Nguyen Thi Hong Trang

Internal Audit Methodology

Improve Internal Audit Methodology in the Case Company

Author Title Number of Pages Date	Nguyen Thi Hong Trang Internal Audit Methodology – Improve Internal Audit Methodology in the Case Company 32 pages + 4 appendices 24 November 2016
Degree	Master of Business Administration
Degree Programme	Master's Degree in Business Informatics
Instructor	Antti Hovi, Senior Lecturer

The purpose of this study was to identify improvement areas in the internal audit methodology used by the Internal Audit team at the case company which is the local subsidiary of a global financial group. The Internal Audit activity of the case company has been recently evaluated by the Institute of Internal Auditors. The overall quality assessment concludes that the Internal Audit activity has a charter, policies and processes that are in conformance with the Mandatory Guidance of the International Professional Practices Framework on Internal Auditing. However, the quality auditors have identified an issue related to traceability among audit documents. This study is aimed to identify root causes for the problem identified by the quality auditors and then suggest improvements to solve the problem.

The qualitative research methodology was utilized in this study. The study started with a thorough analysis of the current internal audit methodology and practice. Next, best practices on the areas of problem were gathered and analyzed based on a literature review and on the author's previous experience as a consultant of a global leading auditing and consulting company. Based on the results of the best practices review and considering also the objectives of the Internal Audit function and the International Professional Practices Framework, solutions to the problem were constructed.

The author recommends the Internal Audit management apply a risk-based approach in planning the internal audit jobs through performing a process risk analysis. The process risk analysis helps refine the audit objectives set in the Internal Audit activity plan and identify other significant areas of concern which need more internal auditors' efforts. In other words, it helps drive the internal audit engagement execution in a more effective and efficient way.

It is recommended that the Internal Audit methodology manual express and emphasize more clearly on the risk-based internal auditing approach and that the strategic objectives, associated risks and risk responses act as a central point connecting documents created throughout an audit cycle.

It is also recommended that the Internal Audit methodology manual underline requirements and/or criteria on traceability among audit documents as well as provide specific instructions on how audit documents should be documented to ensure a positive link among them.

Keywords	audit cycle, internal audit, internal audit methodology, internal audit processes, internal audit plan, risk assessment, risk-based audit

Helsinki
Metropolia
University of Applied Sciences

Contents

Helsinki
Metropolia
University of Applied Sciences

APPENDICES

1   INTRODUCTION

The internal auditing had its origins in ancient times (McNamee, 1995 and Chun in Castanheira at al, 2009). However, the internal auditing role only began to become significant in the management of an organization in the 1940s (Jin'e and Dunjia; Dittenhofer in Castanheira at al, 2009). It was also in 1941 that the Institute of Internal Auditors (IIA), which currently is the most internationally recognized professional association on internal auditing, was founded (Theiia.org, 2016a). The IIA sets international standards for the profession, acts as the principal researcher and educator of the profession, and is the only one provides globally accepted internal audit certifications.

According to Brink (1991), the internal auditing practice earlier than 1941 had a low organizational status and was part of the accounting function in the organization. Since then, with the improvements in audit methods and services, application of technology as well as strengthens in capabilities, internal auditing has gained a higher status in the organization (Brink, 1991). The head of an Internal Audit function is nowadays often a member of the organization's management team and the Internal Audit (IA) function is no longer part of the accounting function, rather it is a separate function independent from the rest of the organization.

Current internal audit practice has a significant role in supporting an organization achieve its objectives through the risk-based audit approach. Starting from the organization's strategies and objectives, internal auditors first identify and evaluate risks that may occur and prevent the organization from reaching its objectives, then verify how well the management is responding to those risks and finally provide objective and independent opinions on how things should be done or could be done better.

The IA function of the case company in this thesis also applies a risk-based audit approach for its activity. The function has recently gone through the first quality assessment by the IIA on the road to complete the IIA's Quality Assurance Review certification.   The overall assessment concludes that the Internal Audit activity is generally in conformance with the Mandatory Guidance of the International Professional Practice Framework on Internal Auditing (IPPF) (IIA, 2016). However, the IIA auditors have identified a traceability issue between audit planning document, risk & control assessment, work program and work papers in responding to the IPPF's Standards 2201 and 2210.

The purpose of this thesis is to find out root causes to the identified issue by analyzing the IA methodology currently practiced by the IA function together with exploring best practices on internal auditing, finally to suggest solutions to solve the issue.

1.1 Background information

1.1.1 Definition of Internal Auditing

According to the International Professional Practices Framework on Internal Auditing that is globally adopted as the formal guidance, internal auditing is

> an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (Theiia.org, 2016a).

The definition states three fundamental aspects of internal auditing: its purpose of helping an organization achieve its objectives, its nature of independence and objectivity and its scope covering the effectiveness and efficiency of risk management, control and governance processes.

1.1.2 International Professional Practices Framework on Internal Auditing

The International Professional Practices Framework (IPPF) is the framework issued by the IIA that imposes guidance to internal audit professionals globally. The IPPF is organized into two categories, mandatory guidance and recommended guidance as shown in Figure 1 below.

The Mandatory Guidance includes Core Principles, Definition of Internal Auditing, Code of Ethics and Standards. Integrity, objectivity, confidentiality and competency are principles of code of ethics as well as core principles of the internal auditing. The Standards category states "fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit performance" (Theiia.org, 2016b).
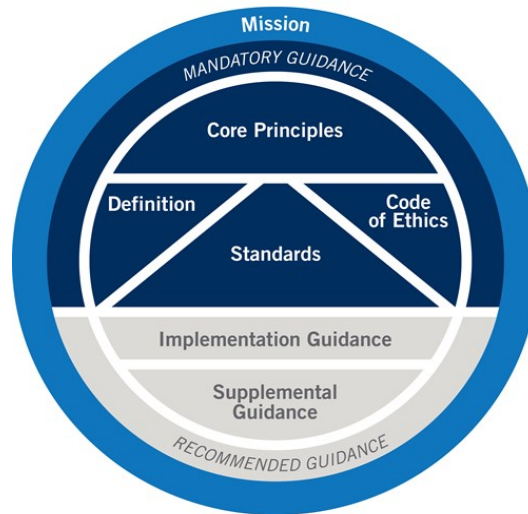
Figure 1. International Professional Practice Framework

(Theiia.org, 2016b)

Conformance with the principles established in the Mandatory Guidance is crucial for the internal auditing practice.

The Recommended Guidance describes "practices for effective implementation of the Definition of Internal Auditing, Code of Ethics, and Standards" (Theiia.org, 2016b). There are 52 standards and corresponding 60 guidance (see Appendix 1).

1.1.3 Description of the case company and its Internal Audit function

The case company in this thesis research is a financial institution that is preferred to stay anonymous. The company is the local subsidiary of a global financial group (the Group). The Group has a long established Internal Audit division (Group IAD) while the local Internal Audit (IA) team of the case company (the Company) has just been set up three years ago to meet the local regulations.

According the Internal Audit Corporate Framework (Group IAD, 2015: 3) adopted by the local company as Internal Audit Policy or Charter and the Company's Governance and Internal Control Policy (The Company, 2016: 20), the IA function in the case company is a permanent function that is independent of any other function or unit in the case company. The IA function reports directly to the Company's Board of Directors or its Audit

Committee and administratively reports to the Chief Executive Officer for day-to-day matters (The Company, 2016). The Head of IA and all internal audit staff have no decision-making power in the Company except those relating to the IA function. This restriction also includes that internal auditors shall not take part into day-to-day functioning of the Company.

In line with the IPPF's Definition on Internal Auditing, the IA mission is to

> provide the Company's Board of Directors and senior management with independent assurance about the quality and effectiveness of the processes and systems of internal control, risk management (current or emerging) and governance, thus helping to safeguard the value of the organization, its solvency and reputation (Group IAD, 2015: 3).

To accomplish the mission, the IA function assesses the effectiveness and efficiency of the aforementioned processes and systems, their compliance with applicable laws and regulations, the reliability and integrity of financial and operational information, and asset integrity (Group IAD, 2015: 3).

