info@isae3402.co.uk
www.isae3402.co.uk

ISAE 3402 IMPLEMENTATION

WHITEPAPER OUTSOURCING ASSURANCE

WHITEPAPER

CONTENT

”

COMPETETIVE ADVANTAGE

ISAE 3402 provides a competitive advantage by distinguishing service organizations from their competitors. Benefits of ISAE 3402 reports range from strengthening and refinement of risk management to gaining confidence in markets by transparency of the control framework. ISAE 3402 creates audit efficiency and reduction to business operations.

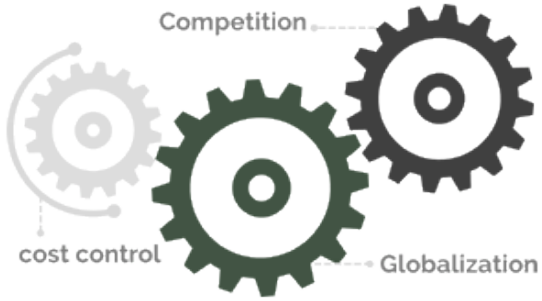
Organizations are continuously searching for opportunities to exploit competitive advantage to increase markets and profits. Organizations are increasingly outsourcing non-core business functions. Nonetheless, is management ultimately responsible for risk management and the implementation of an effective control framework. This has led to increased demand for control assurance for activities performed by third parties

History

A large integrated company that owns manages and directly controls assets was the most popular business model for most of the 20th century. With a healthy focus on diversification to broaden the corporate bases and take advantage of economies of scale. Many large companies developed a new strategy of focusing on their core business to increase flexibility and creativity. This required identifying critical processes and deciding which could be outsourced.

Outsourcing

Because of globalization, increased competition and cost pressure, organizations are outsourcing more of key business functions to service organizations. Outsourcing of core processes will have a direct impact on an organization's financial statements and key business processes. Outsourcing is no longer confined to routine back-office tasks. What are the options to gain confidence over outsourced business processes? How can an organization acquire control and assurance over outsourced processes?



Increase in outsourcing and outsourcing crucial business information also brings increased risks and security concerns. Organizations could suffer operational, financial or even reputational damage because of security deficiencies of outside service organizations. An independent examination of the critical business processes that have been outsourced or IT systems support organizations to identify and control these risks and regain assurance over outsourced processes.

The most common reasons for outsourcing are:

- Control and reduce operating costs
- Improve focus of the company on core processes
- Acquire access to world-class capabilities
- Free internal resources for other purposes
- Increase efficiency in specific functions
- Insufficiency of internal resources
- Share risks with other organizations

The current stage in the evolution of outsourcing is strategic partnerships. Until recently it was axiomatic that organizations could not outsource core competencies. This is changed an ISAE 3402/SOC1 or ISAE 3000/SOC2 are common practice

ISAE 3402

The ISAE 3402 standard, is an international recognized auditing standard issued by the International Auditing and Assurance Standards Board (IAASB). A service organization's auditor's examination is widely accepted, because it represents an in-depth audit of a service organization's control objectives and activities. The control framework and related controls are in detail included in the Systems and Organization Report (SOC). The scope of an ISAE 3402/SOC report consists of controls over information technology and operational processes which impact the finance of an organization.

SOC 1 OR SOC2

SOC reports can be distinguished in SOC1 and SOC2 reports. An ISAE 3402/SOC1 is focused on the financial statements and all processes that impact these. An ISAE 3000 (or SOC2) report is focused on meeting a broader set of user needs, including concerns over privacy, confidentiality and availability of systems. SOC2 reports are based on the Trust Services Principles and Criteria in a modular way.

