

CCAF-FCVI Fellow
2005/2006

Risk Assessment: A Basis for Risk-Based Audit Practices

Strategic Paper by
Grace Mugyabuso



TANZANIA • CANADA

Table of Contents

	Page
Acknowledgement	v
Executive Summary	vii
Introduction	1
Background	1
Objectives of this paper	1
Rationale for a risk-based audit planning in audit practices	1
Overview of Risk	2
Key concepts	2
Sources of risk	3
Nature of risk and control	4
Risk Management Process	4
Risk identification	4
Risk assessment	5
Risk treatment and response	6
Risk monitoring and communication	8
Risk-based audit practices at the Office of the Auditor General (OAG) Canada	8
Integrated Risk Management	9
One Pass Plan	9
Practical example from the team	10
Project Design and Implementation	11
Presentation to Senior Management Group	11
Workshops	11
Pilot Project	11
Reference materials	12
Expertise, guidance, and support	12
Conclusion	12
Bibliography	13
Appendix—Risk assessment case study	14

Acknowledgement

This strategy paper is a result of the training I received during my participation in the CCAF Fellowship Program at the Office of Auditor General of Canada (OAG).

I would like to express my heartfelt thanks to all the partners who work hand-in-hand in this program: CIDA, CCAF, and OAG. Thank you for giving me a chance to participate.

The Financial Management Control team, under the Principal leadership of Clyde MacLellan and Director John Apt, have been a great help to me during my training and work experience in Canada. Thank you very much for your openness and eagerness to share your experience with me.

I owe many thanks to the leadership of the National Audit Office of Tanzania for accepting this Fellowship Program and allowing me to participate.

Special gratitude goes to my husband Deusdedit and my two little boys, Aaron and Abel. Thank you for your patience, understanding, and letting me come to Canada for this program.

Executive Summary

The objective of this research project, “Risk Assessment: A basis for Risk-Based Audit Practice”, is to create a proposal for advanced audit practices in the National Audit Office of Tanzania. The intention is to supplement a cash-and-control focus in our audits with modern risk-based approaches for planning and audit practices in the Office. The focus of these risk-based audit practices is on how well the entity manages its major risks, which can cause challenges as it attempts to reach its objectives.

The paper is based on research and the experience I gained from the CCAF Fellowship Program at the Office of Auditor General of Canada (OAG).

As I wrote this paper, I kept two critical ideas in mind:

- Introduce risk assessment as a basis for planning audits, the key concepts of this approach, and the rationale behind the methodology.
- Explain the “how to” concepts. I inserted an example of what is supposed to be done and how it is being done at the OAG Canada—that is, the Integrated Risk Management Framework, for corporate risk management, and the One Pass Plan methodology for audit operations.

In the National Audit Office of Tanzania (NAOT), we still use the term value-for-money (VFM) instead of performance audit. Therefore, in this strategy paper I may use these two terms interchangeably.

NAOT audit entities are ministries, departments, agencies that receive funds from the Consolidated Fund of the Exchequer Account, and the local government authorities of the United Republic of Tanzania. In this paper, when I refer to departments or entities, I am referring to these NAOT audit entities.

Introduction

Background

1. The National Audit of Tanzania (NAOT) was formerly known as the Exchequer Department of the government of the United Republic of Tanzania. In July 2001, the legislation was reformed and the *Public Finance Act no. 6 of 2001* was introduced. The Act broadened the mandate of the Controller and Auditor General to include value-for-money audits. With this mandate, the Office decided to start a value-for-money unit. The unit is specifically striving to get itself set up to conduct value-for-money audits of the government of Tanzania.

Objectives of this paper

2. The purpose of this paper is to provide guidance to auditors in NAOT by helping them in planning their audits using a risk-based audit approach. This paper will help to build a basis for planning with the expected output of establishing a concise, common, and consistent base for selecting audit topics for both value-for-money and financial audits. For the case of implementing this project, I will start with value-for-money audits. Later, the Senior Management Group will discuss the possibility of extending the project to financial audits.

