ANSWERS TO MISP2 – ASSIGNMENT NO. 5

MISP2-A5Q1 – Business Process Outsourcing and Business Process Reengineering

Some of the IS/IT strategies considered by most businesses include outsourcing, offshoring and backsourcing. It is not generally true that all business process outsourcing results in IS/IT outsourcing.

A5Q1.1 - Under what circumstances would an organization consider IS/IT outsourcing?

ANSWER

An organization would normally consider outsourcing if the identified activities are not its core business or core competencies (i.e. not the activities that it excels over others).

Consider an organization involved in Oil & Gas Explorations, Production, Supply and Marketing like Petronas. There is no point for Petronas to run a complex IS/IT system and network for its information needs, so Petronas has outsourced its IS/IT department completely.

Similarly, in Shell Malaysia there is no point in maintaining a “Mailing and Posting” department in Shell Oil Malaysia. So they outsource it to POS Malaysia, a company that specializes in postal mail etc.

A5Q1.2 - List three (3) advantages and three (3) disadvantages of IS/IT outsourcing.

ANSWER

Advantages of IS/IT outsourcing
1. Outsourced company performed outsourced activities more efficiently
2. Cheaper to the organization to outsource in the long run
3. Outsourced company has experience and expertise in the non-core activities
4. Organization can concentrate on core activities and compete better
5. Outsourced company has wider network and resources
6. Organization can free up internal staff so that they can do higher-value work

Disadvantages of IS/IT outsourcing
1. Organization creates threat to local labor and social issues due to staff lay-offs
2. Remaining employees in organization lose trust in the organization
3. Outsourced employees do not show loyalty to organization because they are paid by the outsourced company and not directly by the organization any more
4. Outsource company service quality and performance levels may degrade and may not be fully maintained in the long run
5. Organization’s sensitive and confidential information – the security access may be compromised due to handling by an external outsourced company
6. Outsourced company wants to look good – so may commit fraud by deliberately providing false or erroneous reports
7. Organization cannot react swiftly to changing market conditions now that those activities are handled by outside outsourced company
8. Organization has limited control on the day-to-day running and operations of the outsourced company due to being bound to contractual obligations


ANSWER

Business Process Re-engineering (BPR) is a redesign of business processes taken by organizations to improve its business performance. Redesign means to look at current processes, scrutinize, evaluate critically and act with results and expectations, like dropping current processes, creating new processes or improving existing processes.

The relationship between BPR and business strategy is direct. Business strategy is about where the company wants to go and what it wants to be in the future. BPR is "redesigning everything" about the business to meet the goals of where it wants to go and wants to be in the future. So BPR is a business strategy.

BPR is a major, radical and revolutionary change. In almost all cases, it is business strategy that drives BPR, i.e. the business determines the need or option to implement or not to implement BPR. The experiences of companies that have undertaken BPR have shown that it is an expensive affair, have turned companies radically into new entities, caused extensive changes to the working environment, changed work processes, its staff, its organization, the company culture and many more. BPR is a major transformation and not a series of small increments in a company’s improvement process.

MISP2-A5Q2 – Considerations for determining the Business IS/IT Strategies.

If you asked a greedy person what he/she wants, you may get an answer like “I would like to have everything like the moon and the sky, etc”. But in reality life has limitations. This simple fact applies equally to organizations and businesses.

A5Q2.1 – Explain the general considerations that led to the formation of business objectives and strategies in terms of what the organization: might do, wants to do, must do and can do.

ANSWER

Might do – based on the environment within which it operates or by moving into new environments. This consideration can be thought of as results from many analyses like SWOT, PACE, PEST, IFE, EFE, CSF, BSC, VCA, merger, acquisition or takeover, etc. This is about choices the organization can take to implement it strategic actions.

Wants to do – based on the values and views of, chiefly the senior executives and stakeholders. This consideration is about the setting up of the
organization’s Vision, Mission and Objectives. An ordinary and low level employee does not determine what the organization should do. The employee just does what is being instructed to do.

**Must do** – things that must be executed if the organization is to survive in the environment, depending on the pressure groups and their influences. This consideration is definitely about the Critical Success Factors (CSF) of the organization.

**Can do** – based on its resources and capabilities. This consideration is about internal strengths and weaknesses of the organization. So the concepts of SWOT, IFE and VCA are directly applicable.

**A5Q2.2** – If you study closely Figure 6.1 on the inputs and tool kit for determining the business strategy, you will find the famous PEST Analysis method. What is the PEST method?

**ANSWER**

PEST analysis stands for “**Political**, **Economic**, **Social**, and **Technological**” analysis and it describes a framework of macro-environmental factors used in environmental scanning. It is also referred to as the STEP, STEEP or PESTLE analysis (Political, Economic, Socio-cultural, Technological, Legal, and Environmental). Recently it was even further extended to STEEPLED, including ethics and demographics.

PEST analysis gives a certain overview of the different macro-environmental factors that a company has to take into consideration when developing its business strategy.