ALLIGNING EXTERNAL REQUIREMENTS TO INTERNAL RISK EXCELLENCE

In outsourcing situations many questions may arise, Are services executed in a controlled manner? How is security dealt with? Who has access to our information? Are sufficient anti-fraud measures implemented? ISAE 3402 provides a solution for these issues.
ISAE 3402 supports organizations in measuring and evaluating risks and aligning the resulting control framework to strategic objectives and these risks. A onetime investment in the framework pays off by improving market confidence and organization excellence

TYPE I AND TYPE II

An ISAE 3402 Type I report includes an opinion of an external auditor on the controls in operation at a specific moment in time. The external auditor examines whether the controls are suitably designed to provide reasonable assurance that the financial statement assertions are accomplished and whether the controls are in place. In a ISAE 3402 Type II report, the external auditor reports also on the operating effectiveness of these controls during a predefined period. ISAE 3402 reports most commonly cover design and operations effectiveness of controls for a 12-month period with continuous coverage from year to year. A report may cover a period with a minimum of six months.

BENEFITS

IMPROVING RISK CONTROL AND TRANSPARANCY

Both users of- and service organizations experience the benefits from SOC1 or SOC2 reports.

Organizations occasionally receive questions on security standards from (prospective) clients; what are the differences between an ISAE 3402/SOC1, ISAE 3000/SOC 2 and an ISO 27001 audit? Which standard is more applicable to our company, ISAE or ISO 27001? What are the advantages and disadvantages of ISAE vs. ISO 27001? In fact ISAE 3402 and ISO 27001 are drastically different kinds of standards with equally dissonant use. The major differences are the form of reporting and the audit performed.

ISAE and security

ISAE 3402 is an attestation from an independent certified accountant or firm that compares the System and Organization Controls (SOC) information against the audit objectives or criteria. In an ISAE 3402 (SOC1) report the IT general controls (ITGC's) and therofor security are included, but the primary scope are financial procedures and controls. An ISAE 3000 (SOC2) report is focussed on the Trust Service Principles which include security, availability and privacy and has more in common with ISO27001. An important distinction is that ISAE 3402 and ISAE 3000 (SOC 2) are reports and ISO27001 is a certification.

ISO 27001

ISO 27001, on the other hand, is a risk-based standard for establishing, implementing, and improving an organization's security framework or ISMS. This standard security framework maintained by the ISO and IEC. The implemented ISO 27001 framework is certified by independent certification bodies. The organization is required to have the procedures and controls described in Annex A of the ISO 27001 framework in place. The resulting security framework mitigates risks through the implementation of the procedures and controls. ISO 27001 is a complete system for assuring information security, and all organizations that implemented ISO 27001 should have at least a system for managing information security.

is

ISO 27001 or ISAE 3402?

The world has changed. ISO 27001 has been the benchmark for information security, but with the information security risks continually evolving, many organizations require a greater level of assurance over information security. ISO 27001 is a single (rigid) set of controls, while ISAE 3402 and 3000 standards are principle based. This implies that the controls cannot be formally implemented, but n work effectively. An auditor will qualify the ISAE 3402 assurance opinion if this is the case. An ISAE 3402/3000 audit is an in-depth audit, focusing on the effectiveness of the risk framework in managing risks. If risks are not effectively managed, this will be exposed in the ISAE 3402 report. This level of transparence is required in the global economy and the continually evolving threat landscape.

ALLIGNING TRANSPARANCY TO SPECIFIC CLIENT REQUIREMENTS

ISAE 3402/SOC1 is intended to support service organizations' customers in a financial audit. ISAE3000/SOC is focussed at a broader set of user needs. Different industries require a different scope and a different SOC reporting. An overview of commonly used report per industry (examples) is outlined below with an overview of the relevant scope.

MANAGED SERVICES

Managed service providers manage infrastructure, servers and applications for diverse clients. ISAE 3402 reports with an ITGC scope are applied

DATACENTERS

Operational and financial systems are housed, that impact financial processes. ISAE 3402/SOC1 (combined with ISAE3000/SOC2) focussed on physical security

FINANCIAL SERVICES

Provided for SOx404 (ICOFR)-purposes or supervisory authorities requirements. Operational and financial processes are in scope

SOFTWARE AS A SERVICE

Applications that are related to operational or financial processes with an (in)direct impact on the annual report. ITGC;s are in scope of the ISAE 3402/SOC1 reports

HR AND PAYROLL

All personal and salary processes with an impact on the annual report or financial processes are in scope of the ISAE 3402/SOC1 report of HR Service providers.

