CHAPTER 7: CONCLUSION & RECOMMENDATION

7.1 Identify the Strengths and Weaknesses of Organizations

By analyzing the results, the industry norm and control limits of each and every process are identified. Based on the aggregate results, the organizations are categorized into five groups as, Very weak, Weak, Average, Good and Very good.

Further these results can be used to identify the level of control of the processes in the organizations individually, to identify the strength and weakness in processes of information system function against the industry norm. As example the results of the assessment of the organization 1 is shown in table 7.1.

Table 7.1 The Result of the Individual Level Assessment of the Organization 1

Process	Marks (Percentage)	Category	Industry Average	Percentage Deviation from Average
General Management	17	Very Weak	55	-70
System Implementation	55	Average	52	6
Availability	46	Week	56	-18
Performance Monitoring	39	Very Weak	55	-29
Capacity Planning	46	Week	52	-12
Problem Management	38	Week	48	-21
Change Management	33	Very Weak	52	-38
Security Management	20	Very Weak	54	-63
Disaster Recovery	24	Very Weak	47	-49
Document Management	20	Very Weak	49	-59
Procurement Management	55	Average	56	-2
Quality Management	3	Very Weak	45	-94

In above table, 2nd column shows the assessment marks scored by the organization 1 for each process. 3rd column shows the categorizations based on the aggregate values of the processes. 4th column shows the industry norm or average value. 5th column shows the percentage deviation of the marks of the process, from the industry average of the process, for organization 1. {(column 2-column 3)*100/column 3} In that column positive sign is for the values above the average and the negative sign is for the values bellow the average.

7.2 Priority Based on the Controls of the Process

When improving the process more priority is necessary to be given to the weaker processes. Table 7.2 shows the results extracted for the organization 1.

Table 7.2 Priority List Based on the Control of the Process for Organization 1

Process	Percentage Deviation from average	Priority marks
Quality Management	-94	12
General Management	-70	11
Security Management	-63	10
Document Management	-59	9
Disaster Recovery	-49	8
Change Management	-38	7
Performance Monitoring	-29	6
Problem Management	-21	5
Availability	-18	4
Capacity Planning	-12	3
Procurement Management	-2	2
System Implementation	6	1

2nd column shows the percentage deviation of the average and the results are in ascending order. Weakest process is on the top of the list while the strongest process is at the bottom of the list. 3rd column shows the points given to the process based on the priority of the process, considering the strength or weakness of the process. As the weakest process needs the highest attention and needs more priority, it is allocated with 12 points while strongest process is allocated with 1 point and other processes get respective points based on the position of the priority list.

7.3 Priority Based on the Importance of the Process

Out of these twelve processes the priority of each process depends on the industry and the nature of the organization also. If a company outsourcers its IT operation, procurement management has very high priority. If the organization has gone for a new system recently, the system development will have higher importance. If the organization has critical online transaction processing system, the availability process gets higher priority. If the growth rate of the organization is high, performance monitoring and the capacity planning will have higher priority. If the environmental factors related to the organization, (political, economic, technical etc) change rapidly, change management process will have

higher priority. If the organization deals with high sensitivity of data, the security management process will have high priority. If the nature of the organization is such that it may face physical and logical threats, security management and disaster recovery will have higher priority. If the IT requirement varies quickly, configuration and document management will have high priority. Ultimately it depends on the nature of the organization; hence it is necessary to identify the organizational level priorities of the processes individually. Schiesser(2003) gives the following approach that can be used to identify the organizational level priorities.

The members in the steering committee are individually asked to list up the process in order of importance, based on their individual judgment. (Most important process is on the top of the list while least importance process is at the bottom of the list). 12 points are allocated to the top most process and 1 point is allocated to the bottom most process and the others get respective points based on their position in the list. Get the average values for each and every process based on the values given by the individual members in the steering committee. Prepare the list of the process in descending order of the average value. (Most important process on the top of the list while the least important process is at the bottom of the list)

Assume that the table 7.3 shows the process in order of importance for the organization 1.

Table 7.3 The Order of the Importance of the Process for the Organization 1

Process	Points
Availability	12
Problem Management	11
Performance Monitoring	10
Security Management	9
Disaster Recovery	8
Quality Management	7
General Management	6
Change Management	5
Configuration Management	4
Capacity Planning	3
Procurement Management	2
System Implementation	1

In the above table 2nd column shows the points given to the process based on the importance of the process. Most important process is allocated with 12 points while the least important process is allocated with 1 point and the other processes get respective points based on the position in the list.

7.4 Overall Priority of the Process

Two lists of priorities considering the strengths and weaknesses of the processes and priorities considering the importance of the processes are discussed in detail under sections 7.2 and sections 7.3 respectively.

In evaluation the overall priority of the process it is recommended to consider both the parameters.

Table 7.4 shows the overall priorities list for the organizations 1

Table 7.4 Overall Priorities of the Processes

Process	Considering the controls	Considering the importance	Overall priority
Security Management	10	9	90
Quality Management	12	7	84
General Management	11	6	66
Disaster Recovery	8	8	64
Performance Monitoring	6	10	60
Problem Management	5	11	55
Availability	4	12	48
Document Management	9	4	36
Change Management	7	5	35
Capacity Planning	3	3	9
Procurement Management	2	2	4
System Implementation	1	1	1

In above table 2nd column shows the priority based on the control strengths and weaknesses of the processes (from sections 7.2). 3rd column shows the priority based on the importance of the process (from sections 7.3) 4th column shows the overall priority considering both the factors. (The vales of the column 4 are calculated by multiplying column 2 and column 3.) The process having the highest overall priority is at the top of the list while least overall priority is at the bottom o f the list.

7.5 Implementation of the Improvements

Through the assessment & analysis, strengths and weaknesses of the processes and the priorities of improvements of the processes are identified. The assessment was done in the policy level (more in strategic level) based on the technical level detail study done by auditors. Though the evaluation is done in strategic level, the improvement should be done in an operational or technical level. Therefore it is necessary to have details of technical level investigations to implement the improvements. Because of this an organization needs a dedicated group of people continually working to identify the areas for improvement and compliance monitoring of the processes for continuous improvement of the IS functions. In other words the organization needs an internal audit department to conduct detail level investigations regularly.

7.6 Importance of the Internal Audit Department

Following facts lead to the conclusion that it is essential to have the internal audit department to improve the IS function in the organizations.

- Based on the observations under sections 6.2 and 6.3
  It is observed that the level of the overall assessment is high when the operations of the internal audit department is high (Better the internal audit department better is the overall performance of the IS functions)
- As an essential factor to implement the process improvement it is necessary to have an internal audit department and that is discussed under section 7.5

7.7 Development of Internal Audit Department

The importance of the internal audit department is identified and discussed under section 7.6. This section briefly discusses how to establish and manage internal audit department mainly based on the facts discussed by Weber (1999)

Managing the information system audit function involves the traditional management function; planning, organizing, staffing, leading and controlling.

Two types of plans are formulated when managing the information system audit function; long run and short run plans. Goals on long run planning are to provide an overall direction for the information system audit function and to ensure that adequate resources are available to discharge the responsibilities effectively and efficiently. Goals on short run planning are to put in place a risk management program that will enable to evaluate systematically the exposures that face the organization.

Organizing the information system audit function involves addressing four issues.

- Establishing formally the legitimacy of the information system audit function within the organization.
- Determining whether the information system audit function should play staff role or a line role within an organization's overall audit function.
- Determining whether the information system audit function should be centralized or decentralized.
- Determining how the information system audit function should be resourced.

The legitimacy and role of the information system audit function should be established via an audit charter. If information system auditors play a staff role, they will assist the general staff auditors by providing the specialist advice on technologically complex matters associated with computers. If they play a line role, they will be an integral part of any audit team. Many factors affect the decision on whether the information system staff functions should be centralized or decentralized. Probably the most important factor, however, is whether the organization in which the information system audit function is placed, is itself centralized or decentralized. How well the information system audit function is resourced will depend in part on how well long run and short run planning activities are undertaken.

The staffing function involves sourcing and recruiting information system audit staff, appraising and developing information system audit staff and determining suitable carrier paths for information system audit staff. In terms of sourcing and recruitment, a long-standing issue is whether it is better to recruit staff, which primarily have an information technology background, or staff, which primarily have auditing background. Careful staff appraisal and development is critical within the information system audit function because staff need to remain proficient in technical, social and managerial skills.

Providing suitable career paths for information system auditors is often difficult because many organizations employ small number of information system auditors.

Under the leading of the information system audit group, it is necessary to achieve harmony of the objective at three levels. First, actions taken by the individual auditors need to be congruent with the overall objective of the specific audit in which they participate. Second each audit needs to be undertaken in such a way that its outcomes are congruent with those established under the short-term plan of the information system function. Third the activities of the information system audit function overall must help the organization to achieve its mission and goals. To achieve harmony of objectives, leadership process must be adjusted to take into account the needs of the individual information auditors.

Control needs to be exercised at the level of individual audits and the level of the overall information system audit function. At the level of the individual audits, some important control strategies are to state and document clearly the objective of an audit, to monitor and evaluate the process, to subject the audit work performed to independent review, to report carefully the result of an audit, and obtain feedback from the stakeholders in an audit on their views about the quality of audit. At the level of the overall information system audit, some important control strategies are, to undertake the periodic detailed reviews of selected audits, to regular review information system audit standard, polices and procedures, and to use benchmarking to evaluate how well the information system audit function is performing relative to information system audit functions within other organizations.