3. In this paper, I have outlined the process and procedures for planning an effective risk-based audit.

4. Although NAOT has not yet issued a specific report on performance auditing, it has been doing comprehensive audits for years, along with its annual financial audits on public accounts, audits of local government authorities and audits of special donor-funded projects. This is evidenced by reading various annual reports issued by the Office.

Rationale for a risk-based audit planning in audit practices

5. Risk-based audit planning is the modern audit practice that involves planning and executing an audit basing on significant risks to an audit entity. For NAOT, this practice will shift the current focus of our audits from cash-and-control to areas that are significant to all Tanzanians.

6. The rationale behind this approach is to do the following:

- Help preserve and document NAOT's knowledge of government entities and the risks to which they are exposed.
- Support the decision making process within the Office in regard to audit topics selection. With a risk-based audit plan, priority will be given to areas of significant

risks and so will the execution of the audits. Due care is exercised here, which will add value to our methodologies.

- Provide common entity risk profile analyses for audit planning purposes. This helps to document a consistent, systematic, and integrated approach for assessing our audit entities in a language that is common to all auditors in the Office.
- Focus efforts on identifying, monitoring and managing risks to the Office in the process of selecting audit topics and executing audits. This is mainly concerning the corporate risk management.
- Give an opportunity for the Office to assure Parliament that it is devoting its efforts to the most important areas.
- For its own corporate risks, the practice will serve NAOT to get an awareness of its own corporate challenges, identify the risks, and to find ways to mitigate those challenges.

These practices, in turn, will help to build the Office's credibility and demonstrate its professionalism and objectivity.

Overview of Risk

Key concepts

7. Definition of risk. Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives¹.

8. The Office of Auditor General (OAG) of Canada defines risk as "the probability that an event or action may adversely affect the organization, such as exposure to financial loss, loss of reputation, or failure to deliver the program with economy, efficiency, cost-effectiveness or taking into account the environmental implications."²

9. In simple terms, risk is a challenge that an organization faces in its day-to-day activities.

10. Risk assessment. Risk assessment involves establishing the context for a risk, identifying, analyzing, evaluating, and treating risks. It "includes asking several key questions:

- What may go wrong?
- What is the probability of it going wrong?

¹ Treasury Board of Canada Secretariat

² Intranet, Performance Audit Bus Tour—Risk Assessment definitions.

- What are the consequences?
- Can the risk be minimized or controlled?"³

11. Assessing the degree of risk requires knowledge of the audit subject and sound judgement, which will help to determine what to audit and to know how to conduct the audit.

12. Risk management⁴. Risk management is a systematic and repeatable process for identifying, assessing, responding to, and monitoring risks to key objectives. Good risk management is proactive, not reactive, and is linked to setting priorities and allocating resources. It provides managers with a systematic approach to setting the best course of action under uncertainty. It supports risk-based audit practices.

Sources of risk

13. The internal and external business conditions inherently expose an entity to risk. These sources among others are

- Internal business conditions
 - size and complexity of an entity's operations
 - degree of knowledge required
 - degree and recentness of change
 - legislative and regulatory requirements
 - workload and transaction volumes
 - degree of dependencies
 - geographical dispersion
- External business conditions
 - new public management trends
 - political influences
 - shifting public values and demographics
 - global environment
 - volatility of international markets
 - market trends and trade
 - regulatory and legislative constraints
 - financial constraints.

³ OAG Intranet, Performance Audit Bus Tour.

⁴ Definition consistent with OAG Risk Management Policy

Nature of risk and control

14. Inherent risk is an expression of the likelihood and impact of a specific event or circumstance, before controls are considered. Inherent risk considers the underlying business conditions and operating environment of an entity.
15. Residual risk provides a description of the remaining level of risk (likelihood and impact) to an objective or outcome after taking into consideration the controls or other mitigation measures in place.
16. Controls are actions taken by management to enhance the likelihood of achieving established objectives and goals.

Risk Management Process⁵

17. Generally, a risk management process involves the key steps depicted in the following diagram. A detailed explanation follows in paragraphs 18–28.



