Implementing and maintaining ISAE 3402
Implementing and maintaining ISAE 3402
Contents

Introduction 4
Purpose and background 5
Benefits to the service organization 7
How Ernst & Young helps 8
Successful continuance after implementation 10
Contacts 11
Introduction

Although many businesses have been outsourcing portions of their work for years now, outsourcing is still becoming more popular by the day. This is especially driven by increased globalization, technological evolutions and the need for standardised business processes. Outsourcing is any task, operation, job or process that could be performed by employees within the user organisation, but is instead contracted to a third party (service organisation) or another group company for a period of time.

Some examples for the financial sector are:

• Asset managers that perform asset management services for different parties within the group company.
• Pension administrators who perform the administration for pension funds.
• Claim service companies that perform claim handling services for large insurers.

The widespread use of outsourcing requires organizations to better manage their risks associated with the outsourced services. More specifically, the user organisation requires a degree of assurance that the service organisation has a well established internal control framework that is operating effectively. New regulations, regulatory authorities and supervisory boards also ask for specific controls over outsourced procedures.

For SOC 2 and SOC 3 reporting the International Standard on Assurance Engagements (ISAE 3000) and national equivalents (e.g., Attestation Standards (AT) in the US) are used.

For Service Organisation Control (SOC) reporting a distinction has been made in three types of reports:

• SOC 1 – Reports on controls over processing that impacts the financial statements, typically produced using ISAE 3402 (issued by the International Auditing and Assurance Standards Board) or SSAE 16 (issued by the American Institute of Certified Public Accountants). Distribution would be restricted to users of the services.

A ISAE 3402 or SSAE 16 engagement is an examination (similar to an audit) of a description produced by the service organisation of the system(s) they operate on your behalf which are relevant to your internal control processes.

• SOC 2 – Reports on non-financial processing based on one or more of the Trust Services criteria on security, privacy, availability, confidentiality and processing integrity, and including the description on the services provided and the controls tested. Distribution would be restricted to users of the services.

• SOC 3 – Again, a report on non-financial processing based on the Trust Services criteria. A SOC 3 report can be distributed to anyone, but only contains management’s assertion that they have met the requirements of the chosen criteria and the auditor’s opinion on this assertion.

This brochure outlines the purpose and background of the ISAE 3402 standard, its main benefits and key operational insights for implementing and maintaining.
Purpose and background

ISAE 3402 deals with assurance engagements undertaken by an auditor to provide a report for use by user entities and their auditors on the controls at a service organization that provides a service to user entities that is likely to be relevant to user entities’ internal control as it relates to financial reporting. The collaboration between the user organization, service organization and their respective auditors is visualized in the figure below.

The user organization is an entity that outsourced part of its business to a service organization. Formal agreements regarding the outsourced services are recorded in a contract and/or Service Level Agreement (SLA). Under the ISAE 3402 standard the service organisation has five primary responsibilities:

1. Prepare and present a complete and accurate description of the ‘system’ (i.e. the internal control framework).
2. Specify the control objectives.
3. Identify the risks that threaten the achievement of the control objectives.
4. Design, implement and maintain controls to provide reasonable assurance that the control objectives will be achieved.
5. Provide a written assertion to accompany the description as to the completeness and accuracy of the information provided and state the criteria used as a basis for making the assertion.

The auditor of the service organisation (service auditor) shall subsequently determine if all relevant aspects of the ISAE 3402 standard are adequately addressed by the system description. In addition, the service auditor determines if mentioned controls exist, are adequately designed and operated effectively (only type II) during a certain period. The service auditor provides an opinion to the ISAE 3402 report. The auditor of the user organisation (user auditor) can subsequently rely on the service auditor opinion, when auditing the user organization financial statements.

“ISAE 3402 could provide competitive advantage, since it is a method of distinguishing a service organization from its competitors”
Types of ISAE 3402 reports

There are two types of reports, Type I and Type II. Type I reports provide:

• A description of the service organisation’s system and controls supported by a management assertion and an auditor’s opinion on the fairness of that description, and whether the controls had been placed into operation.
• A management assertion and an auditor’s opinion on whether the controls are appropriately designed to meet the control objectives.

A Type II report adds a management assertion and an auditor’s opinion on the operating effectiveness of controls in addition to the opinions provided in a Type I report.
Benefits to the service organization

The ISAE 3402 standard provides assurance to clients that the service organization has appropriate controls in place. In the table below potential benefits and expected results of an ISAE 3402 engagement are listed:

<table>
<thead>
<tr>
<th>Meeting client needs</th>
<th>Managing costs</th>
<th>Improving your business</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mixed team, breaking through the silo’s</td>
<td>• Efficient ISAE 3402 framework</td>
<td>• Measuring and evaluating your performance</td>
</tr>
<tr>
<td>• Planning (preset activities en timelines)</td>
<td>• Appropriate number and mix of controls</td>
<td>• Root cause analysis for service level disputes</td>
</tr>
<tr>
<td>• Managed expectations</td>
<td>• Scope which is tailored to the wishes and demands of the users</td>
<td>• Managed contractual obligations</td>
</tr>
<tr>
<td>• No legal liability while all agreements made are recorded</td>
<td>• Appropriate and sufficient control evidence (documentation)</td>
<td>• Managing client support costs</td>
</tr>
<tr>
<td>• Complete and accurate risk assessment</td>
<td>• Accurate and complete populations to facilitate sampling</td>
<td>• Leveraging the knowledge of an outsider that is evaluating your business processes</td>
</tr>
<tr>
<td>• Scope which is tailored to the wishes and demands of the users</td>
<td>• High reliance of work performed by Internal Audit</td>
<td>• Commercial benefits</td>
</tr>
<tr>
<td>• Use of the appropriate reporting standards</td>
<td>• Integrated ISAE 3402 framework</td>
<td>• Increased user satisfaction</td>
</tr>
<tr>
<td>• SLA and SLR, which provide full coverage of and insight in the services provided</td>
<td>• Cost savings while adding value</td>
<td>• Additional comfort to management on the design and operation of controls</td>
</tr>
</tbody>
</table>

