Template 22 : Understanding the IT environment

With increased automation of systems and processes amongst the public sector entities, it is necessary for the Internal Audit Function to gather and document information on the audit client's IT (Information Technology) systems. This information will enable the internal auditors gain an understanding of the client's hardware and software, IT staff and the nature and extent of any known exposures and review the controls specific to the audit client's IT systems as part of its regular audit process. Auditors may get in touch with the IT staff to obtain relevant information. The following standards highlight the importance of information technology in the audit process.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

2110.A2 – The internal audit activity must assess whether the information technology governance of the entity supports the entity's strategies and objectives.

An independent review of the IT systems by IT Auditors will be required where the IT environment is complex to gain increased assurance regarding their reliability, security and resilience of its IT systems.

Kindly complete the questionnaire carefully in as much detail as possible.

PART I : DOCUMENTING THE IT ENVIRONMENT

1. <u>IT Organization</u>

Obtain details of the IT Organization, include an IT entity chart if possible.

2. Main characteristics of systems and environments

For each business process, state the IT systems that support the initiation, processing, recording and reporting of transactions.

Business process/sub-process transaction	Application system	Transactions	Database	Operating system	Location	External links
List each business process	What is the name of the application system(s) used to process transactions in the business process?	Approximately how many transactions are processed by the application system during a given period?	Where is data processed on the application systems stored? What is the name and version of the database?	What operating system does the application(s) and database(s) run on – and version?	Where is the hardware and software physically located?	Are there any external links accessing data processed in this business process?

For each of the application systems, provide details about the type of application system, number and location of users and whether changes have been made during the period under review.

Application system name	Category of application system	Purpose	Modules within the application	Implementation date	Number and location of users	Changes during the period
	Is the application system*: - off the shelf - packaged - in-house developed / bespoke - ERP	What is the primary purpose of the application	What modules does the application have	When was the application system implemented?	How many users are there and where are they located i.e. Multi-location or multi-national?	Have there been any changes to the system (or reports generated from the system) during the period?

* Definitions:

- off the shelf - purchased from a vendor, implemented with minimal IT support and restricted from any changes being made
- packaged - bought from vendor, requiring IT support for implementation with customization /modification permitted
- in-house developed/bespoke – developed specifically for the entity internally or by a software developer, changes and developments can be made
- ERP – Enterprise Resource Planning systems consist of a number of integrated modules for multiple business processes/activities
- Multi-location or multi-national – are there multiple instances of the application in different locations, are there users in multiple locations

Security Software
Does the entity use security software other than that which is built into the application and operating systems?
Comments

Internal network
How are systems networked internally within the organization?
Comments

| |
| |

Perimeter network
What is the nature of any perimeter network, to allow authorized access and restrict unauthorized access from external parties?
Comments

Interfaces

Describe how data is passed from one system to another (if applicable)

Interface/journal name /description	Nature	Frequency	Manual/ Automated	Responsibility
	What data is contained in the interface?	*How often does the interface occur?*	*Is the interface manual (eg a manual posting) or automated?*	*Who is responsible for running the interface?*

Reliance on spreadsheets and reports

Spreadsheets and reports description	Nature and purpose	Frequency	Nature	Responsibility
	What data is contained in the spreadsheet/report?	*How is the spreadsheet/report produced?*	*What is the report/spreadsheet used for?*	*Who is responsible for producing the report / spreadsheet and who receives/uses it?*

3. **IT Activities during the period under review**

Developments

Have there been any new systems implemented or developments/upgrades to existing systems during the period under review?	YES / NO
Comments	
Where new systems/upgrades or changes to systems have been implemented, are these tested prior to running them?	YES / NO
Comments	

Hardware and software changes	
Has any new hardware or software been implemented or have there been any significant software enhancements during the period under review?	YES / NO
Comments	

Security changes

Have there been any significant changes in the IT security architecture or the administration of security?	YES / NO
Comments	

Problems	
Are there any known or developing problems with systems (e.g., frequent occurrences of financial system and data recoveries or other signs of instability)	YES / NO
Comments	

Data corruption	
Is there any known data corruption, security breaches or other incidents that could have an impact on the financial statements	YES / NO
Comments	

Management's responses to risks arising from information systems and technology
How has the management responded to risks arising from information systems and technology?
Comments

4. Other changes during the period under review

Changes in business activities and/or risks	
Have there been any significant changes in the entity's business activities or risks that could impact the ability of systems to reliably process and maintain transactions and balances, for example because of a change in the nature or volume of transactions?	YES / NO
Comments	

Changes in accounting or regulatory requirements

Significant changes in accounting or regulatory requirements that have system or business process implications	YES / NO
Comments	

Changes in staff	
Significant changes in operations or significant staff turnover	YES / NO
Comments	

Structure, policy and processes	
Have there been any significant changes in the entity structure or policies and procedures (including manual controls) within key business processes or within the IT function	YES / NO
Comments	

PART II: ASSESSING THE COMPLEXITY OF THE IT ENVIRONMENT

The purpose of this form is to enable the auditor to assess the general complexity of the entity's information system (IS) environment with a view to deciding whether or not to seek the assistance of the specialist IT auditor in evaluating entity's information systems controls and also to enable the auditors to assess the inherent risk relating to use of information technology by the entity.

