

The Pennsylvania State University

The Graduate School

The Mary Jean and Frank P. Smeal
College of Business Administration

Addressing Security in the e-Business On-demand Environment

A Paper in Business Administration

by

Aparna Prasad

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

May, 2004

Date of Approval:

Nirmal Pal
Executive Director,
e-Business Research Center,
Paper Supervisor

Akhil Kumar
Associate Professor,
Department of Supply Chain and
Information Systems
Paper Co-Supervisor

John E. Tyworth
Chairman,
Department of Supply Chain and
Information Systems,
and Professor of Supply Chain Management

Abstract

An on-demand business is one which is flexible enough to respond to any fluctuations in the running of the business. What differentiates an on-demand business from its competition is the fact that it is responsive in real time – as the events occur. This is possible only because all its business processes are thoroughly integrated and the IT infrastructure exists in an on-demand operating environment¹.

This concept has somewhat evolved over the years. On-demand computing means that the IT infrastructure which includes, computing, storage and other resources are brought and made available to the company as a whole or to a particular process on an as-needed basis. What is not needed is kept in the general pool of resources which is made available to others and essentially the ‘pay as you go’ theory is followed. This concept can be applied both to the resources and services supplied by a third-party service provider, and to the sharing of resources among the internal users of a business².

While there is no doubt that there is an immense amount of value delivered from this concept, there are still some major concerns that are inhibiting businesses from fully utilizing the power of on-demand, the most important one being Security. In this paper we shall discuss how security should be addressed when transitioning to an on-demand world, and then apply the findings of our study to the Strategic Alignment Model³.

Table of Contents

List of Figures	v
List of Tables	vi
1.0 Study Objective and Scope	1
2.0 e-Business on demand – Concept	3
3.0 e-Business on Demand –Strategy	7
4.0 The Strategic Alignment Model	11
5.0 Information Technology Security – Concept	16
6.0 Business Impact Analysis	21
7.0 Risk Assessment	29
8.0 Security Concerns in the on-demand environment	36
8.1 Security Concerns with respect to Architecture	38
8.2 Security Concerns with respect to Skills	41
8.3 Security Concerns with respect to Processes	43
8.4 Summary Table	48
9.0 Security Concerns - Post on-demand	49
10.0 Conclusion	51
11.0 Future Research	53
Bibliography	55
References	58
Appendix – A	59

List of Figures

Figure 3-1	9
Figure 4-1	12
Figure 5-1	17
Figure 5-2	19
Figure 6-1	23
Figure 6-2	24
Figure 6-3	27
Figure 7-1	30
Figure 7-2	33

List of Tables

Table 7-1	34
Table 8-1	48

Acknowledgements

I would like extend my heartfelt gratitude to the following people who have guided me through the different stages of my research.

1. Nirmal Pal, Director e-Business Research Center, Penn State University
2. Dr. Akhil Kumar, Associate Professor, Smeal College of Business, Penn State University
3. K.K Mookhey, Chief Technology Officer, Network Intelligence Pvt. Ltd, India
4. Brian Geffert, Senior Manager- Enterprise Risk Services, Deloitte U.S
5. Mark Ernest, ITS Distinguished Engineer, IBM U.S
6. Dr. Birgit Pfitzmann, Senior Researcher, IBM Zurich Research Lab

1.0 Study Objective and Scope

Businesses have always had to deal with circumstances beyond their control, and adapt their strategies and processes to either take advantage of these situations or at the very least ensure their business continues to deliver in a changing environment. Irrespective of political climates, geographical locations, industry segments, or market positions, businesses have realized that it really never is 'business as usual'. This is true more so now, than ever before. Not only do businesses have to deal with traditional market dynamics, but they also have to deal with situations that would have been unimaginable earlier - big-ticket Merger & Acquisition deals like HP-Compaq, Time-Warner-AOL, and IBM-PWC to name a few, IT outsourcing and offshoring, economic recession, collapse of large corporations like Tyco, Enron, WorldCom, etc., emergence of new markets such as those in China, South-east Asia, South America etc., and the omnipresent network security threats.

This requires that companies become more nimble and responsive to these rapid and dynamic changes, primarily by maximizing the utilization and deployment of information technology and associated processes. The e-business on-demand model created by IBM formulates this concept into a business model that is responsive, focused, variable, and resilient. At the same time any paradigm shift, such as the move to an on-demand environment, must be accompanied by stringent security controls that will ensure that the risk involved in such a move is clearly assessed and minimized.

This paper looks at the e-business on-demand strategic model, and explores the security implications associated with it. It discusses ways and means in which the information systems risks present within the model can be managed and the returns from this strategy can be maximized. All this is explained in relation to the strategic alignment model which emphasizes the need for aligning an organization's business strategy with its IT strategy and infrastructure.

2.0 e-Business on-demand – Concept

The complexities of businesses driven by globalization, commoditization, the slow growth in economy, and various technological shifts have brought to light the increasing number of environmental shifts in the business world. Of course, this phenomenon is not new i.e. the business world has always faced changes from time to time. So the question is what's new? The answer lies in the approach that needs to be taken in order to make a business more nimble. Or in other words, enabling a business in a way that it can take on whatever the world throws in at it.

Environmental shifts in the business world are a fusion of three main elements, namely, Business Transformation, Information Technology Enablement, and Culture. Business transformation is all about reinventing what you do, and how you do it³. It is essentially about companies re-examining their core competencies and determining what processes they should be doing themselves versus identifying where they should partner with others. In the process of business transformation, technology acts as an enabler and not just technology for its sake. Understanding this difference is critical.

Let us take a quick look at the strategy most companies in the early 1990s adopted in order to keep up with the environmental fluctuations. In an effort to become more IT oriented, they started to invest heavily in technology, for technology's sake. In other words they aggressively acquired assets and waited to realize its business value. The return on investment was not always as expected, and the technology sat idle or would go

underutilized. This is probably why technology is crucial in enabling the first element of business transformation as move is made towards becoming an on-demand business. The third and most important of these elements is of course the culture. It is the most important because it brings out the people factor behind the whole process. Becoming an on-demand business means changing the way we look at things. It means reinventing the enterprise not only from the business stand point but also from the customer's, the various business partners', the supplier's and the employees that make up the business ¹.

Having said all this, let us now move on to the core of what e-Business on-demand is. It is all about making businesses more nimble and giving them the ability to take on whatever the world throws at them. More formally, it can be defined as follows;

An enterprise whose business processes – integrated end-to-end across the company with key partners, suppliers and customers – can respond with speed to any customer demand, market opportunity or external threat.

There are broadly four characteristics that define an on-demand business;

1. **Responsive:** These companies are capable of sensing changes in the environment and can respond dynamically, whether to unpredictable fluctuations in supply or demand, emerging customer, partner, supplier and employee needs, or unexpected moves by their competitors ⁵.

2. **Variable:** These companies are able to adapt to cost structures and business processes flexibly. The companies can hence reduce risks and drive business performance at higher levels of productivity, cost control, capital efficiency and financial predictability ⁵. This concept is based on the idea of looking at IT as a 'utility', with a 'pay as you go' business model. The challenge for the IT department of the organization will be to strike the necessary balance between capacity/capability provided 'in-house' versus what to choose to purchase from a utility in an on-demand fashion.
3. **Focused:** These companies are committed to concentrating on core competencies and differentiating tasks and assets. The companies thus leverage on tightly integrated strategic partners to manage selected tasks ranging from manufacturing, logistics and fulfillment to HR and financial operations ⁵.
4. **Resilient:** These companies are prepared for unexpected changes and threats – be there computer viruses, earthquakes, or sudden spikes in demand. The model requires new business systems and processes that are robust and able to bounce back in real time ⁵.

Additionally, from an infrastructure standpoint, an e-business on-demand has four essential characteristics:

1. It is *integrated* .i.e. systems are seamlessly linked across the enterprise and across its entire range of customers, partners, and suppliers.
2. It uses *open standards*, so different systems can work together and link with devices and applications across organizational and geographic boundaries.

3. It is *virtualized* i.e. to make the best use of technology resources and minimize complexity for users; it uses grids to make the collective power of computing resources in the grid available to anyone in the grid who needs them.
4. It has *self-healing and autonomic capabilities*⁹. So, it can respond automatically and work around problems, security threats, and system failures. This means that technology takes over the basic management itself. It self-configures self-heals, self-optimizes, and self-protects, much like the human autonomic nervous system. It manages software upgrades, balances workload to optimize overall system performance and automatically takes action against viruses or denial-of-service attacks.

The next chapter discusses the strategy involved in moving to an on-demand business and the relevance of the Strategic Alignment Model.