FULFILMENT

Fulfilment, distribution or printed press is outsourced to specialised companies. Operational (logistic) and financial processes are in scope of the ISAE 3402/SOC1

SOC stands for “System and Organization Controls.” These were formerly Service Organization Control reports. SOC is a suite of reports originated in the US. ISAE 3402 aligns with the US Statement on Standards for Attestation Engagements (SSAE) 18 US standard. An ISAE 3402 report provides assurance on a service organization’s description of its system and the suitability of the design and operating effectiveness of it controls through a Service Auditor’s Report.

ISAE 3402 SOC1

In an ISAE 3402 SOC1 report, organizations define their own control objectives and controls and align these with customer’s needs. The scope of an ISAE 3402 is typically all operational and financial controls that have an impact on the financial statements, and the IT General Controls (e.g., security management, physical and logical security, change management, incident management and systems monitoring and. In other words, if your organization is hosting financial information that could affect your client’s financial reporting, then a ISAE 3402 SOC1 audit report makes the most sense for your organization to pursue, and will likely be requested of you. The ITGC’s, operational controls and financial controls are in scope of the ISAE 3402 SOC1 audit.

In a SOC 1 audit control objectives, which are used to accurately represent internal control over financial reporting (ICOFR) are required to be included if the organization is subject to SEC filings in the US.

ISAE 3000 SOC2

In ISAE 3000 SOC2 reports the Trust Services Principles and Criteria (TSP’s) are applied. The TSP’s are a set of specific requirements developed by the AICPA and Canadian Institute of Chartered Accountants (CICA) to provide assurance over security, availability, confidentiality, processing integrity, and privacy. An organization can choose the different aspects that are relevant to their customer’s needs. A ISAE 3000 SOC2 report can cover one or more principles. If your organization is hosting or processing other types of information for your clients that does not impact their financial reporting, then a ISAE 3000 SOC 2 is more relevant. In this instance, your clients are likely concerned whether you are handling their data in a secure way, and if it is available to them in the way you have contracted it to be. A SOC 2 report, similar to a SOC 1 report, evaluates internal controls, policies, and procedures.

SOC1 or SOC2?

Organizations that process, host or manage systems or information that impact financial reporting should always provide an ISAE 3402 SOC1. ISAE SOC2 is applicable if all systems and processes are unrelated to financial reporting. Datacenter-, IaaS, Paas providers typically report hybrid, with both an ISAE 3402 SOC1 for finance related processes and systems and ISAE 3000 SOC2 for unrelated processes and systems. The content of both reports will be identical.

IMPLEMENTATION

INVEST IN APPROACH AND FRAMEWORK

ANALYSE RISKS, PLAN THE PROJECT, PREPARE SYSTEM DESCRIPTION AND PERFORM READINESS ASSESMENT

Implementing ISAE 3402 requires effective planning, leadership involvement, thorough analysis of processes and reliable resources and project management.

An ISAE 3402 project typically starts with an implementation phase in which the SOC-report is prepared. The overall success of an ISAE 3402 project is highly dependent of the alignment of the service organizations' control objectives and framework to the needs and requirements of all stakeholders.

RISK EXCELLENCE

SERVICE ORGANIZATIONS // USERS

An ISAE 3402 audit provides benefits to the service organization and users by improving audit efficiency, aligning risk management to outsourced operations and comply with regulatory requirements.

SERVICE ORGANIZATION

Service organization experience significant improvement of risk management, strengthening- and alignment of controls to risk and improvement of audit efficiency. Market confidence improves as a consequence of more transparency and insight in risks and the framework managing these risks. ISAE 3402 reduces number of audits and business interruption.

USERS

Security and risk concerns are reduced. Detailed insight and external confirmation of a professional auditor will improve understanding and align your processes to the processes of your suppliers. In general comfort over outsourced aspects of your business is gained in an effective and transparent way. Gain efficiency in reviewing and assessing external audits.