A list of processes and their controls to be covered under the information system audit is shown in table 7.5. A weight factor is introduced to the table as the different processes having different levels of impact depending on the nature of the organization been investigated, which is described in section 7.3 in detail.

Table 7.5 Process and Controls

Process (variable)	Controls (indicators)	Weight
1. General Management	1.1 Senior management involvement in Information System (IS) function.	
	1.2 Role of the IT steering committee in IS function.	
	1.3 Evaluation of planning function.	
	1.3.1 Identify the goals of the IT department considering the business goals. (long term & short term goals)	
	1.3.2 Identify the resources necessary to achieve the goals. (h/w, s/w, people)	
	1.3.3 Identify the cost & the benefits of acquiring the resources.	
	1.3.4 Activity plan to achieve the goals and objectives .	
	1.3.5 IT budget.	
	1.4 Evaluation of organizing function.	
	1.4.1 Location of the information system function in the company organization structure.	
	1.4.2 Staffing. (recruiting, development, termination)	
	1.4.3 The structure of the IT department.	
	1.4.4 Roles and responsibilities of the IT department.	
	1.4.5 Coordination/communication between the other departments.	
	1.5 Evaluation of leading function.	
	1.5.1 Motivation of staff.	
	1.5.2 Communication between employer and employees.	
	1.5.3 Career development, training and guidance at individual level.	
	1.5.4 Individual goal setting and Performance evaluation.	
	1.6 Evaluation of controlling function.	
	1.6.1 Actual results against the plans.	
	1.6.2 Controlling the IS activities. (policies, procedures, standards)	
	1.6.3 Compliance monitoring & corrective actions.	
	1.6.4 Controlling of users.(service level agreements, transfer pricing etc)	
2 System Implementation (acquisition & development)	2.1 Problem /opportunity analysis (SWOT analysis) carried out.	
	2.2 Feasibility of the project carried out. (economic, technical etc)	
	2.3 Detail Investigation of the existing system and the problems faced identified.	
	2.4 Requirement of the new system identified.	
	2.5 Organization job design (business process reengineering) carried out.	
	2.6 Solution design, construction and testing processes done.	
	2.7 Identifying hardware/system software requirements (sizing) carried out and acquired.	
	2.8 Operational procedures developed, the users trained for their tasks, procedure manuals, training manuals available.	
	2.9 Conversion process from existing system to new system done.(e.g. data cleansing before migration, data migration & testing , parallel run etc)	
	2.10User acceptance obtained. (users of the system have actively participated in developing the solution)	
	2.11Post implementation review conducted to identify the effectiveness of the implementation.	
3 Availability of Resources for the Production Operation	3.1 The availability and reliability standards (service level agreements) established for the resources. (applications, system, network etc)	
	3.2 Data availability to assess the availability of the resources. (mean time between failures (MTBF), mean time to repair (MTTR))	
	3.3 Actions been taken to improve Reliability (MTBF) and Maintainability. (MTTR)	
	3.4 Availability of the server environment for the production operation.	

		3.5 Availability of the database & application software for the production operation.	
		3.6 Availability of the network environment.	
		3.7 Availability of desktop environment.	
		3.8 Availability of peripherals.	
4	Performance Monitoring & Tuning	4.1 Identify the resources to be tracked & managed. (application, system, network, peripherals etc)	
		4.2 Performance parameters such as response time, transaction volumes, service level during the peak periods etc are identified.	
		4.3 The priorities of resource allocation for different processes identified.	
		4.4 Decided the performance indicators. (what to measure, when and how to measure etc)	
		4.5 Analyze the performance indicators to identify the load imbalances and bottlenecks.	
		4.6 The way to determine what should be done to improve the performance.	
		4.7 Timely improving the system performance by tuning, balancing the system, performance trouble shooting, reconfiguring etc.	
		4.8 Timely reporting the results to the relevant parties like capacity planners, senior management etc.	
5	Capacity Planning	5.1 Identify the key resources to be planed. (server, database, network, peripherals, desktop)	
		5.2 Measure the utilization and performance of the resources currently available. (performance monitoring)	
		5.3 Identify the excess capacity.	
		5.4 Workload forecasting from the relevant parties/users.	
		5.5 Map the work load forecast into resource requirement.	
		5.6 Predict what time the existing capacity will be over.	
		5.7 Develop the resources acquisition plan to meet the future requirements.	
6	Problem Management/ Technical Support	6.1 The procedures adapted to inform the problems identified.	
		6.2 Recording mechanism of the problems.	
		6.3 Timely escalating the problem and user acceptance.	
		6.4 Analyze the trends of the problems, implementing remedial measures to control the problems.	
		6.5 Technical support for end users.	
		6.6 Training the end users in IT activities.	
7	Change Management	7.1 Role of the change control board to cope up with the change management.	
		7.2 Formal change request procedures been adopted to request a change.	
		7.3 Analyze the necessity of the change (cost benefit analysis) and the impact of the change.	
		7.4 Approve the changes for implementation.	
		7.5 Prioritize and schedule the changes of the requests.	
		7.6 Design, construction and test the change.	
		7.7 Implement and acceptance of the change.	
		7.8 Follow up process of the change carried out.	
8	Security Management	8.1 Identify the information system assets.	
		8.2 Value the information system assets.	
		8.3 Identify the threats faced by each and every resource.	
		8.4 Threats likelihood assessment. (possibility of occurring the threats)	
		8.5 Exposure analysis. (the extent of the exposure of the resources to the threat)	
		8.6 Controls adjustment to overcome the threats.	
		8.7 Reporting to the management.	

9	Disaster Recovery	9.1 Emergency plan. (the actions to be taken, persons to be informed etc)	
		9.2 Backup plan. (types of backups, frequency, procedure, responsible person, storage etc)	
		9.3 Recovery plan.	
		9.4 Test plan.	
		9.5 The level of the insurance coverage of the IS resources.	
10	Configuration / Document Management	10.1Availability of the documentation of the hardware software configuration, policies, procedures , operational manuals etc.	
		10.2The ownership of the document defined. (created , checked, approved, used etc)	
		10.3The accuracy and thoroughness of the documents.	
		10.4The format and readability of the documents.	
		10.5The updateability and the currency of the documents.	
		10.6Accessibility and the storage of the documents.	
		10.7Usability and effectiveness of the documents.	
11	Procurement Management	11.1Procurement planning. (what to procure and when, what to outsource, etc)	
		11.2Solicitation planning. (identify the product requirement, potential sources, preparing RFPs, developing evaluation criteria etc)	
		11.3Solicitation. (obtaining the quotations, bids, offers or proposals as appropriate)	
		11.4Source selection. (evaluating prospective vendors, negotiating contracts and awarding the contact)	
		11.5Contract administration. (monitoring contact performance, contact modification etc)	
		11.6Contract closure. (completion and the settlement of the contract)	
12	Internal Auditing/ Quality Management	12.1The existence of the internal audit /quality control department.	
		12.2Identify and develop the quality goals.	
		12.3Developing and & maintaining standards for IS function.	
		12.4Monitoring the compliance with QA standards.	
		12.5Identifying the areas for improvement.	
		12.6Regular Reporting to the management of QA function.	
		12.7Training of QA standards and procedures of the users.	

7.8 Conclusion

7.8.1 Accomplishment of Objectives

Objective 1: Identify the areas to be assessed under the information system function

12-process model is used to identify the activities that come under information system function and use the same to assess the information system functions in the organizations.

Objective 2: Assessment of organizational information function

The information system functions in the organizations are assessed by using the 12 process model through auditors. Instead of a technical level approach, a higher-level strategic approach is used for the assessment.

Objective 3: Identify the strengths and the weaknesses in information systems

Based on the assessment, the aggregate levels of controls in the information system function are identified. These aggregate values are used to identify the control strengths and weaknesses in the information system of the organizations individually.

Objective 4: Recommendation to implement the improvements of the IS function

Based on the findings of the research, priorities of implementing the improvements of the information system functions are discussed. The necessity of the internal audit department for effective information system is identified. Establishment of the internal audit department for an organization is discussed briefly.

7.8.2 Further Study

As this is an initial investigation, general controls, which are valid for any type of industry, are considered. This can be improved for a particular industry sector by identifying specific controls relating to the industry and hence strengths and weaknesses of the controls for the specific industry.

Assessment and improvement (improvement based on assessment) will be more meaningful if the related parties contribute constructively towards information system management controls and audit. In this context several institutions as given bellow can contribute to improve the information system function through controls.

- Professional body
- Regulatory and legislative body
- Consultancy organizations
- Institutes in IT education
- Organizations themselves

Professional body

The leading international professional organization for information system auditors is the information system control and audit association (ISCA). The ISCA has more than 15,000 members in more than 100 countries. It has local chapters in more than 50 countries

The five hallmarks of a profession are the

- Existence of the common body knowledge
- Existence of the standards of competence
- Conduct of valid and reliable examinations to assess the competency
- Existence of a code of ethics
- Enforcement of the code of ethics through the disciplinary mechanism

ISACA has sought to put in place all five hallmarks. It worked to define a common body of knowledge for information system auditors. This body of knowledge has been articulated and published in COBIT (control objective for information and related technology). ISACA has also defined standards of competency in relation to information system audit independence, technical competence, work performance, audit reporting, audit follow up, and audit charter. An examination competence called the certified information system audit examination is conducted internationally by the ISCA. The

ISCA has formulated a code of professional ethics and put in place the disciplinary mechanism for its members.