3.0 e-Business on-demand – Strategy

The environmental shifts discussed in the previous section have brought to light the need for businesses to go beyond the static business models, and move towards a far more flexible and dynamic environment. Businesses today need technology not only to achieve more control over their processes and integrate them, but also to tackle business problems that may arise during this process, and then work towards becoming more efficient and responsive to customer needs and to the changing market dynamics.

There are basically two major forces that drive the on-demand initiative. The first of course is the marketplace, i.e. the customers and the business partners, and the second driving force is the technology itself. The need for increasing business process sophistication and the sophistication of technology by itself has generated a point of intersection between technology and business. This fusion point is essentially what drives the on-demand initiative ¹.

Becoming an on-demand business is all about flexibility, variability, and affordability. It is about business transformation i.e. helping the business move from a relatively static model (where it is difficult for processes to integrate), to a more flexible and dynamic process model. This means that businesses will have to identify their core competencies and the associated critical processes. On the whole there could be five main categories for these critical processes ⁴;

- Improving the customer relations

- Improving the product development process
- Supply chain management
- People and organization management
- Technology optimization.

Once these critical processes mentioned above are identified, businesses can tap all the opportunities of becoming a better on-demand business.

The main idea is to simplify the business's infrastructure so as to enable the business to support the requirements of an on-demand operating environment. The operating environment can be understood better by sub-dividing it further into (a) the Application environment and (b) the Systems environment ⁵. This is explained as follows;

- (a) The Application environment provides the right platform for the integration of applications and processes.
- (b) The System environment enables the simplification of the existing infrastructure, so as to make the business more robust and responsive to the changing market demands.

It is however necessary to understand that the operating environment which is conducive to an on-demand business is the one that maintains a balance between adaptability and over-simplification. Since, aligning a company's business strategy with its IT strategy will help offset any business risks that may be associated with reinventing the enterprise.

For example, customer intimacy can be seriously damaged if the infrastructure is over-consolidated ⁴.

Let us now move on to the changing trends of the marketplace that support the on-demand wave. The following chart (*figure 3.1*) depicts these changing trends as we move away from the traditional computing towards utility services.

	Traditional Computing		Utility Services
IT Infrastructure	Peak usage	➔	Required usage
Capacity Provisioning	Varying lead times	➔	Nominal procurement; short lead times
Charge-back	Estimated allocation	➔	Usage-based billing
User Management	Dedicated business analyst	➔	Self-service
Capital Investment	Large-scale, up-front investments	➔	Incremental investments
Cost Profile	Asset-based fixed costs	➔	Services-based variable costs

Figure 3.1 (Source: IBM ⁴)

Up until now companies were buying technology for a fixed price, but as we go forward, the processes will be made more flexible so as to allow companies to adopt the “pay as you go” methodology. This of course raises other issues of having to create a financial model for supporting the business’s infrastructure and the IT requirements around it. We shall abstain from including this in our discussion since it is beyond the scope of this paper. For now we shall briefly discuss the strategic alignment model³ that was developed by N. Venkatraman, and J.C Henderson, to understand the relevance of

aligning a company's business strategy with its IT strategy, and also to get an idea of where security fits into the e-Business on-demand framework.

4.0 The Strategic Alignment Model

Strategic alignment enables a firm to maximize its IT investments and achieve harmony with its business strategies and plans, leading to a greater profitability. Alignment is important to firms for numerous reasons. The most important ones being; (1) to facilitate the development of synergistic business and IT strategies, (2) allowing firms to focus on the application of IT to improve business efficiency and effectiveness, and (3) preventing the misapplication of technology within the firm. By analyzing the factors which benefit or enable alignment, and those which hinder or inhibit it, organizations can concentrate on the application of IT to enable their business strategy. This harmony can be extended and applied throughout the organization as technology is used to create a more focused and responsible organization³.

The strategic alignment model expatiates on the need for alignment between an organization's business and IT domains. There are essentially four domains that make up the alignment model – Business Strategy, IT Strategy, Organizational Infrastructure, and IT Infrastructure³. Each domain is sub-divided into three sub-domains which constitute the different dimensions of various relationships that can exist between these domains. The model by itself is depicted in the diagram (*figure 4.1*) below, and each domain is explained further.

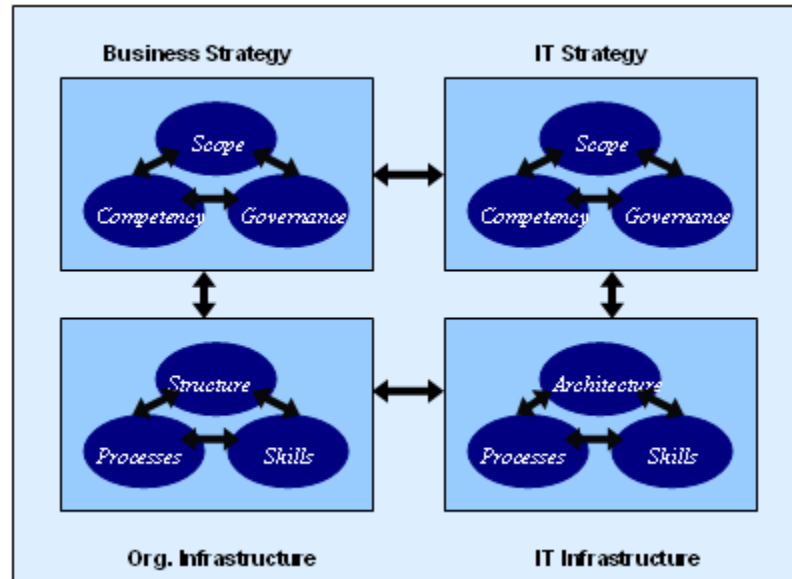


Figure 4.1 (Source: Strategic Alignment Model³)

- (1) The **Business Strategy** domain comprises of three main elements that help put together the organization's business strategy.
- (a) **Business scope** focuses on the choices pertaining to product-market offerings.
 - (b) **Distinctive competencies** are those attributes of strategy that contribute to a distinctive comparative advantage over other competitors; pricing, quality, value added services, and superior distribution channels, are a few to name.
 - (c) **Business governance** is the choice of structural mechanisms that are offered to help organize the business operations which help form the continuum between markets and the hierarchy i.e. strategic alliances, joint ventures, and licensing.

(2) The concept of **IT Strategy** has been around for a while, but is still open to differing definitions and assumptions. By drawing an analogy to business strategy, we can conceptualize IT strategy in three dimensions;

(a) **IT scope** includes different types and ranges of IT systems and capabilities that are potentially available to an organization i.e. autonomic systems, robotics, imaging systems etc.

(b) **Systemic competencies** are those distinctive attributes of IT competencies that contribute positively to the creation of new business strategies, or for that matter help support an existing business strategy.

(c) **IT governance** offers choices of structural mechanisms that are required to obtain the required IT capabilities, involving issues such as deployment of proprietary networks versus common networks, and strategic choices pertaining to the development of partnerships to exploit IT capabilities and services, including outsourcing.

(3) **Organizational Infrastructure** includes the different processes, skills and administrative infrastructure required for carrying out key activities.

(a) **Administrative infrastructure** comprises of the organizational infrastructure, and the various roles associated with the administration of an organization.

(b) The **Processes** articulate the work flows and the associated information flows that are required to carry out the key process activities.

(c) The *Skills* sub-domain comprises of the skills repository that supports any given business strategy.

(4) The **IT Infrastructure** domain in many ways is analogous to the organization infrastructure and processes domain.

(a) The *Architecture* sub-domain includes the various options pertaining to systems, applications, data, networks, and technology configurations.

(b) *Processes* include the work processes central to the operations and management of the IT infrastructure, including processes for systems development and maintenance, and systems monitoring and control.

(c) *Skills* include the various choices pertaining to the knowledge and capabilities required to effectively manage the IT infrastructure within the organization.

The strategic alignment model is more than just the articulation of the underlying axes, the four domains, and their constituent dimensions. It derives its value from the different types of relationships between the four domains; bi-variant fit, cross-domain alignment, and strategic alignment. The paper on ‘Strategic Alignment: Leveraging Information Technology for Transforming Organizations’ by J.C Henderson, J.C and N.Venkatraman³, listed in the references section describes the model and these relationships in further detail.

Let us now try to understand the relevance of this model. The strategic alignment framework applies the strategic alignment model to reflect the view that the success of any business depends a lot on the vital link between business strategy, IT strategy, organizational infrastructure and processes, and IT infrastructure and processes. It is unrewarding to work on any one of these areas in isolation, or harmonize only business strategy and IT strategy.

