applications. The Butler minimizes governance and puts services over costs. IT can provide an opportunity to enhance services for a Butler company. This type of company needs IT that won't get in the way of business. IT applications that can help anticipate business needs are also ideal for these companies. Grant Thornton considers themselves this type of IT user, as well as most other professional service companies.

A company that is a risk taker, but uses IT for strategic roles, as opposed to a utility role, is categorized as The Entrepreneur. These companies need IT for full integration and risk management. They have little time for governance and strive to know "what" not "how." IT offers the opportunity to stream line governance issues to save them time and costs. Web B2C and consumer financial service companies generally fall into The Entrepreneur category.

The Grinder profile includes companies that are risk adverse and employ IT for utility. This type of company needs predictability and reliability for IT applications, in

addition to low cost. Grinder companies also place value on lowering unit costs. This is an area of opportunity for IT. A company could use IT to increase efficiency and cut costs. These companies can also use IT for benchmarking, which is important for their businesses. Mineral extraction companies are an example of The Grinder classification for IT use.

The final categorization is The Team Player. This type of company is risk adverse and expects to use IT strategically, as opposed to for utility. These kind of companies “work well with others,” so they need compatible IT applications. They also value time over cost, which is an opportunity for IT to increase productivity and save time. Another opportunity for IT in these companies is to make businesses process more efficient to effectively and quickly reach solutions. These companies highly value IT alignment with the rest of the business because they promote collaboration. Most auto manufacturing companies and deregulating utilities companies are categorized as The Team Player for IT opportunities. The break down Grant Thornton provides shows how IT can provide opportunities to many types of companies to manage risks at their selected levels while still staying in their business model.

Overall, IT can play a significant role in successful strategy, including risk management. Technology can make processes more efficient, reduce redundancies and identify risks. However, IT itself needs to be managed as well. IT applications cause risks and need to be monitored similarly to other business systems. Companies must be sure to monitor any additional risks that IT solutions may impose. Looking at specific company situations will help illustrate the role IT can play in risk management.

In the Grant Thornton lecture^{vii}, two case studies were given to show the implementation of Enterprise Risk Management into an organization. The first company discussed was a “multinational manufacturer of printing and copying equipment, parts and services.”^{viii} Due to the nature of the business, this company was heavily involved with logistics. Additionally, the company has a need for standardization and communication across multiple companies. Taking all these factors into consideration, the company set an objective to provide global monitoring for print quality. This environment, along with the set objective, provided an opportunity for an IT application to be implemented. The company used an IT application that monitored the print quality multi nationally. The global ability of this technological implementation provided the company to service an expanded customer base while still retaining the appropriate quality level. The new system helped them mitigate the risk of printing quality deterioration while expanding into new markets. However, it introduced additional risks such how the company will deal with expanding economies of scale and the quality of service the new system provides. To protect them from this additional risk, management implemented a system that performs real-time quality system reporting.

The second study that Grant Thornton presented^{ix} was a Not-For-Profit company. This particular company assesses the performance of individual achievement in education on standardized exams. In order to assess performances, this company uses psychometric and statistical research. The company set an objective to offer additional online services for certain customers. This objective is a great opportunity for the use of IT applications. IT can help develop the new online system as well as test it and provide training. Using IT in this situation mitigates the risk of losing customers to the growing online market.

It also seizes the opportunity to reach out to a younger market. However there is a significant risk added. The data the company wants to put online is sensitive and must be protected. The risk of hackers getting this information is of high magnitude. This company was able to add additional IT applications to protect against this risk. The company added user access logs to help guard against the risk of loss of security. Additionally, they performed monitoring measures to make sure that the added risk avoidance measures were successfully keeping hackers from getting into the system.

SPSS is a company involved in analytic software.^x This company serves as an example of successful risk management involving IT applications. In order to perform their business services, the company must be very technologically based. They use IT applications for analysis tools for analysts and organizations that require advanced mathematical and statistical functions, in addition to marketing to new clients. By building an IT portfolio and monitoring it, SPSS was able to transform their IT to better align with their business objectives.

The trend in computing was switching from monolithically computing to network computing. This changed control from being centralized to widely distributed and included offshore outsourcing. These changes required SPSS to update their IT portfolio. They started by setting a clear mission statement that included their new desire for growth and enterprise performance. As SPSS started implementing processes and controls to support the new mission, it became clear that IT was not completely aligned. Management decided the company needed a fundamental shift in culture and chose to use a maturity model (Exhibit 2)^{xi}. The four directions of this model are

1. Fast, secure, properly integrated, 100% available systems

2. Exceptional Customer Service
3. Effective Internal IT Controls, Fully Compatible
4. Engaged as a Business Partner Contributing to the Enterprise Mission

Mastering three of these components solves the IT alignment problem SPSS was facing. Based on the maturity model, the SPSS management tried to put together a service delivery model and integrate internal controls into their model. The company was able to withstand the changing environment of the industry by drilling down to the fundamental issues and designing IT applications to support them.