The effectiveness of the operation of a professional body in Sri-Lanka is to be investigated.

Regulatory body

Controls of the information system are assured through the legislative framework. Is there a appropriate legislation and a regulatory body to control the information system related activities in the society of Sri Lanka? This is a vast area to be explored.

Consultancy companies

There are very few organizations currently conducting information system audit as external auditors in Sri-Lanka. There is a larger vacuum in this area to be explored in detail.

Institutes in IT education

There are several institutions that contribute to the IT education in Sri Lanka. It includes government universities private and affiliated universities and institutions. The contributions of these institutions towards information system control & audit are to be explored.

Industry itself

Ultimately the organization itself is necessary to identify the importance of the information system control and audit for the effective information system. It is necessary to explore the readiness of the organizations in information system controls and audit.

REFERENCES

American Institute of Certified Public Accounts (1988), *Statement on Auditing Standards no. 47: Audit Risk and Materiality in Conducting Audit*, American Institute of Certified Public Accounts.

American Institute of Certified Public Accounts (1990), *Audit Guide: Statement on Auditing Standards No. 55: Consideration of the Internal Control Structure in Financial Statement*, American Institute of Certified Public Accounts.

Bannan, John (1996), Needs Analysis Considerations, *EDPACS* (March), 8-13.

Boynton, Andrew and Zmud, R. (1987), Information Technology Planning in the 1990's: Direction for Practice and Research, *MIS Quarterly* (March), 59-51.

Cerullo, Michael J. (1981), Accountants Role in Computer Contingency Planning, *The CPA Journal* (January), 22-26.

Cohen, Fred (1997), Information System Attacks: Preliminary Classification Scheme, *Computers & Security*, 16(1), 29-46.

International Organization for Standardization (1991), *ISO 9126: Software Product Evaluation – Quality Characteristics and Guideline for Their Use*, International Organization for Standardization.

Parker, Don B. (1981), *Computer Security Management,* Reston Publishing Company.

Schiesser, Rich (2003), *IT System Management*, Prentice-Hall.

Strong, M.,Yang, W. and Richard, Y. (1997), Data Quality in Context, *Communications of ACM* (May), 103-110.

Ragozzino, Pat P. (1990), IS Quality – What is it?, *Journal of System Management* (November), 15-16.

Redman, C. (1995), Improve Data Quality for Competitive Advantage, *Sloan Management Review* (Winter), 99-107.

Wand, Y and Weber, Ron (1989), A Model of Control and Audit Procedure Change in Evolving Data Processing System, *The Accounting Review* (January), 87-107.

Weber, Ron (1999), *Information Systems Control and Audit*, Pearson Education.

ANNEXURE 1: RISK ASSESSMENT GUIDELINE

The level of the required controls of the information system activities depends on the risk faced by the organization.
E.g. if there is high risk, it is necessary to have a high control over the activity.
Unfortunately there is no hard & fast rule to quantify the risk. Hence we use several approaches to identify the risk faced by the organization.

Approach 1: Type of industry (Porter & Miller (1985) information intensity matrix)
Depends on the nature of the industry

Information intensity of value chain		
High	Delayed (e.g. oil refining, legal services) (High risk)	Drive (e.g. banking, education, airline) (Very high risk)
Low	Delivery (e.g. cement, bricks) (Low risk)	Dependent (e.g. fashion) (Average risk)
	Low	High

Information intensity of the product

Approach 2: Type of the organization (McFarland et al.'s (1983) strategic grid model)
Depends on the nature of the organization

Importance of future systems		
High	Turnaround organization (High risk.)	Strategic organization (Very high risk)
Low	Support Organization (Low risk)	Factory (Average risk)
	Low	High

Importance of current systems

Approach 3: Management approach (based on McFarland et al.'s (1983) strategic grid model)
Depends on the management of the organization

Future expectations of the management		
High	Need more control & management involvement. (High risk)	Continuous management attention needed (Very high risk)
Low	Need more involvement (Low risk)	Less future expansions (Current risk is high but low future risk)
	Low	High

Current expectations of Management

Approach 4: People's involvement (based on McFarland et al.'s (1983) strategic grid model)
Depends on the people's involvement

Usage of the Knowledge		
High	Need more training (Very high risk)	Knowledge updating necessary (High risk)
	Need of knowledge management (Low risk)	Low motivation, low opportunities (High risk)

Low — Low — High

Knowledge of the people

Approach 5: Usage of the information (based on McFarland et al.'s (1983) strategic grid model)
Depends on the effectiveness of the usage of the information

Usage of information		
High	Need to have more information (Very high risk.)	Availability and usage of the information is high (High risk)
	Availability and usage of the information is low (Low risk)	Need to use information effectively (High risk)

Low — Low — High

Availability of information

Approach 6: Technological requirements (based on McFarland et al.'s (1983) strategic grid model)
Depends on the technological requirement

Technological requirement		
High	Need to use high technology (Very high risk.)	Use high tech as required, need to be alert (High risk)
	Possibility of having technological improvement (Low risk)	Cost overrun (Average risk)

Low — Low — High

Availability of technology

Based on the overall risk, the required level of the controls can be decided as follows.

Identified Risk	**Required Controls**
Very Low Risk	Very Low Controls
Low Risk	Low Controls
Average Risk	Average Controls
High Risk	High Controls
Very High Risk	Very High Controls

ANNEXURE 2: RESEARCH QUESTIONNAIRE

Introduction

My name is Priyanga Keerthiwansa and I am studying for MBA in IT degree of the University of Moratuwa, Sri-Lanka.

I am conducting a research under the topic of "***Assessment of the controls of information system function in auditing perspective in organizations of Sri-Lanka***" as a partial fulfillment of the requirement of the degree.

The purpose of this questionnaire is to collect the required information for the research. The answers for the questionnaire will be treated as highly confidential.

Your participation is very much appreciated.

Thank you
Priyanga Keerthiwansa
(MBA/PG/IT 02/9110)

Guideline

1. Questionnaire consists of two sections. Section one is for the general information of your client and section two is for the evaluation of the processes in information system (IS) function.
2. Section two consists of 12 processes that come under IS function. Each process consists of several control points.
3. In assessment, each control point is allocated with a maximum of 10 marks. Please follow the guideline given below in allocating the marks.

Category	Marks
Very poor	0-2
Poor	2-4
Average	4-6
Good	6-8
Very good	8-10

4. When allocating the marks for the control point, please consider the required level of the control, by identifying the IT risk faced by the organization. (Risk assessment guide line is provided to you separately)
   e.g.
   Online transaction processing system, **90% availability** of the application system, may be put into a **poor** category while batch processing system, **75% availability** of the application system, may be put into a **good** category.
5. Please avoid leaving the field blank. Please write "irrelevant" instead.

Section 1 - General information

Industry (Please don't write the organization's name)	
Turnover (in Rs.)	
IT budget (in Rs.)	
No of staff	
No of IT staff	
Audit date	
Period end (month)	
Period end (year)	

Section 2 - Assessment information system

Process	Controls	Marks
1. General Management	1.1 Senior management involvement in Information System (IS) function.	
	1.2 Role of the IT steering committee in IS function.	
	1.3 Evaluation of planning function.	
	1.3.1 Identify the goals of the IT department considering the business goals. (long term & short term goals)	
	1.3.2 Identify the resources necessary to achieve the goals. (h/w, s/w, people)	
	1.3.3 Identify the cost & the benefits of acquiring the resources.	
	1.3.4 Activity plan to achieve the goals and the objectives.	
	1.3.5 IT budget.	
	1.4 Evaluation of organizing function.	
	1.4.1 Location of the information system function in the company organization structure.	
	1.4.2 Staffing. (recruiting, development, termination)	
	1.4.3 The structure of the IT department.	
	1.4.4 Roles and responsibilities of the IT department.	
	1.4.5 Coordination/communication between the other departments.	
	1.5 Evaluation of leading function.	
	1.5.1 Motivation of staff.	
	1.5.2 Communication between employer and employees.	
	1.5.3 Career development, training and guidance at individual level.	
	1.5.4 Individual goal setting and Performance evaluation.	
	1.6 Evaluation of controlling function.	
	1.6.1 Actual results against the plans.	
	1.6.2 Controlling the IS activities. (policies, procedures, standards)	
	1.6.3 Compliance monitoring & corrective actions.	
	1.6.4 Controlling of users.(service level agreements, transfer pricing etc)	
2. System Implementation (acquisition & development)	2.1 Problem /opportunity analysis (SWOT analysis) carried out.	
	2.2 Feasibility of the project carried out. (economic, technical etc)	
	2.3 Detail investigation of the existing system and the problems faced identified.	
	2.4 Requirement of the new system identified.	
	2.5 Organization job design (business process reengineering) carried out.	
	2.6 Solution design, construction and testing processes done.	
	2.7 Identifying hardware/system software requirements (sizing) carried out and acquired.	
	2.8 Operational procedures developed, the users trained for their tasks, procedure manuals, training manuals available.	
	2.9 Conversion process from existing system to new system done.(e.g. data cleansing before migration, data migration & testing , parallel run etc)	
	2.10 User acceptance obtained. (users of the system have actively participated in developing the solution)	
	2.11 Post implementation review conducted to identify the effectiveness of the implementation.	
3. Availability of Resources for the Production Operation	3.1 The availability and reliability standards (service level agreements) established for the resources. (applications, system, network etc)	
	3.2 Data availability to assess the availability of the resources. (mean time between failures (MTBF), mean time to repair (MTTR))	
	3.3 Actions been taken to improve Reliability (MTBF) and Maintainability. (MTTR)	
	3.4 Availability of the server environment for the production operation.	