After studying the alignment model closely, it is evident that most issues that will arise as a result of an on-demand transition are in some way or the other a subset of each domain of the model, and also their respective sub-domains. From a process perspective there are issues pertaining to change management that would result from a business transitioning to an on-demand environment. From an architecture perspective there are issues pertaining to open architecture, and from a skills perspective there are of course knowledge management related issues that will have to be addressed. The objective of including the alignment model in our discussion is not only to re-emphasize the importance of IT which when acts as enabler of the business strategy, helps to achieve a competitive and strategic advantage for the enterprise, but also to address security concerns that may arise as a result of this transition.

5.0 Information Technology Security – Concept

What is security? In very simple terms, security is all about protecting one's assets. Hence, in addressing security, one needs to be able to answer three main questions ⁶;

- (1) What are we trying to protect?
- (2) What is the impact?
- (3) What are the associated risks?

Once these three questions are answered, we can go a long way in identifying and solving potential security problems. On a broad level, security can be divided into two main categories – Physical security, and Logical security. While each of these areas in their own way are very important, with the advent of client-server technology and the internet, logical security has naturally gained more importance over the years.

The focus of our discussion will be on logical security (*referred to as 'security' throughout the paper*), and more importantly on information security. As such security has a wide scope that includes several different areas of life. Within security, there are numerous classifications and specialized areas. Each area is either interrelated or interdependent with other areas of security. The diagram (*figure 5.1*) below depicts how technology, hardware, people, and procedures are all woven together as a security fabric.

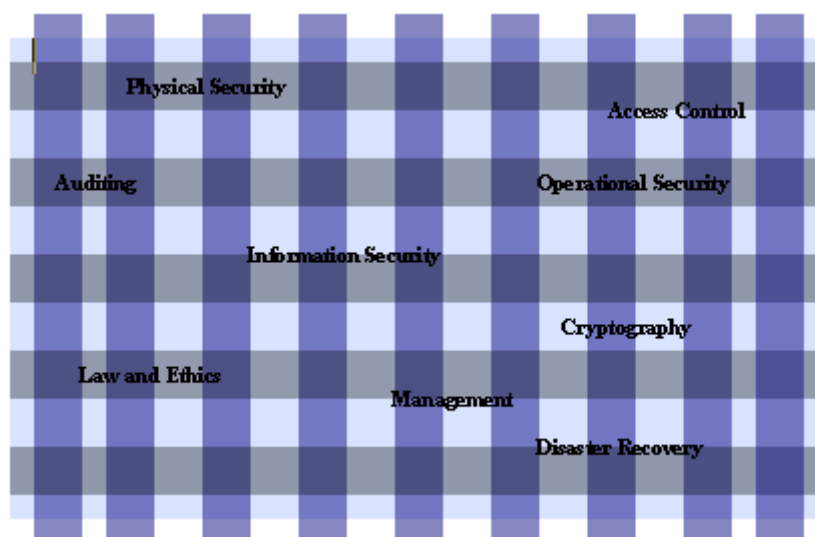


Figure 5.1 (Source: CISSP Guide⁷)

Physical security is interrelated with information security, database security lies on top of operating system security, operations security affects how computer systems are used, disaster recovery deals with systems in emergency situations, and almost every instance has some type of legal or liability issue tied to it⁷. So in the end technology, hardware, people, and procedures have security as an underlying foundation.

Going further, let us now try and understand the fundamental principles of security, or in other words, the C-I-A of security i.e. **C**onfidentiality, **I**ntegrity, and **A**vailability. These are explained briefly as follows;

- (1) *Confidentiality* provides the ability to ensure that the necessary level of secrecy is enforced at each junction of data processing and prevention of unauthorized disclosure⁷.
- (2) *Integrity* is upheld when the assurance of accuracy and reliability of information and systems is provided, and unauthorized modification of data is prevented⁷.

(3) *Availability* ensures reliability and timely access to data and resources to authorized individuals ⁷.

All security controls, mechanisms, and safeguards are implemented to provide one or more of these principles, and all the risks, threats and vulnerabilities are measured in their potential capability to compromise one or all of the C-I-A principles ⁷.

It is important to understand that threats can come from a variety of sources. External threats range from electronic joy-riders to systematic hackers. Internal threats can come from legitimate users attempting to do things that they aren't supposed to, with motivations ranging from curiosity and mischievousness to malice and industrial espionage ⁶. In an e-Business on-demand situation we will encounter many or all of such types of problems. The effective solution lies in designing responses to various scenarios, while being aware of the fact that each scenario is different from the other. In some cases the vulnerability could be measured in terms of integrity and availability, or as in most cases, a combination of all the three elements. The venn diagram (*figure 5.2*) below illustrates this point. While confidentiality, integrity, and availability are all subsets of the security objective(s) of the company, the security objective(s) is in turn a subset of the business objective(s) of the company ⁷. This concept has been explained in the previous section 4.0, where we spoke about aligning an organization's business strategy with its IT strategy.

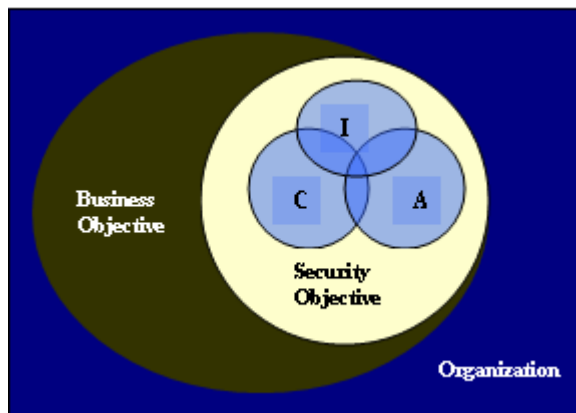


Figure 5.2 (Concept: CISSP Guide⁷)

All in all security is a major concern for all organizations, particularly in the case of information access, for any organization that undergoes a sudden rapid growth, business process re-engineering, or if and when there is a merger and acquisition situation. This is an interesting aspect of security since this situation directly relates to the e-Business on-demand scenario. Normally in such situations, the focus of the business tends to shift towards addressing change management related issues, and there is a strong likelihood of the controls that are required to protect information assets get bypassed or weakened. The critical security measures that the organization has in place so far to protect its information assets should now be expanded to include the potential IT infrastructure and the associated group of people, who will come into the picture as the organization transitions into becoming an on-demand business. While there are others in the industry who believe that an organization's security posture should always include people, processes and information technology, and that an e-Business on-demand situation should merely be an extension of the organization's current security structure, the idea here is to understand the need to address security in such a change situation.

In the remaining sections of this paper, we shall build a security framework around the e-Business on-demand environment and address topics such as Business Impact Analysis, Risk Assessment, and discuss the security concerns for this environment, with respect to the Strategic Alignment Model.

6.0 Business Impact Analysis

Business Impact Analysis as the name suggests is about figuring out what situations will affect a business and to what extent. In more formal terms Business Impact Analysis is defined as a means of systematically assessing the potential inputs from various events or incidents¹⁴.

A simple question such as “What drives a business?” can spark a number of answers. Market Fluctuations, Cash Flow, Product Demand etc. are some of the glossy terms that first come to mind. However, ensuring business continuity at all times, in any given environment, and in the wake of any given change is what truly drives a business. This is where it all comes together. The key to all this of course, is right planning. In order to plan better, the management team must first have a good understanding of the business. Understanding the business involves the following activities;

- (a) Determining the Business Objectives
- (b) Identifying the Mission Critical Activities
- (c) Determining the Services and Products that the business delivers¹¹.

The *Business Objectives* of a company enable it to identify its core-competencies and stay in a given line of business. For this reason, it is essential that the mission statement of the organization and the key supporting aims that indicate the raison d'être of the organization are defined properly¹¹. By defining the business objectives correctly, the

organization can establish the stake holder's expectations and work towards maximizing their returns.

Mission Critical Activities are basically the core processes/activities that enable the business to deliver on its promises. It is important to note that Mission Critical Activities are not only products and services that are the deliverables for the stakeholders of the company, but are also the systemic processes critical to customer service and the stability of the organization ¹². For instance, financial services and products may be the mission critical activities for a bank. But so is the core banking process that enables the deliverables to be delivered.

Typically an organization has many dependencies, both internal and external. These dependencies will either support or provide the Mission Critical Activities. The external influences can be Government Departments, Regulators, Competitors, Trade/Industry Bodies, Professional Associations, Trade Unions, Pressure Groups, and Clients/Customers ¹¹. The Internal influences are typically from within the company, such as from the higher management.

From a company's standpoint defining the Mission Critical Activities is crucial for ensuring a smooth transition into becoming an on-demand business. Thus, when defining the mission critical activities, the management team must take into consideration the various elements of the Mission Critical Activities, and their possible impact on the

business. The following diagram (*figure 6.1*) illustrates the various elements of the mission critical activities.

