Audit Check list 2: Criticality Assessment tool

Multiple IT systems may be in use in an organization. The SAI may not be interested in auditing all the IT applications in the government or a particular organization. Further, some applications may be mission critical applications with lapses having far reaching consequences (eg: eSeva or eCops in Andhra Pradesh) where the SAI may prefer to adopt a vigorous framework like CoBIT in conducting the audit. The SAI may not be interested in a comprehensive audit of a simple MIS in a non-critical department where the information generated by MIS is itself not being used by the organization in decision-making. The nature, extent, scope and rigour of the IT audit and the resources committed for the job are dependent upon the subjective assessment of the risk parameters or in other words, criticality of the application. In order to bring some objectivity into the process, though subjectivity cannot in total be avoided, the following criticality assessment tool may be used to categorise the applications based on criticality.

IT System Risk Assessment Mode *(figures in parentheses depict the points to be given for that parameter)*

	Name of the Office:		
	Preliminary Information		
A.	Name of the Entity		
B.	Nature of the Entity	Headquarters	
		Regional Office	
		Branch Office	
		Unit Office	
		All of the above	
C.	Name of the System		
D.	Short Description of the System		

Questions

1	**Does the system relate to any of the following**		
	Business Critical Operations For example, Airline/Railway reservations, trading operations, telecom, banking operations, bill generation, on-line bill payment, manufacturing and processing etc.	(30)	
	Name of the Office:		
	Preliminary Information		
	Support Functions	(25)	

	For example, Payroll, Inventory, Financial Accounting, Procurement, Marketing etc.		
	E-Governance	(30)	
2	**Investment made in the System**		
	Less than Rs.5 lakh	(5)	
	More than Rs.5 lakh less than Rs.25 lakh	(10)	
	More than Rs.25 lakh less than Rs. 50 lakh	(15)	
	More than Rs. 50 lakh less than Rs. 1 crore	(25)	
	More than Rs. 1 crore	(30)	
3	**General state of computerization in the entity. The entity has computerized**		
	Most of the Business processes	(30)	
	Most of the Accounting and Financial Processes	(25)	
	No business process	(0)	
4	**Number of PCs/Desktops used for the system**		
	More than 100	(30)	
	More than 50, less than 100	(25)	
	More than 20, less than 50	(15)	
	More than 10 less than 20	(10)	
	Less than 10	(5)	
5	**Is the system on the network?**		
	Yes		
	No		
	If the system is on the network, is it connected to		
	Internal LAN and/or on intranet?	(20)	
	WAN and MAN and/or on extranet?	(25)	
	Web based /public domain?	(30)	
6	**The system is functioning at**		
	Only one location	(10)	
	More than one, less than 5 locations	(20)	
	Name of the Office:		
	Preliminary Information		
	More than 5 locations	(30)	

	Is proposed to be expanded in more than one location	(25)	
7	**The entity is dependant on the system in as much as**		
	Outputs are used for business critical operations /revenue generation	(30)	
	Outputs are manually checked ***before*** making payments/raising bills	(10)	
	Outputs are used to prepare Financial Statements	(15)	
	Outputs are not used at all for payment/revenue purposes	(0)	
8	**Even though the system does not deal with financial functions, it processes data of public interest. The nature of data is such that, wrong data may lead to :**		
	Failure of business	(30)	
	Erosion of credibility of the Organization	(15)	
	Financial loss to the entity	(25)	
	None of the above	(0)	
9	**Do the public have access to such data either through web or any other means?**		
	Yes, Public can view the data in a dynamic manner	(15)	
	No, Public cannot view the data	(0)	
	Public can transact on-line	(30)	
10	**Does the System make use of direct links to third parties e.g. EDI**		
	Yes	(20)	
	No	(0)	
11	**Does the Organization have dedicated IT Staff**		
	Nil	(0)	
	Less than 10	(10)	
	More than 10, less than 30	(20)	
	More than 30, less than 70	(25)	
	More than 70	(30)	
12	**Approximately how many persons can be termed as the end-users of the system?**		
	Name of the Office:		
	Preliminary Information		
	Less than 5	(0)	

	More than 5, less than 25	(10)	
	More than 25, less than 70	(20)	
	More than 70, less than 150	(25)	
	More than 150	(30)	
13	**The system is in operation for**		
	More than 10 years	(5)	
	Less than 10 years but more than 5 years	(10)	
	Less than 5 years but more than 2 years	(20)	
	Less than 2 years	(20)	
14	**The system is based on**		
	Batch Processing	(10)	
	On Line Transaction Processing	(25)	
15	**Are there formal change management procedures?**		
	Yes	(0)	
	No	(20)	
	How often changes are made to the applications		
	More than 5 times in a year	(30)	
	Less than 5 times in a year more than twice in a year	(20)	
	Less than twice in a year	(10)	
	Not even once in a year	(5)	
16	**Does the entity have a documented and approved security policy?**		
	Yes	(5)	
	No	(20)	
17	**Does the entity use any security software?**		
	Yes	(5)	
	No	(20)	
18	**Does the entity have a Systems Security Officer?**		
	Yes	(5)	
	No	(10)	
	Name of the Office:		
	Preliminary Information		
19	**Does the entity have a documented and approved**		

	Disaster Recovery Plan?		
	Yes	(0)	
	No	(20)	
20	**Volume of data in the system(including off line data) is approximately**		
	More than 10 GB	(25)	
	More than 2 GB less than 10 GB	(15)	
	Less than 2 GB	(10)	
	Less than 1 GB	(5)	
	Total Score		

As per the IT system risk assessment tool given above, the points scored are graded below:

Points scored as per risk assessment tool	**Classification of risk**
Less than 150	Low
Between 150 and 300	Medium
More than 300	High