For completing this form the auditor should

- review the understanding the IT environment questionnaire
- review last year's working papers : the auditor should confirm that the information remains up to date and accurate;
- tour the entity's computer facilities and observe its IT operations
- interview IT staff and Head of IT and the management responsible for financial operations
- review internal audit reports on IT controls
- Review key entity documents (the IT strategy, the business plan, expenditure profiles).

Key questions	Yes/No	WP ref	Remarks
A. Significant use of IT If the answer to the following question is negative, there is no need to evaluate entity's IT controls.			
Does the entity use IT systems and any application programme for any of its processes?			
B. Non- complex IT system If on the basis of the following questions it is determined that the entity is small or possesses a non-complicated IT environment , auditors may attempt review the general and application controls without seeking the assistance of specialist IT auditor			
Does the entity use a spreadsheet package or a standard, non-modified, off the shelf accounting package like QuickBooks, Ledger Works, and Quicken to process its financial information? Does the entity use mid- range accounting packages such as Navision, Great Plains, AccPac etc to process its financial information? If the entity uses either be-spoke (custom developed) or COTS (commercial off the shelf) systems to process its financial information which of the following modules have been computerized? ● GL ● Cash			

Key questions	Yes/No	WP ref	Remarks
• Payables • Receivables Is it true that there have been minimal, or no changes made to the financial systems since the last audit?			
C. Complex IT environment If the answer to the following questions are in the affirmative, the auditor will seek the assistance of the Specialist IT auditors.			
Does the entity's IS systems use local or wide area networks (LAN or WAN) or both? Does the entity use financial systems which may be characterized as online transaction processing systems? Are the financial applications supported by complex RDBMS (relational Database Management Systems) systems			
D. High risk IS environment			

Key questions	Yes/No	WP ref	Remarks
If the answers to the following questions are in the affirmative , the inherent risk relating to entity's usage of IT may be assessed as maximum			
Does the entity use or planning to introduce an enterprise resource planning (ERP) package Is the entity's IT Budget amounts to approx. 5-10% of entire entity budget ? Is there a significant risk from the entity's use of IT. This can be determined from reviewing any past history of IT related frauds, system failures, the entity's attitude to IT and computer controls			
E. Assessing Cyber Security Risk			
Are senior management and the governing body (audit committee, board of directors, etc.) aware of key risks related to cybersecurity. Do cybersecurity initiatives receive adequate support and priority?			
Has management performed a risk assessment to identify assets susceptible to cyber threats or security breaches, and has the potential impact (financial and nonfinancial) been assessed?			

Key questions	Yes/No	WP ref	Remarks
Are first and second lines of defense collaborating with their peers in the industry (e.g., conferences, networking forums, and webcasts) to keep current with new/emerging risks, common weaknesses, and cybersecurity breaches associated with cybersecurity?			
Are cybersecurity policies and procedures in place, and do employees and contractors receive cybersecurity awareness training on a periodic basis?			
Are IT processes designed and operating to detect cyber threats? Does management have sufficient monitoring controls in place?			
Are feedback mechanisms operating to give senior management and the board insight into the status of the entity's cybersecurity programs?			
Does management have an effective hotline or emergency procedure in place in the event of a cyberattack or threat? Have these been communicated to employees, contractors, and service providers?			
Is the internal audit activity capable of assessing processes and controls to mitigate cyber threats, or does the HIA need to consider additional resources with cybersecurity expertise?			
Does the entity maintain a list of third-party service providers that have system access, including those that store data externally (e.g., IT providers, cloud storage providers, payment processors)? Has an independent cybersecurity examination engagement been conducted to assess the effectiveness of the service entity's controls as a part of their cybersecurity risk management program?			

Key questions	Yes/No	WP ref	Remarks
Has internal audit adequately identified common cyber threats facing the entity (e.g., nation-states, cybercriminals, hacktivists, networked systems, cloud providers, suppliers, social media systems, malware), and incorporated these into the internal audit risk assessment and planning processes?			
F. IT Governance Audit			
Are IT and operational structures clearly defined?			
Are communication channels between IT leaders and organization leaders clearly defined?			
Are executives actively involved in the decision making processes related to IT?			
Does the Accounting Officer (and Heads of Department) have a clear understanding of IT?			
Does the entity strategy address IT? Is there an IT strategy?			
Are organizational improvements through IT resources evaluated?			

Key questions	Yes/No	WP ref	Remarks
Are the sourcing strategies clear and supported by SLAs?			
Are the IT costs known or detailed enough?			
Is it possible to track the organizational value delivered by IT initiatives?			
Are there measures of technical/operational and financial performance in IT?			

Conclusion:

Auditor's assessment of inherent risk from IT

High	
Medium	
Low	

	Date	Initials
Prepared by		
Reviewed by		