Figure 2 below illustrates the independence of Internal Audit function in the case company and Figure 3 explains the relationship between the Group Internal Audit division and the local Internal Audit team of the case company. As seen in Figure 3, the local Internal Audit has also a functional reporting to the Group Internal Audit division in addition to the functional reporting to the local Audit Committee and the local Board of Directors, as required in the Internal Audit Corporate Framework (Group IAD, 2015: 6).
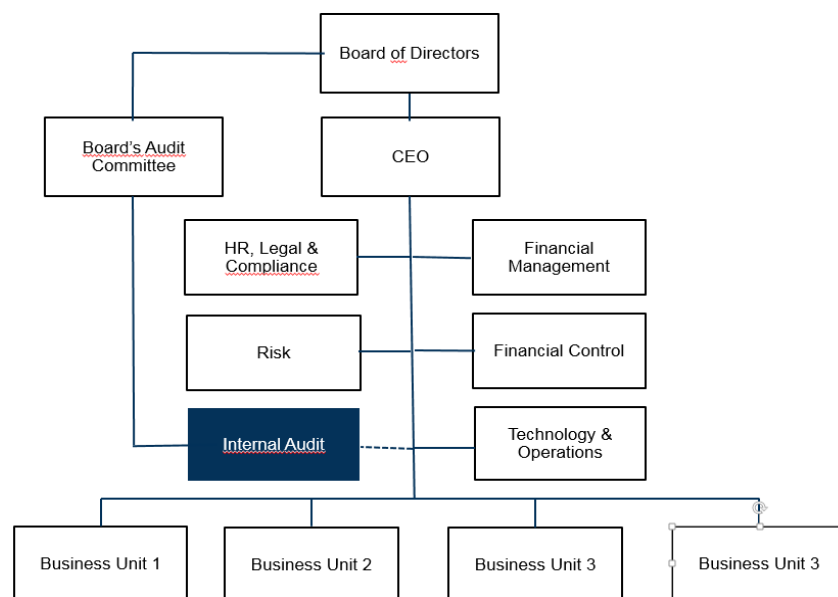

Figure 2. IA as an independent function, adapted from The Company (2016: 16)
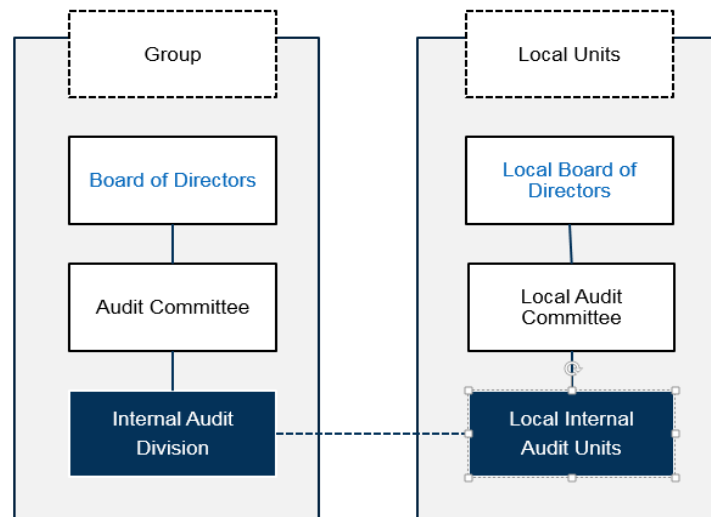
Figure 3. The Group Internal Audit division and local Internal Audit units
(Group IAD, 2015a: 5)

The Group IAD considers as mandatory the compliance of the Definition of Internal Auditing, the Code of Ethics and the Standards included in the IPPF issued by the IIA (refer to section 1.1.1 and 1.1.2 above). As a result, adherence to the IPPF is one of operating principles defined in the Internal Audit Corporate Framework.

According to the Framework, the Group IAD is responsible for establishing Corporate Internal Audit Framework, Internal Audit Methodology and Quality Management System as well as coordinating and supervising of local Internal Audit units (The IAD, 2015b: 5-6).

1.2   Business problem

Recently, the Internal Audit activity of the case company has been evaluated by the IIA. The overall quality assessment concludes that "the Internal Audit activity has a charter, policies and processes that are in conformance with the IPPF's Mandatory Guidance" (IIA, 2016). However, the IIA auditors have identified an issue related to documentation of audit planning and working paper in responding to the IPPF's Standards 2201 - Planning Considerations and 2210 - Engagement Objectives (see Appendix 2 for full details on the two Standards).

The IIA auditors identify that a planning memorandum is used to indicate audit objectives for the audited unit and a work program is adapted to the actual situation being analyzed.

However, the documentation of audit planning and working paper does not give an explicit and simple documentary evidence of traceability between the audit objectives, relevant and significant risks observed for the audited unit and established controls to mitigate these risks, and the tests in the adapted work program that are carried out to achieve the established audit objectives.

1.3   Research question, objectives & outcomes of the research

This thesis is aimed to review again the case company's IA methodology and then suggest improvement opportunities to solve the problem identified by the IIA auditors.

The research question is determined as below:

- How should the Internal Audit methodology be improved to make the documentation of audit planning, work program and working papers traceable?

2   RESEARCH STRUCTURE

This chapter describes the process used to answer the research question.

As illustrated in Figure 4 below, the process starts with a thorough analysis of the current IA methodology and practice to identify possible root causes to the problem. The key input for this As - Is analysis is the Audit Methodology Manual including appendices and templates. In the following step, best practices on the areas identified with the problem will be gathered and analyzed. The pool of best practices will be based on a combination of literature review and the author's previous experience with a global leading auditing and consulting company. Based on the results of the best practices review, solutions to the problem will be constructed and suggested considering the Company's objectives set for the IA activity and the IPPF. The process ends with a summary of the research project, its results and further steps to get the recommendations implemented.
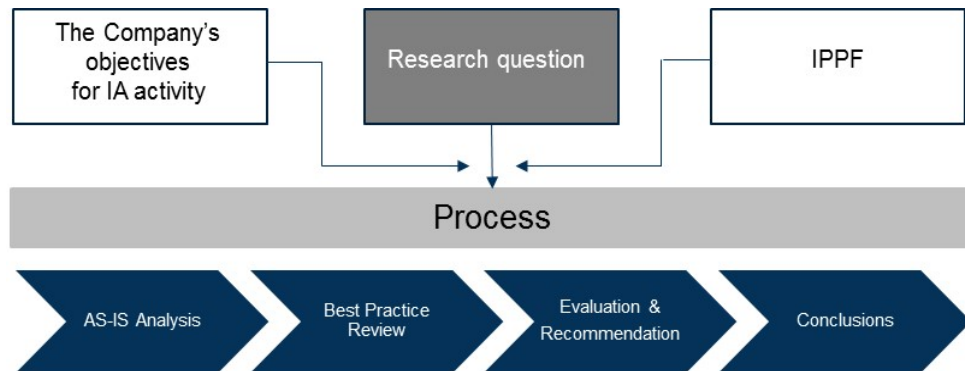
Figure 4. Research process

3 AS-IS ANALYSIS

3.1 General aspects of the current Internal Audit methodology

3.1.1 Audit Cycle

In order to perform its functions and responsibilities, the Internal Audit function follows an Audit Cycle set by the Group Internal Audit division as shown in Figure 5 below. The Audit Cycle follows a risk-driven approach to determine the priorities of the internal audit activity, which is in line with the IPPF's Standards 2010 on Planning.

Figure 5. Risk-driven Audit Cycle, adapted from Local IA (2016: 7)

Risk Assessment

The Risk Assessment exercise is performed at both Corporate and Local level using the AudiNet tool. The result of the risk assessment is the residual risks upon which the Annual Audit Plan is based.

The Group's Audit Methodology Manual (Group IAD, 2016: 103) indicates that risk assessment methodology has been recently developed to adapt to international risk management standards, covering elements of inherent risk and the control environment as well as impact and probability factors.

Following the IPPF's Practice Advisory 2010-1 (IIA, 2009), in developing the IA activity's audit plan, the Group has first developed and updated at least annually the audit universe, which is "a list of all the possible audits that could be performed" (IIA, 2009). In determining the audit universe, extensive and rigorous information has been obtained from various sources. Currently, within each of the geographies in which the IAD is present (Group IAD, 2016: 103), the audit universe consist of three elements: company group (legal companies that are regularly audited jointly), activities/businesses within each company group and processes associated with each activity/business.

The Group is exposed to various risks inherent from the activities/businesses and processes it conducts. The general approach for risk assessment in the annual audit planning is based on the consideration of events that, if occurring, can negatively impact the Group's capacity to achieve its objectives and as a consequence negatively impact its profits and thereby affect its net worth and solvency (Group IAD, 2016: 13).

There are 10 risk classifications identified as associated with the Group's activities/businesses and processes (Group IAD, 2016: 14) e.g. Financial Information Risk, Credit Risk and Operational Risk.

The risk assessment exercise reflects the auditor's perception of the level of risk existing in the activity/business or process evaluated. The exercise is performed with the use of AudiNet application, one of applications in the informational system used by the Group IA globally. AudiNet has a module that allows objectively and uniformly scoring and prioritizing the auditable universe.

.

Inherent risk

Inherent risk is risk that the entity faces without taking into consideration internal controls established to mitigate it (Group IAD, 2016: 104). Colbert and Alderman (1995) share the same view that the auditor do not consider internal controls when evaluating inherent risk. Moller (2013: 66), in other words, defines inherent risk is the risk that the entity is not able to manage or transfer completely or in other words, there will be always some risk inherent in all levels of operations and processes.

