RISKLANE
SOLUTIONS

info@risklane.com
www.risklane.com

STEP-BY-STEP GUIDE

ISAE 3402

COMPLIANCE

CONTENT

GETTING TO KNOW ISAE 3402

ALIGNING EXTERNAL REQUIREMENTS TO INTERNAL RISK EXCELLENCE

In this step-by-step guide, we will provide you with the necessary information on ISAE 3402. The guide consists of information regarding the ISAE 3402 standard, the project phases of ISAE 3402 compliance (defining the scope, the implementation, and the audit), and the benefits of ISAE 3402 for your organization.

As a professional Risk Management, Governance, and Compliance firm we are pleased to provide support with the ISAE 3402 compliance project within your organization. We are more than pleased to answer any questions you might have regarding ISAE 3402.

ISAE 3402

OUTSOURCING | SECURITY OF FINANCIAL PROCESSES

ISAE 3402 is an internationally recognized auditing standard, because it represents an in-depth audit of a service organization's control objectives and control activities, which often include controls over information technology and related processes.

The scope of the examination of the external auditor includes the classes of transactions in the service organization's operations that are significant to the user organization's financial statements, and processes that are specifically defined by the service organization. ISAE 3402 is generally applicable when an independent auditor ("user auditor") is planning the financial statement audit of an entity ("the user organization") that obtains services from another organization ("the service organization").

The service auditor's report, which includes the service auditor's opinion, is issued to the service organization at the conclusion of an ISAE 3402 assurance engagement. ISAE 3402 does not specify a pre-determined set of control objectives or control activities that service organizations must achieve.

OUTSOURCING

Outsourced services require that information from a service organization is acquired to assess and address the risks associated with outsourced services. An ISAE report is an internal control report that provides this information. ISAE 3402 is the standard for assurance on financial processes (or processes with a financial impact for the user organization).

The relevant processes, the risk management framework, and a detailed control matrix need to be described by an organization. The detailed control matrix has to contain control objectives and control descriptions.

After the implementation, all procedures and controls need to be in place. All working procedures, management of the process, and discipline of the organization require uniformity to comply with the described procedures in the report.

INDUSTRIES

Organizations providing services to other organizations, e.g. Asset/Property Managers, Pension Services Providers, Software As A Service (SaaS)-providers, Infrastructure As A Service (IaaS)-providers, Platform As A Service (PaaS)-providers, and Data centre Services providers are generally required to implement an ISAE 3402 report.

If outsourced processes are related to financial processes, ISAE 3402 is relevant. An ISAE 3000 or SOC 2 might be more relevant if the processes are related to General IT Controls (GITC's), Security and/or Privacy.

PROJECT PHASES

PHASE 1
PREPARING THE SCOPE OF THE ISAE 3402 REPORT

PHASE 2
IMPLEMENTING ISAE 3402 WITHIN YOUR ORGANIZATION

PHASE 3
ISAE 3402 AUDIT PROCEDURES

PHASE 1. SCOPE DEFINITION

APPLICABLE TRUST SERVICES CRITERIA

HOW TO DEFINE THE SCOPE OF A ISAE 3402 REPORT ?

The scope of a ISAE 3402 report relates to the financial controls within a service organization relevant to the financial processes in relation to the services provided (or processes with a financial impact for the user organization, if there a no direct financial transactions made).

The ISAE 3402 report should contain an scope section that note the key components of the scope, including the inclusive or carve-out of sub-service providers.

It is required to include details about the type(s) of services provided, the internal control framework (based on the COSO framework) and a description of the General IT Controls.

PREPARE THE SCOPE

The basis for preparing the scope of the ISAE 3402 report are the outsourcing risks (financial, compliance, operational) of the user organization. Risks with regard to the ICT structure should also be defined within this context. For the relevant processes associated with the identified risks, specific control objectives are defined. Based on the prepared control objectives, controls are described to achieve the control objectives and ultimately mitigate the outsourcing risks. The complementary user entity control provide further details regarding the scope, the boundaries of the scope, and the controls that must be in place at the user organization.

In the end the scope of an ISAE 3402 report is up to management to define, although it is the requirement that the processes that can have a financial effect for the user organization are at least included.