ICS is a unit of CITES on the University of Illinois campus. The division runs and operates seven computing labs across campus. They also provide printing services to clients. Additionally, they run an off site business office that handles operating and technological issues for the on campus labs. ICS has a small full time staff, but relies heavily on student employees. Student employees are hired as site- consultants, operations managers and tech managers.

Offering computing services involves many risks. They face the risk of expensive equipment being stolen or damaged. The university recognized this risk and added student employees to help monitor the labs. However, hiring more employees added additional risks for ICS. There is the risk of security breach or false print refunds by employees. It also added management problems because the managers were in the off site office and the employees were working in the labs somewhat unsupervised. At this point, ICS decided to implement IT to minimize those risks. They created employee access logs to be monitored by full time employees to view the time employees logged in and from

which campus lab location. This application minimized many of the risks that occurred from no direct supervision of employees. Although, it added the risk of student managers looking at the logs, not just full time managers. Adding password protection for the logs minimized the added risk. Building on this concept, ICS has been able to have a fully integrated online forum system to effectively communicate with all employees across all lab locations.

ICS faces significant competition for qualified student employees. In order to minimize the risk of being understaffed, ICS put in objective to have flexible scheduling for students. They implemented an online scheduling and subbing system in two hour block shifts (Exhibit 3)^{xii}. This IT applications helped minimize one risk, but also needs caused a risk. ICS needed employee log ins to protect employees from having their schedules manipulated.

ICS has been successful in many of their IT applications, but some of them have not been as successful. Employees are on site with the clients and they know when computers or printers malfunction. They also know when clients need assistance beyond the site consultant's scope. For these issues employees are given a ticketing system. The employees log into the forums system and fill out an electronic error ticket. Tickets are then forwarded to the student managers depending on whether it applied to the operations team or the tech team. If the issue goes past the student mangers scope, they are instructed to direct the client or issue to the correct full time student or division. This system is flawed in two areas. The first area is that the tech and operations teams are students and they do not have regular schedules. So there is no personal responsibility for any individual on the team. A student manager may not be in the office to see the ticket

until much later. This causes a lag in the amount of time it takes from the time a ticket is created to the time it is fixed. This lag ranges from one computer being down, to the entire printing network to be down. Problems like this cause serious inconveniences for the clients and can cause the loss of business. This system needs to be improved in order to be successful for getting equipment fixed in a timely manner.

ICS also has breakdowns in customer service. As a division of CITES, ICS can not handle all issues. Some issues regarding accounts, billing, and user logins/passwords for clients are handled by CITES. When a customer comes to the site consultant, they are then sent to a different division to get the problem fixed. Many times there is a communication break down and the customer gets sent multiple places and it takes significant time to get an answer. This is because the responsibilities of the divisions are not clear and each division thinks it is the responsibility of a different division. Although this risk is not necessarily IT based, it is related to ERM.

A big problem for CITES is that its divisions are not working together. There is a problem on the fundamental level. Implementing an overall ERM system for CITES would really help minimize risks that are unnecessarily occurring. It needs to be seen as a whole company, not as many small divisions. Similar to SPSS, CITES should start by setting an overall missions and objective. From there they can identify risks that affect CITES as a whole, and then drill them down to the division level. There is an opportunity for IT at this point. CITES can set up IT applications for the entire entity. With this kind of system, the risks can be managed on an enterprise level. If CITES reengineers their process and implements an ERM system, many of the problems they are facing in customer service could be avoided.

ERM is a very useful tool for all kinds of businesses. It is a framework that is highly adaptable and can be formatted to fit individual companies. It is a broad concept that can cater to specific and particular needs. ERM is a continuous process that can be constantly updated. In this highly technological and multinational world, IT can play a significant role in carrying out ERM. IT provides many opportunities to improve risk management and risk assessment, although it can cause more risks. Overall, ERM and IT can be used hand in hand to successfully minimize risks and improve business quality.

