The Operational Auditing Handbook
This page intentionally left blank
Contents

Preface xv
Acknowledgements xvii

Part 1  Understanding Operational Auditing 1

1 APPROACHES TO OPERATIONAL AUDITING 3
   Definitions of “Operational Auditing” 3
   Scope 4
   Audit Approach to Operational Audits 12
   Resourcing the Internal Audit of Technical Activities 16
   Productivity and Performance Measurement Systems 19
   Value for Money (VFM) Auditing 22
   Benchmarking 23

2 BUSINESS PROCESSES 27
   Introduction 27
   An Audit Universe of Business Processes 28
   Self Assessment of Business Processes 30
   A Hybrid Audit Universe 30
   Reasons For Process Weaknesses 30
   Identifying the Processes of an Organisation 32
   Why Adopt a “Cycle” or “Process” Approach to Internal Control Design and Review? 35
   Business Processes in the Standard Audit Programme Guides 35
   The Hallmarks of a Good Business Process 36
   Academic Cycles in a University 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>DEVELOPING OPERATIONAL REVIEW PROGRAMMES FOR MANAGERIAL AND AUDIT USE</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Scope</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Practical Use of SAPGs</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Format of SAPGs</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Risk in Operational Auditing</td>
<td>50</td>
</tr>
<tr>
<td>4</td>
<td>GOVERNANCE PROCESSES</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Internal Control Processes being Part of Risk Management Processes</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Risk Management Processes being Part of Governance Processes</td>
<td>76</td>
</tr>
<tr>
<td></td>
<td>Objectives of Governance, Risk Management and Control Processes</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>The COSO View of Objectives</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>Should there be a Single Set of Objectives?</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>The Internal Governance Processes</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>The Board and External Aspects of Corporate Governance</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>The Board’s Assurance Vacuum</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>Risk and Control Issues for Internal Governance Processes</td>
<td>84</td>
</tr>
<tr>
<td></td>
<td>Risk and Control Issues for the Board</td>
<td>87</td>
</tr>
<tr>
<td></td>
<td>Risk and Control Issues for External Governance Processes</td>
<td>90</td>
</tr>
<tr>
<td>5</td>
<td>RISK MANAGEMENT PROCESSES</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Objectives of Risk Management</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Essential Components of Effective Risk Management</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>The Scope of Internal Audit’s Role in Risk Management</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Tools for Risk Management</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>The Risk Matrix</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>Risk Registers</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>Risk Management Challenges</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>Control Issues for Risk Management Processes</td>
<td>112</td>
</tr>
<tr>
<td>6</td>
<td>INTERNAL CONTROL PROCESSES</td>
<td>116</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>116</td>
</tr>
<tr>
<td></td>
<td>Paradigm 1: COSO on Internal Control</td>
<td>118</td>
</tr>
<tr>
<td></td>
<td>Paradigm 2: Turnbull on Internal Control</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>Paradigm 3: COCO on Internal Control</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>Paradigm 4: A Systems/Cybernetics Model of Internal Control</td>
<td>130</td>
</tr>
<tr>
<td></td>
<td>Paradigm 5: Control by Division with Supervision</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>Paradigm 6: Control by Category</td>
<td>137</td>
</tr>
</tbody>
</table>
7 REVIEW OF THE CONTROL ENVIRONMENT

Introduction 147
Control Objectives for a Review of the Control Environment 147
Risk and Control Issues for a Review of the Control Environment 148
Fraud 149

8 REVIEWING INTERNAL CONTROL OVER FINANCIAL REPORTING—THE SARBANES-OXLEY APPROACH

Introduction 151
Costs and Benefits 154
2007 SOX-LITE 155
Revised Definitions of “Significant Deficiency” and “Material Weakness” 156
Using a Recognised Internal Control Framework for the Assessment 157
Risk and Control Issues for the Sarbanes-Oxley s. 302 and s. 404 Compliance Process 171

