Combined audit

An efficient approach lowers your audit burden

Introduction

So, as a security officer or information risk manager, you have just guided the organization through an audit. Lengthy conversations with auditors asking difficult and important questions. It has been long and intensive days. Fortunately, the ISAE 3402 audit or the SOC 2 audit is over for this year! On to the ISO 27001 audit. This is scheduled for next week. With mostly the same topics, questions and similar documentation.
That can be smarter, right?

As auditors of Grant Thornton and BSI, we see that there is often overlap in the scope for ISAE 3402/SOC 2 and ISO 27001 audits. By systematically combining these audits and streamlining the scope with regard to ISAE 3402/SOC 2 and ISO standards, organizations make an efficiency improvement. This reduces the audit burden. In addition, the auditors for both investigations reinforce each other. Typically a case of one and one is more than two!

For example, the collaboration between Grant Thornton and BSI has already contributed to accelerating and improving the audit process at several organizations.

What features and benefits does Grant Thornton and BSI's joint approach bring you? In this white paper we provide you with a clear overview of the overlap between the two audits. In addition, Jorg Voeten of CM.com will share his experience with the combined audit of Grant Thornton and BSI.

What are your advantages with a combined audit?

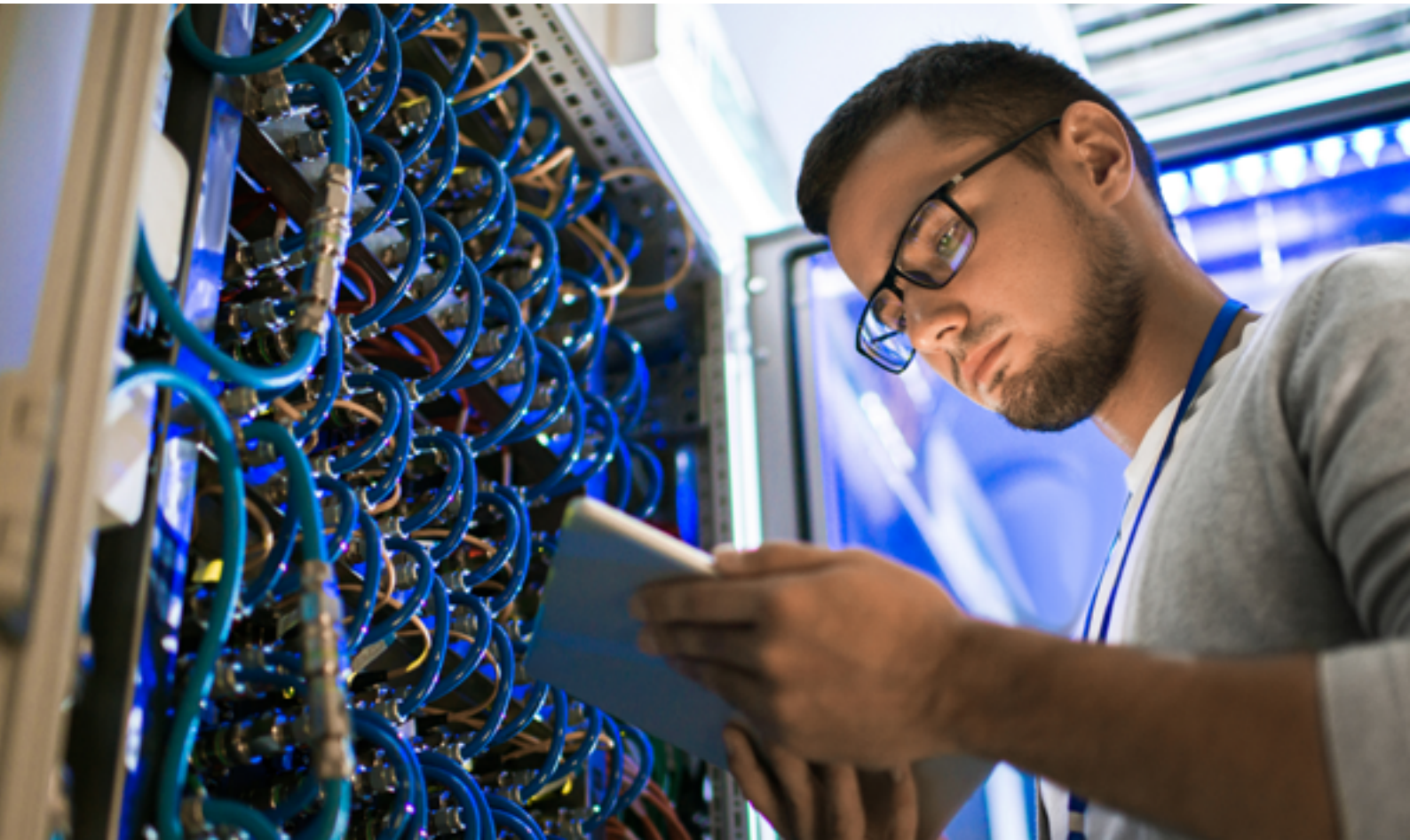
Efficiency in scheduling audit days
The simultaneous interviews save you time. In addition, you collect the information and documentation you need once for the combined audit days instead of spreading it over different moments in the year.