	3.5 Availability of the database & application software for the production operation.	
	3.6 Availability of the network environment.	
	3.7 Availability of desktop environment.	
	3.8 Availability of peripherals.	
4. Performance Monitoring & Tuning	4.1 Identify the resources to be tracked & managed. (application, system, network, peripherals etc)	
	4.2 Performance parameters such as response time, transaction volumes, service level during the peak periods etc are identified.	
	4.3 The priorities of resource allocation for different processes identified.	
	4.4 Decided the performance indicators. (what to measure, when and how to measure etc)	
	4.5 Analyze the performance indicators to identify the load imbalances and bottlenecks.	
	4.6 The way to determine what should be done to improve the performance.	
	4.7 Timely improving the system performance by tuning, balancing the system, performance trouble shooting, reconfiguring etc.	
	4.8 Timely reporting the results to the relevant parties like capacity planners, senior management etc.	
5. Capacity Planning	5.1 Identify the key resources to be planed. (server, database, network, peripherals, desktop)	
	5.2 Measure the utilization and performance of the resources currently available. (performance monitoring)	
	5.3 Identify the excess capacity.	
	5.4 Workload forecasting from the relevant parties/users.	
	5.5 Map the work load forecast into resource requirement.	
	5.6 Predict what time the existing capacity will be over.	
	5.7 Develop the resources acquisition plan to meet the future requirements.	
6. Problem Management/ Technical Support	6.1 The procedures adapted to inform the problems identified.	
	6.2 Recording mechanism of the problems.	
	6.3 Timely escalating the problem and user acceptance.	
	6.4 Analyze the trends of the problems, implementing remedial measures to control the problems.	
	6.5 Technical support for end users.	
	6.6 Training the end users in IT activities.	
7. Change Management	7.1 Role of the change control board to cope up with the change management.	
	7.2 Formal change request procedures been adopted to request a change.	
	7.3 Analyze the necessity of the change (cost benefit analysis) and the impact of the change.	
	7.4 Approve the changes for implementation.	
	7.5 Prioritize and schedule the changes of the requests.	
	7.6 Design, construction and test the change.	
	7.7 Implement and acceptance of the change.	
	7.8 Follow up process of the change carried out.	
8. Security Management	8.1 Identify the information system assets.	
	8.2 Value the information system assets.	
	8.3 Identify the threats faced by each and every resource.	
	8.4 Threats likelihood assessment. (possibility of occurring the threats)	
	8.5 Exposure analysis. (the extent of the exposure of the resources to the threat)	
	8.6 Controls adjustment to overcome the threats.	
	8.7 Reporting to the management.	

9. Disaster Recovery	9.1 Emergency plan. (the actions to be taken, persons to be informed etc)	
	9.2 Backup plan. (types of backups, frequency, procedure, responsible person, storage etc)	
	9.3 Recovery plan.	
	9.4 Test plan.	
	9.5 The level of the insurance coverage of the IS resources.	
10. Document Management	10.1 Availability of the documentation of the hardware software configuration, policies, procedures , operational manuals etc.	
	10.2 The ownership of the document defined. (created , checked, approved, used etc)	
	10.3 The accuracy and thoroughness of the documents.	
	10.4 The format and readability of the documents.	
	10.5 The updateability and the currency of the documents.	
	10.6 Accessibility and the storage of the documents.	
	10.7 Usability and effectiveness of the documents.	
11. Procurement Management	11.1 Procurement planning. (what to procure and when, what to outsource, etc)	
	11.2 Solicitation planning. (identify the product requirement, potential sources, preparing RFPs, developing evaluation criteria etc)	
	11.3 Solicitation. (obtaining the quotations, bids, offers or proposals as appropriate)	
	11.4 Source selection. (evaluating prospective vendors, negotiating contracts and awarding the contact)	
	11.5 Contract administration. (monitoring contact performance, contact modification etc)	
	11.6 Contract closure. (completion and the settlement of the contract)	
12. Internal Auditing/ Quality Management	12.1 The existence of the internal audit /quality control department.	
	12.2 Identify and develop the quality goals.	
	12.3 Developing and & maintaining standards for IS function.	
	12.4 Monitoring the compliance with QA standards.	
	12.5 Identifying the areas for improvement.	
	12.6 Regular Reporting to the management of QA function.	
	12.7 Training of QA standards and procedures of the users.	

Please write comments if any

ANNEXURE 3: DETAILS RESULT SHEET

Organization	1	2	3	4	5	6	7	8	9	10
Industry	Eng	Manufac	Automob	Invest	Telecom	Group	Cargo	Retail	Group	Bank
Turnover		50M			500M	13B				
IT budget		1M			5M	5M				
Staff	25	7100	200	70	80	400			250	
IT staff	Outsource	5	5	4	8	25	5	4	10	20
Period End (month)	March	March	March	March	Dec	March	March	March	March	March
Period End(year)	2006	2006	2006	2006	2005	2006	2006	2006	2006	2006
1.1 Senior management involvement in Information System (IS)	1	6	5	3	3	8	7	5	7	4
1.2 Role of the IT steering committee in IS function.	0	5	4	NA	1	8	6	5	7	4
1.3.1 Identify the goals of the IT department considering the	2	3	4	2	3	6	5	5	8	5
1.3.2 Identify the resources necessary to achieve the goals. (h/w,	3	5	3	2	5	6	5	5	7	5
1.3.3 Identify the cost & the benefits of acquiring the resources.	3	6	4	2	4	5	5	5	7	5
1.3.4 Activity plan to achieve the goals and the objectives.	4	6	3	1	3	7	5	5	8	6
1.3.5 IT budget.	5	5	2	5	3	7	NA	NA	7	6
1.3 Planing function.	3.40	5.00	3.80	2.40	3.60	6.20	5.00	5.00	7.40	5.40
1.4.1 Location of the information system function in the company	2	3	5	4	5	7	6	6	8	4
1.4.2 Staffing. (recruiting, development, termination)	NA	7	5	4	3	6	6	6	7	4
1.4.3 The structure of the IT department.	NA	6	4	1	3	9	5	6	7	4
1.4.4 Roles and responsibilities of the IT department.	NA	6	4	2	3	7	6	6	8	4
1.4.5 Coordination/communication between the other departments.	2	5	4	2	3	7	6	6	8	5
1.4 Organizing function.	2.00	5.40	4.60	2.60	3.40	7.20	5.80	6.00	7.60	4.20
1.5.1 Motivation of staff.	2	6	5	3	2	5	5	5	6	6
1.5.2 Communication between employer and employees.	3	7	5	NA	3	7	5	5	8	6
1.5.3 Career development, training and guidance at individual level.	2	8	2	4	3	7	5	5	8	6
1.5.4 Individual goal setting and Performance evaluation.	2	6	4	3	3	5	5	5	7	6
1.5 Leading function.	2.25	6.75	4.00	3.33	2.75	6.00	5.00	5.00	7.25	6.00
1.6.1 Actual results against the plans.	2	6	2	2	4	7	5	5	7	4
1.6.2 Controlling the IS activities. (policies, procedures, standards)	0	6	1	3	5	7	5	5	5	4
1.6.3 Compliance monitoring & corrective actions.	2	6	2	3	3	7	5	4	6	5
1.6.4 Controlling of users.(service level agreements, transfer pricing	NA	6	4	4	3	7	5	4	7	5
1.6 Controling function.	1.33	6.00	2.25	3.00	3.75	7.00	5.00	4.50	6.25	4.50
1 General Management	1.66	5.69	3.94	2.87	2.92	7.07	5.63	5.08	7.08	4.68
2.1 Problem /opportunity analysis (SWOT analysis) carried out.	NA	6	4	4	1	4	4	4	5	3
2.2 Feasibility of the project carried out. (economic, technical etc)	NA	6	4	2	1	4	4	4	8	3