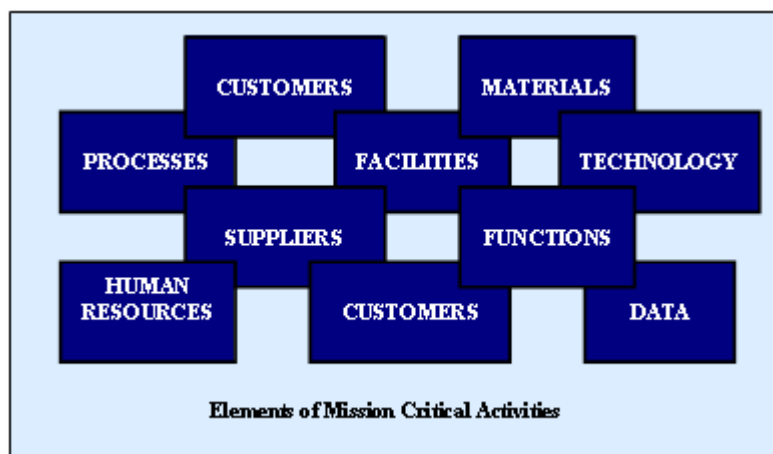


Figure 6.1 (Source: BCM – Good Practice Guide ¹¹)

Understanding the business and identifying its Mission Critical Activities, their dependencies, and the single points of failure consists of two distinct complementary processes. The first is Business Impact Analysis, and the second is Risk Assessment and Analysis¹¹. Risk Assessment has been covered in detail in the next section.

Once the organization's Mission Critical Activities have been identified along with their dependencies and single points of failure, the next step is to determine the impact upon the organization if any of these are disrupted as a result of the on-demand transition. The level of impact also provides a challenge and review process whereby the activities and their dependencies can be assessed as to their mission criticality and rating in any business continuity prioritization process¹¹. The review process will essentially take into account the *Recovery Time Objectives* and the *Recovery Point Objectives*. The time,

within which the activities are recovered, if they have been disrupted or interrupted/lost is called the Recovery Time Objective. The more critical the activity, the lesser is the Recovery Time Objective. The Recovery Point Objective is defined as the extent to which the disrupted activity needs to be restored. The following diagram (*figure 6.2*) below depicts the overall Business Impact Analysis process.

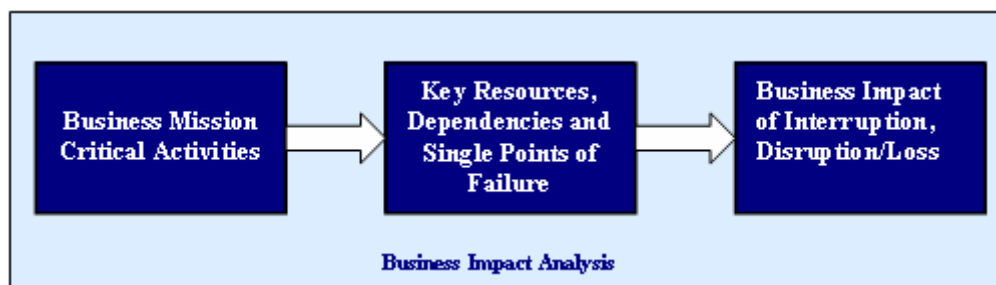


Figure 6.2 (Source: BCM – Good Practice Guide ¹¹)

The process as such involves identifying the Mission Critical Activities, followed by determining key resources, dependencies and single points of failure, and finally analyzing the business impact of interruption, or disruption/loss. The types of impacts and their effects are categorized into *Financial*, and *Non-Financial* impacts. The impacts are categorized further into Catastrophic, High, Medium and Low sub-categories. These are represented in the form of a matrix known as the Business Impact Analysis Matrix. This has been included in Appendix- A of this paper.

Normally the results of the *Business Impact Analysis* are used to handle business continuity situation in lieu of disaster recovery. However, in this paper we shall study

Business Impact Analysis from a slightly different perspective where we shall look at the on-demand transition as a factor that can affect business continuity to an extent.

The following hypothetical example has been formulated to explain the importance of a Business Impact Analysis in an on-demand scenario. It also illustrates the alignment between the Business Strategy and the IT Infrastructure domains of the Strategic Alignment Model that was addressed in section 4.0.

Consider the case of a typical hospital. The Mercy Trust Fund Hospital is an acute care hospital offering medical, surgical, obstetric and pediatric services to residents of five rural counties in central Pennsylvania. The hospital boasts of employing 790 co-workers, 144 physicians and 187 licensed beds.

On an average they have about 400 patients everyday. The Accounts Receivable and Bills Collection Department handles each patient's bills processing and forwards the bills to their respective insurance companies, based upon the information provided by the patients. Every night a batch process runs to transmit these files containing the invoices to the respective insurance companies. This process is handled by the Information Technology (IT) Department of the hospital.

In order to make sure that the daily process runs effectively, and to keep up with the pace of an increasing number of patients and an increase in the associated paperwork with respect to the insurance companies, the hospital purchased additional servers and

expanded their hardware/software requirements. What started happening was that their IT group started expanding very quickly, and the fast changing technological demands were taking a large share of their IT budget. Also, as they started expanding their infrastructure, it was becoming hard for them to become more adaptive to the changing requirements of the insurance companies, since some of the insurance companies were more up to speed with the changing technological trends. For instance some of the insurance companies were now demanding that the files be sent to them in a more secure format, and other quality standards be met with at all times. The situation demanded that The Mercy Trust Fund Hospital became more flexible and adaptive, or in other words became an on-demand organization. A business impact analysis was then carried out to study the financial and non-financial impacts. Based upon the results of the analysis they outlined the following course of action;

1. While they would be responsible for their database servers. The web servers and the EDI servers however, were to be outsourced to a third party subcontractor who ran a server grid (/server farm) so that resources could be added as and when there was an increase in demand.
2. The task of monitoring the batch process was to be sub-contracted to a company which specialized in this area. The subcontractor's team would however report to a smaller team in The Mercy Trust Fund Hospital's IT group, which would be the single point of contact with all the insurance companies.

After the Business Impact Analysis, a Risk Assessment was carried out in order to analyze this risks and take suitable actions to mitigate them.

A decision was taken to have a core Data Security group, and a Process Control group within the Hospital's IT Department. The Data Security group would be responsible for all security related issues, and if in the long term a need to change the subcontractor arose for any reason, the hospital would have complete ownership of the process and the core security team would be able to handle the transition without any security breaches.

In this way The Mercy Trust Fund Hospital took their first step towards becoming an on-demand organization. Their biggest advantage was of course that they had succeeded to a large extent in aligning their Business Strategy with their IT Infrastructure and Strategy. The diagram (figure 6.3) below depicts this relation.

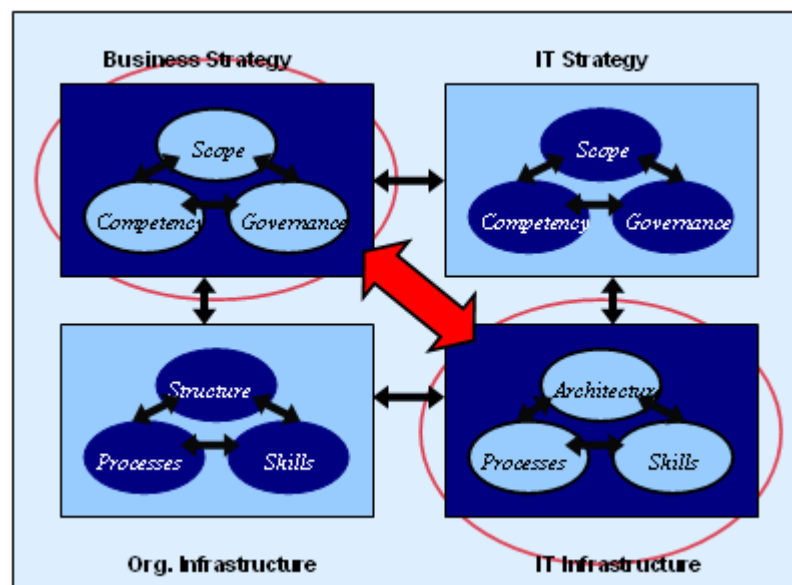


Figure 6.3 (Source: Strategic Alignment Model³)

The next section addresses Risk Assessment from an on-demand perspective and explains the findings with respect to the Strategic Alignment Model.

