

## Strategic Information Systems Planning (SISP) and Strategic Information Security Planning (SISecP) In Malaysian Government Agencies

Md Hafiz Selamat<sup>a</sup>, Mohd Adam Suhaimi<sup>b</sup>, Husnayati Hussin<sup>c</sup>

<sup>a</sup>Faculty of Computer Science and Information Systems  
Universiti Teknologi Malaysia, Skudai, Johor.  
Tel: +607-5532423, Fax: +607-5565044, E-mail: hafiz@fsksm.utm.my

<sup>b</sup>Kulliyah of Information Communication Technology  
International Islamic Univeristy Malaysia, Gombak, Selangor  
Tel: +603 - 61965601, Fax: +603 - 61965179, E-mail: <sup>b</sup>adam@iiu.edu.my; <sup>c</sup>husnayati@iiu.edu.my

### Abstract

*Strategic information systems and strategic information security are two different attributes in information systems world. Information systems security must be integrated with business plan[6] and strategic information systems planning must be align with business plan. This study aims to investigate the contribution of information security attributes to the strategic information systems planning in the organization especially to the Malaysian Government Agencies. Strategic information system planning (SISP) is an exercise or ongoing activities that enable organization to develop priorities for information system (IS) development[1]. A completes SISP approach is a combination of methods, processes and implementation[2]. As a new business strategies and information technologies are both rapidly moving targets, it is a very challenging task to produce an effective plan that achieves business objectives with efficient information systems support[3]. Organization invest very large amount of time and money in the SISP project. In a typical SISP project, term of key managers, users, selected clients, and IS specialist are formed[3] and planning methodology is chosen. On the other hand, Information security planning is to mitigate risk associated with the processing of information with confidentiality, integrity and authenticity[6] with ten main domain areas as common body of knowledge in information security. Finally, this study will explore both attribute of SISP and SISecP usage in information systems planning.*

**Keywords:** *strategic information systems planning, strategic information security; information systems security*

### 1.0 ICT Strategic Plan Overview

Information and Communication Technology (ICT) is an increasing powerful tool for improving the delivery of the government service, enhancing ICT development opportunities and participating in global marketplace. A strategy is the pattern of missions, objectives, policies, and significant resource utilization plans stated in such a way as to define what business the agency is in (or is to be in) and the kind of agency it is or is to be, therefore strategy and business visions are closely linked. A complete statement of strategy will define:

- Service line and the customers;
- Customers segments for which services are to be designed;
- Channels through which these customers will be reached;
- The means by which the operation is to be financed;
- Service objectives; and
- The "image" which the agency will project to its customers.

Planning for information systems, as for any other system, begins with the identification of organizational needs. In order to be effective, development of any type of computer-based system should be a response to need-whether at the transaction processing level or at the more complex information and support systems levels. Such planning for information systems is much like strategic planning in management.

Objectives, priorities, and authorization for information systems projects need to be formalized. The systems development plan should identify specific projects slated for the future, priorities for each project and for resources, general procedures, and constraints for each application area. The plan must be specific enough to enable understanding of each application and to know where it stands in the order of development. Also the plan should be flexible so that priorities can be adjusted if necessary. King [5] in his recent article has argued, strategic capability architecture - a flexible and continuously improving infrastructure of organizational capabilities - is the primary basis for a company's sustainable competitive advantage. He has emphasized

the need for continuously updating and improving the strategic capabilities architecture.

Relationship between information system functions and corporate strategy was not of much interest to Top Management of firms. Information Systems were thought to be synonymous with corporate data processing and treated as some back-room operation in support of day-to-day mundane tasks. In the 80's and 90's, however, there has been a growing realization of the need to make information systems of strategic importance to an organization. Consequently, strategic information systems planning (SISP) is a critical issue. In many industry surveys, improved SISP is often mentioned as the most serious challenge facing IS managers.