Risk identification

18. Risk identification is identifying and understanding the events that may prevent an entity from achieving its objectives. It involves analyzing risk factors—that is, analyzing all the factors, drivers, and sources of risk that the entity is exposed to. Brainstorming on the causes and effects of the risk is the key step here (i.e. identifying the audit universe).

⁵ Adapted from OAG training on Risk Management by INTERIS “Experts in Managing Risk”.

19. Risk identification involves

- reviewing an entity's key documents, including the entity's mandate document (the enabling legislation), strategies for meeting stakeholders' needs, and minutes of executive meetings;
- interviewing key senior management, to understand their views toward the entity's objectives and their roles and responsibilities in achieving those objectives; and
- interviewing entity's stakeholders—understanding who the stakeholders of the entity are and what their expectations are will help to build awareness and identify key risks to achieving their expectations.

Risk assessment

20. Risk assessment involves

- measuring risks based on the residual (net) exposure, by considering the adequacy and effectiveness of control systems;
- assessing the current controls or risk mitigation practices; and
- analyzing residual risk exposure by identifying likelihood and impact.

21. The techniques for assessing risks include

- control models, questionnaires, and risk-control matrices to determine how well the identified risks are managed;
- qualitative and quantitative rating of risks (likelihood and impact); and
- qualitative ranking through brainstorming, structured interviews, and paired comparisons.

22. Factors to consider

- How well are the controls working to manage the likelihood or impact of risks?
- Have there been any recent incidences of control breakdown? If so, will this have an impact on the risk level?
- What are the specific consequences for the organization if such risks materialize? Is it financial, reputational, operational, strategic, or environmental?
- Does the organization have excessive controls? They can be as damaging and costly as insufficient controls, as they consume human resources and could slow down processes.

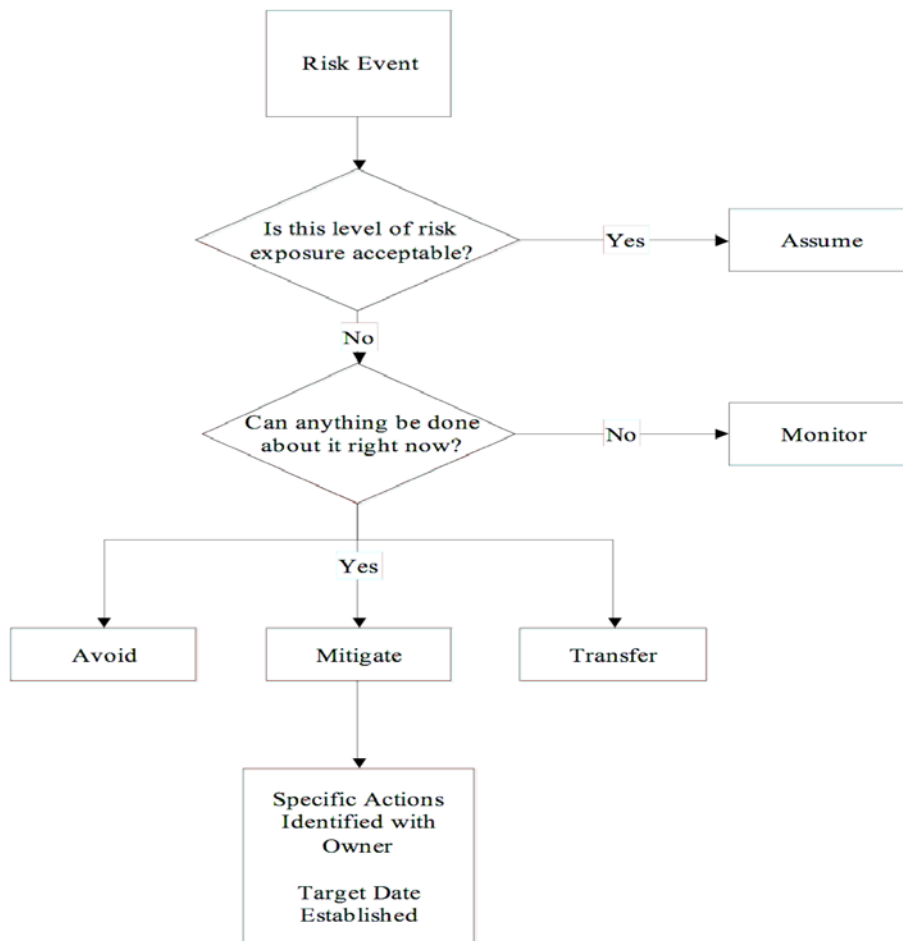
Risk treatment and response

23. Risk treatment. Make decisions about risk treatment in a way that balances the cost of risk mitigation against the probable cost of the exposure. The techniques are

- cost-benefit analysis,
- action planning, and
- established escalation criteria.