It is established in the IA methodology that an auditable entity's initial inherent risk in a specific local unit of the Group is the combination of inherent risk of the three elements that make up the audit universe: process, company group and activity/business. Inherent risk is thereby calculated for each existing process, group, and activity and the result obtained is applied to each auditable entity making up the universe.

According to the IA methodology, different approaches are used to evaluate inherent risk to processes, to the company group and to activities/business as explained below.

Inherent risk to processes

When evaluating inherent risk to processes, two following factors shall be taken into consideration (Group IAD, 2016: 104):

- Impact of such event, if it occurs.
- Probability that a risk event happens in a specific process.

In order to attain homogeneity in the risk assessment process, assessment of impact and probability is carried out centrally at the Group level with the exception of technology risk due to its particular nature will be locally assessed using different method. Local adjustments can be made to the centralized Group assessment if they are supported with proper justifications (Group IAD, 2016: 106).

The assessment of impact and probability is performed using a risk events catalogue defined for each risk that is associated with a process (e.g. 12 risk events defined for credit risk, 9 risk events for market risk). Events are actual occurrences of a risk that lead

to a negative impact or loss. A level of impact, which reflects the criticality if an event actually occurred, has been pre-assigned in the risk events catalogue. Probability of occurrence is higher when there are more likely risk events occurring in a process (Group IAD, 2016: 104-105).

Inherent risk to groups

The methodology established for evaluating company groups seeks to measure their risk through relative importance and, therefore, criticality of the group based on business and operations in a specific geography (Group IAD, 2016: 106). A series of quantitative (e.g. profit, income volume, asset volume) and qualitative criteria (e.g. significant organizational changes, special focus by regulators) has been used to obtain a score for each group.

Inherent risk to activities/businesses

The Audit Methodology Manual (The Group IAD, 2016: 107) states that risks associated with activities/businesses are measured by their relative importance and therefore, criticality of the activity based on business and operations in a specific geography. A questionnaire is, therefore, used for risk assessment of each activity, which covers the following aspects:

- Impact on the geography's strategic plans
- Regulatory pressure
- Specific legal requirements
- Influence of the environment

The assessment of activities/businesses is conducted at both Corporate and Local level to take into account particularities of the local geography.

In certain activities/businesses and processes, the assessment of inherent risk described above is complemented by a risk profile assessment using both quantitative (e.g. Non-Performing Loan or NPL ratio is one of ratios that indicates the quality of credit management process) and qualitative factors (e.g. regulatory complexity, complexity of processes) (Group IAD, 2016: 107-108).

Residual risk

Next, the residual risk for each activity/business and process is determined by subtracting control environment from the inherent risk as shown in Figure 6 below.
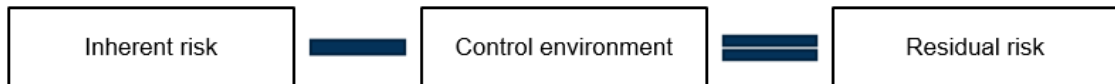

Figure 6. Residual risk as a result of subtracting control environment
from inherent risk, adapted from The local IA (2016: 8)

The assessment of control environment consider the past 3 years' audit ratings which is also the Audit Cycle period, recommendations and their status of implementation in addition to possible opinions from internal and external parties, annual compliance report, regulators' assessment, units' self-assessment on risk and controls. If no audit rating exists, whether as a result of audits performed without ratings or no audits performed during the last three-year cycle, the control environment rating is set in the mid-level scale, representing a neutral control environment (Group IAD, 2016:109-112).

Finally, a risk matrix is created as the final output of the risk assessment (see Appendix 3 for the risk matrix sample extracted from the AudiNet tool).

Annual Audit Plan

The Annual Audit Plan is the result of both the bottom-up analysis and the top-down analysis as presented Figure 7, which is in line with the IPPF's Practice Advisory 2010-1 (IIA, 2009). In addition to inclusion of jobs that are shown in the risk assessment, the Annual Audit Plan includes all jobs that the IA function must carry out to comply with specific regulatory or supervisory requirements. Furthermore, jobs that arise as requirements by the Board of Directors or Audit Committee will be included in the Audit Plan as well as jobs suggested by the Company's senior management in the various communication forums and that the IA function considers suitable.
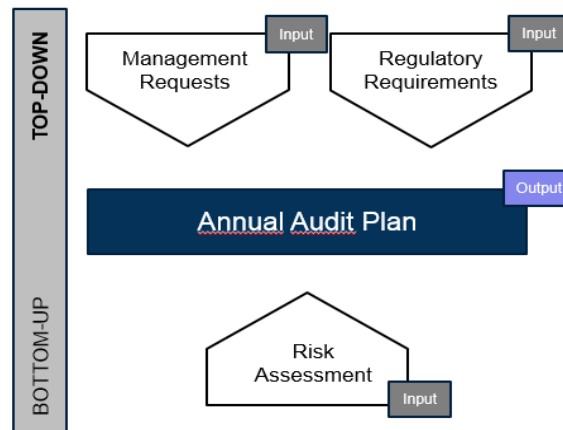
Figure 7. Annual Audit Planning,

adapted from The local IA (2016: 8)

Jobs in the audit plan are proposed based on the priorities showed in the risk matrix. For example, if the residual risk result is "Cause for concern", the audit of that activity/business or process must be carried out within the next 12 months as shown in Table 1.

Table 1. Relationship between residual risk score, its assessment,

and its link with the three-year audit cycle

(Group IAD, 2016: 113)

Residual risk [7]	Assessment	Colour	Audit Cycle
>3	Cause for concern	🔴	12 months
2-3	To be watched closely	🟡	24 months
1-2	Normal	🟢	36 months
<1	Not cause for concern	⚫	Outside of cycle

One can see in the Annual Audit Plan document which activity/business or process and associated risks will be audited throughout the year but not details on the scope of work for each audit. Detailed scope of work is determined later when the job starts and documented in the Audit Engagement Plan document (see section 3.1.2 below).

The AudiNet tool has a planning module that enables planning all audit jobs that will be conducted during the year, considering the risks matrix results and available staff resources.

Execute Audits

Once the Annual Audit Plan is finalized and approved, audit jobs will be conducted within the estimated timeline. Modifications (e.g. change in execution date or cancellation) to the Annual Audit Plan is possible but written justifications are required and certaine changes needs appropriate level of approval (Group IAD, 2016: 22).

AudiNet application is used to store recommendations, to analyze consistency between the importance of recommendation and rating assigned, to store the report and any other documentation in the electronic file and finally to distribute the report.

TeamMate EWP is an audit software program that is used for filing Audit Engagement Plan document, work program, work papers and evidence found during an audit.

Monitoring of Recommendations

As defined in the Audit Methodology Manual (Group IAD, 2016: 23), this phase deals with monitoring of all actions identified by the internal auditors to correct relevant deficiencies or weaknesses in the Company's governance, risk management or internal control system. The cycle will close when a new audit for the same unit takes place or when the level of implementation is concluded as satisfactory.

AudiNet has s a module that indicates the level of implementation of each recommendation and automatically retrieves reports about the degree of compliance and percentage of implementation of a specific business, unit, risk, etc (Group IAD, 2016: 153).

Reporting

This activity per the methodology (Group IAD, 2016: 23) refers to frequent reporting to the Board or its Audit Committee on the execution of annual audit plan including changes to the plan, the most significant findings from the audit jobs and escalation of recommendations that are not implemented by the agreed date.

3.1.2   Internal Audit Processes

This section analyses current processes to execute individual audit jobs (or audit engagements) determined in the Annual Audit Plan.

Figure 8 below is an overview of processes together with their inputs, activities and outputs.
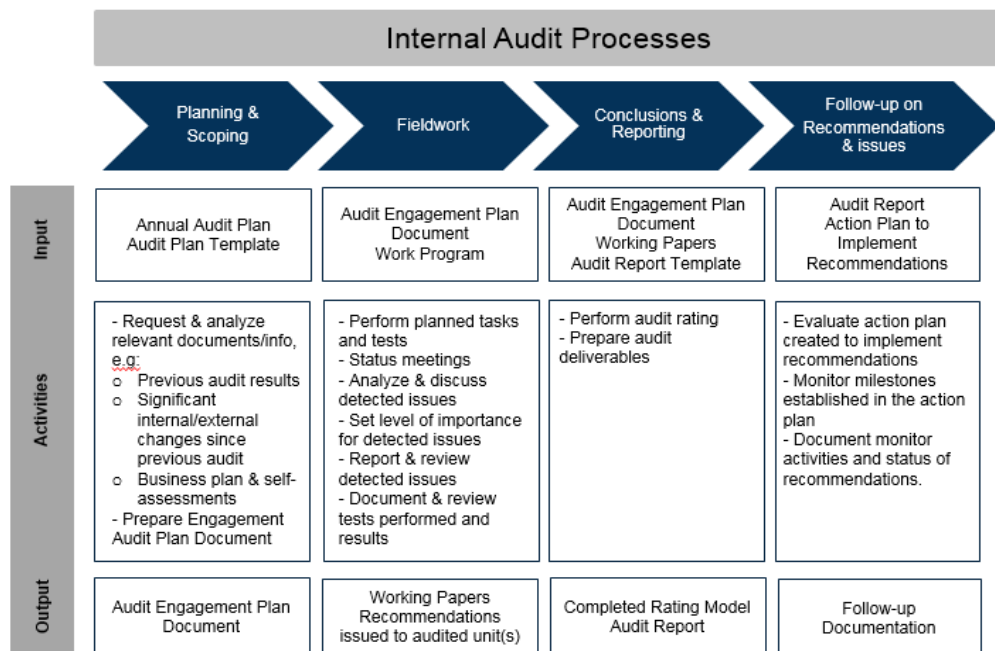
Figure 8. Internal Audit Processes

Planning & Scoping

An audit job starts with the planning and scoping process with Audit Engagement Plan document as the output.