Organizations nowadays depend largely on computer based Information Systems (IS) for a vital part of their operation. IS comprise the information that is being stored, or in any way processed by an organization, the hardware and software that constitutes the configuration of computer systems, a social system that is formed by the actions and relations among the IS users, as well as a set of procedures that guide the users' actions. Under this perspective, IS have not only a technical part, but also a social dimension. IS are of high significance to organizations across a wide range of economic sectors. In consequence, their proper function and unobstructed operation is a critical issue that has attracted the attention of both IS research and practice. Information systems security management is a stream of management activities that aim to protect the IS and create a framework within which the IS operates as expected by the organization.

## 2.0 What is Strategic Information Systems Planning (SISP)?

IS/IT planning is the organized planning of IT infrastructure and applications portfolios done at various level of organization. It is very important to both user and planner because end user do IS/IT planning for their own units; end user must participate in the corporate planning, therefore they must understand the process; corporate planning determines how the IS/IT look like and determine what applications end user can deploy. Finally the future of every unit in the organization will be impacted by the IS/IT infrastructure.

SISP is the process of identifying a portfolio of computer-based applications to serve an organization best. Ideally, the organization makes SISP part of its strategic business planning process to link the resulting IT strategy to the business strategy. SISP also includes the specification of databases and systems to support those applications. SISP may encompass the selection of conventional applications that best fill the organization's current and future needs. SISP also may entail the search for new applications with the potential to create an advantage over competitors.

To perform SISP, an organization usually carries out a major, intensive study. Most follow one of several, similar well-defined and documented methodologies; a few spend the time on their own versions. Committees of users and IS specialists are more common, often using the methodology's vendor for training and guidance. During the multi-steps study, a portfolio of applications is defined, along with appropriate priorities, databases, data elements, and a network of computers and communications equipment to support them. The study also provides a schedule for their development and installation. The organization periodically updates the plan after its initial approval.

SISP basically address four general issues; aligning IS/IT plan with the organizational business plan; designing IS/IT architecture for organization in such a way that user, applications and databases can be integrated and network together; efficiently allocating information systems development and operational resource among competing applications and finally planning information project in order to complete on time and within budget and include the specific functionalities.

## 3.0 The Perspective of Strategic Information Systems Planning

In order to put the planning for strategic information systems in perspective, the evolution of information systems according to the three-era model[7] is pertinent. According to this model there are three distinct, albeit overlapping, eras of information systems, dating back to the 60's. The relationship over time of the three eras of information systems is shown in table 1 below:

Table 1: The Three Era Model of Information Systems[7]

	ERA	CHARACTERISTICS
60s	Data Processing (DP)	Standalone computers, remote from users, cost reduction function.
70s & 80s	Management Information Systems (MIS)	Distributed process, interconnected, regulated by management service, supporting the business, user driven.
80s & 90s	Strategic Information Systems (SIS)	Networked, integrated systems, available and supportive to users, relate to business strategy, enable the business - business driven.

Applications in the overall Data Processing (DP), Management Information Systems (MIS) and Strategic Information Systems (SIS) area need to be planned and managed according to their existing and future contribution to the business. Traditional portfolio models consider the relationship of systems to each other and the tasks being performed rather than the relationship with business success.

#### 4.0 SISP Methodology

The task of strategic information systems planning is difficult and often organizations didn't know how to do it. Strategic information systems planning is a major change for most organizations, from planning for information systems based on users' demands to those based on business strategies. Strategic information systems planning can change the planning characteristics in major ways. For example, the time horizon for planning changes from 1 year to 3 years or more and development plans are driven by current and future business needs rather than incremental user needs. Increase in the time horizon is a factor which results in poor response from the top management to the strategic information systems planning process as it is difficult to hold their attention for such a long period.