9 BUSINESS/MANAGEMENT TECHNIQUES AND THEIR IMPACT ON CONTROL AND AUDIT

Introduction 178
Business Process Re-Engineering 178
Total Quality Management 181
Delayering 187
Empowerment 189
Outsourcing 191
Just-In-Time Management (JIT) 195

10 CONTROL SELF ASSESSMENT

Introduction 199
Survey and Workshop Approaches to CSA 200
Selecting Workshop Participants 200
Where to Apply CSA 200
CSA Roles for Management and for Internal Audit 201
Avoiding Line Management Disillusionment 202
Encouragement from the Top 203
| Facilitating CSA Workshops, and Training for CSA | 204 |
| Anonymous Voting Systems | 205 |
| Comparing CSA with Internal Audit | 205 |
| Control Self Assessment as Reassurance for Internal Audit | 206 |
| A Hybrid Approach—Integrating Internal Auditing Engagements with CSA Workshops | 206 |
| Workshop Formats | 207 |
| Utilising CoCo in CSA | 208 |
| Readings | 210 |
| Control Self Assessment | 210 |

### 11 EVALUATING THE INTERNAL AUDIT ACTIVITY

| Introduction | 214 |
| Ongoing Monitoring | 214 |
| Periodic Internal Reviews | 215 |
| External Reviews | 216 |
| Common Weaknesses Noted by Quality Assurance Reviews | 217 |
| Internal Audit Maturity Models | 218 |
| Effective Measuring of Internal Auditing’s Contribution to the Enterprise’s Profitability | 219 |
| Control Objectives for the Internal Audit Activity | 232 |

### Part II Auditing Key Functions

### 12 AUDITING THE FINANCE AND ACCOUNTING FUNCTIONS

<p>| Introduction | 239 |
| System/Function Components of the Financial and Accounting Environment | 239 |
| Control Objectives and Risk and Control Issues | 240 |
| Treasury | 241 |
| Payroll | 243 |
| Accounts Payable | 246 |
| Accounts Receivable | 248 |
| General Ledger/Management Accounts | 251 |
| Fixed Assets (and Capital Charges) | 253 |
| Budgeting and Monitoring | 256 |
| Bank Accounts and Banking Arrangements | 258 |
| Sales Tax (VAT) Accounting | 261 |
| Taxation | 263 |
| Inventories | 266 |
| Product/Project Accounting | 268 |</p>
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>AUDITING SUBSIDIARIES, REMOTE OPERATING UNITS AND JOINT VENTURES</td>
<td>276</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>276</td>
</tr>
<tr>
<td></td>
<td>Fact Finding</td>
<td>277</td>
</tr>
<tr>
<td></td>
<td>High Level Review Programme</td>
<td>278</td>
</tr>
<tr>
<td></td>
<td>Joint Ventures</td>
<td>279</td>
</tr>
<tr>
<td>14</td>
<td>AUDITING CONTRACTS AND THE PURCHASING FUNCTION</td>
<td>285</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>285</td>
</tr>
<tr>
<td></td>
<td>Control Objectives and Risk and Control Issues</td>
<td>285</td>
</tr>
<tr>
<td></td>
<td>Contracting</td>
<td>289</td>
</tr>
<tr>
<td></td>
<td>Contract Management Environment</td>
<td>290</td>
</tr>
<tr>
<td></td>
<td>Assessing the Viability and Competence of Contractors</td>
<td>295</td>
</tr>
<tr>
<td></td>
<td>Maintaining an Approved List of Contractors</td>
<td>297</td>
</tr>
<tr>
<td></td>
<td>Tendering Procedures</td>
<td>299</td>
</tr>
<tr>
<td></td>
<td>Contracting and Tendering Documentation</td>
<td>302</td>
</tr>
<tr>
<td></td>
<td>Selection and Letting of Contracts</td>
<td>304</td>
</tr>
<tr>
<td></td>
<td>Performance Monitoring</td>
<td>306</td>
</tr>
<tr>
<td></td>
<td>Valuing Work for Interim Payments</td>
<td>308</td>
</tr>
<tr>
<td></td>
<td>Contractor’s Final Account</td>
<td>310</td>
</tr>
<tr>
<td></td>
<td>Review of Project Outturn and Performance</td>
<td>313</td>
</tr>
<tr>
<td>15</td>
<td>AUDITING OPERATIONS AND RESOURCE MANAGEMENT</td>
<td>317</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>317</td>
</tr>
<tr>
<td></td>
<td>System/Function Components of a Production/Manufacturing Environment</td>
<td>318</td>
</tr>
<tr>
<td></td>
<td>Control Objectives and Risk and Control Issues</td>
<td>318</td>
</tr>
<tr>
<td></td>
<td>Planning and Production Control</td>
<td>318</td>
</tr>
<tr>
<td></td>
<td>Facilities, Plant and Equipment</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>Personnel</td>
<td>324</td>
</tr>
<tr>
<td></td>
<td>Materials and Energy</td>
<td>327</td>
</tr>
<tr>
<td></td>
<td>Quality Control</td>
<td>330</td>
</tr>
<tr>
<td></td>
<td>Safety</td>
<td>332</td>
</tr>
<tr>
<td></td>
<td>Environmental Issues</td>
<td>335</td>
</tr>
<tr>
<td></td>
<td>Law and Regulatory Compliance</td>
<td>338</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>339</td>
</tr>
</tbody>
</table>
Labour Relations 430
Company Vehicles 432

