Audit Plan

The audit function should formulate both long-range and annual plans. Planning is a basic function necessary to describe what must be accomplished, include budgets of time and costs, and state priorities according to organizational goals and policies.

The objective of audit planning is to optimize the use of audit resources. To effectively allocate audit resources, internal audit departments must obtain a comprehensive understanding of the audit universe and the risks associated with each universe item.

The intent of the audit plan is to provide an overall approach within which audit engagements

can be conducted. It provides the guidance for auditing the organization’s integral processes.

Financial Application	IT Area / Vulnerability	Threat-Source	Likelihood Determination		Impact		Risk	Risk Rating[a]	Recommended Control	Action Priority
			Likelihood Level	Probability Assigned	Magnitude of Impact	Impact Level Value				
Financial Application #2 (FA2)	Information Security / FA2 owners do not periodically review user access privileges.	Unauthorized users (hackers, terminated employees, and insiders)	Very High	1.00	High	75	Users possess privileges that are not consistent with their job functions, allowing unauthorized or incorrect modifications to FA2's data, which could cause management decisions based upon misleading information.	75	User access privileges within FA2 are periodically reviewed by application owners to verify access privileges remain appropriate and consistent with job requirements.	Very High
	Information Security / Terminated user accounts are not removed from FA2.	Unauthorized users (terminated employees)	Very High	1.00	High	75	Terminated users can gain access to FA2 and view or modify its financial information.	75	The security administrator is notified of employees who have been terminated. Access privileges of such employees are immediately changed to reflect their new status.	Very High

Financial Application	IT Area / Vulnerability	Threat-Source	Likelihood Determination		Impact		Risk	Risk Rating[a]	Recommended Control	Action Priority
			Likelihood Level	Probability Assigned	Magnitude of Impact	Impact Level Value				
Financial Application #2 (FA2)	Information Security / FA2 owners do not periodically review user access privileges.	Unauthorized users (hackers, terminated employees, and insiders)	Very High	1.00	High	75	Users possess privileges that are not consistent with their job functions, allowing unauthorized or incorrect modifications to FA2's data, which could cause management decisions based upon misleading information.	75	User access privileges within FA2 are periodically reviewed by application owners to verify access privileges remain appropriate and consistent with job requirements.	Very High
	Information Security / Terminated user accounts are not removed from FA2.	Unauthorized users (terminated employees)	Very High	1.00	High	75	Terminated users can gain access to FA2 and view or modify its financial information.	75	The security administrator is notified of employees who have been terminated. Access privileges of such employees are immediately changed to reflect their new status.	Very High

Financial Application	IT Area / Vulnerability	Threat-Source	Likelihood Determination		Impact		Risk	Risk Rating[a]	Recommended Control	Action Priority
			Likelihood Level	Probability Assigned	Magnitude of Impact	Impact Level Value				
	Change Control Management / Test results for FA2 upgrades are not approved by management, prior to their implementation into production.	Unauthorized application changes and modifications	Low	0.25	High	75	FA2 changes are not properly authorized. Implementation of such changes could result in invalid or misleading data.	18.75	Changes to FA2 are tested and approved by management prior to their implementation in production in accordance with test plans and results.	Low

[a] Computed by multiplying the "Probability Assigned" and the "Impact Level Value."

IT audit plan, after gathering a comprehensive understanding of the audit universe and the risks associated with each universe item,should:

- 1. List the audit objectives and describe the context
- 2. Develop the audit schedule
- 3. Create the audit budget and define scope
- 4. List audit team members, describe audit tasks, determine deadlines

- Objectives and Context

The objective and context of the work are key elements in any audit environment and should not be overlooked. They are simply the basis by which all audits should be approached.

The objective is what is trying to be accomplished. The context is the environment in which the work will be performed.

- Audit Schedule

Internal auditing departments create annual audit schedules to gain agreement from the board on audit areas, communicate audit areas with the functional departments, and create a project/resource plan for the year. The audit schedule should be linked to current business objectives and risks based on their relative cost in terms of potential loss of goodwill, loss of revenue, or noncompliance with laws and regulations.

Annual schedule creation is the process of determining the total audit hours available, then assigning universe items (audit areas) to fill the available time.

- Audit Budget and Scoping

The scope of an audit defines the area(s) (e.g., relevant financial applications, databases, operating systems, networks, etc.) to be reviewed. The names of the financial applications and databases should also be described along with their hosting information (e.g., server location, etc.). The scope should clearly identify the critical business process supported by the selected financial application. This association typically justifies the relevance of the application and, hence, its inclusion as part of the audit. The scope should further state the general control areas, control objectives, and control activities that would undergo review.