24. Risk response. Some decisions to mitigate risks may lead to another risk and cost. The best practice is to use the cost-benefit analysis for every control on risks.

25. The following illustration shows the process for responding to risks:



26. When responding to risks, consider the following:

- What types and levels of risk is management willing to accept? Management are expected to communicate on the level of risks they are willing to tolerate. This should be clear and reflected in the risk map for all employees in the Office.
- When and why should a risk be escalated? Establish escalation rules that support risk decisions.
- What actions are needed to manage risk within tolerable levels?
- How much will risk management cost?
- Is risk management tied directly to risk sources, root causes, and/or control weaknesses?
- Are management actions clear and measurable, and are owners and resolution dates clearly identified and tracked?

27. The following table shows how management should respond to the level of exposure for each risk:

Level of exposure	Required response	
	Management's actions	Monitoring
High risk	<ul style="list-style-type: none"> • Escalate the risk to the Executive (Senior Management)—Mandatory • Develop a risk mitigation action plan to mitigate the risk level in 6 months—Required • Make significant investments or reallocate resources—Possible 	Required monitoring by Executive as defined in risk action plan (weekly/monthly action plan)
Moderate risk	<ul style="list-style-type: none"> • Transfer the risk to Permanent Secretary or their designate. • May have to mitigate or monitor the risk or make changes to policies or operating procedures 	Periodic monitoring by the Permanent Secretary or their designate (quarterly or annually)
Low risk	<ul style="list-style-type: none"> • Manage the risk using existing policies and procedures • Investigate opportunities to reallocate resources to areas of high risk 	No monitoring required

28. Risk response strategy. In responding to risks, the following strategies are available. A strategy may be applied depending on how intense the risk is to the entity. The risk manager may:

Response strategy	Action
Avoid	The organization will not undertake the activity—the risk associated with it is unacceptable.
Mitigate	The risk owner (the entity's unit under risk) will take action prior to the occurrence of the risk to either reduce the likelihood that it will occur, and/or mitigate the impact, should it occur.
Monitor	The risk owner (the entity's unit under risk) will not do anything before the risk occurs. However, the owner will develop a contingency plan to control the impact if the risk does occur.
Assume	The risk owner (the entity's unit under risk) accepts the risk and will not prevent its occurrence or mitigate its impact.
Transfer or Escalate	The risk owner (the entity's unit under risk) does not have the control authority to deal with the risk and will transfer or escalate risk management to another party.

Risk monitoring and communication

29. Information on risk needs to be communicated for monitoring purposes. Responsibility for risk monitoring should be explicitly designated and simply stated. A dialogue is encouraged to help build a risk-smart organization and to avoid surprises.

30. Factors to consider

- Who needs what information, at what level, and how often?
The frequency of the monitoring and reporting should be determined in part by the action plan and the nature of business conditions
- How will increasing risk levels be identified?
Risk indicators should provide early warning signs.

Risk-based audit practices at the Office of the Auditor General (OAG) Canada

31. At OAG Canada, there are two risk levels. The first is at the Corporate Services level. This is a requirement of the Treasury Board of Canada, for which the Deputy Auditor General is responsible. The second risk level is the audit entities risk analyses, which the Assistant Auditors General deal with in audit operations for their areas of responsibilities.

32. Paragraphs 33 to 40 give a distinct explanation on the risk assessment levels. In paragraph 41, I inserted a practical example of the audit I was involved with in my OAG team assignment.