19 AUDITING RESEARCH AND DEVELOPMENT 437
   Introduction 437
   System/Function Components of Research and Development 437
   Control Objectives and Risk and Control Issues 437
   Product Development 438
   Project Appraisal and Monitoring 442
   Plant and Equipment 445
   Development Project Management 447
   Legal and Regulatory Issues 450

20 AUDITING SECURITY 453
   Introduction 453
   Control Objectives and Risk and Control Issues 454
   Security 454
   Health and Safety 457
   Insurance 460

21 AUDITING ENVIRONMENTAL RESPONSIBILITY 463
   Introduction 463
   Environmental Auditing 465
   The Emergence of Environmental Concerns 465
   EMAS—The European Eco-Management and Audit Scheme 466
   Linking Environmental Issues to Corporate Strategy and Securing Benefits 467
   Environmental Assessment and Auditing System Considerations 468
   The Role of Internal Audit 470
   Example Programme 470

Part III Auditing Information Technology 477

22 AUDITING INFORMATION TECHNOLOGY 479
   Introduction 479
   Introduction to Recognised Standards Related to Information Technology and Related Topics 480
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>IT STRATEGIC PLANNING</td>
<td>489</td>
</tr>
<tr>
<td>24</td>
<td>IT ORGANISATION</td>
<td>493</td>
</tr>
<tr>
<td>25</td>
<td>IT POLICY FRAMEWORK</td>
<td>496</td>
</tr>
<tr>
<td>26</td>
<td>INFORMATION ASSET REGISTER</td>
<td>502</td>
</tr>
<tr>
<td>27</td>
<td>CAPACITY MANAGEMENT</td>
<td>511</td>
</tr>
<tr>
<td>28</td>
<td>INFORMATION MANAGEMENT (IM)</td>
<td>514</td>
</tr>
<tr>
<td>29</td>
<td>RECORDS MANAGEMENT (RM)</td>
<td>524</td>
</tr>
<tr>
<td>30</td>
<td>KNOWLEDGE MANAGEMENT (KM)</td>
<td>542</td>
</tr>
<tr>
<td>31</td>
<td>IT SITES AND INFRASTRUCTURE (INCLUDING PHYSICAL SECURITY)</td>
<td>554</td>
</tr>
<tr>
<td>32</td>
<td>PROCESSING OPERATIONS</td>
<td>559</td>
</tr>
<tr>
<td>33</td>
<td>BACK-UP AND MEDIA MANAGEMENT</td>
<td>562</td>
</tr>
<tr>
<td>34</td>
<td>REMOVABLE MEDIA</td>
<td>566</td>
</tr>
<tr>
<td>35</td>
<td>SYSTEM AND OPERATING SOFTWARE (INCLUDING PATCH MANAGEMENT)</td>
<td>570</td>
</tr>
<tr>
<td>36</td>
<td>SYSTEM ACCESS CONTROL (LOGICAL SECURITY)</td>
<td>576</td>
</tr>
<tr>
<td>37</td>
<td>PERSONAL COMPUTERS (INCLUDING LAPTOPS AND PDAs)</td>
<td>580</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>38</td>
<td>REMOTE WORKING</td>
<td>585</td>
</tr>
<tr>
<td>39</td>