Reduced pressure on the organization from audits
Employees from your organization are prepared for the combined audit days. This offers certainty and peace of mind for their planning. The auditors come together at the same times.

Shared starting point of auditors
Grant Thornton and BSI auditors are aware of each other's audit approach. This ensures a more efficient audit process and a more complete overview of your organization when it comes to information security.

Implementation ISAE 3402/SOC 2 & ISO 27001
Grant Thornton and BSI both provide independent final reports. Because the auditors know where their expertise lies, they benefit from each other's expertise. Both organizations will provide you within their technical space with recommendations for realizing further improvements. You can implement the advice within your organization. You will benefit from this in subsequent audit cycles.

A combined final presentation
The final presentation of the combined findings feeds your improvement agenda and helps you organize organizational processes even better. This ensures consistent and sustainable management of information management.



Basics about ISAE 3402, SOC2 and ISO 27001

What do you achieve with ISAE 3402?
The International Standard on Assurance Engagements (ISAE 3402) focuses on the quality of service and risk management in processes that you perform on behalf of your clients.

With an ISAE 3402 report, you, as a service organization, are accountable to your customers for the control of the processes that you implement, insofar as these processes and services have an impact on the financial reporting of your customers (the user organizations).

As a service organization, you demonstrate with an ISAE 3402 report how you guarantee quality, risk management and compliance within the outsourced processes. The ISAE 3402 standard offers you the scope to determine the content of the accountability based on your own scope determination and estimated risks.

Do take into account the information and assurance needs of your users to whom you provide the report.

What do you achieve with SOC 2?
The American Institute of Certified Public Accountants' System and Organization Controls Reporting (SOC 2) standard is another auditing standard with a similar purpose.

This standard is aimed at providing assurance from you as a service organization to your user organizations about the quality of service and risk management for the processes that you perform on behalf of clients and that have no direct impact on the financial reporting of your users. This includes cloud services and other IT services from service providers. Like ISAE 3402, SOC 2 is a standard for informing and accounting for your external stakeholders.

The main difference is that the scope of a SOC 2 report relates to information security, privacy, availability, confidentiality and integrity of data and not directly to the financial aspects.

What do you achieve with ISO 27001?
The international standard for information security (ISO 27001) helps organizations with the process-based design and security of information and data.

This systematic approach ensures that information security management is fully integrated into your organization. Information security affects every department of the organization, right down to your customer base and financial data. A data breach is very annoying for companies and their stakeholders. Thanks to a sound information security policy (according to ISO 27001), you reduce data risks and protect the reputation of your organization. An ISO 27001 certification also meets the laws and regulations in the field of information security.

The information security policy can differ per organization, so you can lay down your information and data security even more precisely with specific standards such as data privacy management (ISO 27701) and information management in healthcare (NEN 7510).

Market experience

Grant Thornton and BSI have already started offering the combined audit for ISAE 3402/SOC2 and ISO 27001. The listed company CM.com wanted to make the organization audit more efficiently. CM.com is an international provider of cloud software and commercial communication, with this service CM.com facilitates an excellent customer experience for their clients.