Planning is important for conducting audit work and for managing the job. The planning document is also helpful for the preparation of the audit report in the later process. Mandatory contents of an Audit Engagement Plan document include (more details in Appendix 4):

- *Audit objectives*: what the audit aims to achieve.
- *Scope of work*: the magnitude and boundaries of activities, objectives, and exposures to be reviewed.
- *Approach*: the nature of the work to be performed.
- *Risks to be reviewed*.

- *Limitation of scope.*
- *Work program and rating model to be used.*
- *Audit team, reviewer (s) and distribution of tasks.*
- *Duration*: estimated timeline for the completion of the audit.
- *Analysis of relevant information:* e.g. brief on activity/business or process to be audited, previous audit results, external reviews
- *Audit deliverables*: describes the type of reporting to be provided.

According to the Audit Methodology Manual (Group IAD, 2016: 25), purpose of planning for individual audit jobs is to become familiar with the activity and other essential aspects of the audited activity beforehand and thereby identify the risks that it exposes to and existing controls to mitigate those risks. This aim is in line with the IPPF's Standard 2201 (see Appendix 2 for the contents of the Standard). In fact, risks and controls associated with the activity/business and process have been preliminarily evaluated in the annual audit planning. But there is no indication in the methodology manual that risks identified in the audit engagement planning shall be linked to risks identified earlier in the annual audit planning. There is also no specific requirements in the methodology manual on setting audit objectives, whether they shall be reflected the results of risk and control assessment in accordance with the IPPF's Standard 2210 (see Appendix 2 for the contents of the Standard). Specific instructions on analyzing associated risks and controls in the audit engagement planning are especially necessary, as there may be jobs in the Annual Audit Plan that are determined based on management requirements (refer to Figure 7 above).

Regarding the work program, the Group Internal Audit division has created various work programs to audit different activities/areas in the Group e.g. credit risk management and finance. In general, the local IA team is able to find one relevant work program from the standard work program inventory in order to cover audit objectives of the job with possibility of modifications based on the particularities of the unit. If the local team does not use that standard work program or use it with modifications, reasons for such option must be adequately justified. The standard work programs have pre-defined objectives and test procedures to be performed to achieve these objectives. The standard work programs are all very extensive as they are supposed to cover a full scope audit. Therefore, the methodology (Group IAD, 2016: 29) allows the team leader to decide which test procedures that are not performed with justification of not being applicable in every case. Additional tests in addition to standard work program are also possible.

However, there is no indication in the methodology manual that there shall be a link between audit objectives determined in the Audit Engagement Plan document and those defined in the work program. Therefore, there were cases that a standard work program was selected without considering modifications of pre-defined audit objectives to match with audit objectives defined in the Audit Engagement Plan.

Fieldwork

After the audit engagement planning is completed, auditors will perform their assigned tests in the selected or adapted work program.

Work programs are structured by assigning specific risk(s) covered by each audit test and the risk factor in which the conclusion must be evaluated. This structuring helps the auditor better assess the direction of each test, facilitating a subsequent determination of the audit rating in the later phase (see section "Conclusion & Reporting" below). For example, the associated risk and rating factor are assigned as below for one test in the work program on Financial Management:

Test #4. Obtain the latest independent audit and supervisory body reports and analyze the most relevant aspects highlighted in these reports and potential issues detected, checking their current status

Associated risk	Financial Information Risk
Rating factor	Accounting Balances and Financial Statements

As instructed in the Audit Methodology Manual (Group IAD, 2016: 29-30), if the test result is unsatisfactory, the auditor should report any detected issues to the team leader, who may require additional testing or increase the sample. The auditors shall also discuss the detected issues with the audited units and objectively assess the received comments. The comments obtained in this manner shall be included in the work papers, if appropriate. The purpose of these discussions and prior reviews is to provide the audited unit an opportunity to clarify and express their points of view on the findings, to corroborate the accuracy of information used and findings obtained as well as to analyze the need to perform additional tests.

The application of audit tests and the findings obtained shall be reflected in the auditors' work papers. Work papers are a permanent expression of the work conducted by members of the audit team and required actions on which their findings are based. Work papers are considered sufficient if they meet the following criteria (Group IAD, 2016: 30):

- Information sources used and information considered e.g. names of people providing information, names of documents reviewed.
- Scope of work carried out.
- Audit tests performed.
- Results of audit tests.
- Adequate and sufficient evidence to support findings, if any.

Conclusion & reporting

Once all tests in the work program are completed and documented, auditors will perform the audit rating and prepare audit deliverables. Rating for the audit is carried out using the rating model identified in the Audit Engagement Plan document.

A rating model is built together with the related work program by the Group Internal Audit division. The model is built in a flexible in the way that it permits adaptation to the variety of existing audit approaches (Group IAD, 2016: 41). Certain factors, or even risks, may be rated as inapplicable in some audits, and new models may be created (if necessary) to handle new approaches but should be always in accordance with the implemented work methodology.

The rating model pre-defines assessment factors to the activity or the process that is being evaluated. As the methodology explains (Group IAD, 2016: 43), these factors are indicated in relevant tests of the work program (see "Fieldwork" section above), so that the auditor easily identifies if there are related weaknesses and makes an assessment.

Follow-up on recommendations and issues

The methodology manual (Group IAD, 2016: 62) emphasizes that recommendations monitoring is an essential process in the audit cycle that seeks to demonstrate proper commitments by audited unit(s) on improving the internal control system. Auditors will evaluate the adequacy of created action plan, monitor each of the established milestones

in the plan and support audited units to achieve desired objectives, without carrying out actions that could compromise its independence. Monitoring activities & status of recommendations need to be recorded in an appropriate manner.

3.2   Traceability issue and the root causes

Figure 9 below visualizes all documents created along the IA function's Audit Cycle mentioned in section 3.1 above together with audit tools used to prepare and store those documents. The documents, which starts with the risk assessment documentation and ends with the report of IA activity are stitched together to express the opinion how well the organization is responding to risks that may occur and prevent it from achieving strategies and objectives. Risks associated with the organization's strategies and objectives and risk responses are, therefore, the central point of all those documents. However, this central point is not clearly traced in the audit engagement plan, work program and work papers, marked in Figure 9 below.

Even though the IA function adopts a risk-based audit approach in accordance with the IPPF, the approach is not explicitly introduced at the beginning and further explained in the methodology manual. Indeed, the term "risk-based" is mentioned only once in a later chapter on quality management system (Chapter 5). Strategic objectives, associated risks and risk responses as the central point connecting documents created throughout the Audit Cycle is not, therefore, underlined.
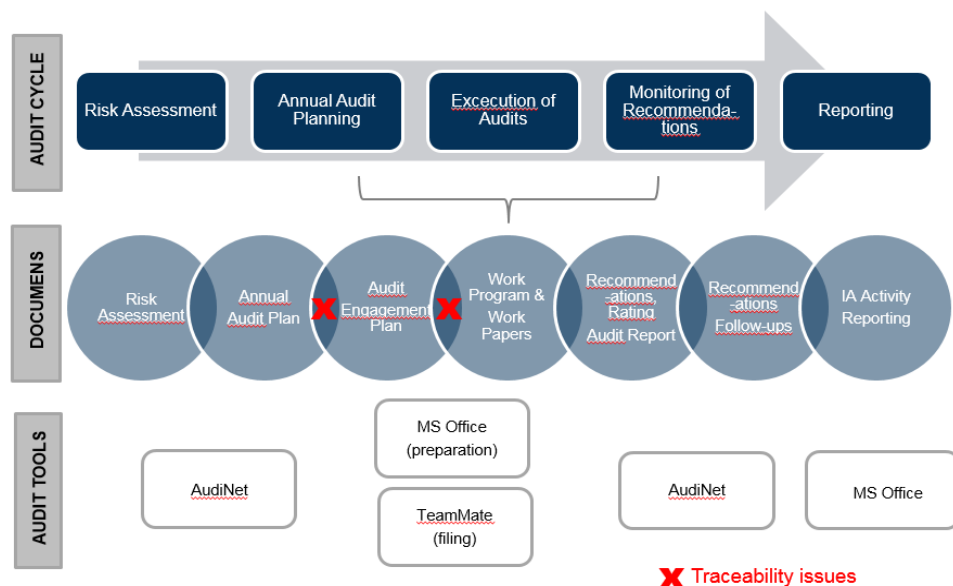

Figure 9.   Documentation along audit cycle and traceability issue

4   BEST PRACTICES

This chapter is aimed to identify and analyze best practices on the internal audit methodology with a focus on areas identified with the problem in the case company. The pool of best practices has been gathered mainly based on the author's previous experience as a consultant of a global leading auditing and consulting company and on a literature review.