2.3	Detail Investigation of the existing system and the problems faced	6	6	3	3	1	7	4	4	7	4
2.4	Requirement of the new system identified.	NA	7	2	4	2	7	4	4	7	4
2.5	Organization job design (business process reengineering) carried	NA	6	3	4	3	5	4	4	6	3
2.6	Solution design, construction and testing processes done.	6	6	4	2	4	6	4	4	NA	4
2.7	Identifying hardware/system software requirements (sizing) carried	6	6	3	3	5	5	5	4	8	4
2.8	Operational procedures developed, the users trained for their tasks,	5	6	2	2	1	7	4	4	8	3
2.9	Conversion process from existing system to new system done.(e.g.	NA	5	4	NA	3	7	4	4	8	4
2.10	User acceptance obtained. (users of the system have actively	5	7	1	1	2	4	4	4	6	4
2.11	Post implementation review conducted to identify the effectiveness	5	7	1	NA	1	3	3	3	6	2
2	System acquisition & Development	5.50	6.18	2.82	2.78	2.18	5.36	4.00	3.91	6.90	3.45
3.1	The availability and reliability standards (service level agreements)	5	6	3	4	3	5	5	4	6	4
3.2	Data availability to assess the availability of the resources. (mean	2	7	4	4	1	0	5	4	6	4
3.3	Actions been taken to improve Reliability (MTBF) and	2	6	4	3	1	0	5	4	7	4
3.4	Availability of the server environment for the production operation.	2	6	4	2	6	5	4	4	8	4
3.5	Availability of the database & application software for the	7	6	3	2	6	8	6	4	8	4
3.6	Availability of the network environment.	7	7	7	4	6	8	6	5	8	4
3.7	Availability of desktop environment.	7	6	6	4	6	8	6	5	8	4
3.8	Availability of peripherals & facilities.	5	7	6	3	6	8	6	5	8	4
3	Availability	4.63	6.38	4.63	3.25	4.38	5.25	5.38	4.38	7.38	4.00
4.1	Identify the resources to be tracked & managed. (application,	3	6	5	2	3	4	NA	5	7	4
4.2	Performance parameters such as response time, transaction	5	6	3	4	3	4	5	5	7	4
4.3	The priorities of resource allocation for different processes	3	7	4	4	1	4	5	4	7	5
4.4	Decided the performance indicators. (what to measure, when and	4	7	4	3	2	3	5	4	5	4
4.5	Analyze the performance indicators to identify the load imbalances	5	6	3	3	1	7	5	4	4	4
4.6	The way to determine what should be done to improve the	4	7	2	4	2	3	5	4	6	4
4.7	Timely improving the system performance by tuning, balancing the	5	7	4	2	2	8	5	4	8	4
4.8	Timely reporting the results to the relevant parties like capacity	4	6	4	2	2	8	5	4	5	4
4	Performance Monitoring	3.88	6.50	3.63	3.00	2.00	5.13	5.00	4.25	6.13	4.13
5.1	Identify the key resources to be planed. (server, database, network,	5	6	5	1	4	7	5	5	8	5
5.2	Measure the utilization and performance of the resources currently	5	6	5	2	4	7	5	5	7	4
5.3	Identify the excess capacity.	4	4	4	0	3	2	5	5	4	4
5.4	Workload forecasting from the relevant parties/users.	5	6	4	0	2	5	5	5	4	4
5.5	Map the work load forecast into resource requirement.	5	7	5	3	3	3	5	5	4	4
5.6	Predict what time the existing capacity will be over.	5	7	4	4	1	5	5	5	3	4
5.7	Develop the resources acquisition plan to meet the future	3	6	3	2	3	8	5	4	3	3
5	Capacity Planning	4.57	6.00	4.29	1.71	2.86	5.29	5.00	4.86	4.71	4.00

6.1 The procedures adapted to inform the problems identified.	5	6	4	2	5	7	3	4	6	4
6.2 Recording mechanism of the problems.	2	7	4	2	5	7	3	6	2	4
6.3 Timely escalating the problem and user acceptance.	5	6	2	3	5	7	3	6	6	5
6.4 Analyze the trends of the problems, implementing remedial	4	7	2	3	3	8	3	6	7	5
6.5 Technical support for end users.	5	6	2	5	5	8	3	6	7	5
6.6 Training the end users in IT activities.	2	7	1	2	3	9	3	5	7	4
6 Problem Management	3.83	6.50	2.50	2.83	4.33	7.67	3.00	5.50	5.83	4.50
7.1 Role of the change control board to cope up with the change	4	6	3	1	2	5	3	4	7	4
7.2 Formal change request procedures been adopted to request a	2	5	2	0	2	8	3	4	2	4
7.3 Analyze the necessity of the change (cost benefit analysis) and the	2	6	2	2	3	3	3	4	5	4
7.4 Approve the changes for implementation.	4	7	3	3	2	5	3	4	4	5
7.5 Prioritize and schedule the changes of the requests.	4	6	3	2	3	4	3	4	6	4
7.6 Design, construction and test the change.	4	7	2	2	3	5	3	4	7	4
7.7 Implement and acceptance of the change.	4	6	2	1	2	3	3	4	7	4
7.8 Follow up process of the change carried out.	2	7	2	2	2	5	3	4	6	4
7 Change Management	3.25	6.25	2.38	1.63	2.38	4.75	3.00	4.00	5.50	4.13
8.1 Identify the information system assets.	2	7	4	3	4	5	3	5	7	4
8.2 Value the information system assets.	2	6	5	4	2	7	3	5	6	4
8.3 Identify the threats faced by each and every resource.	2	7	4	2	3	5	3	4	6	4
8.4 Threats likelihood assessment. (possibility of occurring the threats)	2	6	1	1	3	3	3	4	6	5
8.5 Exposure analysis. (the extent of the exposure of the resources to	2	7	4	0	2	3	3	4	6	4
8.6 Controls adjustment to overcome the threats.	2	6	4	1	5	5	3	4	6	4
8.7 Reporting to the management.	2	7	4	1	4	5	3	4	7	4
8 Security Management	2.00	6.57	3.71	1.71	3.29	4.71	3.00	4.29	6.29	4.14
9.1 Emergency plan. (the actions to be taken, persons to be informed	1	6	4	0	2	5	2	3	2	4
9.2 Backup plan. (types of backups, frequency, procedure, responsible	2	7	5	0	3	6	2	2	4	4
9.3 Recovery plan.	1	6	5	1	4	7	2	2	2	4
9.4 Test plan.	5	7	3	0	4	3	4	2	3	4
9.5 The level of the insurance coverage of the IS resources.	3	6	2	2	2	2	5	3	3	4
9 Disaster Recovery	2.40	6.40	3.80	0.60	3.00	4.60	3.00	2.40	2.80	4.00
10.1 Availability of the documentation of the hardware software	2	7	3	2	2	3	5	4	3	4
10.2 The ownership of the document defined. (created , checked,	2	5	3	2	3	3	5	4	3	3
10.3 The accuracy and thoroughness of the documents.	2	6	2	3	2	3	5	4	4	3
10.4 The format and readability of the documents.	2	6	1	4	3	2	5	4	2	3
10.5 The updateability and the currency of the documents.	2	7	1	5	2	2	5	3	3	4
10.6 Accessibility and the storage of the documents.	2	6	2	6	2	6	5	4	2	4

10.7 Usability and effectiveness of the documents.	2	7	2	4	2	5	5	4	2	4
10 Document Management	2.00	6.29	2.00	3.71	2.29	3.43	5.00	3.86	2.71	3.57
11.1 Procurement planning. (what to procure and when, what to	6	6	4	5	2	6	5	4	7	4
11.2 Solicitation planning. (identify the product requirement, potential	NA	7	3	3	2	7	5	3	7	4
11.3 Solicitation. (obtaining the quotations, bids, offers or proposals as	6	6	3	4	5	6	5	3	6	4
11.4 Source selection. (evaluating prospective vendors, negotiating	7	6	4	4	5	7	5	3	6	4
11.5 Contract administration. (monitoring contact performance, contact	3	6	4	3	5	7	5	3	6	4
11.6 Contract closure. (completion and the settlement of the contract)	NA	6	NA	4	1	3	5	3	5	4
11 Procurement Management	5.50	6.17	3.60	3.83	3.33	6.00	5.00	3.17	6.17	4.00
12.1 The existence of the internal audit /quality control department.	0	7	0	1	2	3	3	2	4	3
12.2 Identify and develop the quality goals.	0	6	0	0	3	1	3	2	3	4
12.3 Developing and & maintaining standards for IS function.	0	7	1	1	2	2	3	2	4	4
12.4 Monitoring the compliance with QA standards.	0	6	1	1	3	4	3	2	3	4
12.5 Identifying the areas for improvement.	2	7	1	3	3	5	3	2	4	4
12.6 Regular Reporting to the management of QA function.	0	6	3	1	3	5	3	2	3	4
12.7 Training of QA standards and procedures of the users.	0	7	0	1	2	4	3	2	4	4
12 Quality Management	0.29	6.57	0.86	1.14	2.57	3.43	3.00	2.00	3.57	3.86
Overall Assessment	3.29	6.29	3.18	3.42	2.96	5.22	4.17	3.97	5.42	4.04

Summary (Average values as percentage)

Organization	1	2	3	4	5	6	7	8	9	10
1 General Management	16.63	56.92	39.42	28.70	29.17	70.67	56.33	50.83	70.83	46.83
2 System acquisition & Development	55.00	61.82	28.18	27.80	21.82	53.64	40.00	39.09	69.00	34.55
3 Availability	46.25	63.75	46.25	32.50	43.75	52.50	53.75	43.75	73.75	40.00
4 Performance Monitoring	38.75	65.00	36.25	30.00	20.00	51.25	50.00	42.50	61.25	41.25
5 Capacity Planning	45.71	60.00	42.86	17.14	28.57	52.86	50.00	48.57	47.14	40.00
6 Problem Management	38.33	65.00	25.00	28.33	43.33	76.67	30.00	55.00	58.33	45.00
7 Change Management	32.50	62.50	23.75	16.25	23.75	47.50	30.00	40.00	55.00	41.25
8 Security Management	20.00	65.71	37.14	17.14	32.86	47.14	30.00	42.86	62.86	41.43
9 Disaster Recovery	24.00	64.00	38.00	6.00	30.00	46.00	30.00	24.00	28.00	40.00
10 Document Management	20.00	62.86	20.00	37.14	22.86	34.29	50.00	38.57	27.14	35.71
11 Procurement Management	55.00	61.67	36.00	38.33	33.33	60.00	50.00	31.67	61.67	40.00
12 Quality Management	2.86	65.71	8.57	11.43	25.71	34.29	30.00	20.00	35.71	38.57
Overall Assessment	32.92	62.91	31.78	24.23	29.60	52.23	41.67	39.74	54.22	40.38

