Public
Cloud
Group

FOR SAAS, TECH-START-UPS & SMES

The ISO 27001 Quick Start Guide.

A hands-on Guide to passing the Audit the first time. Including 37 real audit questions and insights from an auditor's perspective.

germany@pcg.io
+49 (0) 7159 497920

More information at
www.pcg.io

Welcome!

Thank you for downloading this guide. I have created it to provide you with expert guidance on your journey to ISO 27001 certification. Use it whenever relevant for your project.

How to achieve ISO 27001 quickly & securely without taking 1000 detours.

How can you achieve ISO 27001 quickly and safely, without unnecessary delays or mistakes? Imagine your company as a high-security vault where valuable information is safeguarded. That's what ISO 27001:2022 certification enables you to do.

It acts as a quality stamp, showing your customers: "We take information security seriously." Even though it sounds complex, you can **achieve this level of information security within 6 months**. All it takes is clear goals, proper planning, and full team commitment.

In other words: Think of it like climbing a mountain – you need a guide who plans the route carefully and adapts it to the group's needs. Implementing ISO 27001:2022 works in a similar way. This practical guide will show you the necessary steps to successfully pass the audit on your first try.

Fabian Weber
Head of Compliance, PCG

Fabian Weber

HEAD OF COMPLIANCE AT PCG

Compliance has been my passion for over 10 years. Within this field, I was able to help numerous start-ups, scale-ups, and SMEs to achieve their ISO goals three times as fast. Thanks to these learnings, we now complete projects with up to 70% less effort and 50% lower costs. Our success rate is 100%.

This hands-on guide offers you valuable insights into your own ISO 27001 certification process.

The 5 Most Important Steps to Get Started.

01. Management Commitment: The Foundation for ISO-Success.

Make ISO certification a **top priority**! The support and commitment of top management are crucial to ensure that the ISO process gets the necessary resources and attention – according to the principle of **leading by example**. Regular updates and involvement in key decisions demonstrate that management is serious about information security.

Management must establish **a clear vision for information security** and embed it into the corporate culture. This encourages the entire team to work together towards the same goals.

Security matters should always be communicated directly to management, allowing them to make risk-based decisions. Likewise, regular communication from management about the **company's security goals** keeps everyone motivated.

MISCONCEPTION
"A signed contract is enough, and management just needs to appoint someone responsible for information security."

02. A Clear Timeline is Your Best Friend.

Without a clear start and finish, it is easy to lose direction. Begin with a **kick-off meeting** to set your goals, and use monthly check-ins to stay on track.

From our experience, without external support, ISO projects can take 12–24 months. With expert guidance, this can be reduced to up to 3 months.

Once you have set a start and end date, it is crucial to look for an auditor that suits you best.

MISCONCEPTION
"We'll start now and think about the deadline later."

Keep in mind that your ISO certification is influenced by various factors, including other internal projects, employees on holiday or parental leave, and, most importantly, the availability of external auditors, who are often booked up to six months in advance.

03. Appointing a Chief Information Security Officer (CISO).

Every ship needs a captain.

The **CISO leads your security programs**, ensuring it stays on course. The person chosen should have a deep understanding of the company and the ability to engage key stakeholders.

Select someone with substantial experience and the necessary authority. CISOs may need to focus on technology, processes, or strategy, depending on company's needs. Resources are also key when filling this role. The CISO is formally appointed through an official letter.

If a separate role isn't feasible, consider the growing demand for this expertise. Ensure the CISO has at least 1–2 days per week to develop the ISMS and the necessary time and training to implement ISO effectively, within the set timeline and budget.

MISCONCEPTION
"An intern can handle this task." (he has far too little insights into the company) or "Peter from IT can manage this alongside his regular duties." (lack of resources).

04. GAP Assessment: Understanding Your Current Status.

Before starting, you need to **understand where you currently stand**. A GAP assessment helps you do exactly that.

Take the time to review all your existing security measures and policies. Identify any gaps – this is your starting point.

We provide a comprehensive template for this. Often, external consultants are brought in to offer a neutral assessment and create a clear roadmap for successful implementation.

MISCONCEPTION
"I can handle the GAP assessment on my own." Keep in mind, many questions require evaluation by qualified experts, who then translate the findings into an actionable plan.

05. Building the Project Team.

While you may move faster alone, working as a team will take you further. Thus, a committed project team is essential for success.

Identify the relevant stakeholders from key departments, and **start with a kick-off meeting** to align everyone and delegate tasks. Ideally, manage the project on a central platform to keep progress on track, ensuring that the necessary personnel resources are available.

Typical departments involved include IT Operations & Development, HR, Purchasing, Facility Management, Legal, and others. In most projects, IT tools and hardware make up only 20%, while the remaining 80% is about processes, guidelines, awareness, and a robust security management system.

MISCONCEPTION
"ISO is just an IT project." This often leads to key departments or interfaces being overlooked. However, ISO 27001 imposes specific requirements on various departments, particularly HR, Purchasing, and Facility Management, which must be actively involved in the process.

Conclusion.

Implementing ISO 27001 requires thorough planning and **strong commitment from top management**, which forms the foundation for successful certification. The focus should always be on fostering a company-wide security culture, setting realistic goals, and allocating the necessary resources.

To avoid common pitfalls, assign **clear responsibilities**, conduct a comprehensive GAP analysis, and build a dedicated, motivated team. **These roles work together like interconnected gears**, essential for establishing and improving your Information Security Management System (ISMS).

Additionally, ensure a detailed roadmap is created, resources are mobilised, and the initiative is well-communicated within the company. **Working with external experts** can help accelerate the process and navigate the ISO 27001 certification journey smoothly.

Auditor Insights.