<td>EMAIL</td>
<td>590</td>
</tr>
<tr>
<td>40</td>
<td>INTERNET USAGE</td>
<td>598</td>
</tr>
<tr>
<td>41</td>
<td>SOFTWARE MAINTENANCE (INCLUDING CHANGE MANAGEMENT)</td>
<td>605</td>
</tr>
<tr>
<td>42</td>
<td>NETWORKS</td>
<td>609</td>
</tr>
<tr>
<td>43</td>
<td>DATABASES</td>
<td>613</td>
</tr>
<tr>
<td>44</td>
<td>DATA PROTECTION</td>
<td>616</td>
</tr>
<tr>
<td>45</td>
<td>FREEDOM OF INFORMATION</td>
<td>627</td>
</tr>
<tr>
<td>46</td>
<td>DATA TRANSFER AND SHARING (STANDARDS AND PROTOCOL)</td>
<td>636</td>
</tr>
<tr>
<td>47</td>
<td>LEGAL RESPONSIBILITIES</td>
<td>645</td>
</tr>
<tr>
<td>48</td>
<td>FACILITIES MANAGEMENT</td>
<td>648</td>
</tr>
<tr>
<td>49</td>
<td>SYSTEM DEVELOPMENT</td>
<td>651</td>
</tr>
<tr>
<td>50</td>
<td>SOFTWARE SELECTION</td>
<td>655</td>
</tr>
<tr>
<td>51</td>
<td>CONTINGENCY PLANNING</td>
<td>658</td>
</tr>
<tr>
<td>52</td>
<td>HUMAN RESOURCES INFORMATION SECURITY</td>
<td>661</td>
</tr>
<tr>
<td>53</td>
<td>MONITORING AND LOGGING</td>
<td>667</td>
</tr>
<tr>
<td>54</td>
<td>INFORMATION SECURITY INCIDENTS</td>
<td>671</td>
</tr>
<tr>
<td>55</td>
<td>DATA RETENTION AND DISPOSAL</td>
<td>680</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>56</td>
<td>ELECTRONIC DATA INTERCHANGE (EDI)</td>
<td>688</td>
</tr>
<tr>
<td>57</td>
<td>VIRUSES</td>
<td>691</td>
</tr>
<tr>
<td>58</td>
<td>USER SUPPORT</td>
<td>694</td>
</tr>
<tr>
<td>59</td>
<td>BACS</td>
<td>696</td>
</tr>
<tr>
<td>60</td>
<td>SPREADSHEET DESIGN AND GOOD PRACTICE</td>
<td>699</td>
</tr>
<tr>
<td>61</td>
<td>IT HEALTH CHECKS</td>
<td>707</td>
</tr>
<tr>
<td>62</td>
<td>IT ACCOUNTING</td>
<td>710</td>
</tr>
</tbody>
</table>

Appendix 1  Index to SAPGs on the Companion Website  712  
Appendix 2  Standard Audit Programme Guides  719  
Appendix 3  International Data Protection Legislation  729  
Appendix 4  International Freedom of Information Legislation  763  
Appendix 5  Information Management Definitions  835  
Appendix 6  IT and Information Management Policies  839  

Bibliography  852  
Index  859  

Preface

The durability of this Handbook is indicated by the fact that the previous edition, first published in 1997, was in print until this second edition appeared. The Handbook was designed to fill a gap by providing an up-to-date guide to operational auditing, taking a business process approach. The format makes the book friendly as a practical Handbook.