Exhibit 3.4 Example of a Budget for an IT Audit

Company Name					
IT Budget					
Fiscal Year 20XX					
	Audit Professional				
Audit Area	*Staff/ Senior*	*Manager*	*Partner*	*Total Hours*	
Planning					
Review work papers from the prior year, if applicable; prepare IT budget; conduct planning meetings; prepare planning memo; prepare initial request of information and send to company personnel, etc.	3.0	1.0	0.0	4.0	
First year. Gather and document an understanding of the organization and its IT environment, including how the organization utilizes computer system and which applications impact critical business/financial processes, among others. *Subsequent years.* Review and update the understanding of the organization and its IT environment obtained from the prior year.	3.0	1.0	0.0	4.0	
Conduct planning meeting with company personnel.	1.0	1.0	1.0	3.0	
Subtotal	7.0	3.0	1.0	11.0	11%
Fieldwork					
Document/update understanding of the organization's IT environment and perform tests of IT controls *(per General Control IT area).*					
Information Systems Operations	16.0	0.0	0.0	16.0	
Information Security	17.0	0.0	0.0	17.0	
Change Control Management	20.0	0.0	0.0	20.0	
Subtotal	53.0	0.0	0.0	53.0	53%

Exhibit 3.4 (*Continued*) Example of a Budget for an IT Audit

Company Name					
IT Budget					
Fiscal Year 20XX					
	Audit Professional				
Audit Area	*Staff/ Senior*	*Manager*	*Partner*	*Total Hours*	
Review, Reporting, and Conclusion					
Review and document action(s) taken by company's Management to correct last year's IT audit findings/ deficiencies.	2.0	0.0	0.0	2.0	
Document IT audit findings/ deficiencies and opportunities to improve existing controls.	3.0	0.0	0.0	3.0	
Assess and classify identified IT audit findings/deficiencies.	1.0	0.0	0.0	1.0	
Draft IT Management letter listing all IT audit findings/deficiencies and opportunities to improve existing controls. Forward letter to IT Management for review.	0.0	1.0	1.0	2.0	
Conduct status meetings, internally or with IT personnel.	1.0	0.0	0.0	1.0	
Review work papers evidencing IT audit work performed.	0.0	9.0	4.0	13.0	
Exit meeting with IT personnel to discuss audit and results.	0.0	1.0	0.0	1.0	
Address and clear review notes from audit management (Manager and Partner) and conclude audit.	11.0	2.0	0.0	13.0	
Subtotal	18.0	13.0	5.0	36.0	36%
Grand Total	78.0	16.0	6.0	100.0	100%
			Staff/Senior	78.0	78%
			Manager	16.0	16%
			Partner	6.0	6%

Exhibit 3.5a Example of Scoping for Financial Applications

Company Name												
Financial Applications and their Association with Business Processes												
Fiscal Year 20XX												
Purpose: To identify relevant applications by mapping them to their corresponding business process(es). An "X" in the table on the right identifies the business process supported by the application. For example, the *SAP* application is used by (or supports) the *Financial Reporting*, *Expenditures*, *Inventory Management*, and *Revenue* business processes. This association typically justifies the relevance of the application and, hence, its inclusion as part of the audit.												
						Business Process Supported						
#	*Application*	*Brief Description*	*Processing Environment (Operating System Where the Application Is Installed On)*	*Database Management Software*	*Physical Hosting Location—Application and Database*	*Financial Reporting*	*Expenditures*	*Payroll & Personnel*	*Inventory Management*	*Investment*	*Revenue*	*Fixed Assets*
1	SAP	Includes the general ledger, expenditures, inventory management, and revenue accounting modules.	UNIX	Oracle	Local Data Center, Second Floor; Company's Headquarters [location]	X	X		X		X	
2	Infinium	Manages the payroll.	AS/400	Oracle	Local Data Center, Second Floor; Company's Headquarters [location]			X				

Exhibit 3.5a (*Continued*) Example of Scoping for Financial Applications

Company Name												
Financial Applications and their Association with Business Processes												
Fiscal Year 20XX												
Purpose: To identify relevant applications by mapping them to their corresponding business process(es). An "X" in the table on the right identifies the business process supported by the application. For example, the *SAP* application is used by (or supports) the *Financial Reporting, Expenditures, Inventory Management,* and *Revenue* business processes. This association typically justifies the relevance of the application and, hence, its inclusion as part of the audit.												
						Business Process Supported						
#	*Application*	*Brief Description*	*Processing Environment (Operating System Where the Application Is Installed On)*	*Database Management Software*	*Physical Hosting Location—Application and Database*	*Financial Reporting*	*Expenditures*	*Payroll & Personnel*	*Inventory Management*	*Investment*	*Revenue*	*Fixed Assets*
3	APS/2	Manages investments.	Windows	Oracle	Local Data Center, Second Floor; Company's Headquarters [location]					X		
4	Timberline	Manages long term and fixed assets.	Windows	Oracle	Local Data Center, Second Floor; Company's Headquarters [location]							X

Exhibit 3.5b Example of Scoping for General Computer Control Objectives and Activities