7.0 Risk Assessment

A *risk* is defined as the possibility of something unwanted or unbecoming happening. Whether it is from a business standpoint or a technology standpoint, how effectively an organization can manage its risks determines how efficiently it can run in any given environment. The underlying premise is that ‘computers can never be fully secured’. There is always a risk, whether it is from a trusted employee who defrauds the system or a fire that destroys critical resources⁸. From section 2.0 we are now clear on the concept of e-business on-demand and what it means for an organization to become an on-demand business. Let us now go deeper in our study to understand the risks that are associated with this process, and the importance of evaluating these risks and managing them in the right manner.

Accepting risks and selecting cost-effective controls to reduce the probability of the risk occurring are two basic functions of a formal process called *Risk Assessment*. Risk Assessment in fact, is an element of *Risk Management*. Where, *Risk Management* is the formal process of assessing risks, taking steps to reduce risks to an acceptable level, and then maintaining that level of risk⁸. The other element of risk management is *Risk Mitigation*. The diagram (*figure 7.1*) below illustrates on a high level how risk management works.

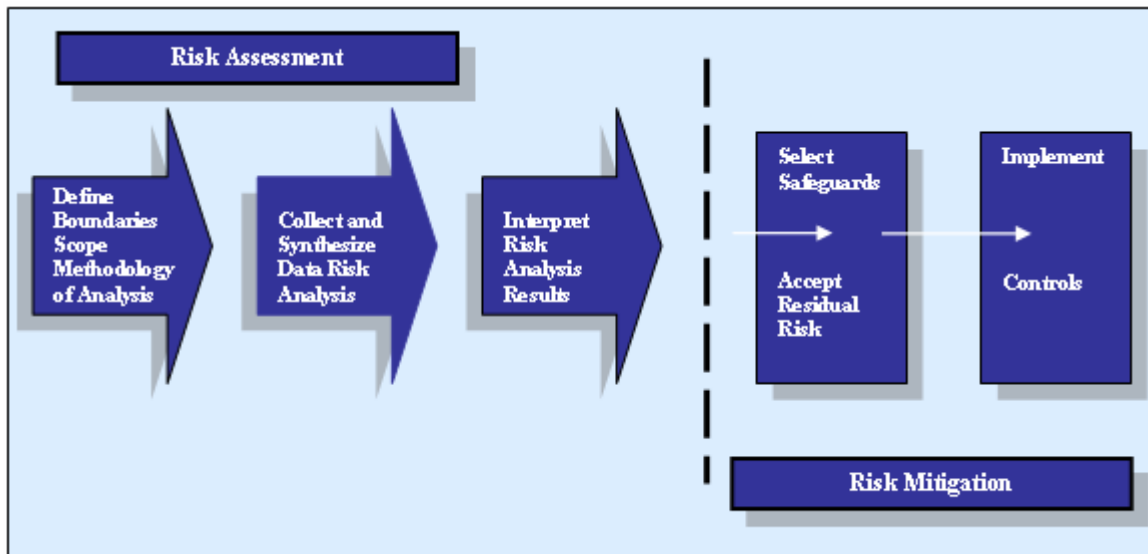


Figure 7.1 (Source: NIST Handbook ⁸)

For the sake of controlling the scope of this paper we shall focus (but not limit) our discussion to risk assessment and its elements. And then try and understand its significance in an on-demand scenario.

Risk Assessment is a systematic consideration of:

- (a) The business harm likely to result from a security failure, taking into account the potential consequences of the loss of Confidentiality, Integrity, or Availability of the information and other assets;
- (b) The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented ¹⁰

The assessment is essentially to help guide and determine the appropriate management action, setting the priorities for managing information risks, and for implementing the controls required to protect the organization against these risks ¹⁰. Risk Assessment

should ideally be carried out in a multi-layered fashion. This basically means that the assessment should start at a high level and then go deeper as the resources are prioritized, so that the prioritization of risks starts from specific risks to more general ones. In an on-demand situation this would mean that the assessment needs to be performed in a manner that addresses high priority risks associated with the organization's transition to on-demand first, and then addresses all other risks.

The following hypothetical example has been formulated to explain the importance of risk assessment in an on-demand scenario. It illustrates the risks identified in the process, with respect to the sub-domains of the Strategic Alignment Model that was addressed in section 4.0. This basically helps us to understand security better in terms of a direct relation to the alignment model.

XYZ Inc. is one of the leading Radiation Therapy Systems provider in the United States with annual revenue of \$ 0.78 billion, and targeted revenues of over \$1 billion for the current financial year. Their core-competency is building simulated applications for radiation therapy, and their business model is built around three main activities;

- (a) Medical Research
- (b) Application Development and Product Support
- (c) Marketing

The business around a core-competency of this nature is highly technology driven. The changing trends of technology therefore have a direct impact on the Architecture, Processes, and Skills of the organization. Additionally since all medical companies in the United States are under the scrutiny of Government organizations such as the FDA, a high standard of quality needs to be maintained in order to ensure that the procedures followed are safe and risk free. Since there is a direct impact on human lives, other standards such as ISO 9002 also need to be adhered to on a continual basis.

In order to become an on-demand business i.e. by becoming more adaptive and flexible to the changing technological trends, XYZ Inc. carried out a Business Process Analysis. The motivation behind this was to evaluate their existing processes and identify a process that can be outsourced to a third party subcontractor. The associated impact was then determined by a Business Impact Analysis. Outsourcing Application Development to an overseas subcontractor was identified as one of the options. A detailed risk assessment was then carried out. The risks (not all) arising from the on-demand transition have been categorized into the three sub-domains of the alignment model. They are listed as follows in the diagram (*figure 7.2*) below;

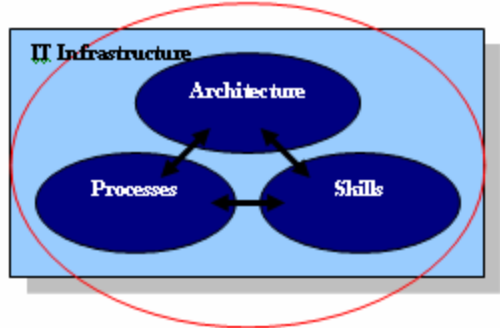
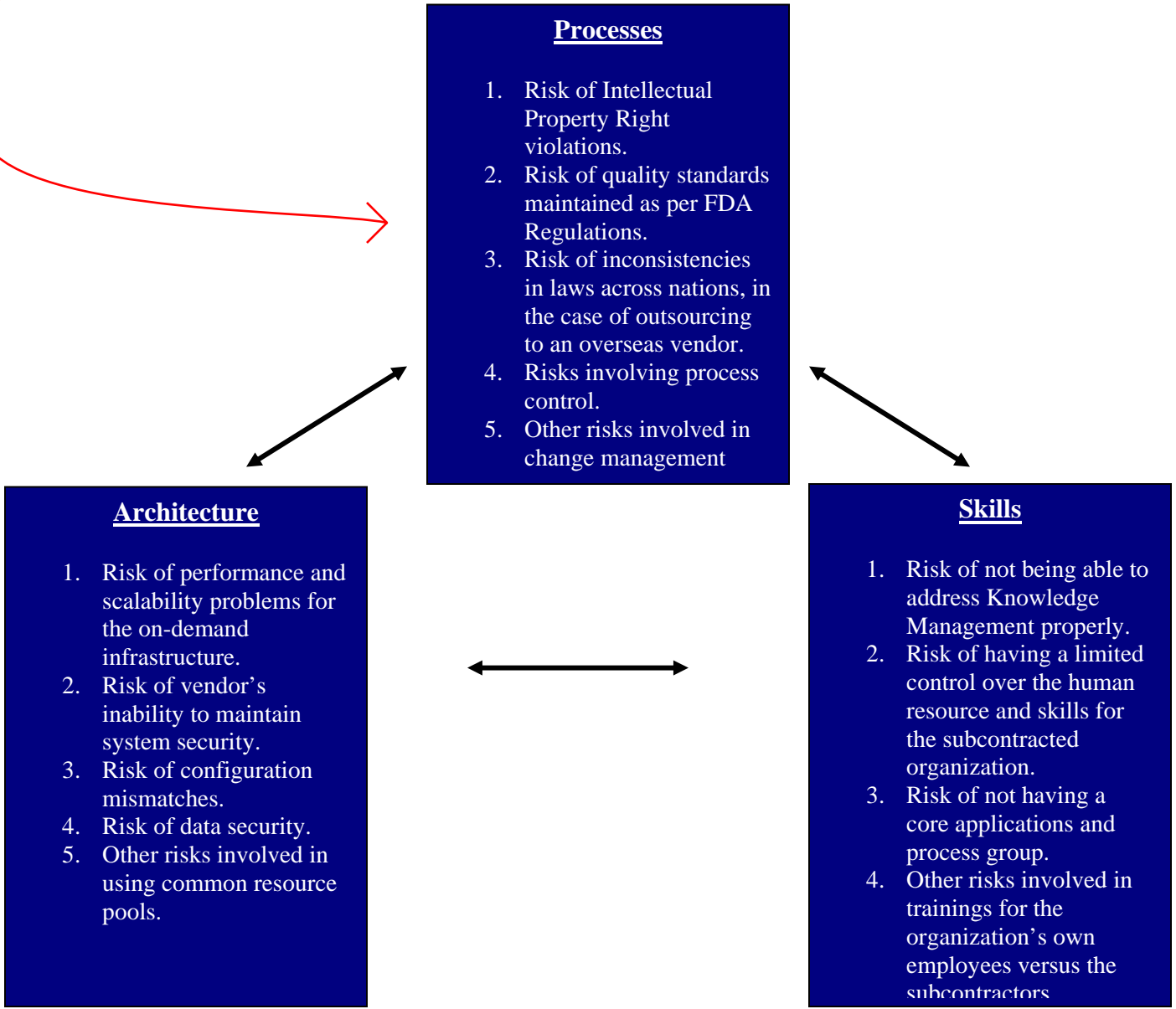
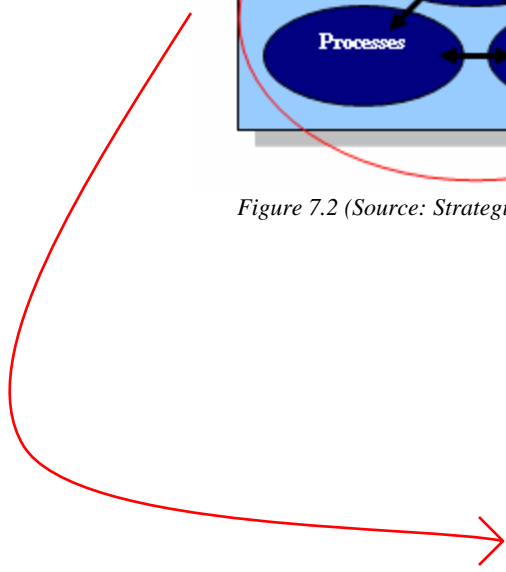