New content for this edition includes in-depth consideration of governance processes, risk management processes and internal control processes. We have radically updated and much extended the content on auditing information technology, and our treatment of international data protection legislation and international freedom of information legislation does, we believe, give thorough and innovative coverage of these important contemporary topics. Indeed, users of this Handbook will find it gives them most of the up-to-date toolkit they need to provide an effective audit service in the field of information technology. Because compliance with s. 404 of the Sarbanes-Oxley Act has resulted in a widely applied approach to assessing the effectiveness of internal control over financial reporting, we have given that attention too. Readers will find more detailed coverage of control self assessment, and we have also included a chapter on assessing the internal audit activity. Where appropriate we have aligned this edition to the latest Standards of The Institute of Internal Auditors and to the pronouncements of other bodies.

The Handbook is intended as a companion for those who design self assessment programmes of business processes to be undertaken by management and staff. Likewise it is a mentor for internal auditors and consultants who conduct audits on behalf of others. We have developed the book to cater for private, public and not-for-profit sectors and to be a basis for designing value-for-money audit approaches. We also believe that external auditors dealing with financial and accounting systems and often engaged in management audits will find the book of value and should have it in their libraries.

At the same time we have had in mind the professional qualification requirements in this subject area of The Institute of Internal Auditors, with the intention that this book will be a suitable standard text. Particularly with the student in mind we have where appropriate supported specific points with cross-referenced notes which appear at the end of each chapter, and there is a comprehensive bibliography.
The book’s timeliness comes partly from the mix of business processes included, and the contemporary treatment given to each. In part it comes from the ways we have attempted to weave in the contemporary approaches and issues of, for instance, business process re-engineering, just-in-time management, downsizing, delayering, empowerment, environment, ethics, control self assessment and IT. In part it is a matter of the risk evaluation techniques which we describe as often being appropriate aids for those who must review and evaluate business processes.

The Handbook aims to raise the consciousness of the underlying issues, risks and objectives for a wide range of operations and activities. In other words, it aims to stimulate creative thought about the business context of operational audit reviews. In practice, it would be an extremely difficult task to define a set of universal panacea approaches to the audit of the various operational areas of any organisation, as the driving motivations and the contexts into which they are set would vary between entities. In adopting a business oriented stance supported by practical examples of the key questions to resolve, we hope that audit creativity will be encouraged rather than stifled by over-prescriptive programmes and routines. Readers will need to take account of their own experiences and the relevant aspects of the cultures prevailing within their organisations, and bring these to bear on the contents of this book, so that a suitably tailored approach to auditing operations emerges.

We have attempted to distinguish between on the one hand approaching audit work according to the way a business is structured, and on the other hand seeking to identify and then assess the natural business processes that step across organisational parts. It is often the latter approach to audit work that has the greatest potential to add value.

We are confident that the “real world” pedigree of this book will make it eminently useful for practising auditors, line managers, consultants, and those who intend to become qualified as operational auditors.

We would appreciate readers’ comments and advice for future editions.

Andrew Chambers
Management Audit LLP
The Water Mill
Moat Lane
Old Bolingbroke
Spilsby
Lincolnshire
PE23 4ES
England

Tel. & fax: +44 (0)1790 763350
Internet tel.: +44 (0)207 099 9355
Internet fax.: +44 (0)207 099 3954
Email: ProfADC@aol.com
Web: www.management-audit.com

Graham Rand
grahamrand@btinternet.com
Mobile: +44 (0)7729 374074
Acknowledgements

We thank our many clients and friends who have been the stimulus for much of the content and approach of this book. We are grateful to those who have kindly read through the full manuscript with care, making many useful suggestions which we believe have led to a better book. We have quoted from many sources: in every case we have endeavoured to provide full attribution for the material we have used and to obtain the appropriate permissions. If there has been any oversight on our part we apologise and would like to correct it at our first opportunity.