Exhibit 1

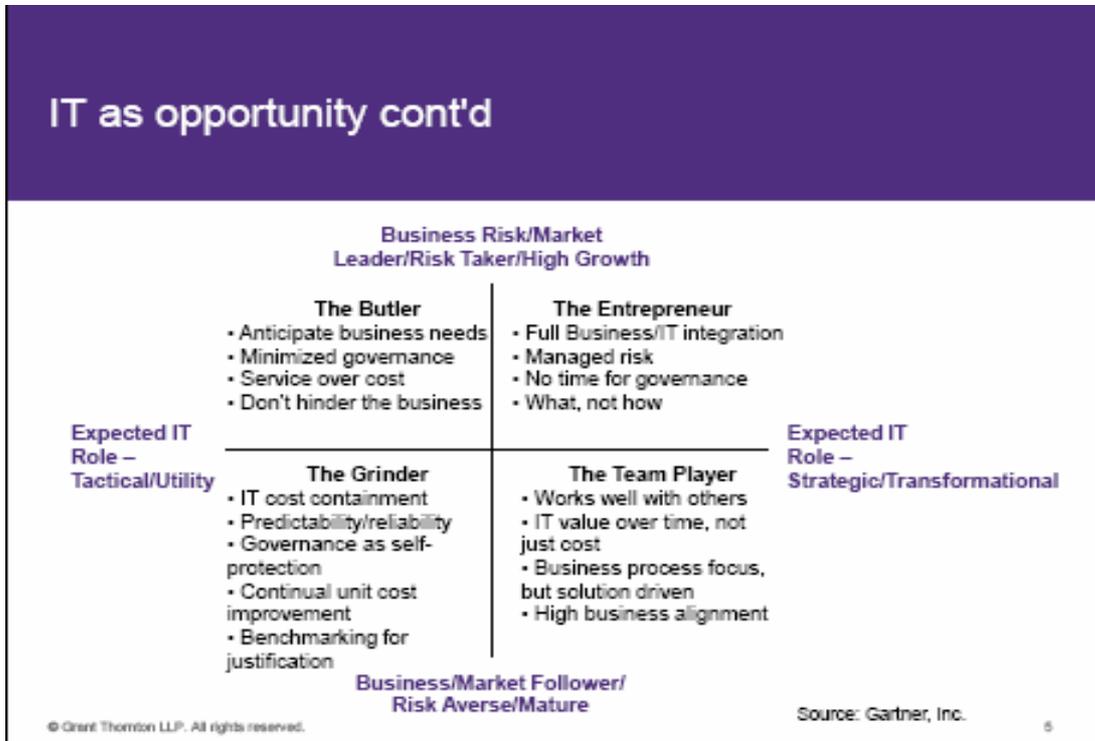


Exhibit 2

> **Start with True North...**

Fast, secure, properly integrated,
100% available systems.

Engaged as a
Business Partner
Contributing to the
Enterprise Mission



"Exceptional"
Customer Service

Effective Internal
IT Controls, Fully
Compliant

© 2008 SPSS Inc.

30

Exhibit 3

		Semester		Date																					
		Fall 2008		Wednesday		Week: 16		View		Today															
Wednesday, 10 Dec 2008																									
	BOH1	BOH2	ENG1	ENG2	MOD	MUS	NEV	OPC	OR	UG1	UG2	UN1	UN2	WH											
00:00															00:00										
01:00										vlee29					01:00										
02:00															02:00										
03:00					kasbohm2										03:00										
04:00										vander8					04:00										
05:00															05:00										
06:00										vander8					06:00										
07:00															07:00										
08:00	jolson3	dettmar2			available		chall20		icbeck2	rwoodbu2		bdurbin2		cwdt2	08:00										
09:00	jolson3	dettmar2	sok2	kbksa2	available	izucker2	chall20			rwoodbu2	rmooreh2		dcallic2		09:00										
10:00	available	dettmar2			rwildy2		chall20	available	ppatino2	rwoodbu2		mhaney2		rmok2	10:00										
11:00	available	dettmar2	istromb2	dburns2	rwildy2	nguyen21					rmooreh2		mealmer2		11:00										
12:00	available	daylor4			rwildy2		gooding2	cpolhem2	foivo2	tmevans2			ahoke2	bmc dona4	12:00										
13:00	available	available	smerr2		rwildy2										13:00										
14:00	available	available		edevers2	rwildy2	acallah2					aizang2		vmlewis2		14:00										
15:00	available	available	kelrov2		rwildy2		gooding2		iwitt	cismith8	icbeck2		ghelan2	altoms2	15:00										
16:00	available	available		tmevans2	cpolhem2	bfranks2					rmok2		vmlewis2		16:00										
17:00			kelrov2		dettmar2		gooding2		izucker2	skearns2		ppatino2		icbeck2	17:00										
18:00			ihaddad2		dettmar2	crussel3	cpolhem2		weiruwu2	skearns2	ischuma2		foivo2	arakai2	18:00										

-
- ⁱ "Enterprise Risk Management." 2004. 1 Dec. 2008
<http://http://www.coso.org/publications/erm/coso_erm_executivesummary.pdf>.
- ⁱⁱ Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ⁱⁱⁱ Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^{iv} Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^v "Enterprise Risk Management." 1 Dec. 2008
<http://http://en.wikipedia.org/wiki/enterprise_risk_management>.
- ^{vi} Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^{vii} Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^{viii} Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^{ix} Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^x Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^{xi} Hertzberg, John, and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management." BADM 559 Presentation. University of Illinois, Champaign. 22 Oct. 2008.
- ^{xii} "ICS." Schedules Page. University of Illinois. 1 Dec. 2008 <<http://ics.uiuc.edu/forums>>.