4.1   Risk - based audit approach concept

The IPPF's Standards 2100 positions the internal audit activity's nature of work as systematic, disciplined, and risk-based approach. Risk-based approach shall be applied in planning for the IA activity (Standards 2010) and planning for audit engagements (Standards 2201 and 2210). This means that various risks shall be evaluated during the planning stages (Colbert and Alderman: 1995), those risks that prevent the organization and its business processes from achieving the established objectives.

Several studies show that the adoption of a risk-based approach is positively correlated to the accomplishment of the internal audit activity's objectives, which are to help the organization improve its effectiveness of risk management, control, and governance processes (see Definition of Internal Auditing in section 1.1.1 above). Colbert and Alderman (1995) explain as the risk-based or risk-driven approach focuses the internal auditor's efforts on high risk areas, it is generally more effective (i.e. in identifying errors) and more efficient (i.e. efforts put on high risk areas). McNamee (1997) claims that the way internal auditors focus on risk, broaden their perspective to include all risk management techniques and then assess the auditable areas in an environment of risk adds more value to the organization. Bechara and Kapoor (2012) view that the internal auditors' systemic and risk-based approach of viewing risks through the spectrum of strategic objectives supports a more targeted and efficient audit.

Allot (in Castanheira at al. 2009) specifically identifies that risk-based internal auditing has increasingly made significant contributions to effective risk management. After recent economic happenings, Bechara and Kapoor (2012) notice that companies around the world increasingly rely on internal auditors for their business understanding and approach in risk identification and risk mitigation measures.

A study by Castanheira at al. (2009) concludes that the number of organizations applying risk-based approach for planning is generally high in the financial industry. Za´rate (in Castanheira at al. 2009) argues that as the financial industry is more advanced in terms of risk management, due to regulatory requirements, so there are more organizations in the financial industry that apply the risk-based internal auditing approach.

4.2 Internal audit activity planning

4.2.1 Enterprise risk assessment

As explained in section 4.1 above, risk-based internal auditing involves performing risk assessments in the audit planning stages. According to McNamee (1997), in planning for the IA activity (macro level), risk assessment shall be performed to identify, measure, and prioritize risks so that focus is placed on the areas that are threaten by higher degree of risks. In planning individual audit engagements (micro level), risk assessment is used again to helps identify the most significant audit areas, based on that the auditors design a work program that "tests the most important controls, or to test the controls at greater depth or with more thoroughness" (McNamee, 1997). Indeed, a study of internal auditing practices in Ireland by the IIA – UK and Ireland and KPMG Ireland (in Castanheira et al. 2009), found that 89 percent of internal audit departments uses the risk-based approach when planning annual internal audit activity and 93 percent uses a risk-based approach in their audit engagements.

The risk assessment at the macro level is also called "enterprise risk assessment" in some organizations' methodologies. In enterprise risk assessment, strategic risks related to the whole organization's strategies and objectives are identified and assessed. Also key processes that mitigate strategic risks are identified. In other words, the enterprise risk assessment focuses on the organization's "as is" strategic risk profile and drives the development of an internal audit plan.

During the risk assessment processes, interviews are often conducted with management personnel to obtain information regarding: the organization's vision and strategies; significant business processes and their objectives; key risks which impact the achievement of vision, strategy, and/or objectives; risk impact and likelihood to the organization; and management's assessment of the effectiveness of the processes and controls the company has established to manage those risks. A significant process is any process that is

associated with and manages a strategic risk to the organization's objectives. The business processes included in the internal audit plan, in general, are those processes that the organization has established to manage the most significant risks to the organization.

Other inputs for enterprise risk assessment include business and industry knowledge and information from the previous internal audit, if available.

The identified risks are then ranked according to the pre-defined criteria. Information is collected on management's perceptions regarding:

- Gross risk - The significant risks to the organization's objectives that must be managed well to support the achievement of those objectives, regardless of the effectiveness of the processes and controls implemented to address those risks.
- Residual risk - The remaining level of risk to the organization's objectives once the effects of existing business processes and controls are considered.

Next, the areas and business processes to be audited are determined and prioritized based on the perceived risk (either gross/inherent or residual/exposure).

Process level risk analysis may be performed as part of the enterprise risk assessment to either gain further understanding of a significant process or business unit or later performed as part of the internal audit execution, to assist in the scoping of a particular internal audit engagement. For example, as a result of the enterprise risk assessment, the financial reporting process may have been identified as a high risk area for the organization. In order to better understand what areas of financial reporting process are the higher risk areas, further risk analysis at the process level may be necessary.

Documentation for the process risk analysis often includes narrative description of process with flowcharts, strategic risks that the process is associated with, process level risks and established internal controls, process risk matrix which shows the relationship between the impact and the likelihood of the occurrence of the identified process risks and their relative significance.

4.2.2   Internal audit activity plan

Finally, the IA Plan is developed based on the outcomes of the risk assessment exercise or the enterprise risk assessment. In addition to the business processes identified during the risk assessment exercise, other processes/projects may be selected for inclusion in the IA Plan. These internal audit projects may be identified through specific requests from the organization's management and/or the audit committee based on issues they believe are important to the organization, follow-up reviews associated with a prior internal audit projects, and any other areas of concern discovered over time that are approved by the audit committee for addition to the IA Plan.

In conclusion, inputs to the internal audit planning could typically include a combination of the following:

- Outcomes of a risk assessment (enterprise and process risk), including key risks and associated internal controls.
- Requirements from management and/or audit committee.
- Industry information.
- Results from external audits and reviews.
- Previous internal audit results.

When using an enterprise risk assessment to develop the IA Plan, the number of strategic and/or process risks may be relatively large, generating an extensive list of audit projects for potential inclusion in the IA Plan. Internal auditors then consider the results of risk assessments, process analyses and other information with professional judgment in scoping the audit projects to be included in the IA Plan.

The internal audit plan, even once approved by the audit committee, is inherently dynamic and may need modifications over time as various factors associated with the organization's internal and external environment evolve and impact the organization's business. Therefore, it is industry practice to develop a strategic internal audit plan of two to three years with a detailed internal audit plan for 12 months that is subject to at least an annual update. The audit engagement teams should monitor the relevance of the approved IA Plan and suggest necessary updates to reflect the evolving risk profile of the organization. The IA Plan maintenance process may be also formally carried out through formally revisiting the enterprise risk assessment and resulting internal audit projects

periodically through the year. Many organizations establish a quarterly process, typically coinciding with quarterly audit committee meetings, for reviewing internal audit progress for the quarter, discussing significant issues identified during that quarter, and evaluating proposed modifications to the IA Plan for the remaining period of the year. In any case, regardless of the specific timing and nature of the update process, open lines of communication should be maintained and available between key internal audit stakeholders when events arise requiring decision-making in periodic audit committee meetings.

4.2.3   Internal audit engagement execution

Once the IA Plan is approved, internal audit engagement execution, including development of an engagement plan, a work program and test procedures, is carried out. Internal audit activities are performed in this process based on the understanding gained through enterprise risk assessment, internal audit planning and process risk analysis, if any. During this phase of the Audit Cycle, internal auditors according the audit methodology focus on providing findings and performance improvement opportunities to the organization.

The following activities by order are normally conducted during the internal audit execution phase:

- Process Risk Analysis
- Develop Work Program
- Execute Work Program
- Document Test Results & Evidence
- Report Results i.e. Identified Issues

4.2.4   Process risk analysis

A process risk analysis performed at the beginning of the execution phase is aimed to serve as a risk-based scoping exercise for the development of an effective and efficient work program which focuses work efforts on key areas to the business process. The extent of work performed for the process risk analysis is dependent upon the level of work performed during the enterprise risk assessment. If the risk assessment for planning the IA activity is developed without some form of process-level analysis, the IA Plan will be more general in nature and will tend to be focused on gross risks at the strategic

level. In that situation, additional work will be required during the planning and scoping stage of each engagement in order to develop an effective and efficient work program.