Integrated Risk Management

33. In response to requirement of the Treasury Board of Canada Secretariat⁶, OAG Canada has developed its own Policy on Risk Management as well as the Integrated Risk Management (IRM) framework⁷. To fulfil its mandate, OAG Canada uses the IRM framework to assess the corporate key risks based on its values and objectives, by assessing the mitigation controls and communicating the Executive Committee's risk tolerance levels. The IRM framework is the communication tool for risk management in OAG Canada.

One Pass Plan

34. The OAG Canada uses a One Pass Plan (OPP) approach for a more systematic, integrated, and risk-based entity audit planning. OAG Canada uses this approach to analyze the audit entities and their risk profile when it plans for performance audits. The following steps make up the OPP approach.

- **Interviews and document review**
 - Conduct interviews and receive feedback from senior entity management, personnel that have experience with the department, and stakeholders.
 - Review department's key documents—corporate plans, Integrated Risk Management framework, performance reports to Parliament, and internal audit reports.
 - Complete the “what we did” template, which lists key interviews held and key resource documents used.
- **Document the knowledge of the entity**
 - Ensure a thorough understanding of the entity's objectives, expected results and responsibilities, key stewardship responsibilities of the entity, quantitative information on size of responsibility, and key mandate and financial authorities that apply to entire entity.
 - Prepare the “Knowledge of Entity” template—a template that summarizes the entity's enabling legislation, other key mandate and financial authorities, mission and objectives, high-level strategies to achieve objectives, and business and operational structure.

⁶ <http://www.tbs-sct.gc.ca> Integrated Risk Management framework

⁷ OAG Integrated Risk Management framework.\RISK ASSMT\OAG IRM Framework.doc.

- **Prepare entity risk and control profile**
 - Identify significant external factors, challenges, and opportunities that the entity needs to manage well—including OAG Canada recommendations that have not been implemented.
 - Consider factors that will have significant impact on the entity and that the entity must respond to, by managing the impact or taking the opportunity to improve efficiency and effectiveness.
 - Discuss risks with external stakeholders, including entity’s clients, partners, and suppliers.
- **Risk profile used for chapter proposals**
 - The risks identified will be used to plan for audits to be done over four years. Chapters are now proposed and given due dates for submission to the Parliament (for tabling). The chapters should be linked to the OAG mandate and focus area.
- **Low risk areas**
 - The risks that are ranked low are not just ignored. The audit teams may use them to plan for an audit that may not be as important as the areas with high and medium rankings. These low risks may be considered for reporting as audit notes, which the Auditor General reports separately in shorter chapters. An audit on these risk rankings will, therefore, depend on the availability of audit resources.
- **Review with the Executive Committee⁸**
 - The last step is to present the OPP to the Executive Committee. The presentation is kept at a high level by focussing on the key risks to the entity that have not been properly mitigated.

Practical example from the team

35. The Government of Canada introduced travel cards in all its government departments. The OAG Financial Management Control team is now auditing the system, and the report will be tabled in April 2007. In the appendix to this strategy paper, there is a practical example of risk assessment from the audit for the travel card program.

⁸ The whole process of One Pass Plan has to have the Executive Committee’s approval.

Project Design and Implementation

Presentation to Senior Management Group

36. The first thing I will do to implement my project is meet with the NAOT Senior Management Group (SMG) to introduce to them the methodology of risk-based audit planning in performance auditing. The agenda is to explain the importance of adapting risk-based audit practices in all our audit products. The target date for this proposed meeting is within three months of June 2006.

Workshops

37. I expect to conduct two workshops to introduce risk-based audit practices. Depending on availability of resources and support from the Office and our support partners in donor countries (for example, the Sweden National Audit Office), I will be able to conduct more workshops in future with all auditors in the Office.

38. Workshop for senior managers. I am planning to conduct a one-day workshop for the SMG on the risk assessment and risk management methodologies. The target group is not necessarily the whole SMG, rather, the senior managers that are responsible for planning audits in the Office. I will depend on SMG support for the timing of the workshop, organizing the training, and providing transportation to senior managers not based in Dar es Salaam. The target date for this workshop is within six months of June 2006.