Organization	11	12	13	14	15	16	17	18	19	20
Industry	Retail	Bank	Hotel	Automob	Atomob	Manufac		Ruber	Shipping	Travel
Turnover										
IT budget										
Staff	40	120	80							
IT staff	5	30	2	10	4	12	6	12		8
Period End (month)	March	Dec	March	March	March	March	Dec	March	March	March
Period End(year)	2006	2005	2006	2006	2006	2006	2005	2006	2006	2006
1.1 Senior management involvement in Information System (IS)	6	6	6	8	8	7	8	7	4	4
1.2 Role of the IT steering committee in IS function.	6	5	6	7	5	7	NA	7	4	4
1.3.1 Identify the goals of the IT department considering the	6	4	7	8	4	6	3	6	4	4
1.3.2 Identify the resources necessary to achieve the goals. (h/w,	7	6	7	7	6	6	4	6	4	4
1.3.3 Identify the cost & the benefits of acquiring the resources.	6	6	8	7	6	6	NA	6	4	4
1.3.4 Activity plan to achieve the goals and the objectives.	6	7	4	7	6	6	NA	6	4	4
1.3.5 IT budget.	6	6	7	7	6	NA	3	NA	4	4
1.3 Planing function.	6.20	5.80	6.60	7.20	5.60	6.00	3.33	6.00	4.00	4.00
1.4.1 Location of the information system function in the	6	5	5	8	7	7	8	7	4	4
1.4.2 Staffing. (recruiting, development, termination)	6	7	6	7	6	6	4	6	4	4
1.4.3 The structure of the IT department	6	4	4	8	6	7	6	7	4	4
1.4.4 Roles and responsibilities of the IT department.	6	6	5	8	7	7	6	7	4	4
1.4.5 Coordination/communication between the other	6	7	6	8	7	7	8	7	4	4
1.4 Organizing function.	6.00	5.80	5.20	7.80	6.60	6.80	6.40	6.80	4.00	4.00
1.5.1 Motivation of staff.	6	6	6	7	5	7	NA	7	4	4
1.5.2 Communication between employer and employees.	6	7	6	7	5	7	6	7	4	4
1.5.3 Career development, training and guidance at individual	6	7	3	7	5	6	6	6	4	4
1.5.4 Individual goal setting and Performance evaluation.	6	7	6	7	5	6	2	6	4	4
1.5 Leading function.	6.00	6.75	5.25	7.00	5.00	6.50	4.67	6.50	4.00	4.00
1.6.1 Actual results against the plans.	6	8	5	6	7	7	NA	7	4	4
1.6.2 Controlling the IS activities. (policies, procedures,	6	9	3	6	7	7	2	7	4	4
1.6.3 Compliance monitoring & corrective actions.	6	7	5	6	6	7	6	7	4	4
1.6.4 Controlling of users.(service level agreements, transfer	7	7	3	6	6	7	2	7	4	4
1.6 Controling function.	6.25	7.75	4.00	6.00	6.50	7.00	3.33	7.00	4.00	4.00
1 General Management	6.08	6.18	5.51	7.17	6.12	6.72	5.15	6.72	4.00	4.00
2.1 Problem /opportunity analysis (SWOT analysis) carried out.	7	8	5	5	5	5	3	5	4	4
2.2 Feasibility of the project carried out. (economic, technical etc)	6	9	6	5	6	6	NA	6	5	4

2.3	Detail Investigation of the existing system and the problems faced	6	8	5	7	6	6	6	6	5	5
2.4	Requirement of the new system identified.	6	8	4	7	6	6	8	6	5	5
2.5	Organization job design (business process reengineering) carried	7	8	5	7	6	7	NA	7	5	5
2.6	Solution design, construction and testing processes done.	7	9	5	7	7	7	6	7	5	5
2.7	Identifying hardware/system software requirements (sizing)	6	6	5	7	7	7	6	7	5	5
2.8	Operational procedures developed, the users trained for their	6	7	3	7	7	7	3	7	5	5
2.9	Conversion process from existing system to new system	6	7	4	7	7	7	6	7	5	5
2.10	User acceptance obtained. (users of the system have actively	6	7	6	7	6	7	6	7	5	5
2.11	Post implementation review conducted to identify the	6	6	4	7	5	5	6	5	5	5
2	System acquisition & Development	6.27	7.55	4.73	6.64	6.18	6.36	5.55	6.36	4.91	4.82
3.1	The availability and reliability standards (service level	7	8	2	8	7	7	3	7	4	4
3.2	Data availability to assess the availability of the resources. (mean	7	1	3	7	7	7	7	7	4	4
3.3	Actions been taken to improve Reliability (MTBF) and	7	4	6	7	7	7	7	7	4	4
3.4	Availability of the server environment for the production	7	7	6	7	6	6	6	6	4	4
3.5	Availability of the database & application software for the	6	6	8	7	7	7	8	7	4	4
3.6	Availability of the network environment.	6	7	7	7	6	7	8	7	4	4
3.7	Availability of desktop environment.	6	7	8	7	6	7	3	7	4	4
3.8	Availability of peripherals & facilities.	6	6	8	7	7	7	8	7	5	5
3	Availability	6.50	5.75	6.00	7.13	6.63	6.88	6.25	6.88	4.13	4.13
4.1	Identify the resources to be tracked & managed. (application	6	7	5	7	7	7	6	7	5	5
4.2	Performance parameters such as response time, transaction	6	8	5	7	6	7	6	7	4	4
4.3	The priorities of resource allocation for different processes	6	8	NA	6	7	7	7	7	4	4
4.4	Decided the performance indicators. (what to measure, when and	6	8	5	6	7	7	7	7	4	4
4.5	Analyze the performance indicators to identify the load	6	8	4	6	7	7	7	7	4	4
4.6	The way to determine what should be done to improve the	6	8	4	6	6	6	7	7	4	4
4.7	Timely improving the system performance by tuning, balancing	6	8	4	6	5	5	7	6	4	4
4.8	Timely reporting the results to the relevant parties like capacity	6	8	6	6	5	5	6	5	5	5
4	Performance Monitoring	6.00	7.88	4.71	6.25	6.25	6.38	6.63	6.63	4.25	4.25
5.1	Identify the key resources to be planed. (server, database,	7	9	6	6	5	5	6	5	5	5
5.2	Measure the utilization and performance of the resources	7	8	6	6	5	5	6	5	5	5
5.3	Identify the excess capacity.	7	9	4	6	5	5	5	5	4	4
5.4	Workload forecasting from the relevant parties/users.	6	9	4	6	5	5	5	5	4	4
5.5	Map the work load forecast into resource requirement.	6	8	2	6	5	5	6	5	4	4
5.6	Predict what time the existing capacity will be over.	6	9	2	6	5	5	4	5	4	4
5.7	Develop the resources acquisition plan to meet the future	6	9	4	5	6	6	4	6	4	4
5	Capacity Planning	6.43	8.71	4.00	5.86	5.14	5.14	5.14	5.14	4.29	4.29

6.1	The procedures adapted to inform the problems identified.	6	6	2	5	4	4	4	4	4	4
6.2	Recording mechanism of the problems.	7	9	2	6	4	4	3	4	4	4
6.3	Timely escalating the problem and user acceptance.	7	9	4	6	4	4	NA	4	4	4
6.4	Analyze the trends of the problems, implementing remedial	6	8	NA	6	4	4	4	4	4	4
6.5	Technical support for end users.	6	8	6	6	5	5	5	5	4	4
6.6	Training the end users in IT activities.	6	8	6	6	5	5	5	5	4	4
6	Problem Management	6.33	8.00	4.00	5.83	4.33	4.33	4.20	4.33	4.00	4.00
7.1	Role of the change control board to cope up with the change	6	9	3	6	6	6	6	6	5	5
7.2	Formal change request procedures been adopted to request a	6	9	3	7	6	6	6	6	5	5
7.3	Analyze the necessity of the change (cost benefit analysis) and the	6	8	5	7	6	6	6	6	5	5
7.4	Approve the changes for implementation.	6	8	7	7	6	6	6	6	5	5
7.5	Prioritize and schedule the changes of the requests.	6	8	6	7	6	6	6	6	5	4
7.6	Design, construction and test the change.	6	8	6	7	6	6	6	6	4	4
7.7	Implement and acceptance of the change.	6	9	7	7	6	6	6	6	4	4
7.8	Follow up process of the change carried out.	6	7	6	7	6	6	6	6	4	4
7	Change Management	6.00	8.25	5.38	6.88	6.00	6.00	6.00	6.00	4.63	4.50
8.1	Identify the information system assets.	6	8	5	7	5	6	6	7	5	5
8.2	Value the information system assets.	6	7	6	7	7	7	7	7	5	5
8.3	Identify the threats faced by each and every resource.	6	7	6	7	7	7	7	7	4	4
8.4	Threats likelihood assessment. (possibility of occurring the	6	9	6	7	7	7	7	7	4	4
8.5	Exposure analysis. (the extent of the exposure of the resources to	6	8	4	7	5	5	6	5	4	4
8.6	Controls adjustment to overcome the threats.	6	7	4	7	5	5	6	5	4	4
8.7	Reporting to the management.	6	7	5	7	3	5	6	5	4	4
8	Security Management	6.00	7.57	5.14	7.00	5.57	6.00	6.43	6.14	4.29	4.29
9.1	Emergency plan. (the actions to be taken, persons to be informed	7	8	1	6	4	3	3	3	4	5
9.2	Backup plan. (types of backups, frequency, procedure,	7	7	5	7	5	5	5	5	4	5
9.3	Recovery plan.	7	7	5	7	4	3	3	3	4	5
9.4	Test plan.	7	8	2	7	5	5	5	5	4	5
9.5	The level of the insurance coverage of the IS resources.	7	7	6	7	5	5	5	5	4	4
9	Disaster Recovery	7.00	7.40	3.80	6.80	4.60	4.20	4.20	4.20	4.00	4.80
10.1	Availability of the documentation of the hardware software	6	7	2	7	6	6	6	6	4	4
10.2	The ownership of the document defined. (created , checked,	6	7	NA	7	6	6	6	6	4	4
10.3	The accuracy and thoroughness of the documents.	6	8	4	7	6	6	6	6	4	4
10.4	The format and readability of the documents.	6	7	5	7	6	6	6	6	4	4
10.5	The updateability and the currency of the documents.	6	7	6	7	6	6	6	6	4	4
10.6	Accessibility and the storage of the documents.	6	7	4	7	6	6	6	6	4	4