SISP methodology is a standard set of techniques and supporting tools to study the organization to produce SISP[8]. Generally, several methodologies were applied for SISP success[9]. The SISP team normally uses methodologies as a guideline in the SISP process. To accomplish SISP, the organization should identify the application portfolio, databases definition elements of data network and communication to support the applications. So, the SISP is a complex task [10]. Preparing the schedule for study, analysis, development and installation of information systems also required appropriate methodologies.

Methodologies for application is depends on the scope of the study and it can be dragged from several week to several months[9]. There are various types of methodologies and the SISP team should select to support their purposes. Most of the methodologies are owned and referred to the designer or consultant of the methodology [11][12]. Some vendor such as Anderson Consulting, Pro planner, Price Waterhouse Copper and many others provide SISP methodologies integrated with the software package in CASE tool. This tool need standard environment, common approach, standard vocabulary and standard user interface. CASE tools also provide communications and integration and then let various user works simultaneously on different part of study [9][12]. The previous review found the SISP methodology indicates five main components to produce SISP Plan as figure 2.0. They are project initiation, organizational analysis, identifying IT strategy, identifying the benefit from the use of IT and finally, designing the implementation plan[12]

#### 4.1 The Strategic IS/IT Planning Process

The planning process in strategic IS/IT planning consist input, output and processing activities[7]. Figure 3.0 shows the input and outputs of the planning process. The input activities are internal business environment, external business environment, internal IS/IT environment, and external IS/IT environment. Internal business environment is the current business strategy, objective, resources, processes and the culture and values of the business. External business environment are the economic, industrial and competitive climate in which the organization operates. Internal IS/IT environment is the current IS/IT perspective in the business, its maturity, business coverage and contribution, skills, resources and technological infrastructure. The current application portfolio of existing systems and systems under development, or budgeted but not yet under way also part of the internal IS/IT environment. External IS/IT environment is the technology trend and opportunities and the use made of IS/IT by external bodies.

The output activities are IS/IT management strategy, business IS strategy and IT strategy. IS/IT management strategy is the common elements of the strategy that apply throughout the organization, ensuring consistent policies where needed. Business strategy is how each unit or function will deploy IS/IT in achieving its business objectives. Alongside each of these are application portfolios to developed for the business unit and business models describing the information architecture of each unit. The portfolios may include how IS/IT will be used at some future date, to help the units to achieve their objective. IT strategy is a policy and strategies for the management of technology and specialist resources.

#### 4.3 Strategic Information System Planning in Malaysia

There are a few SISP researchers in Malaysia and the first researcher is Isa[4] and is about SISP in the Islamic perspective[12]. He explore and introduce new values of SISP which never reveal before such as a concept of tawheed (unity), khalifah (trusteeship), worship, ilm (knowledge), halal (praiseworthy), haram (blameworthy), adl (social justice) zulm (tyranny), istislah (public interest) dhiya (waste). Isa also explore the practice of SISP among Islamic Organization in Malaysia such as Jabatan Kemajuan Islam Malaysia, Lembaga Urusan Tabung Haji and Institute Teknologi Mara (now Universiti Teknologi Mara). Another researchers are Zurina[13] and Maslinda [13]. Their researchs are SISP team satisfaction during the completion of SISP and SISP practice selected private sector in Malaysia. Experience in SISP, knowledge and team working are contribute to SISP satisfaction[14][12] and most of private sector in Malaysia have SISP and they are aware the important of SISP to improve organizational activities[13][12]. They

also discover the formation of information systems department in their organization contribute to the success of SISP process. Selamat [15], is using the framework produce by Ward [7] in the secondary school resource environment as a case study. There is a different between Institute of Higher Learning (IHL) business compare to business organization in their SISP framework [16]. The SISP study Malaysia's IHLs is not in depth compare to the IHL in US and Europe. This study need to be highlighted and enhance in order to increase their understanding and SISP implementation in the organization. Suraya[17] was developed a prototype SISP tools which combining combine and automate several planning techniques in a single system and the output is information architecture and also will be the input for the system prototype development.