INCLUSIVE OR CARVE-OUT?

If a service organization (partly) outsources its processes, this is a so-called subservice organization. The service organization determines whether the relevant controls of the subservice organizations are described. The ISAE 3402-guidelines prescribe two methods for this; the carve-out method and the inclusive method.

When using the carve-out method, the description of the service organization explicitly states that the controls of the subservice organization and the related control objectives are not included in the description of the controls and the scope of the audit by the auditor of the service organization. When using the inclusive method, the service organization states that the controls of the sub-service organization are included in the description of the controls. A carve-out method can be used if the subservice organization has a ISAE 3402 (SOC 1) or SOC 2 report in place.

”

COMPETETIVE ADVANTAGE

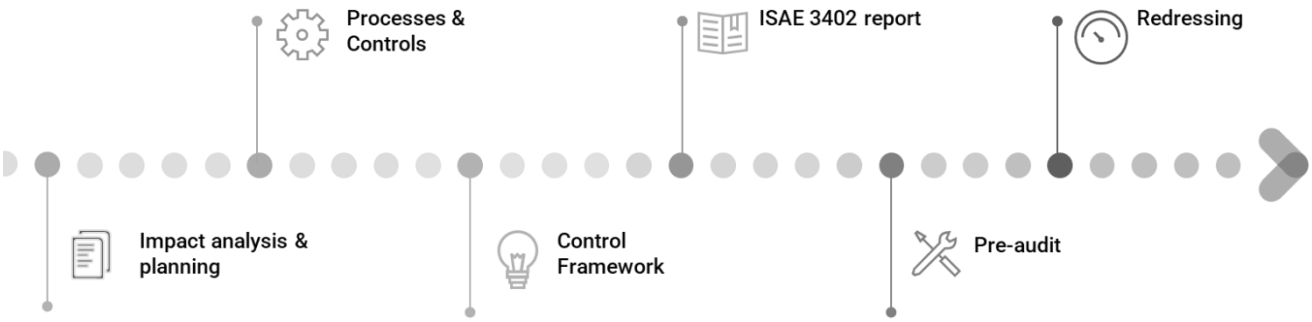
ISAE 3402 PROVIDES A COMPETITIVE ADVANTAGE BY DISTINGUISHING SERVICE ORGANIZATIONS FROM THEIR COMPETITORS.

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 OF BUSINESS INEFFICIENCIES.

PHASE 2. IMPLEMENTATION

STEP-BY-STEP-APPROACH



01

IMPACT ANALYSIS & SCOPING

In Phase 1, the impact (GAP analysis) of the implementation is determined. Based on the impact and the defined scope of the implementation, a detailed plan is prepared in which the various milestones are identified and arrangements with management are made.

02

PROCESSES & CONTROLS

In Phase 2, interviews are held to identify risks, determine the impact and the existing working method, and take note of the information present within the organization. The organization' controls are then described according to the ISAE 3402 requirements, based on the information obtained from the interviews. These are recorded in a control matrix; a matrix containing the control objectives and related controls. Proactive advise on the implementation of any missing controls (including process descriptions) will be provided during this phase.

Personal approach
Professional results

03

CONTROL FRAMEWORK

In Phase 3, the internal control framework will be described based on the most recent COSO framework (COSO 2013) and the general section of the reporting is prepared. In the general section a description of the processes, the organization and the General IT Controls is included.

04

ISAE 3402 REPORT

In Phase 4 the complete ISAE 3402 report is prepared based on the individual sections and additional sections such as the management statement and the complementary user entity controls. Phase 4 results in a draft ISAE 3402 report, which is discussed in detail with relevant staff. The organization implements any identified problem areas and associated missing controls within the organization during this phase.

05

PRE-AUDIT

After the preparation of the report, a pre-audit or 'walkthrough' is carried-out in Phase 5. During the pre-audit the controls are tested, and possible problem areas will be identified prior to the final audit. During this phase, the organization provides the documentation and evidence required.