Andrew Chambers
Graham Rand
This page intentionally left blank
Part I:
Understanding Operational Auditing
DEFINITIONS OF "OPERATIONAL AUDITING"

Business processes often step across the frontiers between sections within a business, requiring high standards of coordination between different organisational parts. Control is often weaker where coordination is required between sections that are organisationally separate. Internal auditors are likely to be more productive if they focus considerable attention to the points of interface between organisational parts where coordination is required but is more difficult to achieve than within a single section of the business. Furthermore, internal auditors are likely to be more productive if a significant proportion of the audit engagements they perform are of natural business processes that step across the business’s organisational frontiers. We state this up front as it is so important, and we shall explore this innovative audit approach in detail in Chapter 2 when we have established some fundamentals in this chapter.

The term “operational auditing” conjures up different images for internal auditors. It may be used to mean any of the following:

The audit of operating units such as manufacturing plants, depots, subsidiaries, overseas operating units, and so on. While the audit scope may cover only accounting, financial and administrative controls it may be broadened in scope to cover the administrative and operational controls, risk management and governance processes of the operating unit under review. To impose general scope limitations for internal audit activities is inconsistent with the global Standards of The Institute of Internal Auditors (www.theiia.org).

The audit is how the functional areas of a business (such as sales, marketing, production, distribution, HR, etc.) account for their activities and exercise financial control over them. This meaning of operational auditing acknowledges that the internal auditing activity should review all the operational areas of the business, but
too narrowly specialises in the audit of accounting and financial controls. It is likely
to imply that the internal auditing activity is representing only the finance director or
the chief accountant in providing assurance about accounting and financial control
across the business.

The audit of any part of the business (operating unit, functional area, section,
department or even business process, etc.) where the audit objective is to review
the effectiveness, efficiency and economy with which management is achieving
its own objectives. Depending upon how broadly one defines internal control, the
approach to operational auditing goes further than a review of detailed internal con-
trol procedures since management’s objectives are not achieved merely by adhering
to satisfactory systems of internal control.

The classic management writers, Koontz, O’Donnell and Weihrich, endorsed
this approach to operational auditing:

An effective tool of managerial control is the internal audit, or, as it is now coming to be
called, the operational audit ... Although often limited to the auditing of accounts, in its
most useful aspect operational auditing involves appraisal of operations generally ... Thus
operational auditors, in addition to assuring themselves that accounts properly reflect the facts,
also appraise policies, procedures, use of authority, quality of management, effectiveness of
methods, special problems, and other phases of operations.

There is no persuasive reason why the concept of internal auditing should not be broadened
in practice. Perhaps the only limiting factors are the ability of an enterprise to afford so
broad an audit, the difficulty of obtaining people who can do a broad type of audit, and the
very practical consideration that individuals may not like to be reported upon. While persons
responsible for accounts and for the safeguarding of company assets have learned to accept
audit, those who are responsible for far more valuable things—the execution of the plans,
policies and procedures of a company—have not so readily learned to accept the idea.1

**SCOPE**

A key issue for a business and its internal audit function to decide upon is whether
the scope of internal audit work in an operational area of the business should be
restricted to a review of the appropriateness of, and extent of compliance with,
key internal controls or should be a more comprehensive review of the operation
generally.

The Committee of Sponsoring Organizations (COSO) view of internal con-
trol rightly sees one of the three objectives of internal control as being to give
“reasonable assurance” of “effectiveness and efficiency of operations”:

Internal control is broadly defined as a process, effected by the entity’s board of directors,
management and other personnel, designed to provide reasonable assurance regarding the
achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.2
So COSO’s broad view of internal control is that internal control (i.e. management control) is everything that management does in order that there is reasonable assurance the business will achieve all of its objectives. A narrower view of internal control is that it is only one of a number of facets of management—among others being planning, organising, staffing and leading. It is true that these facets overlap and an internal audit which intends to focus more narrowly on key internal controls is likely to need to address planning, organising, staffing and/or leadership issues to some extent, since deficiencies in these may weaken control. But there will be many aspects of planning, organising, staffing and leading which are neutral in their effect on the functioning of key controls but which contribute to providing reasonable assurance of the achievement of efficient and effective operations.