A process risk analysis is an important tool for determining the scope of an internal audit engagement. Similar to the enterprise risk assessment, this is commonly performed through interviews and discussions. These interviews and discussions are typically conducted with those individuals who are familiar with the process, such as process owners or control owners. The process risk analysis is often briefly described with workflows. The analysis will provide the basis for scoping individual audit jobs.

When performing process risk analysis, internal auditors analyze how the process is managed against leading practices, e.g. industry standards and guidelines, regulator's expectations and other published leading practice information. Ultimately, the appropriate practice to the organization will be the one that supports the organization achieve its strategic objectives within the context of its processes and structure.

4.2.5   Development of work program

The work program designs test procedures to be carried out to assist internal auditors in assessing the organization's existence and effectiveness of internal controls established to mitigate risks.

To build the internal audit work program for an audit engagement, internal auditors should be aware of risks and controls associated with the activity in review. As this understanding will help determine the focus areas for testing. The work program will focus on testing of internal controls that associated with the prioritized risks identified. But if control the design of a control is found not good or the control is not operating, it may not be necessary to test internal controls.

Table 2 below shows simplified examples of how test procedures of a work program can be determined based on the process risk analysis.

Risk ID	Process risk - Gross	Control	Strength of control design	Process risk – Residual	Considerations for test procedures
1	High	A	Strong	Low	Test if control is operating and effective as designed.
2	High	B	Weak	High	Control inadequacy issue is noted. Reevaluation of control design is recommended.
3	Medium	C	Strong	Low	Test if control is operating and effective as designed. Risk may be over controlled. Consider a cost-benefit analysis.
4	Low	D	Strong	Low	Not a focus.

Table 2 – Test procedures based on process risk analysis - Examples

For example, control A that moves risk #1 from an unacceptable level to an acceptable low level. Normally in this case, test procedure is to test if the control is operating effectively as designed. Regarding risk #2, control design is assessed as weak, so it is necessary to reevaluate the control design.

Test procedures in the program should be created with flexibility so that they can be modified using auditors' professional judgement but at the same with sufficient guidance for the auditors to understand and follow. Test procedures should be also effectively designed so that sufficient evidence can obtain to meet audit objectives while least efforts are made. The effectiveness of an internal control should be assessed in two perspectives, its consistent operation and the outcome of the control.

There are generally two types of internal audit procedures:

- Tests of design are associated with the internal control design and is primarily performed during the process risk analysis.
- Tests of effectiveness confirm whether key internal controls identified during process risk analysis are in existence and are operating effectively as intended.

4.2.6   Work program execution and documentation

All test procedures should be referenced to the work papers. In the internal auditing practice, internal auditors are required to document work papers adequately and sufficiently with traceability. Especially, test evidence should be clearly documented in the work papers so another person is able to draw the same conclusions when reviewing it. In addition, work papers should be signed and dated by the preparer and the reviewer. Finally, there should be a positive link between the test procedures with the scope defined in the audit engagement plan.

4.2.7   Reporting

An audit report is the means to communicate internal audit activity's results. Regarding the report content, it is important that the reported results are adequately and clearly supported with the work papers. Findings in Internal audit report should agree to findings in the work papers, which in turn should agree to the supporting evidence.

When applied thoroughly, reporting under the risk-based internal audit methodology provide the management with information if there are areas that are identified as having unacceptable residual risk, or areas that can be better optimized to effectively manage the strategic and process risks.

4.2.8   Documentation traceability

Regarding the traceability among different documents throughout the Audit Cycle, McNamee (1997) emphasizes there should be a clear link between the audit objectives, the objectives of the audited unit, and the organization's strategies and objectives. The audit objective should be "related to the risks faced by the auditable unit in its effort to meet its established objectives" (McNamee, 1997). An effective risk-based audit plan should start with the organization's strategic objectives because risks are only relevant in the context of these objectives (Bechara and Kapoor, 2012). Audit tests in the work program are then designed to obtain sufficient evidence supporting the audit objectives.

5   RECOMMENDATIONS

The analysis of best practices in chapter 4 shows that the case company's current IA methodology is largely aligned with the professional standards (i.e. IPPF) and practice in general and with the financial services industry practice in particular.

Firstly, the IA function applies a three-year Audit Cycle with a detailed annual audit plan that is subject to the annual review and update.

Secondly, the IA function's methodology follows a systematic and risk-based approach to determine the priorities of the IA activity. Particularly, a systematic risk assessment is used to plan the IA activity which identifies and prioritizes risks that may prevent the Company from achieving those strategic objectives. The risk assessment when completed provides a risk matrix of residual risks concluded for each activity/business and process. Residual risk is the outcome of subtracting control environment from inherent risk. The matrix of residual risks in turn provides the basis for a 3-year audit plan of which areas that are threaten by higher degree of risks require to be audited within the next 12 months. Inputs for the assessment of control environment in the current IA methodology, which include the recent audits' ratings and recommendations, the status of implementation and third parties' evaluation, are also in line with the market practice.

Thirdly, the IA activity plan is based on both bottom-up analysis (risk assessment) and top-down analysis (by considering requirements from management, audit committee and regulatory environment). The IA activity plan is flexible which means modifications, subject to appropriate approval, are possible when various factors associated with the organization's internal and external environment evolve and impact the organization's business.

Finally, the execution of individual audit jobs determined in the IA activity plan follows steps similar to those observed in the industry which are scoping, work program building, work program execution and reporting. The IA methodology also includes templates e.g. audit engagement plan and establishes criteria on certain documentation e.g. sufficiency criteria for work papers.

However, the author has identified some aspects in the methodology and documentation templates that could be considered for improvements in order to meet the IPPF's Standards 2201 and 2210. The following sections will discuss on these aspects together the improvement proposals.

5.1 Internal audit methodology

As described in section 3.1.1 above on the Audit Cycle applied in the case IA function, the risk assessment performed for planning the IA activity is developed with some form of process-level risk analysis. For each auditable entity, it is established in the audit methodology that inherent risk shall be assessed for all three elements that make up the audit universe: process, company group, and activity/business. Assessment of inherent risk to processes is calculated based on applicable risks to them (from a list of 10 risks mentioned in section 3.1.1) and, for each risk, based on impact and probability of risk events occurring. Then, the residual risk of each process is determined by subtracting control environment from inherent risk. Whether a process will be included in the Annual Audit Plan or to be audited within 24 months or 36 months of the three-year Audit Cycle depends on its residual risk scoring result.

The assessment of process risk at this level under the current IA methodology helps identify and prioritize processes that carry higher risk in the audit universe to be included in the IA activity plan. But it does not well indicate which areas in the process are of significant concern. Applying a standard work program to execute the audit, a requirement established in the current IA methodology, without an audit focus therefore can be a challenge to the audit team as all standard work programs are massively designed.

A process risk analysis with an aim to gain a deep understanding of process helps resolve this constraint. It analyzes essential aspects of a process including process objectives, critical success factors (CFS), key performance indicators (KPI), inputs, outputs, activities together with the associated risks and internal controls. It is a normal practice that such process risk analysis is performed at the beginning of an audit to help internal auditors identify significant areas of the process that need an audit focus and then build a right work program that effectively and efficiently achieve audit objectives. The analysis of process objectives, means by which the process controls its performance (e.g. CFS, KPI), significant risks to the process and means to keep them to an acceptable

level, are also requirements set by the IPPF's Standards 2201 on Planning Considerations and Standards 2210 on Engagement Objectives (refer to Appendix 2 for details of two Standards).

Considering the benefits of process risk analysis analyzed above, the author proposes to apply also a risk-based approach in planning audit engagements using a process risk analysis. This is risk-based approach at the so-called "micro level" (Castanheira et al, 2009) in addition to the risk-based approach at the macro level performed earlier to determine the IA activity plan.

The process risk analysis will be part of the Audit Engagement Plan document. Instructions on how to perform the analysis can be an additional annex to the manual. The analysis can be conducted through interviews and discussions with those individuals who are familiar with the process. "The more respondents interviewed, the more comprehensive and in depth the insights will be" (Bechara & Kapoor, 2012). Internal auditors can also conduct a survey to get more understanding on the process activities, risks and associated controls, and to invite comments and suggestions from the auditees according to the IPPF's Practice Advisory 2210.A1-1 (see Appendix 2 for details). Management's own assessment of risks associated with the activity under review could be considered as well according the same Practice Advisory. Another possible consideration is to establish a line of communication with the company's risk team in order to receive information about risks and remediation activities on a regular basis which will be used as inputs to planning an audit engagement. Investing in such relationships is one of 5 bold steps to transform internal audit image according to Chambers (2014):

> The most critical component of "trusted advisor" is trust, and trust depends on a solid relationship. The CAE cannot alone build and sustain relationships. The entire internal audit team must be invested in the process.

"CAE" stands for Chief Audit Executive in the Chambers' statement.