10.7 Usability and effectiveness of the documents.	6	8	6	7	6	6	6	6	4	4
10 Document Management	6.00	7.29	4.50	7.00	6.00	6.00	6.00	6.00	4.00	4.00
11.1 Procurement planning. (what to procure and when, what to	7	9	7	7	6	6	6	6	4	5
11.2 Solicitation planning. (identify the product requirement, potential	7	8	6	7	7	6	6	6	4	5
11.3 Solicitation. (obtaining the quotations, bids, offers or proposals as	7	7	6	7	7	6	6	6	4	5
11.4 Source selection. (evaluating prospective vendors, negotiating	7	7	6	7	6	6	6	6	4	5
11.5 Contract administration. (monitoring contact performance, contact	6	8	5	7	6	6	6	6	4	4
11.6 Contract closure. (completion and the settlement of the contract)	6	9	6	7	6	6	6	6	4	4
11 Procurement Management	6.67	8.00	6.00	7.00	6.33	6.00	6.00	6.00	4.00	4.67
12.1 The existence of the internal audit /quality control department.	6	8	6	6	5	6	5	5	4	5
12.2 Identify and develop the quality goals.	6	7	4	6	6	5	6	6	4	4
12.3 Developing and & maintaining standards for IS function.	6	8	5	6	6	6	6	6	4	4
12.4 Monitoring the compliance with QA standards.	6	8	3	6	6	6	6	6	4	5
12.5 Identifying the areas for improvement.	6	8	4	6	6	6	6	6	4	4
12.6 Regular Reporting to the management of QA function.	6	8	3	6	6	6	6	6	4	4
12.7 Training of QA standards and procedures of the users.	6	8	2	6	6	6	6	6	4	4
12 Quality Management	6.00	7.86	3.86	6.00	5.86	5.86	5.86	5.86	4.00	4.29
Overall Assessment	6.27	7.54	4.80	6.63	5.76	5.82	5.62	5.85	4.21	4.33

Summary (Average values as percentage)

Organization	11	12	13	14	15	16	17	18	19	20
1 General Management	60.75	61.83	55.08	71.67	61.17	67.17	51.50	67.17	40.00	40.00
2 System acquisition & Development	62.73	75.45	47.27	66.36	61.82	63.64	55.50	63.64	49.09	48.18
3 Availability	65.00	57.50	60.00	71.25	66.25	68.75	62.50	68.75	41.25	41.25
4 Performance Monitoring	60.00	78.75	47.10	62.50	62.50	63.75	66.25	66.25	42.50	42.50
5 Capacity Planning	64.29	87.14	40.00	58.57	51.43	51.43	51.43	51.43	42.86	42.86
6 Problem Management	63.33	80.00	40.00	58.33	43.33	43.33	42.00	43.33	40.00	40.00
7 Change Management	60.00	82.50	53.75	68.75	60.00	60.00	60.00	60.00	46.25	45.00
8 Security Management	60.00	75.71	51.43	70.00	55.71	60.00	64.29	61.43	42.86	42.86
9 Disaster Recovery	70.00	74.00	38.00	68.00	46.00	42.00	42.00	42.00	40.00	48.00
10 Document Management	60.00	72.86	45.00	70.00	60.00	60.00	60.00	60.00	40.00	40.00
11 Procurement Management	66.67	80.00	60.00	70.00	63.33	60.00	60.00	60.00	40.00	46.67
12 Quality Management	60.00	78.57	38.57	60.00	58.57	58.57	58.57	58.57	40.00	42.86
Overall Assessment	62.73	75.36	48.02	66.29	57.51	58.22	56.17	58.55	42.07	43.35

Organization	21	22	23	24	25	26	27	28	29	30
Industry	NGO	Textile	Clothing	Eng	Manufac	Manufac	Food	Manufac	Banking	Telecom
Turnover										
IT budget										
Staff	50	30					100	50	1500	70
IT staff	2	6	5	5	5	9	26	1	150	20
Period End (month)	Dec	March	March	March	March	Dec	Dec			Aug
Period End(year)	2005	2006	2006	2006	2006	2005	2005	2006	2006	2006
1.1 Senior management involvement in Information System (IS)	8	6	4	4	5	5	7	2	10	6
1.2 Role of the IT steering committee in IS function.	8	7	4	4	5	NA	7	3	10	5
1.3.1 Identify the goals of the IT department considering the	6	6	7	7	7	7	6	4	9	5
1.3.2 Identify the resources necessary to achieve the goals. (h/w,	8	6	6	6	6	9	6	6	8	4
1.3.3 Identify the cost & the benefits of acquiring the resources.	7	5	5	5	5	8	6	5	9	5
1.3.4 Activity plan to achieve the goals and the objectives.	7	6	6	6	5	8	6	6	10	3
1.3.5 IT budget.	8	7	6	6	6	8	6	8	10	NA
1.3 Planing function.	7.20	6.00	6.00	6.00	5.80	8.00	6.00	5.80	9.20	4.25
1.4.1 Location of the information system function in the company.	5	5	6	5	5	9	6	6	9	10
1.4.2 Staffing. (recruiting, development, termination)	5	5	4	6	6	8	7	7	7	8
1.4.3 The structure of the IT department.	8	6	2	2	2	8	7	4	6	6
1.4.4 Roles and responsibilities of the IT department.	10	7	4	4	4	9	7	5	8	6
1.4.5 Coordination/communication between the other	NA	7	6	6	6	8	7	5	5	5
1.4 Organizing function.	6.50	6.00	4.20	4.60	4.60	8.40	6.80	5.40	7.00	7.00
1.5.1 Motivation of staff.	8	5	6	6	6	8	7	6	10	6
1.5.2 Communication between employer and employees.	10	4	6	6	6	8	7	7	10	NA
1.5.3 Career development, training and guidance at individual	6	4	4	4	4	8	7	8	9	NA
1.5.4 Individual goal setting and Performance evaluation.	4	5	6	6	6	NA	7	7	NA	NA
1.5 Leading function.	7.00	4.50	5.50	5.50	5.50	8.00	7.00	7.00	9.67	6.00
1.6.1 Actual results against the plans.	6	3	6	6	6	7	6	6	8	6
1.6.2 Controlling the IS activities. (policies, procedures,	7	6	4	4	4	8	6	5	6	5
1.6.3 Compliance monitoring & corrective actions.	7	6	4	4	4	7	6	6	6	7
1.6.4 Controlling of users.(service level agreements, transfer	6	7	2	2	2	6	6	7	7	7
1.6 Controling function.	6.50	5.50	4.00	4.00	4.00	7.00	6.00	6.00	6.75	6.25
1 General Management	7.20	5.83	4.62	4.68	4.98	7.28	6.63	4.87	8.77	5.75
2.1 Problem /opportunity analysis (SWOT analysis) carried out.	4	7	4	2	4	7	5	6	8	6
2.2 Feasibility of the project carried out. (economic, technical etc)	6	7	4	4	4	7	5	7	8	7