ISAE 3402 BENEFITS

ALLIGNING RISK MANAGEMENT
STRUCTURED APPROACH

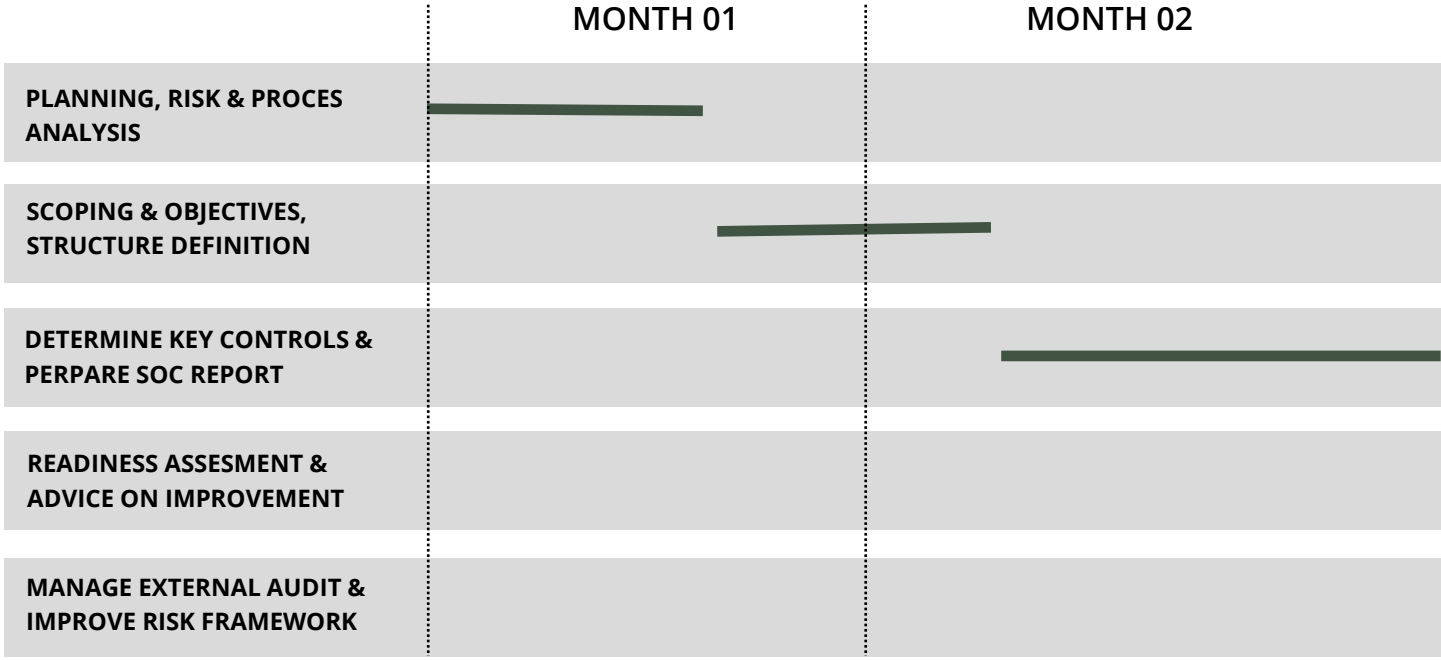
COMPLIANCE
INTEGRATE REGULATION

AUDIT EFFICIENCY
LESS AUDITS

MARKET CONFIDENCE
BY TRANSPARANCY

PROJECT PLANNING

TIMELINE



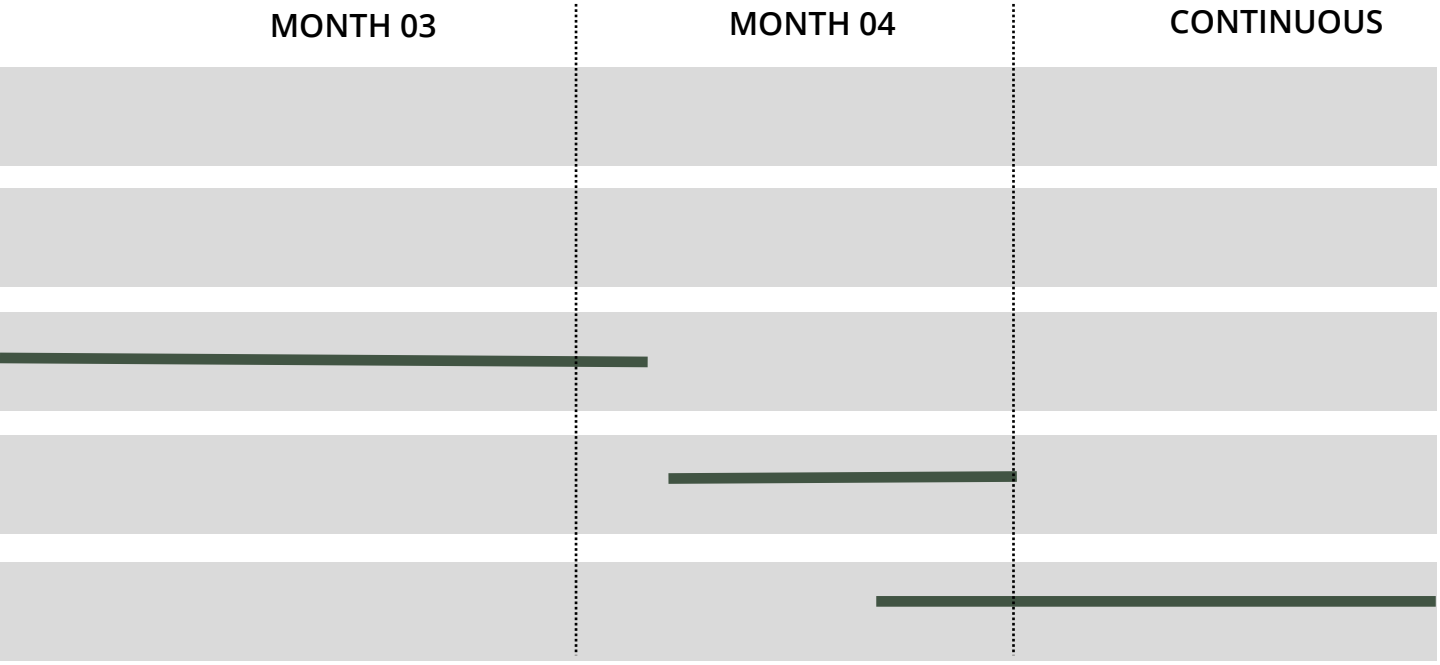
PLANNING, RISK & PROCESS ANALYSIS

Preset activities and timeline, manage expectations of management. Perform a complete and accurate risk assessment in which different levels and functions are involved.

SCOPING & OBJECTIVES, STRUCTURE DEFINITION

Adjust scope to needs and requirements of all stakeholders (user organization, auditors). Determine control objectives based on the annual reporting of typical user organization.

An ISAE 3402 implementation framework costs for an average organization (<100 employees) typically 2-4 months depending on complexity of processes, size of the organization and available resources.



DETERMINE KEY CONTROLS & PERPARE SOC REPORT

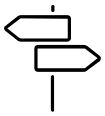
Determine key controls based on defined control objectives and prepare SOC report consisting of a description of the control framework, control matrix (objectives and controls) and other sections.

READINESS ASSESSMENT & ADVICE

Assess effectiveness of controls by performing walkthroughs and advice different functions on improvement of procedures. Benchmark report with leading practices for SOC reports

MANAGING AUDIT & IMPROVEMENT

Align internal project with external auditors on timing, process and expectations. Thoroughly evaluate ISAE 3402 project and process and consider internal and external developments.



MORE INFORMATION

THE NEXT STEPS

CONTACT ISAE3402.CO.UK

Get in touch with on the ISAE3402 SOC Experts and discuss your specific needs and requirements for the implementation of ISAE 3402 in your organization. Please send an email to info@isae3402.co.uk with your specific requirements.

DISCLAIMER

ISAE3402.CO.UK

CONTACT

EMAIL:
info@isae3402.co.uk