Finally, when the risk-based internal auditing is applied, it is the strategic objectives, their associated risks and risk responses that act as a central point connecting documents created throughout an Audit Cycle. For that reason, the risk-based approach and this central point should be clearly and consistently expressed and emphasized throughout the IA methodology manual.

5.2 Documentation criteria

In order for the Audit Engagement Plan to be connected with the IA Plan, there is a need to underline in the IA methodology that the audit objectives should be aligned with those preliminarily determined during the planning phase of the IA activity. There is also a need to highlight that the process risk analysis is aimed to further refine the initial audit objectives set in the IA activity plan and to identify other significant areas of concern. These aspects are recommended by the IPPF's Practice Advisory 2210-1 on Engagement Objectives (see Appendix 2 for details of the Practice Advisory). The final audit objectives should be related to the "risks faced by the auditable unit in its effort to meet its established objectives" (McNamee, 1997). This is especially important when the audit tools used for the IA planning (AudiNet) and for the engagement planning (MS Word for preparation and TeamMate for filing) are not integrated together.

In addition, in order to ensure the traceability between the Audit Engagement Plan and the Work Program, the IA methodology manual and its templates should underline that the final audit objectives determined in the Audit Engagement Plan be fully reflected in the Work Program. Test procedures in the Work Program are then designed to obtain evidence supporting the audit objectives. The test procedures should focus on internal controls that associated with the prioritized risks identified in the process risk analysis. However, it may not be beneficial to test a internal controls if it is known to have substantial issues in either design or effectiveness.

When a standard Work Program is selected for the audit, the methodology should be flexible in the way that allows the team leader to modify pre-defined audit objectives and test procedures in the standard Work Program to match with the audit objectives defined in the Audit Engagement Plan.

Next, regarding documenting work papers, in addition to current criteria on sufficiency of work papers documentation, the IA methodology should also require a connection between test procedures performed and the scope defined in the Audit Engagement Plan.

Finally, regarding the audit report, which is the outcome of an audit, it is important that the reported results are adequately and clearly supported with the work papers. According to McNamee (1997), in order to demonstrate that a risk-based approach has been used for the audit, the following three aspects should be considered in the audit report:

1. The scope part includes a risk assessment result with brief description of identified risks and associated controls.
2. The findings and recommendations part is "discussed in risk terms and reference the key risk areas in the audit scope section".
3. The overall conclusion part is focused on "discussing risk and management's response to risk as the primary result of the audit".

6 CONCLUSIONS

6.1 Objective vs. outcome

The thesis was aimed to review again the case company's Internal Audit methodology and then suggest improvement opportunities to solve the problem identified during the quality review.

The qualitative research methodology was utilized in this study. The study started with a thorough analysis of the current internal audit methodology and practice. Next, best practices on the areas of problem were gathered and analyzed from a literature review and from the author's previous experience as a consultant of a global leading auditing and consulting company. Based on the results of the best practices review and considering also the objectives of the IA function and the IPPF, solutions to the problem were constructed.

The author recommends the IA management apply a risk-based approach in planning internal audit jobs through performing a process risk analysis. Leading practices show that the process risk analysis helps refine audit objectives set in the IA activity plan and identify other significant areas of concern which need more internal auditors' efforts. In other words, it helps drive the internal audit engagement execution in a more effective and efficient way.

It is recommended that the IA methodology manual express and emphasize more clearly on the risk-based internal auditing approach and that the strategic objectives, associated risks and risk responses act as a central point connecting documents created throughout an audit cycle.

It is also recommended that the IA methodology manual underline requirements and/or criteria on traceability among audit documents as well as provide specific instructions on how audit documents should be documented to ensure a positive link among them.

6.2   Next steps

In order to get the improvement suggestions implemented, the author suggests the following steps to be carried out:

1. Execute one pilot audit project applying improvement suggestions.
2. Quality check of the executed audit and draw lessons to be considered in the next steps.
3. Identify related sections in the IA methodology manual that need revisions.
4. Design a process risk analysis template and identify necessary changes in the current audit engagement plan template together with drafting detailed instructions to complete these documents.
5. Draft a proposal on suggestions to the methodology team of the Group's Internal Audit division, attached with proposed changes in the methodology manual & templates.
6. Provide training to the whole IA team on the changes once the proposal is approved.

REFERENCES

Bechara, M. and Kapoor, G. (2012): "Maximizing the Value of a Risk-Based Audit Plan", The CPA Journal, Vol. 82, No. 3.

Brink, V.Z. (1991): "Forward from Fifty", The Internal Auditor, vol. 48, no. 3, pp. 8.

Castanheira, N., Lima Rodrigues, L. and Craig, R. (2009): "Factors associated with the adoption of risk-based internal auditing", Managerial Auditing Journal, 25(1), pp. 79–98.

Chambers, R. (2014): "5 Bold Steps to Transform Internal Audit's Image", the IIA's Internal Auditor Magazine, [Online], Available: https://iaonline.theiia.org/5-bold-steps-to-transform-internal-audit-image [27 October 2016].

Colbert, J. and Alderman, C. (1995): "A risk-driven approach to the internal audit", Managerial Auditing Journal, 10(2), pp. 38–44.

Group IAD (2015a): "General Aspects of IA Model".

Group IAD (2015b): "Internal Audit Corporate Framework".

Group IAD (2016): "Audit Methodology Manual".

IIA (2009): "Practice Advisory 2010-1 Linking the Audit Plan to Risk and Exposures".

IIA (2016): "External Quality Assessment Closing Presentation".

Local IA (2016): "Internal Audit Governance and Organizational Procedure".

McNamee, D. and McNamee, T. (1995) 'The transformation of internal auditing', *Managerial Auditing Journal*, 10(2), pp. 34–37.

McNamee, D. (1997), "Risk-based auditing", Internal Auditor, vol. 54, no. 4, p. 22.

The Company (2016): "Governance and Internal Control Policy".

Theiia.org (2016a). The IIA's Official Website. "About the IIA", [Online], Available: https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx [27 October 2016].

Theiia.org (2016b). The IIA's Official Website. "Definition of Internal Auditing", [Online], Available: https://global.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx [09 October 2016].

Theiia.org (2016b). The IIA's Official Website. "Standards and Guidance", [Online], Available: https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx [20 October 2016].

APPENDICES

Appendix 1 Overview of IPPF's Standards and Recommended Guidance
(*Source: theiia.org*)

Standards	Recommended Guidance
1000 - Purpose, Authority, and Responsibility	IG 1000 - Purpose, Authority, and Responsibility
1010 – Recognizing Mandatory Guidance in the Internal Audit Charter	IG 1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter
1100 – Independence and Objectivity	IG 1100 – Independence and Objectivity
1110 – Organizational Independence	IG 1110 – Organizational Independence
1111 – Direct Interaction with the Board	IG 1111 – Direct Interaction with the Board
1112 – Chief Audit Executive Roles Beyond Internal Auditing	
1120 – Individual Objectivity	IG 1120 – Individual Objectivity
1130 – Impairment to Independence or Objectivity	IG 1130 – Impairment to Independence or Objectivity PA 1130.A1-1 – Assessing Operations for which internal auditors were previously responsible PA 1130.A2-1 Internal Audit's Responsibility for other (non-audit) functions
1200 – Proficiency and Due Professional Care	PA 1200-1 Proficiency and Due Professional Care
1210 – Proficiency	PA 1210-1 Proficiency PA 1210.A1-1 Obtaining External Service Providers to support or complement the Internal Audit Activity
1220 – Due Professional Care	PA 1220-1 Due Professional Care
1230 – Continuing Professional Development	PA 1230-1 Continuing Professional Development

Standards	Recommended Guidance
1300 – Quality Assurance and Improvement Program	PA 1300-1 Quality Assurance and Improvement Program
1310 – Requirements of the Quality Assurance and Improvement Program	
1311 – Internal Assessments	PA 1311-1 Internal Assessments
1312 – External Assessments	PA 1312-1 External Assessments PA 1312-2 External Assessments: Self Assessments with Independent Validation PA 1312-3 Independence of the External Assessment Team in the Private Sector PA 1312-4 Independence of the External Assessment Team in the Public Sector
1320 – Reporting on the Quality Assurance and Improvement Program	PA 1320-1 Reporting Results of the Quality Assurance and Improvement Program
1321 – Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"	PA 1321-1 Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"
1322 – Disclosure of Nonconformance	PA 1322-1 Disclosure of Nonconformance with the International Standards for the Professional Practice of Internal Auditing (standards)
2000 – Managing the Internal Audit Activity	
2010 – Planning	PA 2010-1 Linking the Audit Plan to Risk and Exposures PA 2010-2 Using the Risk Management Process in Internal Audit Planning
2020 – Communication and Approval	PA 2020-1 Communication and Approval
2030 – Resource Management	PA 2030-1 Resource Management
2040 – Policies and Procedures	PA 2040-1 Policies and Procedures
2050 – Coordination and Reliance	PA 2050-2 Assurance Maps
2060 – Reporting to Senior Management and the Board	PA 2060-1 Reporting to Senior Management and the Board