06

REDRESSING

During Phase 6, as a result of the pre-audit, improvements in controls and the management system are implemented and solutions are prepared for the identified problem areas. Solutions are provided that can be implemented within the organization and the ISAE 3402 report. Phase 6 will result in the final ISAE 3402 report.

LEAD TIME

In general, the processing time of the first four phases will be between six to eight weeks, depending on the commitment and availability of employees. The required availability of employees is expected to be one to two days per week during that period.

The processing time of Phases 5 and 6 is between two and four weeks. The required availability of employees is expected to be one day per week during that period.

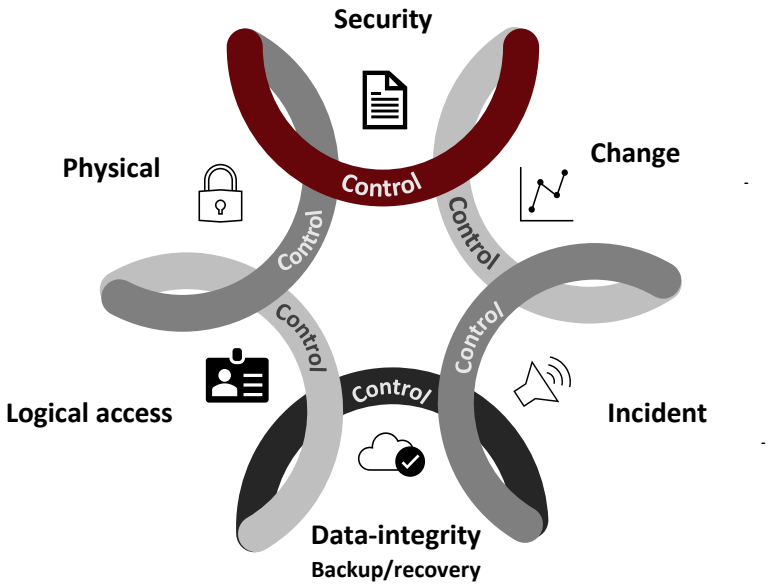
DEFINING CONTROLS

CONTROL TYPES EXPLAINED

A control framework always consists of General IT Controls, application controls, manual controls, and monitoring controls. These controls together form the control framework with which risks are managed. The monitoring controls act as a secondary 'filter' for irregularities that have not been detected by the primary management controls. The internal control framework always consists of a set of controls; controls that work together. This set of controls ensures that risks are effectively controlled.

GENERAL IT CONTROLS

The General IT Controls are the controls that ensure that there are sufficient security and data integrity measures in place to ensure that financial information is accurate and complete for the purpose of the financial statements. An internationally recognized framework for the General IT Controls is the COBIT 5.0 framework.



APPLICATION CONTROLS

Application controls are automated controls within a system or application that are set up (e.g. by means of a script) that could guarantee, among others, the completeness and integrity of input and output of data, authorization and authentication of data and users and availability of systems.

MANUAL CONTROLS

The manual controls are the controls performed by an authorized individual within the user organization. This can vary from testing software releases, to authorizing financial transactions in the financial administration or authorizing backup reports. The application controls support the manual controls.

MONITORING CONTROLS

The ISAE 3402 guidelines do not explicitly prescribe entity level controls or monitoring controls. However, it is good practice to describe monitoring controls in the 3402 report. Ideally, the company level controls are aligned with the COSO framework. Other monitoring controls are included within the control matrix per process.

PHASE 3. THE AUDIT

QUALITY ASSURANCE AUDITS

THE ISAE 3402 AUDITS

An ISAE 3402 report allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. The service auditor's report, which includes the service auditor's opinion, is issued to the service organization at the conclusion of the audit.

ISAE 3402 does not specify a pre-determined set of control objectives or control activities that service organizations must achieve. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach for the audit of financial statements. A service auditor may issue two types of reports; a Type I report or a Type II report.