Company Name			
General Computer Controls Objectives and Activities Selected			
Fiscal Year 20XX			
#	*IT Area*	*Control Objective*	*Control Activity*
1	Information Systems Operations	ISO 1.00 - IT operations support adequate scheduling, execution, monitoring, and continuity of systems, programs, and processes to ensure the complete, accurate, and valid processing and recording of financial transactions.	ISO 1.01 - Batch and/or online processing is defined, timely executed, and monitored for successful completion. ISO 1.02 - Exceptions identified on batch and/or online processing are timely reviewed and corrected to ensure accurate, complete, and authorized processing of financial information.
2	Information Systems Operations	ISO 2.00 - The storage of financial information is appropriately managed, accurate, and complete.	ISO 2.02 - Automated backup tools have been implemented to manage retention data plans and schedules. ISO 2.04 - Tests for the readability of backups are performed on a periodic basis. Results support timely and successful restoration of backed up data.
3	Information Systems Operations	ISO 3.00 - Physical access is appropriately managed to safeguard relevant components of the IT infrastructure and the integrity of financial information.	ISO 3.02 - Physical access is authorized, monitored, and restricted to individuals who require such access to perform their job duties. Entry of unauthorized personnel is supervised and logged. The log is maintained and regularly reviewed by IT management.

4	Information Security	ISEC 1.00 - Security configuration of applications, databases, networks, and operating systems is adequately managed to protect against unauthorized changes to programs and data that may result in incomplete, inaccurate, or invalid processing or recording of financial information.	ISEC 1.02 - Formal policies and procedures define the organization's information security objectives and the responsibilities of employees with respect to the protection and disclosure of informational resources. Management monitors compliance with security policies and procedures, and agreement to these are evidenced by the signature of employees. ISEC 1.06 - Consistent with information security policies and procedures, local and remote users are required to authenticate to applications, databases, networks, and operating systems via passwords to enhance computer security.
5	Information Security	ISEC 2.00 - Adequate security is implemented to protect against unauthorized access and modifications of systems and information, which may result in the processing or recording of incomplete, inaccurate, or invalid financial information.	ISEC 2.02 - System owners authorize user accounts and the nature and extent of their access privileges. ISEC 2.04 - Users who have changed roles or tasks within the organization, or that have been transferred, or terminated are immediately informed to the security department for user account access revision in order to reflect the new and/or revised status. ISEC 2.05 - Transmission of sensitive information is encrypted consistent with security policies and procedures to protect its confidentiality.
6	Change Control Management	CCM 1.00 - Changes implemented in applications, databases, networks, and operating systems (altogether referred to as "system changes") are assessed for risk, authorized, and thoroughly documented to ensure desired results are adequate.	CCM 1.03 - Documentation related to the change implementation is adequate and complete. CCM 1.05 - Documentation related to the change implementation has been released and communicated to system users.

#	*IT Area*	*Control Objective*	*Control Activity*
8	Change Control Management	CCM 3.00 - Changes implemented in applications, databases, networks, and operating systems (altogether referred to as "system changes") are appropriately managed to reduce disruptions, unauthorized alterations, and errors which impact the accuracy, completeness, and valid processing and recording of financial information.	CCM 3.01 - Problems and errors encountered during the testing of system changes are identified, corrected, retested, followed up for correction, and documented.
9	Change Control Management	CCM 4.00 - Changes implemented in applications, databases, networks, and operating systems (altogether referred to as "system changes") are formally approved to support accurate, complete, and valid processing and recording of financial information.	CCM 4.04 - An overall review is performed by management after system changes have been implemented in the live or production environment to determine whether the objectives for implementing system changes were met.

- Audit Team, Tasks, and Deadlines
- The audit plan must include a section listing the members of the audit, their titles and positions, and the general tasks they will have. For instance, a typical audit involves staff members, seniors,managers, or senior managers, and a partner, principal, or director (PPD) who will be overseeing the entire audit.

At a staff level (usually those auditors with less than 3 years of experience), most of the field work is performed, including gathering documentation, meeting with personnel, and creating audit work papers, among others.

Senior-level auditors not only supervise the work of staff auditors, but guide them in performing the work (e.g., accompany staff auditors to meet with users, assist the staff in selecting what specific information should be gathered, how to document such information in the working papers, etc.).

The managers or senior managers (senior managers are typically involved as part of large audits) that supervise the audit work prepared by the staff and reviewed by the senior. Managers perform detailed reviews of the work papers and ensure the audit objectives have been achieved. Managers meet frequently with audit clients, and provide them with audit status, preliminary findings identified, hours incurred and left to finish,etc. Managers also provide frequent status of the audit work to the PPD assigned, to which they report directly.

PPDs tend to rely on the detailed reviews performed by managers or senior managers, and also ensure the overall objectives of the audit have been achieved.

Deadlines should be well-thought of taking into account the information and resources that must be available to perform the audit work within the established requirements.

An audit planning memo (“planning memo”) is part of the auditor working papers and documents the sections just described. The planning memo is typically prepared by the audit engagement senior, and reviewed by the manager before submitting it to the PPD for approval. Appendix 1 shows the format of a typical IT planning memo, including the procedures which may be performed by an IT auditor in connection with an audit engagement. The planning memo may

be tailored for the specific facts and circumstances of the audit engagement. This includes removing sections which are not applicable. The memo in Appendix 1 includes some wording in italics

that is either enclosed within brackets or parentheses. This format is used to indicate information to be replaced as applicable, or that guides the completion of the memo.