Standards	Recommended Guidance
2070 – External Service Provider and Organizational Responsibility for Internal Auditing	
2100 – Nature of Work	
2110 – Governance	IG 2110 - Governance
2120 – Risk Management	PA 2120-1 Assessing the Adequacy of Risk Management Processes PA 2120-2 Managing the Risk of Internal Audit Acitivity PA 2120-3 Internal Audit Coverage to Risks to Achieve Strategic Objectives
2130 – Control	PA 2130-1 Assessing the Adequacy of Control Proceses PA 2130.A1-1 Information Reliability and Integrity PA 2130.A1-2 Evaluating an Organization's Privacy Framework
2200 – Engagement Planning	PA 2200-1 Engagement Planning PA 2200-1 Using a Top-down, Risk-based Approach to Identify Controls to be Assessed in an Internal Audit Engagement
2201 – Planning Considerations	
2210 – Engagement Objectives	PA 2210-1 Engagement Objectives PA 2210.A1-1 Risk Assessment in Engagement Planning
2220 – Engagement Scope	
2230 – Engagement Resource Allocation	PA 2230-1 Engagement Resource Allocation
2240 – Engagement Work Program	PA 2240-1 Engagement Work Program
2300 – Performing the Engagement	PA 2300-1 Use of Personal Information in Conducting Engagements
2310 – Identifying Information	
2320 – Analysis and Evaluation	PA 2320-1 Analytical Procedures

Standards	Recommended Guidance
	PA 2320-2 Root Cause Analysis
	PA 2320-3 Audit Sampling
	PA 2320-4 Continuous Assurance
2330 – Documenting Information	PA 2330-1 Documenting Information
	PA 2330.A1-1 Control of Engagement Records
	PA 2330.A1-2 Granting Assess to Engagement Records
	PA 2330.A2-1Retention of Records
2340 – Engagement Supervision	PA 2340-1 Engagement Supervision
2400 – Communicating Results	PA 2400-1 Legal Considerations in Communicating Results
2410 – Criteria for Communicating	PA 2410-1 Communication Criteria
2420 – Quality of Communications	PA 2420-1 Quality of Communications
2421 – Errors and Omissions	
2430 – Use of "Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*"	
2431 – Engagement Disclosure of Nonconformance	
2440 – Disseminating Results	PA 2440-1 Disseminating Results
	PA 2440-2 Communicating Sensitive Information Within and Outside the
	PA 2440.A2-1 Communicating Outside the Organization
2450 – Overall Opinions	
2500 – Monitoring Progress	PA 2500.A1-1 Follow-up Process
2600 – Communicating the Acceptance of Risks	IG 2600 – Communicating the Acceptance of Risks

Appendix 2 IPPF's Standards 2201, 2210 and Related Practice Advisories
(*Source: theiia.org*)

Standards 2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.

- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.

- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.

- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

Standards 2210 – Engagement Objectives

Objectives must be established for each engagement.

- **2210.A1 –** Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

- **2210.A2 –** Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

- **2210.A3 –** Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.

Practice Advisory 2210-1 Engagement Objectives

(Primary related Standards 2210 Engagement objectives)

1. Internal auditors establish engagement objectives to address the risks associated with the activity under review. For planned engagements, the objectives proceed and align to those initially identified during the risk assessment process from which the internal audit plan is derived. For unplanned engagements, the objectives are established prior to the start of the engagement and are designed to address the specific issue that prompted the engagement.

2. The risk assessment during the engagement's planning phase is used to further define the initial objectives and identify other significant areas of concern.

3. After identifying the risks, the auditor determines the procedures to be performed and the scope (nature, timing, and extent) of those procedures. Engagement procedures performed in appropriate scope are the means to derive conclusions related to the engagement objectives.

Practice Advisory 2210.A1-1 Risk Assessment in Engagement Planning

*(Primary related Standards 2210.A1 Engagement objectives)*

1. Internal auditors consider management's assessment of risks relevant to the activity under review. The internal auditor also considers:

   - The reliability of management's assessment of risk.
   - Management's process for monitoring, reporting, and resolving risk and control issues.
   - Management's reporting of events that exceeded the limits of the organization's risk appetite and management's response to those reports.
   - Risks in related activities relevant to the activity under review.

2. Internal auditors obtain or update background information about the activities to be reviewed to determine the impact on the engagement objectives and scope.

3. If appropriate, internal auditors conduct a survey to become familiar with the activities, risks, and controls to identify areas for engagement emphasis, and to invite comments and suggestions from engagement clients.

4. Internal auditors summarize the results from the reviews of management's assessment of risk, the background information, and any survey work. The summary includes:

- Significant engagement issues and reasons for pursuing them in more depth.
- Engagement objectives and procedures.
- Methodologies to be used, such as technology-based audit and sampling techniques.
- Potential critical control points, control deficiencies, and/or excess controls.
- When applicable, reasons for not continuing the engagement or for significantly modifying engagement objectives.

Appendix 3 The Case Company's Risk Matrix example

(*Source: extract from AudiNet application used by the IA team*)

ACITIVITY/BUSINESS	RISK ASSESSMENT								SIZE		LAST AUDIT RATING			RECOMMENDATIONS FOLLOW-UP		FINAL ASSESSMENT			NEXT AUDIT					
	FINANCIAL INFORMATION RISK	CREDIT RISK	MARKET RISK	OPERATIONAL RISK	TECHNOLOGY RISK	COMPLIANCE RISK	BALANCE RISK	APPRAISAL	SIZE	APPRAISAL	LAST AUDIT DATE	LAST AUDIT RATING	APPRAISAL	RECOMMENDATIONS FOLLOW-UP	APPRAISAL	PRIORITY	PRIORITY FINAL LEVEL	LAST DATE AUDIT	MONTHS	MAX DATE	START DATE	CORE	ALL RATED
A	5	3		2	3	3		76	MEDIUM	66	aug.13	C+	60	100	0	63	TO BE WATCHED CLOSELY	02.08.2013	24	02.08.2015		S	TRUE
B	4	3		2	3	1		70	SMALL	33	aug.13	C+	60	100	0	55	TO BE WATCHED CLOSELY	02.08.2013	24	02.08.2015		S	TRUE
C				2	3			58	LARGE	100	okt.13	B	40	100	0	54	NORMAL	18.10.2013				N	TRUE
D				2	3			58	LARGE	100	okt.13	B	40	100	0	54	NORMAL	18.10.2013				N	TRUE
E	2			2	2			40	LARGE	100	okt.13	B	40	100	0	45	NORMAL	18.10.2013				N	TRUE
F	1			2	1			22	SMALL	33	okt.13	B	40	100	0	26	NO CAUSE FOR CONCERN	18.10.2013				N	TRUE

Inherent risk   Significance   Control environment   Residual risk
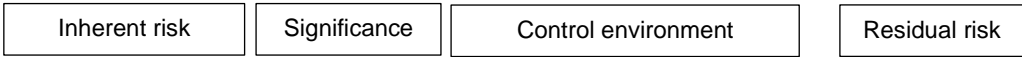
Audit Plan

Appendix 4 – The Case Company's Audit Plan Document Template
(*Source: IA methodology manual – summary only*)

1. AUDITED UNIT
   - Identification of the audited unit, business, activity or process.

2. OBJECTIVES AND WORK PROGRAMME
   Description on
   - Audit objectives and scope
   - Risks to be reviewed
   - Any limitations to a specific scope, risks that will not be reviewed, etc.
   - Work program that will be used to conduct tests required. If standard work programs built by the Group Internal Audit Division are not used, justifications and alternative work tests must be explained.

3. WORK TEAM
   - Composition of all auditors assigned to the job and number of days assigned to each member.

4. PARTIES RESPONSIBLE FOR THE REVIEW
   - Names & positions.

5. ESTIMATED DURATION OF WORK
   - Estimation of audit duration.

6. PRELIMINARY INFORMATION
   Description of all relevant aspects that contribute to knowledge of the situation, complexity, or problems of the audited unit and its activity will be included. For example:
   a. Rating and the most significant aspects of the previous audit.
   b. Organizational chart, unit's business, and significant changes.

c. Analysis on economic situation of the country and sector as well as circumstances that may affect the evolution of the unit's business.

d. Analysis of applicable regulations that may affect tests or findings related to accounting treatment or internal control system.

e. Result of external audits and reviews by regulatory bodies.

f. Any other relevant aspects.

7. WORK DISTRIBUTION DETAILS

- Distribution of tasks among audit team members.

8. CONCLUDING DOCUMENTS:

Indicate the final audit documents established according to the methodology:

- Audit Report (with or without rating), Audit Note, Audit Certificate or Consulting Note

Place, Date

(Signed)

Team Leader

Reviewed and Approved