Figure 7.2 (Source: Strategic Alignment Model³)



Typically, the results of a risk assessment process are represented quantitatively and/or qualitatively. The qualitative measures are more descriptive, expressed in terms such as high, medium, or low, or rankings on a scale of 1 to 10. The quantitative measures however are expressed in terms of monetary losses⁸. Once the risk assessment process is completed and the results are evaluated, the risks are mitigated and then managed.

After following the entire process described above, XYZ Inc. made their final decision in favor of not subcontracting the application development process. The testing part of the application development i.e. creating automated test suites for the final application, that would help speed up the actual testing, was in turn outsourced.

The table below (*table 7.1*) briefly defines the elements of a Risk Assessment process. It is important to understand their actual meanings since they have an impact on the approach to the risk analysis exercise.

#	Elements of Risk Assessment	Definitions
1	Risk Valuation	The value of an asset(s) is determined. This consists of its intrinsic value and the near-term impacts and long-term consequences.
2	Consequence Assessment	Determines the degree of harm or loss that can occur. It is not limited to the immediate impacts. The more severe the consequence of a threat, the greater the risk to the system, and therefore the organization.

3	Threat Identification	Identifies the threats and determines the likelihood of their occurrence.
4	Safeguard Analysis	Determines the effectiveness of the existing security measures.
5	Vulnerability Analysis	Vulnerabilities may allow a threat to harm the system and hence they contribute directly to the risk. The vulnerability analysis helps identify these vulnerabilities.
6	Likelihood Assessment	Considers the presence, tenacity, and strengths of threats as well as well as the effectiveness of safeguards (or presence of vulnerabilities).

Table 7.1 (Source: NIST Handbook⁸)

The next section elaborates on the different vulnerabilities and security concerns that may contribute to risks in an on-demand scenario. Based upon their nature of influence, they are categorized into the Architecture, Processes, and Skills sub-domains of the strategic alignment model.

8.0 Security Concerns in the on-demand environment

Security is a major concern when an organization undergoes any kind of transformation. Be it through Business Process Re-engineering, a Merger and Acquisition situation, any type of change that would cause a rapid growth or downsizing, or a hybrid of all these situations. Transitioning to an on-demand environment is quite similar to any of these situations, and in many ways is a hybrid situation. In other words, when an organization takes up the on-demand initiative, it may re-engineer its existing business processes, outsource some of the processes, acquire/dispose assets, or increase/decrease team sizes, in order to meet the requirements necessary to become an on-demand business.

For the on-demand transition, most of the critical security measures that are already in place to protect the information assets must be expanded to include the potential processes, infrastructure and people that will come into the picture when the on-demand environment becomes operational. This depends a lot on the strategy adopted since an organization's security posture should really include people, process and information technology in any given scenario. The on-demand environment should merely be an extension of what already exists.

The Strategic Alignment Model described in section 4.0 emphasized on the need for aligning an organization's business strategy with its IT strategy and infrastructure. The reason for this being that, rapid changes in the business environment also result in changes in the IT infrastructure. Thus any decisions made by the management team that

will affect the operational aspect of the business in terms of its goals and a change in the business strategy, will have a direct impact on the IT and human resources side of the business as well, and vice-versa. In such a scenario, security becomes a major concern in the areas of architecture, processes and skills.

In the following sub-sections, we shall discuss the various security issues that can occur in the three given areas – Architecture, Skills, and Processes. At the end of this section, in section 8.4, a table summarizing these issues has been provided for the reader's convenience.

8.1 Architecture

In an on-demand environment, availability of information needs to be addressed first and foremost. It is evident that certain Mission Critical Activities will tend to get disrupted if they depend upon the availability of the expected on-demand infrastructure i.e. hardware, software, physical information processing facilities, telecommunication links, transportation, heating and ventilation systems, etc. Some of the important issues that are likely to arise in the area of *Architecture*, and the suitable solutions that address these issues are described as follows;

- 1) **Scalability:** Performance and Scalability are important security concerns in an on-demand scenario. This does not necessarily mean that the scalability and performance analyses did not exist prior to the organization moving to an on-demand environment. It just means that the analyses will now have to be extended to be carried out with the on-demand scenario in mind.

For instance, the organization's current firewall may not be able to scale up to an on-demand situation, where the traffic may suddenly spurt, or additional interfaces may be required to connect with vendor/clients networks. Additionally load tests will have to be conducted on the servers and existing infrastructure to analyze the current performance, and estimate the performance that would be required once the organization becomes operational in the on-demand environment. The organization must therefore carry out performance audits for

simulated on-demand situations to ensure that the infrastructure can indeed support the requirements for future.

- 2) **System Security:** In order to ensure that the systems are fully secure. The selected vendor/subcontractor who will provide infrastructural support must make sure that the systems are pre-hardened and ready for the on-demand environment. The selected vendor must also follow the organization's or their own security standards for configuring, deploying and maintaining the IT infrastructure
- 3) **Single Points of Failure:** Single points of failure in the on-demand infrastructure must be clearly identified. If the new on-demand infrastructure is expected to be in place for only a short period of time, then the result of the Risk Assessment analysis may vary due to a reduction in Probability of Threats. As a result, certain controls and redundancy may not be considered necessary anymore.
- 4) **Configuration Conflicts:** The organization must ensure that hardware and software configurations proposed to be used by the vendor are consistent with those that are currently being used by the organization in all its facilities.

For instance, the organization may be using a third-party application that is currently supported on Windows 2000 Service Pack 3.0 only, whereas the systems at the vendor's locations may be hardened up till the latest Service Pack,

say Service Pack 4.0. This will result in a version conflict, and the application will therefore fail to perform as desired, or its entire functionality could be affected.

- 5) **Networks:** If new network links need to be established between the organization and the vendor, or between the vendor and the organization's clients, then security concerns for this links must be addressed in order to ensure there is no disruption of the link, and no possible man-in-the-middle attacks.

- 6) **Usage of Common Resource Pools:** The on-demand environment may require the use of servers by the organization, that are located at a server farms or a server grid. This means that the organization might be sharing its allocated resources at the grid with other companies. While sharing a common pool of resources, care must be taken to ensure that the vendor to whom this function has been outsourced, takes added measures to ensure that the organization's data is kept secure at all times and under all circumstances

- 7) **Access control:** Access to information – 'who and why' is a critical element of security. 'Grant only as much control as is required' should be a rule of thumb that should be followed while providing access rights to all those associated with the business after it is operational in the on-demand environment.