**Political factors** include areas such as tax policy, employment laws, environmental regulations, trade restrictions and tariffs and political stability.

**Economic factors** include areas such as economic growth, interest rates, exchange rates and inflation rate.

**Social factors** often look at the cultural aspects and include health consciousness, population growth rate, age distribution, career attitudes and emphasis on safety.

**Technological factors** include ecological and environmental aspects and can determine the barriers to entry, minimum efficient production level and influence outsourcing decisions. It looks at elements such as R&D activity, automation, technology incentives and the rate of technological change.

**MISP2-A5Q3** – Management Information System Security Issues, etc.

In GB3-MIT on page 9, it was said that “**Competitive advantage doesn’t come from the IT investment alone: It comes from the way that the business applies IT to meet strategic goals**”. This statement is one of the core principles that we shall learn in this MISP course.
A5Q3 1 – What is an Intrusion Detection System (IDS)?

ANSWER

An Intrusion Detection System (IDS) is a system implemented to detect unwanted manipulations for entries or intrusions into networks and systems that normally go through as unknown and bad data traffic.

A5Q3.2 – Explain the differences between viruses, worms and Trojan horses.

ANSWER

A virus is a small unit of usually malicious (bad) code that invades a computer program or file, to cause disasters.

A worm is defined as a type of virus that has the ability to copy itself from machine to machine, normally over a network, also to cause disasters.

A Trojan horse is a disguised security-breaking program that is introduced into a computer and serves as a way for an intruder to re-enter the computer in the future, also to cause disasters.

A5Q3.3 – Discuss three (3) reasons why cyber attacks and digital terrorism occur.

ANSWER

Some of the reasons why cyber attacks and digital terrorism occur are:

1. Personal Anger – A person may be very angry psychologically towards a company for being laid-off, as an example. This person decides to plant “viruses” into the company’s network and computers.

2. Hired Service – Some hackers may be hired professionally to break into some company’s network and computers to steal information and later on destroy the systems.

3. Ransom Money – A person may attack a company’s network or computers for blackmail or ransom money like putting viruses or planting logic bombs, etc.

4. Political Motive – Some political organizations are not happy with decisions made by their governments or grouping of governments and decided to attack the computer systems of hospitals, airlines, or government services, etc, unless their views are heard and implemented.

5. Declared War – When countries get into declared or official war against each other, they would first attack the telecommunication systems of each other to cripple and shutdown each other’s war infrastructure.
You are provided with a short article titled “GlobalValue Monitors Its IT Service Contract Compliance with SAS® IT Management Solutions”.

Study the article and answer the following questions:

A5Q4.1 – What is a SLA (Service Level Agreement)? Go to the internet and find SLA.

**ANSWER**

1. **What is** - Service Level Agreement (SLA) is that part of a service contract in which a certain level of service is agreed.

2. **What is not** - An SLA is therefore NOT a type of service contract, but a part of a service contract.

3. A service contract can contain zero, one or more SLAs.

4. A contract containing SLAs is usually referred to as a performance contract.

5. SLAs are becoming more and more popular. They are used extensively for provision of IT services, but also in other fields the popularity of SLAs is growing.

A5Q4.2 - Give three (3) statements that can be considered as SLA in the IS/IT context.

**ANSWER**

Some of the example statements that can be considered as SLAs are provided below.

1. There shall be less than 3 percent per month of telephone calls abandoned while waiting to be answered.

2. The service desk shall answer a call (pick up to answer) within an average time 2 seconds. The telephone pick up must be before the fourth ring.

3. The percentage of First Call Resolution (FCR) for a calendar month shall be no less than 75 percent. The FCR is defined as the resolution of incoming calls without the use of a callback, or without having the caller call back the helpdesk to finish resolving the case.

A5Q4.3 – Translate into simple words what the extracted paragraph below means. It has to do with automated measurements and recording software, i.e. ”... to seek out and acquire SAS IT Management Solutions.”

"In practice, all data containing SLA details are collated in appropriate databases before being interfaced with services and..."
KPIs. Based on the value of service measured and on the specified calculation rules, a score and penalty/incentive for the period are then calculated for each KPI. Based on the results obtained from the associated SLA metadata, the final score and penalty for the period are then calculated for each customer and contract.”

**ANSWER**

The software SAS IT Management Solutions has modules that automatically measure and record the performance of “customer information systems” against some agreed service levels (SLAs). The italicized extracted paragraph above essentially describes how the SAS solution executes it.

The simple explanations are described below. Let us take the example for the case of the SLA that “There shall be less than 3 percent per month of telephone calls abandoned while waiting to be answered”.

1. The specific data (information) from the SLA is first extracted and put into a database. For this example, we grab the numbers **3 percent** and **per month**, then put both into the database of the SAS software solution. The target is “less that 3 percent per month” while the performance measure or KPI is the “percentage of abandoned calls per month”.