#### 4.4 SISP in Malaysian Government Agencies

In the context of Malaysian strategic management practice, the model as shown in figure 4.0 is used as a basic framework. The strategic management is link to strategic management process[17]. There are four main component s in the framework; vision 2020 for Malaysian, present and future challenge, process of transformation, and strategic management (include corporate strategic planning and ICT strategic planning). Three ingredients to complementary in a strategic planning process are strategic thinking, strategic intent and strategic action. Thinking is needed to ensure the acquisition of right knowledge of the total picture, clear direction and change requirements. Thinking must be supported by a strong organizational will or intention, persuasive and convincing in nature. A strong motivational factor attitudinal, and necessary pre-requisite for success [10]. Action refer to action manage by continuous control and monitoring and review. Key performance indicator (KPI) is a necessary tool to measure stability and success of the strategic planning implementation.

Planning is a process, and process has to be able supported by documents and measurement for effective implementation. Process in planning include setting of goals, determining action, allocation of resources and building measurable performance indicators and a positive outcome may be realized in the form of strong rapport, cooperation and collaboration[17]. There is a need for better management control and planning function for managers[17][18]. They identify 29 key issues between 1996 and 2000 and among top ten issues is management focus. Three top five of the issues are related to ICT strategies as follow:

- a. Improving information security including data integrity and quality
- b. Managing integration of data processing, office automation and telecommunication
- c. Aligning IT with the enterprise
- d. Using IT competitive advantage
- e. Improving IT strategic Planning

#### 4.5 Malaysian Public Sector ICT Strategic Plan

In the 8<sup>th</sup> Malaysian plan, information Technology Strategic Plan (ISP) from Agencies is essential as planning document for Government Internet & IT Secretariat to develop Information Technology policies in public sector in line with the National IT Agenda. Malaysian Administration & Man Power Planning Unit (MAMPU) has develops a framework for to assist Agencies to develop their ISP. Currently, Malaysian Public Sector ICT Strategic Plan is a blueprint developed for agencies for the use of ICT, which is both cost effective and aligned with prioritized management and operational needs. This plan will lead to the identification of strategic initiatives, either new or already underway, which can be aided by application systems, technology and governance. It contains several elements that drive the development of the plan; business alignment, vision, allocation and value, enabling, governing and capabilities, and finally action and measurement. An ICT Strategic Plan will address the alignment between the strategic operational requirements of an agency enterprise and the planned and economically justified application of technology assets. This alignment is best achieved when ICT has been deployed as an enabler of one or more cross-functional business processes. The basic interplay between the business strategy area of expertise and the ICT strategy area of expertise is the dynamic between business "requirements push" and "technology pull". The "requirement push" is the direct specification of information and processing needs by the business. However, true competitive advantages are very often gained through "technology pull". This occurs when the business is made aware of opportunities through insight and understanding of the capabilities of technology. Without this insight there may be no customer self-service, costly information exchange, and a disadvantage in establishing eBusiness and eCommerce[19].

The ICT planning approach for Malaysian Public Sector is shown in figure 5.0 below. The methodology adopts the 4-stage approach that answer the why, what, how and when questions for each activities of an ICT strategic Planning formulation. The stages are sub-divide into phases as figure 5.0 and each phases contains steps and detail activities. ICT strategic plan outputs are produce in every phase of this methodology, and categorized into deliverable and interim outputs. Deliverables are provided to the agency for approval, usually making completion of stage and are formal project document. On the other hand, interim outputs are internal project team document that support the mark progress toward the deliverable.

#### 5.0 Information Security Defined

Information security defined as an information security program that plan to mitigate risk associated with the

processing of information in three elements which defined by security professional [2]:

- **Confidentiality.** The prevention of unauthorized use or disclose of information. Privacy is closely related topic that has lately been getting more and more visibility
- **Integrity.** Ensuring that information is accurate, complete, and has not been modified by unauthorized user or process.
- **Availability.** Ensuring that the users have timely and reliable access to their information assets.