8.2 Skills

The on-demand situation is bound to raise a number of issues as far as deployment of people, determination of roles and responsibilities, knowledge management, conflict resolution, user training, etc. are concerned. The Personnel Hiring Policy must therefore be implemented for potential people resources as well, even if these people have not been deployed as yet, but are expected to be deployed once the on-demand environment is operational. Some of these issues from a security stand-point in the area of *Skills*, and the possible solutions are described below;

- 1) **Roles and Responsibilities:** Responsibilities from the security perspective must be communicated to one and all, and clear ownership and roles must be assigned for the new Information Assets.

For instance, if the people who are brought in during the on-demand transition are of senior management levels, then their commitment to IT security must be assured. This can be done by educating and training them on the organization's security objectives, and ensuring that they understand their responsibilities where security is concerned.

- 2) **Training:** Training of the prospective personnel in terms of IT security and the policies of the organization is critical for ensuring an acceptable level of security in the on-demand environment. This must be guaranteed by the vendor/third party

subcontractor in case personnel are being provided by him. The training must also include the systems and applications that are being used in the current infrastructure, as well as those that will be dependent on the new infrastructure.

- 3) **Knowledge Management:** Knowledge management is an important issue in general. The organization must make sure that there are regular knowledge transfers between the subcontractors and the organization's own employees, so that there are never any gaps in the process that the organization is not aware of, thereby ensuring that security breaches do not occur.

- 4) **Conflict resolution:** This is perhaps another key issue which is likely to impact security if not handled properly. The organization's existing Human Resource Policy must address this issue in the extended on-demand scenario as well so that there are no disgruntled employees or subcontractors who can create a backdoor and cause security breaches.

8.3 Processes

If the security concerns of the vendors/subcontractors are not the same as those of the organization's, then an effort should be made to formulate security objectives which are aligned between the two companies. This helps fill up any gaps in the final security process followed in the on-demand environment. Some of the important issues that are likely to arise in the *Processes* area and the suitable solutions that address them are described as follows;

- 1) **Business Impact Analysis:** Any organization that is serious about its IT Security must carry out a *Business Impact Analysis*, followed by a *Risk Assessment* exercise in order to address all possible threats and vulnerabilities. The Business Impact Analysis determines the Mission Critical Activities, their dependencies, and the required resources. This has been addressed in detail previously in section 6.0.

- 2) **Risk Assessment:** After the *Business Impact Analysis* has been completed, the organization must carry out a *Risk Assessment* analysis for those resources that are required to keep the mission critical activities operational at all times.

The Risk Assessment exercise basically aims to determine the following;

- a. Threats that may interrupt or disrupt a Mission Critical Activity.

- b. Vulnerabilities in the organization that could result in materialization of the threat.
- c. Probability of occurrence of threats.
- d. The level of Risk from each threat is then calculated using the following formula:
*(Threat Impact * Vulnerability Level * Probability of Threat)*
- e. Formulate a Risk Mitigation Plan, which may adopt one of the following approaches:
 - (1) Transfer the Risk, e.g. insurance.
 - (2) Accept the Risk, if it is within the acceptable risk levels.
 - (3) Reduce the Risk, put controls in place.
 - (4) Avoid the Risk, eliminate the Threat or Vulnerability.

In the case of the on-demand environment, the organization will have to carry out the Business Impact Analysis and Risk Assessment exercises keeping in mind the potential impact of the on-demand environment, where there may be new Mission Critical Activities, or there might be a change in the risk environment with the addition of new information assets, threats, vulnerabilities, or simply increase/decrease of probabilities. This has been explained in greater detail earlier in the sections 6.0 and 7.0 respectively.

3) **Security Policies and Standards:** Security Policies and Standards should be drafted before the new e-business on-demand infrastructure is brought in. This

must take into account the new infrastructure as well as the new processes and personnel.

- 4) **Business Continuity Planning:** The overall framework adopted by the organization for business continuity planning must incorporate the on-demand environment as well. The part of the final plan that deals with the on-demand infrastructure and processes must be logically consistent with the overall framework. It may also be the case, that the vendor already has a Business Continuity Management process in place. In such a situation, these two plans need to be aligned with each other.

Finally, testing the Business Continuity and Disaster Recovery Plans is as important as formulating it. This testing procedure must take into account potential scenarios in the on-demand environment, even if they don't exist in the current situation. This will of course require co-operation from the subcontractor and it may be necessary to include a clause in the Service Level Agreement with the vendor to allow testing of the business continuity plan at the vendor's location, using their infrastructure and resources.

- 5) **Vendor Audits:** The organization must have a clearly defined Service Level Agreement with the vendor/subcontractor. Periodic audits of their systems, processes and facilities must be carried out by the organization in order to ensure

that they are in a position to fulfill their contractual obligations in the on-demand environment.

- 6) **Legal and Compliance Issues:** The on-demand strategy of the organization must also take into account legal and regulatory requirements. These may in fact even affect the ability of the business to continue providing its deliverables.

For instance, the sudden increase in IT infrastructure will necessitate the purchase of additional software licenses. It is highly probable that the organization suddenly adds new hardware without taking care to ensure that the necessary software licenses have been purchased. The organization should consider purchasing Enterprise-wide licenses wherever applicable.

Additionally, the vendor Service Level Agreement should include a clause to ensure that the vendor takes full responsibility for not violating the organization's Intellectual Property Rights.

- 7) **Process Ownership and Control:** Process ownership and control is an important aspect of the on-demand transition. It is critical for the organization to have complete ownership of their processes and allocate personnel from within the organization who will be responsible for managing the processes and ensuring that no security violations take place.

- 8) **Change Management:** Although Change Management to a large extent is a Human Resource activity, it is a process crucial for the success of the on-demand transition and should be addressed appropriately.

8.4 Summary Table

The table (*table 8.1*) below summarizes all the security issues that were discussed in the previous sub-sections.

A word of caution to the reader; the table does not contain an exhaustive list. It simply addresses the main security issues that can arise when an organization transitions into an on-demand environment.

Security Concerns		
Architecture	Skills	Processes
Scalability	Roles and Responsibilities	Business Impact Analysis
System Security	Training	Risk Assessment
Single Points of Failure	Knowledge Management	Security Policies and Standards
Configuration Conflicts	Conflict resolution	Business Continuity Planning
Networks		Vendor Audits
Server Grids		Legal and Compliance Issues
Access control		Process Ownership and Control
		Change Management

Table 8.1

In the next section we shall address security for a situation where the on-demand environment ceases to exist.

9.0 Security Concerns - Post On-Demand

When the on-demand environment ceases to exist, it does not obviously mean that the organization that was functioning in this environment will also cease to exist. In other words, transitioning out of an on-demand environment should also be given as much importance as transitioning into the on-demand environment.

This basically means that security concerns must also be addressed in equal importance for the situation when the on-demand environment ceases to exist. Some of the fundamental security concerns that should be addressed in such a situation are described briefly under the *Architecture*, *Skills* and *Processes* categories as follows;

- (1) *Architecture*: The IT infrastructure, hardware, software and other resources will have to be returned to the vendor/subcontractor to whom they were outsourced. Therefore, adequate care must be taken to clean hard drives and configurations of systems.
- (2) *Skills*: The people who were brought in when the organization was in the on-demand environment may end up having a considerable amount of information about the organization's systems and processes. Adequate controls will have to be implemented to ensure this knowledge is not misused. These controls could be adopting a strict need-to-know basis for information dissemination and having each of the temporary resources sign strict Non-Disclosure and Non-Compete

agreements with the organization. In addition, Employee Separation Procedures may be modified to take into account temporary separations that may result from the change. Knowledge Management and Knowledge Transfers will have to be scheduled during the transitioning out time in order to bring the organization's employees up to speed with the tasks that the subcontractors were responsible for.

(3) *Process Ownership*: The ownership of the process and a core security group must always be the organization's own employees, and not subcontractors, so that there are no security breaches in the transitioning out process. This also ensures that there are no patent right violations, both in terms of process patents and product patents.

There are several other security issues that are bound to come up during the transitioning out phase for an organization moving out of the on-demand environment. Although these may vary for organizations belonging to different industries, they are nevertheless important for their existence in the long run.

10.0 Conclusion

With the rapidly changing business environment influenced by the growth of the Internet, globalization, nearly complete dependence on IT, and the growing trend of outsourcing, organizations today are being forced to put systems and processes in place which will ensure the continuity of their business in the future. One of the strategies being proposed and considered by major corporations is to become an on-demand business. The idea here being that an organization uses only that IT infrastructure, which it requires, and only when it requires.