2. Then we must set up the correct infrastructure for the telephone system interface such that: the system automatically detects the first incoming call, captures the date-time, counts the number of rings, records the telephone answering pick-up, records the telephone hang-up, captures all events, i.e. the duration and their time-stamps, etc, and insert all those information into the database in real time.

3. From item (1) above, the SAS software system will write the KPI (i.e. performance measure of percentage of calls abandoned per month) and will **configure the calculation** of this measure using the relevant data recorded in the database as explained in item (2).

4. In item (3) above, the calculations not only include the performance monitoring of percentage of abandoned calls per month, but also include monitoring the failures and successes against the SLA target. The failures incur **penalty points** while the successes incur **incentive points**. All these points are again calculated by the SAS software and placed in the database appropriately.

5. Once everything is ready (i.e. item 1 to 4 above), the telephone help desk system will now be fully interfaced with the SAS software solution and ready to run (rock and roll. Ha ha ha). The help desk operation can now run as normal. The configured SAS software is running automatically in the background capturing all the information and providing all the real time values of the configured performance measures (e.g. KPIs, individual call durations, number of rings before pickup, etc).

The paragraph above also said that the SAS software solution can handle many KPIs, many customers and many contracts, simultaneously. Note that our example above
for the “percentage of abandoned calls per month” is just one KPI. In our example we are also talking about one customer and one contract.

From the above, I have therefore translated to you the italicized paragraph in simple words. Thank you kindly. Ha ha ha.

MISP2-A5Q5 – Please refer to PDF file MISP2-MiniCase-Assn5-Q5.pdf.

Information System Security and Control – The Risks and Issues

You are provided with a short article titled “The Risky Business of Data Deletion”. The article was written by J. Nicholas Hoover, in Information Week, Oct. 2, 2006. Study the article and answer the following questions:

A5Q5.1 – What is the article all about i.e. what are the concerns of those companies?

ANSWER

The article is about many data related things for companies. The main issues cover:

- The legal and regulatory requirements for data retention
- The legal and regulatory requirements for data deletion
- The critical data security and data storage challenges

It is simply about which electronic records you must save, for how long to save, when to delete and how you should delete them permanently.

A5Q5.2 – List three (3) cases where deleting data get companies into trouble. List also three (3) cases that not deleting data also land companies into trouble. What should you do to get out of these data deletion/keeping trouble?

ANSWER

Cases where DELETING DATA got companies into trouble

1. Accidental destruction of data - Philip Morris (i.e. the cigarette manufacturing company) was slapped with a $2.7 million fine two years ago after it accidentally destroyed e-mails related to a lawsuit.

2. Intentional destruction of data – The former executive VP of sales at CA (Computer Associates) Stephen Richards, pleaded guilty to obstruction of justice by having created a directory, labeled "incinerate," for the apparent purpose of eliminating documents after the Securities and Exchange Commission issued him a subpoena in the investigation of a $2.2 billion accounting fraud case.

3. Intentional destruction of data - The CA (Computer Associates) CEO Sanjay Kumar reformatted his hard drive after CA was being told by the courts to keep all relevant documents in the investigation of a $2.2 billion accounting fraud case.
Cases where NOT DELETING DATA also landed companies into trouble

1. **Retaining data** - For Enron keeping e-mail around on PCs, servers, and backup tapes gets Enron into trouble. During the investigation of fraud at Enron in 2003, 1.5 million internal messages from 176 employees showed up online, thereby exacerbating (or making it more serious) the embattled company's problems.

2. **Not properly deleting data** – The example of the employee database for Vodafone that had not been properly and permanently deleted in the hard disk landed up being recovered when the hard disk was sold as a used item.

3. **Not properly deleting data** – The example of the business strategy documents for a German truck company that had not been properly and permanently deleted in the hard disk landed up being recovered when the hard disk was sold as a used item.

4. **Not properly deleting data** – The example of the embarrassing detail that a contractor bidding to build a U.S. Navy destroyer is also a transvestite that had not been properly and permanently deleted in the hard disk landed up being recovered when the hard disk was sold as a used item.

A5Q5.3 – As an employee of a company, for example, what do you understand by your role in what data to keep and what data to delete.

“For companies that have a policy and the right tools in place, the final piece of the data management puzzle is making sure employees understand their role. They must know the ramifications of deleting or keeping each piece of data they handle.”

**ANSWER**

1. The company must have a policy to be used by all employees regarding what data to keep, what data to delete, how and where to keep data, how to correctly and permanently delete data, etc. The role of the employee is to abide by this policy.

2. The article in this assignment gives very good suggestions and guidelines on the subject of data retention and data deletion. It was said by Bill Adler, the CEO of software vendor CyberScrub, that before deleting something,

   * you have to be able to say all established retention periods have expired,
   * all audit requirements have been satisfied,
   * there are no pending requests for the information,
   * there is no foreseeable future litigation involving the records

3. On data deletion - The whole process should be centrally managed and auditable, so companies can demonstrate to courts when data was erased, by whom, and deleted data had better actually be just that--deleted.