These three elements (CIA) are the basics around which all security programs are developed. Both of them are linked together in the idea of information protection. The main idea is to show that information is an asset that requires protection.

## 6.0 Public Sector ICT Security

Public Sector ICT Security can be defined as the process of ensuring business continuity and services provision free from unacceptable risk. It also seeks to minimize disruptions or damage by preventing and minimizing security incidents[20]. The security of information within the Government of Malaysia's Information and Communications Technology (ICT) system is a subject of major concern. Threats such as impersonation, malicious code, misuse of data, easily available penetration tools, and powerful analytical techniques contribute in whole or in part to the necessity of providing adequate protection to public sector ICT assets. These threats if left unchecked, will result in painful explanation at the very minimum or untold damage to the country.

Over the years, government agencies have been religiously collecting vast amount of information. It is in the early 70's that these information have been deposited into digital format and since then, these repositories have unknowingly become exposed because of the invaluable information they keep and now in a format easily manipulated without stringent audit trail. The government realizes this and that the government is also aware that there is an urgent need to secure the vast information resource through effective management of the security of ICT systems. In this regard, efforts are being made to ensure Public Sector ICT Security management achieve and maintain a high level of confidentiality, integrity and availability. A comprehensive approach is required in planning, developing, operating and maintaining the government's ICT security processes. The ICT security measures need to be incorporated early, in the requirement specification and design of the ICT system, before the implementation stage to ensure a cost-effective and comprehensive system.

The main steps are assessing the current security strengths and vulnerabilities; developing ICT security policies, standards and processes; designing and develop customized security architecture; and evaluating and selecting the best security system for the organization.

The ICT security process should mirror the management's direction in relation to overall organizational policy; organizational roles and responsibilities; personnel; government's asset classification and control; physical security; system access controls; network and computer management; application development and maintenance; business continuity; compliance to standards as well as legal and statutory requirements; classification and protection of information media; employee awareness programs; and incident reporting and response[20]

## 7.0 Integrating the Strategic IS/IT Planning with Information Security

Integrating both Strategic IS/IT planning process with the Information Security Domain will produce more valuable SISP to the organization. The appropriate domain should include in the SISP process as an input in the external business environment, external IS/IT environment, internal business environment and internal business environment. As for example, security management practice domain should include in all input attributes; security management in internal and external business and IS/IT environment. Beside SISP and Information Security Domain, Computer System Life Cycle should be incorporate in the establishment of SISP, especially in the development or acquisition phase. At this phase, security requirement was identified then incorporate security requirement into specification. Without policy, security practice will be developed without clear demarcation of objectives and responsibilities[21].

## 8.0 Conclusion

Base on the discussion above, there is a need to ensure Public Sector ICT security management achieve and maintain a very high level of confidentiality, integrity and availability in their information systems which can be plan at the early stage. The most appropriate time to plan the security when the information systems plan is conducted. Finally, the strategic security planning should align with the strategic information systems plan.