“ISAE 3402 is a recurring (annual) project. Making a onetime investment in your approach and framework pays off the coming years.”
How Ernst & Young helps you to deliver an ISAE 3402 report to your clients

Our approach is hands on and focused on helping you to meet your requirements in a cost effective manner, by:

- Understanding your clients regulatory and compliance needs and to develop a strategy for meeting those needs.
- Assessing your project plan and align it with the service auditor plan.
- Determining the scope of the report.
- Assisting you to draft the system description.
- Developing the control objectives for your processes.
- Planning an appropriate approach to the risk assessment and identifying the basis for your management assertion.
- Helping your personnel to identify controls and address them to control objectives.
- Benchmarking your report, control objectives and controls with leading practices.
- Testing the operational effectiveness of your controls.
- Reporting on the results of our testing.

We will offer our assistance through workshops and training programs for your organization and evaluate the design and operating effectiveness of the ISAE 3402 control framework and report. We will issue an ISAE 3402 report and a management letter containing findings and recommendations.
Illustrative time horizon for first time adoption and implementation is visualized in the figure below.

<table>
<thead>
<tr>
<th>Building Internal Control framework</th>
<th>Year 1 (t)</th>
<th>Year t + 1</th>
<th>Year t + 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control existence and design</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISAE 3402 Type I report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess control existence, design and operating effectiveness</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISAE 3402 Type II report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous improvement Internal Control framework</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Implementing and maintaining ISAE 3402
Successful continuance after implementation

After successful implementation, annual maintenance of the ISAE 3402 process is necessary to continue the process effectively. It depends on:

- Impact of organizational changes on control environment.
- New legislation and compliance requirement.
- Changes in business and risks.
- Contractual adjustments.
- Changing requirements from user organizations.
- Recommendations from the service auditor.

Our approach to an existing ISAE 3402 process is focused on assisting you in effectively maintaining and optimizing the ISAE 3402 process. Each year we will thoroughly evaluate the complete project and process considering all relevant internal and external developments. We will input our industry knowledge and assess the impact on your processes and our audit work.

The Ernst & Young difference in approach

Experienced professionals - Our service delivery team includes dedicated professionals with significant experience performing ISAE 3402 engagements. This means you will be teaming with people who understand the issues and how critical your programs and projects are to your organisation's success.

Knowledge - Our skilled professional experience and knowledge from working with multiple clients in the financial services industry is fully leveraged to directly benefit your organization.

Perspective - The ISAE 3402 report is not just a tool for meeting clients requirements; it is usually the single best description of your processes and procedures that you can provide your clients. We advise you on how to leverage this communication to enhance your clients understanding of your processes. This perspective is a major part of the Ernst & Young difference.

Ernst & Young helps organisations achieve their business objectives by delivering a wide range of advisory services that are designed to help enhance risk management activities and improve business processes. From our network of member firms around the world, Ernst & Young's 18,000 advisory professionals provide services that help clients assess, improve and monitor their business risks.
# Contacts

## Risk Services

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Tel</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander Beijer</td>
<td>Partner</td>
<td>+31 (0)88-407 11 81</td>
<td>+31 (0)629-08 41 78</td>
<td><a href="mailto:alexander.beijer@nl.ey.com">alexander.beijer@nl.ey.com</a></td>
</tr>
<tr>
<td>Annemiek Mollema</td>
<td>Manager</td>
<td>+31 (0)88-407 41 28</td>
<td>+31 (0)629-08 40 05</td>
<td><a href="mailto:annemiek.mollema@nl.ey.com">annemiek.mollema@nl.ey.com</a></td>
</tr>
</tbody>
</table>

## IT Risk & Assurance

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Tel</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marc Welters</td>
<td>Partner</td>
<td>+31 (0)88-407 41 41</td>
<td>+31 (0)621-25 22 23</td>
<td><a href="mailto:marc.welters@nl.ey.com">marc.welters@nl.ey.com</a></td>
</tr>
<tr>
<td>Mark de Bos</td>
<td>Manager</td>
<td>+31 (0)88-407 14 10</td>
<td>+31 (0)621 25 28 31</td>
<td><a href="mailto:mark.de.bos@nl.ey.com">mark.de.bos@nl.ey.com</a></td>
</tr>
</tbody>
</table>
About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Legal and notarial services are provided by Holland Van Gijzen Advocaten en Notarissen LLP through a strategic alliance with Ernst & Young Belastingadviseurs LLP. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential. Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com

Ernst & Young Advisory is a trade name of Ernst & Young Accountants LLP. This is a limited liability partnership registered in England and Wales with registered number OC335594. Ernst & Young Accountants LLP has its registered office at 1 Lambeth Palace Road, London SE1 7EU, United Kingdom, its principal place of business at Boompjes 258, 3011 XZ Rotterdam, the Netherlands and is registered with the Chamber of Commerce Rotterdam number 24432944.

About Ernst & Young’s Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2013 Ernst & Young Accountants LLP.
All Rights Reserved.

130007

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

www.ey.com/nl

ED None