The important issue is whether internal audit may legitimately draw management’s attention to deficiencies in planning, organising, staffing and leading which, while not weakening the design and operation of key controls, nevertheless impede the achievement of objectives more generally. In the past internal audit was often defined as the independent appraisal of the effectiveness of internal control. The Institute of Internal Auditors’ current (2009) definition of internal auditing, subscribed to globally, is that:

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.3

So, should an enlightened enterprise restrict internal audit to narrow internal control matters, or should internal audit be encouraged to review and report on any matters which may be unsound? Differing positions are adopted in different enterprises. The middle-of-the-road approach is to encourage internal audit to interpret its mission as being the appraisal of internal control (in all its component parts,4 in all operational areas of the business and at all levels of management). If during the course of audit work, other matters are noted which should be of management concern but do not directly have a control dimension, internal audit should be encouraged to report on them.

Beyond the consideration of the point of focus for audit reviews of operational areas, the audit function will have to define those aspects of the organisation which are to be subject to review. In practice, of course, this will vary considerably between organisations, and will be related directly to the nature of the business and the way the organisation is structured. For example, a multinational pharmaceutical company may have its principal manufacturing bases and research and development activities in only those few countries where the economic and commercial environments are most suitable, whereas sales and marketing operations (of varying scale) may exist in every country where there is a proven market for the products.

Although the focus of operational auditing is likely to be on those activities which are most strongly associated with the main commercial markets of the organisation (for example, production, sales, after sales support, service provision, etc.), it is likely that the supporting or infrastructure operations will also need to be reviewed
on the basis that they too contribute to the well-being of the organisation as a whole. At the top level, one possible categorisation of all these areas could be as follows (although this classification will not fit every business or service-provision scenario):

- management and administration
- financial and accounting
- personnel and human relations
- procurement
- stock and materials handling
- production/manufacturing
- marketing and sales
- after sales support
- research and development
- information technology
- contracting.

This particular top level classification would be appropriate for a large organisation involved in product development, manufacturing and sales activities. A modified model would emerge for an organisation (public or private) associated with providing a service (for example, a public health authority or a roadside vehicle repair service).

Below this level of categorisation, there would be specific or discrete activities or systems, each of which may be the subject of a separate operational audit review. The subsequent chapters of this book will predominantly examine operational areas from this systems/activities orientation. For each of the above classifications there will be a number of discrete functions, systems or activities which may be defined within a particular organisation and be subject to examination by the internal auditors. This breakdown of the organisation into a set of separate audit reviews could be said to form the *audit universe* of potential audit projects. For example, the top level classifications noted above could be broken into the constituent systems or activities listed below, each of which could be the subject of an audit review. In some cases the noted subjects may readily align with a department within the organisation (i.e. payroll, human resources, purchasing, etc.). Alternatively, the activities may require coordination between a number of departments or functions (for example, the development of a new product may involve, *inter alia*, the marketing, accounting and research functions). Each organisation will be different and the internal audit function will need to adopt the most suitable definition of their *universe* of potential review assignments in order to match the prevailing structure and style.

A breakdown of the above top level classification into constituent systems or activities is given below:

*Management and administration:*

- the control environment
- organisation (i.e. structure)
- management information
- planning
- risk management
- legal department
• quality management
• estates management and facilities
• environmental issues
• insurance
• security
• capital projects
• industry regulations and compliance
• media, public and external relations
• company secretarial department.

Financial and accounting:
• treasury
• payroll
• accounts payable
• accounts receivable
• general ledger/management accounts
• fixed assets (and capital charges)
• budgeting and monitoring
• bank accounts and banking arrangements
• sales tax (i.e. VAT) accounting
• taxation
• inventories
• product/project accounting
• petty cash and expenses
• financial information and reporting
• investments.