## References

- [1] Doherty, N. F., Marples, C. G. & Suhaimi A. "The relative success of alternative approaches to strategic information systems planning: an empirical analysis". *Journal of Strategic Information Systems*. Vol 8 pp 263-283.
- [2] Earl, M. J. "Experience in strategic information systems planning". *MIS Quarterly* Mac, 1993, pp1-24.
- [3] Hevner, A. R., Berndt D. J. & Studnicki J. "Strategic information systems planning with box structures". *IEEE Proceeding of the 33<sup>rd</sup> Hawaii International Conference on Systems Science*. Hawaii, January 2000.
- [4] Isa, M. "Strategic Information Systems Planning in Islamic Information Systems: A case study for Malaysian Muslim Organization". Ph. D. dissertation, University of Wales, Lampeter. 1997
- [5] King, W. "Creating A Strategic Capabilities Architecture, Information Systems Management", 1995, v.12.
- [6] Wylder, J. "Strategic Information Security", Auerbach Publication, 2004.
- [7] Ward, J. & Griffith, P. "Strategic Planning For Information Systems" (2<sup>nd</sup> Edition). John Wiley & Son, London. 1996.
- [8] Robson, W. "Strategic Management & Information Systems" (2<sup>nd</sup> Edition), 1996, Pitman Publishing, London
- [9] Lederer, A., L., Sethi, V. "Seven Guidelines For Strategic Information Systems Planning, Information Strategy: The Executive's Journal, 07438613, Fall98, Vol. 15, Issue 1, p23, 6p, Auerbach Publications Inc, 1998.
- [10] Malik, R. Preparation of Information technology strategic planning. MAMPU-Intan IT Manager Seminar, INTAN, Kuala Lumpur, 2001. Pp1-11.
- [11] Remanyi, D. Strategic Information Systems, Current Practice and Guidelines, Ph. D. dissertation, Henley Management Collage, 1991, UK.
- [12] Muhamad Nubli. "Source-agent-client component in strategic information systems planning methodology for Malaysian public sector". PhD. Dissertation, Universiti Putra Malaysia, 2004
- [13] Zurina, U., Hassan, M., Mamat, A. & Izura, N. "Kajian Pelaksanaan Perancangan Strategik Sistem Maklumat di Organisasi", Proceeding on REDEC 2001 colloquium, UNITEN, Kajang pp 24.
- [14] Maslinda, N. Hassan, M. & Mamat, A. "Perancangan strategic system maklumat: factor mempengaruhi kepuasan perancang. Proceeding on REDEC 2001 colloquium, UNITEN, Kajang pp 15
- [15] Selamat, M. H., Alias, R. A., Ibrahim, O. & Abdullah, S. "IT Strategic Planning For School Resource Center. Proceeding of the 13<sup>th</sup>. Educational Technology Convention, 19-21 September, 2000, Hotel HillCity, Ipoh, Perak, Malaysia.
- [16] Alinda, R. A., Selamat, M. H., Abdullah, S. & Ishak, I. S. "Strategic Information Systems Planning for IHLs: A preview", Proceeding of the Malaysian Science and Technology Congress 2001 (MSTC 2001), Information and Communication Technology Session, Universiti Science Malaysia, 8-10 Nov, 2001, Malaysia.
- [17] Suraya, M. "Developing a prototype for strategic information systems planning toolkit". 2001, M. Sc. (Computer Science) dissertation. UTM
- [18] Md Zabid Abd Rashid, Han Chun Kwong, & Ronald M. Zigli. "Key Issues in MIS in Malaysia", 16-17 Oct, 1995.
- [19] MAMPU. "Standard, Policies and Guidelines – Malaysian Public Sector ICT Strategic Planning Guide", Version 1.0, Putra Jaya. August 2003.
- [20] MAMPU. "Malaysian public sector management of information & communication technology security handbook (MyMIS)". Putra Jaya., 2002
- [21] Higgins, N. H. "Corporate Systems Security: Towards an integrated management approach". *Information Management & Computer Security*, 1999; 7(5) pp217-222