After determining the scope, it became clear that a combined audit was possible for all parties. CM.com is certified against three ISO schemes in the field of information security:

- ISO 27001
- ISO 27017
- ISO 27018

In addition, CM.com provides an ISAE 3402 report to its customers for the payments service. In the run-up to the certification, the professionals from Grant Thornton and BSI worked closely with Robin Zegwaart, Risk Manager Payments and Jorg Voeten, Lead Risk & Compliance at CM.com. It soon became apparent that the constructive and pragmatic approach of the combined audit was in line with CM.com's quality requirements. According to Jorg Voeten, one of the advantages is the consistency between the standards: "The standards frameworks are in line with each other, since the standards framework for the ISAE 3402 statement is based on the ISO standards."

In addition to substantive benefits in the field of information security and quality, the combined audit also offers organizational efficiency. "Employees' hours are precious. The combined audit ensures that these hours are planned more efficiently and that daily activities continue as smoothly as possible," says Jorg Voeten.

Read the CM.com case study and their certifications with BSI (Dutch)

More information
Would you like to know more about the joint audit of Grant Thornton and BSI? Contact BSI on +31 (0)20 346 0780 or Grant Thornton on +31 (0)88 676 9000.

Or read more about ISAE 3402 and SOC 2 and ISO 27001.

How does the combined process work?

01

Preparatory phase

Does the working method suit all parties? Then we make standards frameworks suitable for your organization. If the standards framework meets the quality requirements of your organization, we will consider optimisations.

* Please note: this is about 'what' we implement, not 'how'. A baseline measurement or pre-assessment helps to define this even more clearly.

02

Planning

Joint planning, including when auditors are on site and when relevant information is available.

03

Elaboration

We work on the documentation request. Even though no documentation is requested prior to ISO 27001, we do use documentation and evidence for an ISAE 3402 audit, for the part of the scope that covers the ISO 27001 audit.

04

Execution

We conduct interviews with the various process owners, with an ISO auditor and ISAE 3402/SOC 2 auditor participating. For example, these process owners hold one-off interviews and explain the supporting documents once. This saves them a lot of time in the crowded agendas.

05

Report

BSI prepares the ISO certificate and Grant Thornton an ISAE 3402 or SOC 2 report.

06

Final presentation

In the final presentation, together we look - with you - at potential improvements that we have identified during the combined audit. This gives your processes an optimization/efficiency boost.

How does Grant Thornton help you?

The professionals at Grant Thornton offer you high-quality services in areas such as accountancy and financial advice, audit and (third party) assurance, tax advice, sustainability & impact services and cyber risk services. We take a pragmatic and proactive approach to your challenges, often exchanging knowledge and expertise with other members of our independent global network.

We are happy to provide and advise you on your ISAE 3402 and SOC 2 audits. We see many organizations that are audited on both ISAE 3402/SOC 2 and ISO 27001. These standards differ in nature, scope and depth, but there is often overlap within these audit programs. As a result, we often examine the same topics within the audit trails.

"The burden of proof from ISAE 3402 audits and ISO 27001 audits correspond (largely) to a large extent, while auditors request this information from the organization at other times. It is cheaper and more efficient to combine those measurement moments. Our approach during an audit trail remains the same and the end result is an assurance report, but we limit the audit burden on your organization."
- **Jeffrey Martens and Christiaan Dommerholt, Grant Thornton**

How can BSI help you?

BSI's auditors constantly review your information and data security processes. Whatever industry your organization is in, BSI, as a global certification body, has experience implementing standards in almost all industries since 1901 and is at the forefront and involved in developing standards, including the creation of ISO 27001, the standard for information security. Information security and data security are more important than ever for your organization's risk management. Our auditors found that many service organizations need ISAE 3402 or SOC 2 audit report in addition to ISO 27001. Because BSI itself does not offer ISAE 3402 or SOC 2 services, it is a logical step for organizations to meet this need together with Grant Thornton.

"In terms of time, money and audit experience, this way of working is the best of both worlds. At the same time, you get two professionals who take a closer look at your business processes. That is a great efficiency boost. Thanks to the international orientation of both organizations, we can also easily implement this at your other European branches."
- Ismail Sarica, ISO 27001 auditor at BSI

Contact us
www.bsigroup.com
+31 (0)20 346 0780