Personnel/Human relations:
• human resources department (including policies)
• recruitment
• manpower and succession planning
• staff training and development
• welfare
• pension scheme (and other benefits)
• health insurance
• staff appraisal and disciplinary matters
• health and safety
• labour relations
• company vehicles.

Procurement (see also Contracting (below)):
• purchasing
• contracting (NB: this subject may be further broken down into a number of discrete subsystems, such as tendering, controlling interim and final payments, etc. see below).

Stock and materials handling:
• stock control
• warehousing and storage
• distribution, transport and logistics.

Production/manufacturing:
• planning and production control
• facilities, plant and equipment
• personnel
• materials and energy
• quality control
• safety
• environmental issues
• law and regulatory compliance
• maintenance.

Marketing and sales:
• product development
• market research
• promotion and advertising
• pricing and discount policies
• sales management
• sales performance and monitoring
• distribution
• relationship with parent company (for overseas or subsidiary operations)
• agents
• order processing.

After sales support:
• warranty arrangements
• maintenance and servicing
• spare parts and supply.

Research and development:
• product development
• project appraisal and monitoring
• plant and equipment
• development project management
• legal and regulatory issues.

Information Technology (IT):
• Auditing Information Technology
• IT Strategic Planning
• IT Organisation
• IT Policy Framework
• Information Asset Register
• Capacity Management
• Information Management (IM)
• Records Management (RM)
• Knowledge Management (KM)
• IT Sites and Infrastructure (Including Physical Security)
• Processing Operations
• Back-up and Media Management
• Removable Media
• System and Operating Software (Including Patch Management)
• System Access Control (Logical Security)
• Personal Computers (Including Laptops and PDAs)
• Remote Working
• Email
• Internet Usage
• Software Maintenance (Including Change Management)
• Networks
• Databases
• Data Protection
• Freedom of Information
• Data Transfer and Sharing (Standards and Protocol)
• Legal Responsibilities
• Facilities Management
• System Development
• Software Selection
• Contingency Planning
• Human Resources Information Security
• Monitoring and Logging
• Information Security Incidents
• Data Retention and Disposal
• Electronic Data Interchange (EDI)
• Viruses
• User Support
• BACS
• Spreadsheet Design and Good Practice
• IT Health Checks
• IT Accounting

Contracting:
• the contract management environment
• project management framework
• project assessment and approval
• engaging, monitoring and paying consultants
• design
• assessing the viability/competence of contractors
• maintaining an approved list of contractors
• tendering procedures
• contract and tendering documentation
• insurance and bonding
• selection and letting of contracts
• management information and reporting
• performance monitoring
• arrangements for subcontractors and suppliers
• materials, plant and project assets
• valuing work for interim payments
• controlling price fluctuations
• monitoring and controlling variations
• extensions of time
• controlling contractual claims
• liquidations and bankruptcies
• contractor’s final account
• recovery of damages
• review of project outturn and performance
• maintenance obligations.

Governance, risk management, internal control:

• internal governance processes
• the board
• external governance processes
• risk management processes
• issues for internal control.

For each of the above constituent activities there is available on the companion website a detailed standard audit programme guide (SAPG) in Word format, which readers can adapt to be more closely applicable to their business activities. This is available on a password protected accompanying website. See Appendix 1 for details. The above list of constituent activities is by no means exhaustive, so we also provide a blank SAPG in Word format for readers to use to develop further business activities.

We also provide in Word format a set of 24 SAPGs relating to some of the activities within financial institutions and a set of 27 applicable to the health sector. The activities covered in these sector-specific sets are:

Sector: Financial institutions

• branch security
• branch operations
• management
• treasury dealing
• investments—new accounts
• investments—account maintenance
• investments—account statements
• secured personal loans
• unsecured loans
• commercial lending—new business
• commercial lending—account maintenance
• cheque accounts
• ATM services
• credit and debit cards