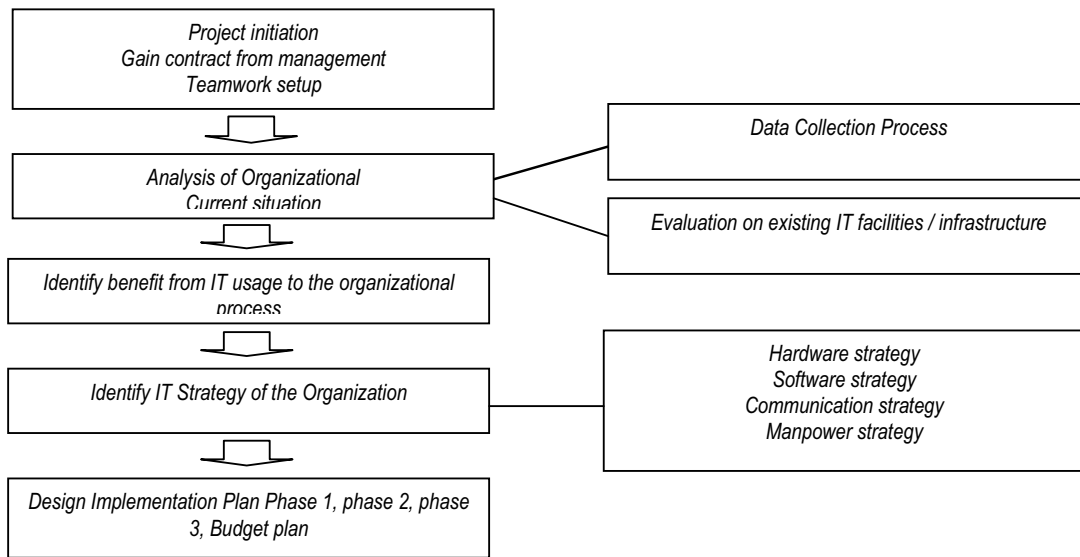


Figure 2.0: Process Involved in SISP Methodologies (Muhammad Nubli, 2004)

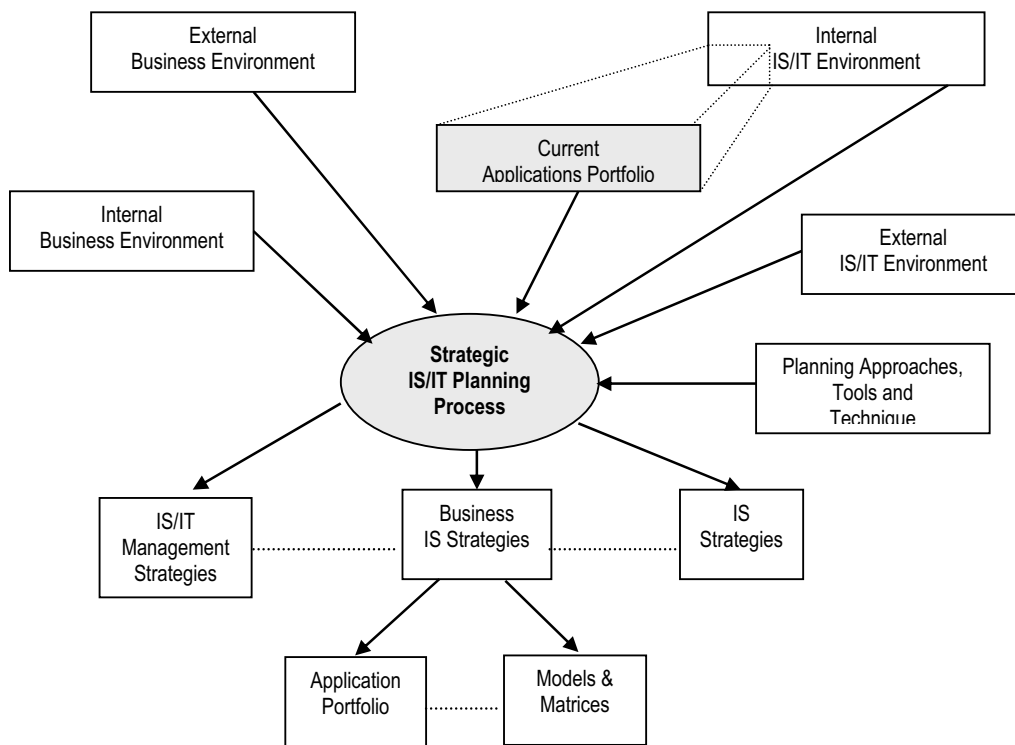


Figure 3.0 The inputs and outputs of the planning process (Ward, 1996)

