Risk assessment tools for effective internal controls

How to identify and mitigate risk using comprehensive surveys of key operational areas

Authors: Jeffrey D. Sherman, B.Comm., M.B.A., C.A. and Colin Braithwaite, B.A.

Editor: Adam Gorley

First Edition: September 2008
Second Edition: October 2010
This guide provides a general introduction to effective internal controls and shows how to build them with strong policies and procedures. It will help you to identify the areas where your organization is most vulnerable to risk and use the cross-references in the Risk Assessment Checklists to identify the specific policies that can be used to address those risks.

Price: $79.95

Authors: Jeffrey D. Sherman, B.Comm., M.B.A., C.A. and Colin Braithwaite, B.A.

Editor: Adam Gorley

First Edition September 2008
Second Edition: October 2010

Library and Archives Canada Cataloguing in Publication

Sherman, Jeffrey D. and Braithwaite, Colin
Risk Assessment tools for effective internal controls/ by Jeffrey D. Sherman and Colin Braithwaite

ISBN 0-9735149-7-3
Print ISSN: 1925-0428
Online ISSN: 1925-0436

1. Auditing, Internal. I. Title.
# Table of contents

1.0 About the guide ........................................................................................................ 6

1.1 What Risk Assessment Checklists are available? .................................................. 7
  1.1.1 Finance and Accounting ................................................................. 7
  1.1.2 Operations ..................................................................................... 7
  1.1.3 Information Technology ................................................................. 7
  1.1.4 Not-for-Profit Organizations ............................................................ 7

1.2 How do you get the Risk Assessment Checklists? .............................................. 7

2.0 Internal Control .................................................................................................... 7

  2.1 Responsibility for internal control ............................................................ 7
  2.2 What is internal control? .......................................................................... 7
  2.3 What is the impact of internal controls? .................................................... 8
      2.3.1 Internal controls and not-for-profits .............................................. 8
  2.4 Mechanisms used for control ..................................................................... 8
  2.5 The role of policies and procedures in internal control ............................ 9
  2.6 We are here to help ................................................................................. 10

3.0 Building a policy manual ..................................................................................... 10

  What makes an effective policy? ............................................................................ 10

  3.1 Task 1 – Defining your policy manual process .......................................... 10
  3.2 Task 2 – Researching your policies .......................................................... 11
  3.3 Task 3 – Writing your policies ................................................................. 11
  3.4 Task 4 – Approving your policies ............................................................ 11
  3.5 Task 5 – Distributing your policies .......................................................... 12
  3.6 Task 6 – Maintaining your policies .......................................................... 12

4.0 Finance and accounting policies ......................................................................... 12

  4.1 Internal control over financial reporting .................................................... 12
  4.2 The broader importance of finance and accounting controls .................... 13
  4.3 Key concepts ............................................................................................ 13
      4.3.1 Accounting processes ................................................................. 13
      4.3.2 Financial accounting ................................................................. 13
      4.3.3 Management accounting ............................................................ 14
      4.3.4 Financial statement assertions .................................................... 15
4.3.5 Key processes and controls
4.3.6 Materiality

5.0 Governance policies

5.1 The importance of governance policies
5.1.1 Strategy and planning
5.1.2 Legal and regulatory controls
5.1.3 Risk management

6.0 Operational policies

6.1 The importance of operational policies
6.2 Operational policies and compliance
6.3 About quality and quality systems

7.0 Information Technology policies

7.1 The role of IT governance
7.2 IT policies and compliance

8.0 Not-for-profit policies

8.1 Governance policies in NPOs
8.2 Controls required for NPOs

9.0 Internal control frameworks

9.1 Internal control frameworks and the Internal Control Library
9.1.1 Finance and Accounting PolicyPro (FAPP)
9.1.2 Information Technology PolicyPro (ITPP)
9.1.3 Not-for-Profit PolicyPro (NPPP)

9.2 COSO Internal Control – Integrated Framework

9.3 Quality control frameworks
9.3.1 ISO 9000
9.3.2 ISO 14000
9.3.3 Why Consider ISO Certification?

9.4 IT control frameworks
9.4.1 COBIT – Control Objectives for Information and Related Technology
9.4.2 ITCG – Information Technology Control Guidelines
10.0 Risk Assessment Checklists

10.1 About the Risk Assessment Checklists

10.2 Risk Assessment Checklists and the Internal Control Library

10.3 Risk Assessment Checklists and Internal Control Frameworks

Appendix A - Sample Policy: Expense Authorization

Appendix B: Finance and Accounting PolicyPro table of contents

Appendix C: Information Technology PolicyPro table of contents

Appendix D: Not-for-Profit PolicyPro table of contents
1.0 About the guide

This guide provides a general introduction to effective internal controls and shows how to build them with strong policies and procedures. The accompanying risk assessment checklists, included free with this guide, provide detailed lists of controls you should consider for your for-profit and not-for-profit organization, and cross references these controls to the relevant policies in the Internal Control Library consisting of Finance & Accounting PolicyPro, Information Technology PolicyPro and Not-for-Profit PolicyPro. With this guide, you can:

1. Identify the areas where your organization is most vulnerable to risk.

2. Use the cross-references in the Risk Assessment Checklists to identify the specific policies that can be used to address those risks.