39. Workshop for middle level managers. I will conduct another workshop for the NAOT middle level managers to teach them risk assessment techniques and the methodology to apply when planning performance and financial audits. The target completion date for this workshop is within one year of June 2006.

Pilot Project

40. This will involve reorienting the Strategic Planning Group. With support of consultants from the Sweden National Audit Office, NAOT formed a Financial Audit Strategy group, which, among other things, was responsible for developing a strategy for NAOT risk assessments for financial audits. I will use this group to

- start a pilot project on Risk-Based Audit Planning, from a performance audit perspective;
- assess risks in entities, which will be approved by the SMG as our pilot project (for this project); and
- develop an audit proposal for those entities based on the result of our risk assessment.

This pilot project is a very important step for me in implementing my project. I look forward to the SMG approving this pilot project, as CCAF will be following up on my project. The target date for this pilot project is within one and a half years of June 2006.

Reference materials

41. After we complete our pilot project, I expect to put together all materials used in our pilot project and make them available in the NAOT library as references for auditors. Depending on the resources available in the Office, the materials will be in the form of a handbook, a CD-Rom, or flash discs.

Expertise, guidance, and support

42. I will also be available as a resource person in the Office to assist colleagues in risk assessment and risk management. Depending on what my assignment in the Office is after this CCAF training, I will provide guidance and support to all auditors who require it.

Conclusion

43. Risk-based audit planning is a modern way to plan an audit. The focus is on how well an entity is managing major risks, not simply focussing on areas of suspected weaknesses. Because auditors are not involved in the day-to-day activities of their audit entities, a risk-based approach to plan and execute the audit will help auditors serve Parliament better. They will be able to set priorities for audits according to what the parliamentarians may consider urgent and important—significant to Tanzanians.

44. The NAOT should be able to adapt the methodology to identify audit priorities and plan future audits, within two years of June 2006. CCAF will follow up on this project as it does for other projects undertaken by participants in the Fellowship Program.

Bibliography

Citizenship and Immigration Canada, (January, 2006) Internal Audit and Disclosure Branch Risk-Based Audit Planning for Assurance and Advisory Services.

Citizenship and Immigration Canada, (January, 2006) Internal Audit and Disclosure Branch Risk Assessment and Audit Program Planning.

OAG, (February, 2006) Risk Management course material by INTERIS—Experts in Managing Risk.

OAG Intranet (September, 2004), Guidance in preparing One Pass Plan.

OAG, (October 26, 2005) PWGSC One Pass Plan by Bruce Sloan.

Treasury Board of Canada Secretariat, (April, 1999), Best practice in Risk Management—Coordinated conclusions from PMN and KPMG.

Treasury Board of Canada Secretariat (May 2003), Integrated Risk Management Framework

Treasury Board of Canada Secretariat, (April, 1999), Review of Canadian Best Practices in Risk Management.

Treasury Board of Canada Secretariat (November, 2001) Risk Management Policy.

Appendix—Risk assessment case study

The audit of travel cards

Background

Travel cards are essentially credit cards that are approved by the employer, and that employees use for expenses when they travel on official business. The benefits of a travel card include

- car, hotel, and life insurance coverage;
- rebates to the government;
- efficient, secure and convenient methods of paying for official government travel related expenses; and
- reduced need for the government to issue travel advances.

Audit rationale: risk

The Office of the Auditor General of Canada (OAG) has determined that there should be an audit of the use of travel cards for several reasons, including

- travel card use has not been recently audited by the Office,
- trends reveal increased use of travel cards since their introduction in 1991,
- recent newspaper articles have highlighted cases where the travel cards have been improperly used,
- the improper use of the travel cards has damaged the government's reputation and credibility, and
- significant resources are needed to address the cases of abuse.

The Financial Management and Control (FMC) team felt that the risks warranted an audit and proposed this to the Performance Audit Management Committee (PAMC). PAMC is comprised of senior executives from OAG Canada that consider all audit proposals to ensure an appropriate decision making framework to initiate performance audits.

PAMC was in agreement with the audit team's risk assessment and approved the audit.

Audit survey

The audit team did a survey to better understand the travel card program, and to document and understand the control framework used to manage the program.