2.3	Detail Investigation of the existing system and the problems faced	5	5	2	2	2	5	5	8	10	6
2.4	Requirement of the new system identified.		6	2	2	2	6	5	7	10	6
2.5	Organization job design (business process reengineering) carried	7	7	2	2	2	6	5	6	9	5
2.6	Solution design, construction and testing processes done.	6	7	2	2	2	6	5	6	8	5
2.7	Identifying hardware/system software requirements (sizing) carried	5	7	4	4	4	7	6	5	7	6
2.8	Operational procedures developed, the users trained for their tasks,	5	6	4	4	4	7	6	7	8	7
2.9	Conversion process from existing system to new system done.(e.g.	6	6	4	4	4	7	6	6	8	6
2.10	User acceptance obtained. (users of the system have actively	6	6	2	2	2	7	6	7	6	7
2.11	Post implementation review conducted to identify the effectiveness	7	6	2	2	2	6	5	4	7	8
2	System acquisition & Development	5.18	6.36	2.91	2.73	2.91	6.45	5.36	6.27	8.09	6.27
3.1	The availability and reliability standards (service level	7	6	2	2	2	6	7	5	8	7
3.2	Data availability to assess the availability of the resources. (mean	7	5	4	4	4	6	7	6	7	6
3.3	Actions been taken to improve Reliability (MTBF) and	7	5	4	4	4	7	6	7	6	5
3.4	Availability of the server environment for the production	NA	6	4	4	4	6	7	6	5	6
3.5	Availability of the database & application software for the	5	6	4	4	4	8	7	6	6	7
3.6	Availability of the network environment.	7	6	4	4	4	8	7	6	7	6
3.7	Availability of desktop environment.	7	7	6	6	6	9	7	6	7	7
3.8	Availability of peripherals & facilities	7	7	6	6	6	8	7	6	7	8
3	Availability	6.71	6.00	4.25	4.25	4.25	7.25	6.88	6.00	6.63	6.50
4.1	Identify the resources to be tracked & managed. (application,	7	7	6	6	6	8	7	4	8	4
4.2	Performance parameters such as response time, transaction	6	7	4	4	4	7	7	5	9	6
4.3	The priorities of resource allocation for different processes	6	7	4	4	4	8	7	6	8	5
4.4	Decided the performance indicators. (what to measure, when and	6	7	4	4	4	8	7	5	7	7
4.5	Analyze the performance indicators to identify the load imbalances	6	6	4	4	4	8	7	6	8	8
4.6	The way to determine what should be done to improve the	6	5	4	4	6	7	7	7	9	9
4.7	Timely improving the system performance by tuning, balancing	7	5	6	6	5	8	7	7	7	7
4.8	Timely reporting the results to the relevant parties like capacity	7	6	5	5	6	7	7	7	6	7
4	Performance Monitoring	6.38	6.25	4.63	4.63	4.88	7.63	7.00	5.88	7.75	6.63
5.1	Identify the key resources to be planed. (server, database, network,	7	8	6	6	4	8	6	5	8	10
5.2	Measure the utilization and performance of the resources currently	7	6	4	4	4	7	6	7	7	10
5.3	Identify the excess capacity.	7	7	4	4	4	8	6	6	6	7
5.4	Workload forecasting from the relevant parties/users.	8	7	4	4	4	8	6	7	7	7
5.5	Map the work load forecast into resource requirement.	8	6	4	4	2	8	6	6	7	10
5.6	Predict what time the existing capacity will be over.	8	7	2	2	2	6	6	7	6	10
5.7	Develop the resources acquisition plan to meet the future	7	6	2	2	2	6	NA	7	3	6
5	Capacity Planning	7.43	6.71	3.71	3.71	3.14	7.29	6.00	6.43	6.29	8.57

6.1	The procedures adapted to inform the problems identified.	7	7	2	2	2	6	5	5	5	5
6.2	Recording mechanism of the problems.	8	5	2	2	2	7	6	5	7	6
6.3	Timely escalating the problem and user acceptance.	6	3	4	4	4	7	6	5	4	7
6.4	Analyze the trends of the problems, implementing remedial	7	3	4	4	4	8	6	4	8	8
6.5	Technical support for end users.	6	4	2	2	2	6	6	3	6	7
6.6	Training the end users in IT activities.	6	3	2	2	2	7	6	5	6	8
6	Problem Management	6.67	4.17	2.67	2.67	2.67	6.83	5.83	4.50	6.00	6.83
7.1	Role of the change control board to cope up with the change	7	6	5	5	5	8	4	3	7	7
7.2	Formal change request procedures been adopted to request a	7	6	2	2	2	7	4	8	5	5
7.3	Analyze the necessity of the change (cost benefit analysis) and the	7	7	2	2	2	8	4	7	6	8
7.4	Approve the changes for implementation.	8	6	4	4	4	7	4	6	8	10
7.5	Prioritize and schedule the changes of the requests.	7	5	6	6	6	8	4	6	7	9
7.6	Design, construction and test the change.	8	4	8	8	8	7	4	5	5	5
7.7	Implement and acceptance of the change.	8	6	8	8	8	8	4	5	6	6
7.8	Follow up process of the change carried out.	8	6	6	6	6	7	4	6	7	10
7	Change Management	7.50	5.75	5.13	5.13	5.13	7.50	4.00	5.75	6.38	7.50
8.1	Identify the information system assets.	6	7	4	4	4	8	7	7	7	9
8.2	Value the information system assets.	6	6	4	4	4	7	7	6	4	8
8.3	Identify the threats faced by each and every resource.	7	6	4	4	4	8	7	6	6	10
8.4	Threats likelihood assessment. (possibility of occurring the threats)	7	6	4	4	4	8	7	7	7	10
8.5	Exposure analysis. (the extent of the exposure of the resources to	7	6	6	6	6	8	7	6	6	8
8.6	Controls adjustment to overcome the threats.	6	7	6	6	6	7	7	6	7	7
8.7	Reporting to the management.	7	7	6	6	6	7	7	7	8	6
8	Security Management	6.57	6.43	4.86	4.86	4.86	7.57	7.00	6.43	6.43	8.29
9.1	Emergency plan. (the actions to be taken, persons to be informed	8	3	2	2	2	7	5	7	8	6
9.2	Backup plan. (types of backups, frequency, procedure, responsible	8	3	4	4	4	8	5	6	9	10
9.3	Recovery plan.	10	3	4	4	4	7	5	3	9	10
9.4	Test plan.	8	2	6	6	6	8	5	4	7	3
9.5	The level of the insurance coverage of the IS resources.	8	3	6	6	6	7	5	5	8	8
9	Disaster Recovery	8.40	2.80	4.40	4.40	4.40	7.40	5.00	5.00	8.20	7.40
10.1	Availability of the documentation of the hardware software	4	4	6	6	6	8	6	5	6	7
10.2	The ownership of the document defined. (created , checked,	4	4	4	4	4	8	6	7	6	6
10.3	The accuracy and thoroughness of the documents.	3	3	4	4	4	7	7	7	8	6
10.4	The format and readability of the documents.	4	2	4	4	4	9	7	6	8	5
10.5	The updateability and the currency of the documents.	4	5	4	4	4	9	7	5	7	7
10.6	Accessibility and the storage of the documents.	4	4	4	4	4	6	7	6	NA	8

10.7 Usability and effectiveness of the documents.	4	5	4	4	4	6	7	6	6	6
10 Document Management	3.86	3.86	4.29	4.29	4.29	7.57	6.71	6.00	6.83	6.43
11.1 Procurement planning. (what to procure and when, what to	6	6	6	6	6	7	7	7	7	8
11.2 Solicitation planning. (identify the product requirement, potential	6	5	6	6	6	6	7	5	8	7
11.3 Solicitation. (obtaining the quotations, bids, offers or proposals as	7	4	6	6	6	6	7	5	8	7
11.4 Source selection. (evaluating prospective vendors, negotiating	7	6	6	6	6	6	7	7	5	6
11.5 Contract administration. (monitoring contact performance, contact	6	5	6	4	4	6	7	6	6	5
11.6 Contract closure. (completion and the settlement of the contract)	6	5	4	6	6	7	6	6	7	7
11 Procurement Management	6.33	5.17	5.67	5.67	5.67	6.33	6.83	6.00	6.83	6.67
12.1 The existence of the internal audit /quality control department.	6	5	2	2	2	8	6	5	8	6
12.2 Identify and develop the quality goals.	6	5	2	2	2	8	6	6	7	7
12.3 Developing and & maintaining standards for IS function.	5	5	4	4	4	6	6	6	6	6
12.4 Monitoring the compliance with QA standards.	5	4	4	4	4	7	6	5	7	4
12.5 Identifying the areas for improvement.	5	6	2	2	2	6	6	6	7	6
12.6 Regular Reporting to the management of QA function.	10	6	4	4	4	6	6	7	8	7
12.7 Training of QA standards and procedures for the users.	8	6	4	4	4	5	6	6	7	4
12 Quality Management	6.43	5.29	3.14	3.14	3.14	6.57	6.00	5.86	7.14	5.71
Overall Assessment	6.55	5.38	4.19	4.18	4.19	7.14	6.10	5.75	7.11	6.88

Summary (Average values as percentage)

Organization	21	22	23	24	25	26	27	28	29	30
1 General Management	72.00	58.33	46.17	46.83	49.83	72.80	66.33	48.67	87.70	57.50
2 System acquisition & Development	51.82	63.64	29.09	27.27	29.09	64.55	53.64	62.73	80.91	62.73
3 Availability	67.10	60.00	42.50	42.50	42.50	72.50	68.75	60.00	66.25	65.00
4 Performance Monitoring	63.75	62.50	46.25	46.25	48.75	76.25	70.00	58.75	77.50	66.25
5 Capacity Planning	74.29	67.14	37.14	37.14	31.43	72.86	60.00	64.29	62.86	85.71
6 Problem Management	66.67	41.67	26.67	26.67	26.67	68.33	58.33	45.00	60.00	68.33
7 Change Management	75.00	57.50	51.25	51.25	51.25	75.00	40.00	57.50	63.75	75.00
8 Security Management	65.71	64.29	48.57	48.57	48.57	75.71	70.00	64.29	64.29	82.86
9 Disaster Recovery	84.00	28.00	44.00	44.00	44.00	74.00	50.00	50.00	82.00	74.00
10 Document Management	38.57	38.57	42.86	42.86	42.86	75.71	67.14	60.00	68.30	64.29
11 Procurement Management	63.33	51.67	56.67	56.67	56.67	63.33	68.33	60.00	68.33	66.67
12 Quality Management	64.29	52.86	31.43	31.43	31.43	65.71	60.00	58.57	71.43	57.14
Overall Assessment	65.54	53.85	41.88	41.79	41.92	71.40	61.04	57.48	71.11	68.79