Risk assessment is the foundation of internal control. Without understanding the risks your organization faces, you cannot take effective measures to eliminate or mitigate them.

The Risk Assessment Checklists are built on the foundation of several of the best-known internal control frameworks, including:

» The COSO Internal Control–Integrated Framework (ICIF) that has become the standard for evaluating internal control over financial reporting in Canada and the United States. Although COSO is most often associated with financial controls, it also covers operational areas such as shipping, receiving, storage and warehousing. The COSO framework is the basis of most of the Finance and Accounting and Operations checklists.

» COBIT (Control Objectives for Information and Related Technology), first published in 1996 by the Information Systems Audit and Control Association. It has become the most widely accepted framework used in evaluating IT controls. The IT Plan and Organize, Acquire and Implement and Deliver and Support checklists are organized according to COBIT 5.1.

» ITCG (Information Technology Control Guidelines), published by the Canadian Institute of Chartered Accountants (CICA) which has guided information technology controls in Canada for many years. The risks to consider in the IT Plan and Organize, Acquire and Implement and Deliver and Support checklists are, for the most part, derived from ITCG.

These internal control frameworks are discussed in more detail later in this guide.

The risks identified in the checklists are crossreferenced to ready-to-use policies within the publications in the Internal Control Library, co-published by First Reference and the CICA. See below for a small sample of the Purchasing Cycle Risk Assessment Checklist.

The Internal Control Library is based on the principle that well-written, well-informed and well-enforced policies and procedures are the best defense against risks that could prevent your organization from meeting its objectives. A sample policy can be found in Appendix A.

<table>
<thead>
<tr>
<th>Purchasing Cycle risks to consider</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comments / Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pur1</td>
<td>Do you ensure that personnel responsible for the purchasing, shipping, receiving and payable functions are competent, adequately trained and supervised? See OP 4.06, see also Human Resources PolicyPro</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Pur2</td>
<td>Do you ensure that expenses are properly authorized? See FN 2.01, 2.02, 2.03, 2.04, 2.07</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Pur3</td>
<td>Do controls exist to ensure corporate buying cards are only issued to authorized staff and personal purchases are not allowed? See FN 2.01, 2.03</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Pur4</td>
<td>Do you ensure that contracts are properly reviewed and authorized? See FN 2.01</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>
If you are the CEO or CFO of an organization that already has risk assessment, risk management and internal control processes in place, the Risk Assessment Checklists will be a very useful input in your existing risk-focused approach.

However, if you are new to risk assessment and risk management, engaged in building a new policy manual or revising an existing manual, this guide also provides guidance on internal controls and the policy creation process.

1.1 What Risk Assessment Checklists are available?

1.1.1 Finance and Accounting
   » The Revenue Cycle
   » The Purchasing Cycle
   » Inventory
   » Payroll
   » Banking and Treasury
   » Fixed Assets
   » Accounting and Reporting
   » Control Environment

1.1.2 Operations
   » Receiving
   » Shipping
   » Operations
   » Sales and Marketing
   » Service

1.1.3 Information Technology
   » Plan and Organize
   » Acquire and Implement
   » Deliver and Support

1.1.4 Not-for-Profit Organizations
   » NPO Governance

1.2 How do you get the Risk Assessment Checklists?

The Risk Assessment Checklists are free with this guide. Visit www.firstreference.com/riskassessment to download the checklists.

2.0 Internal Control

2.1 Responsibility for internal control

Internal controls were once relatively obscure, of interest only to accountants, auditors and financial staff. But times have changed—now company presidents, CEOs, executive directors, boards of directors and CFOs are explicitly charged with responsibility and accountability for internal controls within their organizations.

If you are an executive of a for-profit or a not-for-profit organization, your stakeholders—business owners, shareholders, investors, bankers, funders, insurers, suppliers, customers, employees, or the community at large—hold you responsible for the effectiveness of your internal controls.

Even the smallest organization needs some level of internal control. For an owner-operated business, this may mean something as simple as a separation of duties for accounts payable, where the owner insists that he or she signs the cheques that the accountant prepares. For a small not-for-profit, it may mean governance policies that clearly define the responsibilities of the board of directors and the executive director.

2.2 What is internal control?

Internal control is a process put in place by a board of directors, senior management and all levels of personnel to provide reasonable assurance that the organization will achieve its objectives. The internal control process operates continually at all levels within an organization to mitigate exposure to risks that could prevent it from achieving these objectives.

The board of directors and senior management are responsible for establishing the appropriate culture—the so-called “tone at the top” that fosters the development of an environment in which an effective internal control process can flourish. But everyone in an organization must participate in internal control. Senior managers assign responsibility for establishing specific internal control policies and procedures, and line managers and key employees participate in the policy-writing process by providing input to the policy creation teams. All employees must sign off on approved policies and procedures and are responsible