Moving to an on-demand environment requires a major business process re-engineering effort. This when combined with the phenomenal rise in security attacks makes for a volatile combination. Serious security concerns arise when the organization transitions into, and out of the on-demand environment.

The security concerns are wide-ranging and broadly cover the areas of IT architecture, business processes, and personnel skills. It is therefore paramount in importance that we do not ignore the required security controls in our rush to move into the on-demand environment.

Similarly, transitioning out of the on-demand environment also raises serious control issues that must be addressed in the policies and procedures manual, documented prior to the organization becoming operational in the on-demand environment. Some of the

primary concerns in this area are; issues related to the use of server grid technology where information is stored on servers that are a part of a shared pool of resources, the vendor's ability to provide and sustain the infrastructure for the on-demand situation, the increased dependency on subcontracted personnel, and the awareness levels of users who will play key roles in this transition. In order to clearly identify and address these issues, the organization must anticipate these changes and carry out Business Impact Analysis and Risk Assessment exercises. As a result, the appropriate controls can be envisioned and put into place when the time comes.

Finally, we believe that the on-demand model is here to stay, and so is the reality of security attacks. Therefore, if companies adopt a pro-active on-demand strategy, which addresses the security issues, the entire process can result in a tremendous business gain, with highly reduced security risks.

11.0 Future Research

In this paper security has been addressed on a broad level with respect to the on-demand environment, while elaborating on its direct co-relation with the Strategic Alignment Model. There are however, several other topics within security itself, that can be researched further at a higher level of detail. *Privacy*, and *The impact of globalization with respect to offshoring*, are two interesting topics proposed for future research.

(1) *Privacy*

While basic privacy principles world over have been in existence for a long time, with rapid technological advancements privacy is impacted in more ways than one. For instance, maintaining adequate security for personnel information within an organization is an ongoing challenge for all companies throughout the world. Protecting data and thus ensuring information privacy is critical for organizations to fulfill applicable statutory and regulatory requirements, and hence minimize the potential liability due to negligence

15

When an organization transitions to an on-demand environment these issues are bound to grow exponentially. '*Addressing Privacy in an On-demand Environment*' is therefore, an interesting topic for future research.

(2) Offshoring.

'State Governments will be eligible to receive federal funds only after they certify that the money will not go offshore' - The U.S Workers Protection Act, 2004 ¹⁶.

Globalization has indeed made the world a smaller place by opening up markets in different parts of the world. While many feel that this is a healthy trend as it will prevent market stagnation, there are others who feel threatened by a vast percentage of jobs getting outsourced to other countries. So much so, that it has emerged as a major political issue in the U.S in the year 2004 ¹⁶.

'Addressing the impact of globalization with respect to offshoring' is another interesting topic for future research.

Bibliography

1. Rappa, M. (2004) 'The utility business model and the future of computing services', *IBM Systems Journal*, Vol. 43, No. 1, pp. 32-43.
2. Albaugh, V., and Madduri, H. (2004) 'The utility metering service of the Universal Management Infrastructure', *IBM Systems Journal*, Vol. 43, No. 1, pp. 179-185.
3. Kurtz, C., and Snowden, D. (2003) 'The new dynamics of strategy: Sense-making in a complex and complicated world', *IBM Systems Journal*, Vol. 42, No. 3, pp. 462-470.
4. Grey, W., Katircioglu, K., Bagchi, S., Shi, D., Gallego, G., Seybold, B., and Stefanis, S. (2003) 'An analytic approach for quantifying the value of e-business initiatives', *IBM Systems Journal*, Vol. 42, No. 3, pp. 484-497.
5. Chess, D., Palmer, C., and White, S. (2003) 'Security in an autonomic computing environment', *IBM Systems Journal*, Vol. 42, No. 1, pp. 107-118.
6. Fenn, D. (2002) 'Supplier Continuity: Managing risks across the supply chain', *Continuity*, Vol.6, No.1, pp.4-6.
7. Elliot, D. (2000) 'Three steps to better continuity', *International Journal of Business Continuity Management*, Vol.1, Issue 2, pp.8-10.
8. Chase, R. (1999) 'Brands and intellectual property', *Continuity*, Vol.3, Issue.4, pp.12-14.
9. Chadwick, T. (2001) 'Setting the scene: e-Business Continuity Management Issues', *Continuity*, Vol.5, No.4, pp.7-9.

10. Kirvan, P.F (2000) 'Business Continuity Strategies for call centers', *Continuity*, Vol. 4, No.2, pp.9-10.
11. Meredith, B. (1998) 'Business Impact Analysis', *Continuity*, Vol.2, Issue.1, pp.4-77.
12. AIRMIC (1999) 'A guide to integrated risk management', London.
13. Business Continuity Institute, (2001) 'Getting Started' Business Continuity Institute, Worcester.
14. Crockford, N. (1986) 'An introduction to Risk Management', Woodhead-Faulkner, Cambridge. ISBN 0-85941-322-2.
15. Financial Services Authority. (2002) 'A Business Continuity Management risk matrix', Financial Services Authority, London, pp.1-20.
16. Rassam, C. (1999) 'A matter of control', *Survive*, February Issue, pp.58-59.
17. Matt, B. (2003) 'Computer Security: Art and Science', *Aw Professional*. ISBN 0-20144-099-7.
18. Charles, P., and Shari, P. (2002) 'Security in Computing', Prentice Hall Professional Technical Reference. ISBN 0-13035-548-8.
19. Caelli, W., Dennis, L., and Michael, S. (1991) 'Information Security Handbook', Stockton Press, New York. ISBN 1-56159-018-5
20. Deborah, R., and Gangemi, G. (1991) 'Computer Security Basics', O'Reilly & Associates, Inc.
21. BCS. 'Guidelines on Good Security Practice – An introduction to Business Continuity Management'.

22. Ruthberg, Z., and Tipton, H., eds.(1993)'Handbook of Information Security Management', Auerbach Press.
23. Jaworski, L. (1993) 'Tandem Threat Scenarios: A Risk Assessment Approach', Proceedings of the 16th National Computer Security Conference, Baltimore, MD. Vol. 1, pp.155-164.

Reference:

- ¹ IBM's On Demand Transformation: Reinventing the Enterprise / Linda Sanford / IBM Technology Forum, 2003.
- ² The Catch in On Demand Computing / Mike Karp / Network World Storage in the Enterprise Newsletter, 2003.
- ³ Strategic Alignment: Leveraging Information Technology for Transforming Organizations/ J.C Henderson, and N. Venkatraman / Harvard Business Review, 1999.
- ⁴ Meet the experts on e-business on demand/ Dr. Irving Wladawsky-Berger / IBM Web-cast, 2003.
- ⁵ e-Business on demand – A developer's roadmap / Alfredo Gutierrez / IBM, 2003.
- ⁶ Essential System Administration / Aeleen Frisch/ O'Reilley & Associates, Inc., 1995.
- ⁷ All in one CISSP Certification Exam Guide/ Shon Harris/ McGraw Hill, 2003.
- ⁸ Introduction to Computer Security – the NIST Handbook / National Institute of Standards and Technology/ U.S Department of Commerce, 2003.
- ⁹ What does "e-business on demand" mean to developers? / Michael O'Connell/ IBM, 2003.
- ¹⁰ Information technology — Code of practice for information security management / STANDARD ISO/IEC 17799/ 2000.
- ¹¹ Business Continuity Management – Good Practice Guide / The Business Continuity Institute, 2002.
- ¹² Business Continuity Management Audit Methodology / Network Intelligence India Pvt. Ltd, 2003.
- ¹³ A Guide to Business Continuity Planning / James C. Barnes/ John Wiley & Sons Ltd., 2001.
- ¹⁴ Search Storage definitions / www.searchstorage.com, 2004.
- ¹⁵ Privacy On Demand: What Corporate America Needs to Know about Privacy Laws / Priscilla A. Walter, Cathy Austin, and Lisa M. Thomas/ Northwestern University School of Law, 2002.
- ¹⁶ Federal bill targets offshore labor/ Dinesh C. Sharma/ CNet News.Com, 2004.

Appendix – A

TYPE OF IMPACT AND ITS EFFECTS	IMPACT DESCRIPTORS AND EVENT CATEGORIZATION			
	Catastrophic	High	Medium	Low
FINANCIAL				
Loss of Revenue				
Loss of Shareholder Value				
Penalties				
Bad Debts				
Additional Operating Costs				
NON-FINANCIAL				
Reputation Loss				
Loss of Operational Capacity				
Customer Service				
Regulatory/Legal				
Loss of Market Share				
Loss of Quality				
Brand Tarnish				
Environmental				
Contractual				
Staff Morale				
Political				

Source: BCM Audit Methodology¹²