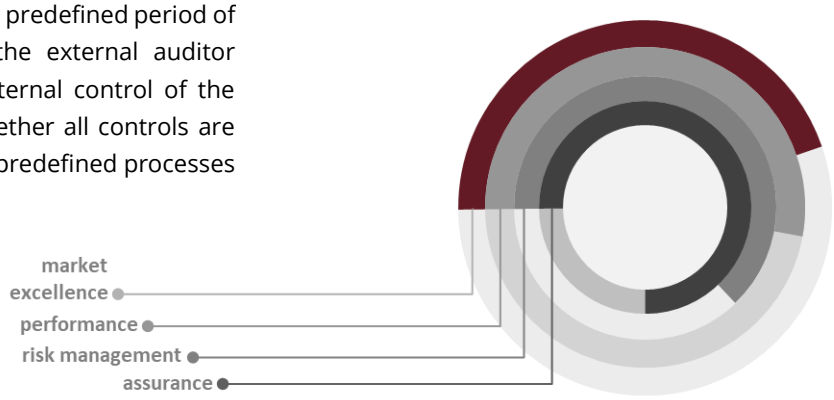
Minimizing business disruption by **effective** project management

TYPE I REPORT

An ISAE 3402 Type I report includes an opinion of an external auditor on the controls placed 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.

TYPE II REPORT

In an ISAE 3402 Type II report, the external auditor reports on the suitability of the design and existence of controls and on the operating effectiveness of these controls in a predefined period of six months minimum. This implies that the external auditor performs a detailed examination of the internal control of the service organization and also examines whether all controls are operating effectively in accordance with the predefined processes and controls.



KEY BENEFITS
OF ISAE 3402 COMPLIANCE

EXPERIENCE THE BENEFITS OF ISAE 3402

ISAE 3402 reports are used by organizations as a marketing tool. New and existing customers immediately recognize that they are dealing with a reliable party. Organizations that do not have such reporting may be missing out on important new opportunities. During the sales process, it is common for a customer to ask their supplier to fill in a questionnaire to gain insights into the current maturity level of the organization. Now, a ISAE 3402 report is likely to provide effective answers to these questions. It will speed up the process considerably. This will also provide the customer the feeling and confidence that processes are indeed in order.

RISK EXCELLENCE

Realises a positive effect on the quality of risk management and the internal control framework.

PROFESSIONALISM

Supports the organization with the professionalisation of internal processes and procedures.

OPPORTUNITIES

Creates opportunities to acquire new customers and retain customers by providing assurance and transparency.

RECOGNISED

ISAE 3402 is widely recognized, because it represents an in-depth audit of a service organization's control activities.

PROVIDING TRUST

Provides confirmations that third-party assurance on ISAE 3402 criteria are met.

SAFE TIME

Safe time by answering partners and customers efficiently, and limits the need for answering IT-questionnaires.

INTRODUCING RISKLANE

INVEST IN EFFICIENCY, VALUE, AND PARTNERSHIP

» ANALYSE RISKS
» PLAN THE PROJECT
» PREPARE SYSTEM DESCRIPTIONS
» PERFORM A READINESS ASSESMENT

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

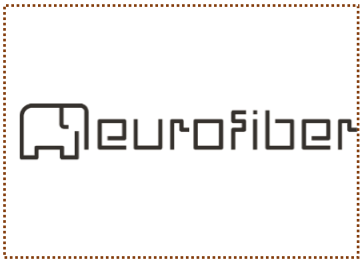
Risklane originates from a 'Big Four' audit firm and is founded in 2004. The result of our background is that we work in accordance with the highest professional standards and have experience in working with tight deadlines. We live by our professional standards and we always deliver the highest quality, whilst continuously striving to meet our clients' needs.

As a consequence of our flat structure and efficient communication framework, we can respond quickly to your requirements. Choosing Risklane implies selecting a professional organization, but also choosing for a personal approach. In our opinion, effective project management, our experience with implementing risk management frameworks in your industry, and professionalism are the basis for excellent results.

As Risklane, we also feel that a good understanding, clear communication, and knowledge of our clients' industry are essential for delivering added value to you as our client. Based on this approach we will inform you on the relevant changes in laws, regulations and other important developments.

OUR SATISFIED CUSTOMERS

REFERENCES



RISKLANE

MANAGE RISK AND RESULT

Risklane Ltd.
1 Fetter Lane
London EC4A 1BR, UK
+44 20 351 446 56
www.risklane.com

Risklane BV
Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.risklane.nl