During an ISO audit, employees are interviewed, configurations and documentation are reviewed, risks are assessed, and an on-site inspection takes place. The auditor verifies all relevant information through various formats.

In this guide, I have summarised the most frequently asked questions that may be directed to your management. Additionally, I have included key tips for handling the often daunting on-site audit.

By addressing these topics thoroughly, you will not only achieve ISO 27001:2022 certification but also gain lasting value from your ISMS.

QUESTIONS FOR THE CEO

As a CEO, you should be prepared to answer the following frequently asked audit questions:

- Strategic alignment: How does the ISMS support the company's business strategy?
- Investment in security: Why is investment in information security crucial for the organisation?
- Cultural change: How do you foster a security culture within the organisation and ensure employees understand its importance?
- Progress tracking: How does management monitor the progress of the ISO 27001 project?
- Management stance: How has the management communicated the importance of information security, and for whom is it critical?
- Key risks: What are the most significant risks facing the organisation?
- Security metrics: Which key performance indicators for information security are the most important?
- Resource allocation: How do you ensure that sufficient monetary and personnel resources are available for information security?
- Operational support: How do you ensure that managers responsible for operational aspects of security are adequately supported?
- Continuous improvement: How do you measure ongoing improvements in your ISMS?

On-Site Audit Checklist.

The on-site audit is your moment to shine.

Avoid common pitfalls by ensuring all necessary documents are easily accessible, and your team is well-prepared. Proactively address any questions from the auditors.

Maintaining a calm, well-informed approach can work wonders. Remember: you have put in the hard work to get to this point. Now is the time to demonstrate it.

GOOD TO KNOW
Your decisions are risk-based, so you can justify them. Everyone starts somewhere; the goal for **your first certification is to establish a solid baseline, not to build Fort Knox!**

As part of the **"Stage 2"** audit, external certifiers will visit your company site and **interview employees.**

They will assess any gaps in your security concepts, such as physical security in compliance with ISO 27001. The auditor will also check the awareness level of your employees and how well ISO requirements have been implemented. Expect them to inspect offices, server rooms, storage areas, and other relevant parts of your organisation.

What Applies to Employees?

The following strategies can help you assess whether these rules are already being implemented internally, or if they are relevant to your organisation:

□ **Retrieve sensitive printouts from printers immediately.**

□ **Follow the 'Clean Desk Policy' (e.g. store documents in cupboards, lock your screen).**

□ **Do not leave windows or doors unattended.**

□ **Close and lock sensitive areas, such as filing cabinets or offices, especially HR and CEO offices.**

□ **Approach unaccompanied strangers, escort them to reception, and report them.**

□ **Strangers must not access secure areas without being registered (e.g. via visitor log).**

□ **Ensure screens and critical information cannot be read through windows or by outsiders.**

□ **Cleaning staff and other third parties should not be left unsupervised, especially in security-sensitive areas (ensure records are kept).**

□ **Only necessary items should be stored in work areas (e.g. no storage boxes in data centres).**

□ **Water pipes must not run above electrical equipment.**

□ **Ensure cabling in offices and other areas does not pose hazards (e.g. tripping).**

□ **Keep safety areas closed at all times.**

□ **Escape routes, fire extinguishers, first-aid kits, and cameras should be clearly marked and easily accessible.**

Other Possible Questions During the Audit Visits.

During an audit, employees might face the following questions:

1. **Who is the Information Security Officer?**
2. **How is new software requested in the company? (e.g., via an IT ticket system)?**
3. **How do you keep your system updated against vulnerabilities?**
4. **What steps do you take in an emergency, and where can you find this information?**
5. **What should you do if you suspect a virus on your computer? (e.g., disconnect from the network and inform IT)?**
6. **Have you received information security training?**
7. **Where can you find your company's central security guidelines?**
8. **Is using private hardware for company purposes allowed?**
9. **Where are company passwords stored?**
10. **What are the guidelines for using external storage devices like USB sticks, and how is compliance monitored?**
11. **Where can you access the list of standard software (e.g., the company-approved Internet browser)?**
12. **Do you receive regular updates from IT regarding threats or risks?**
13. **What processes apply to your daily work?**

VERY IMPORTANT
What to do if an auditor's question cannot be answered?

We are all human, and it is impossible to know everything. However, here is what you can do in such cases:

- **Refer to internal guidelines** and find the answer there.
- If the information isn't available, **consult your Information Security Officer**.
- Provide the required information **as quickly as possible**.
- **Document** the question and the response process to ensure transparency and demonstrate the seriousness of your efforts.

BONUS TIP
On audit day, appoint internal managers to oversee compliance with security requirements and ensure staff is informed accordingly.

Auditor Insights.

I asked an auditor what 5 key topics he focuses on during an initial ISO 27001 certification audit, and here is what he said:

01. WHAT DO YOU LOOK FOR FIRST IN AN ISMS AUDIT?

“I first look at how a company has defined the scope of its ISMS. This reveals how well they understand the ISO 27001 requirements and how carefully they are implementing them.”

02. WHAT COMMON PITFALLS SHOULD COMPANIES AVOID WHEN PREPARING FOR CERTIFICATION?

“Many companies underestimate the importance of documented processes and procedures. It’s not enough to draft policies, you must also document how they are applied in daily business.”

03. WHAT SPECIFIC CHALLENGES SHOULD SMES CONSIDER WHEN IMPLEMENTING AN ISMS AND PREPARING FOR ISO 27001 CERTIFICATION?

“SMEs often face resource constraints, both in finances and personnel. The key challenge is finding customised solutions that are effective without overburdening the company. A pragmatic approach with a focus on risk management is often the most effective.”

04. WHAT ADVICE DO YOU HAVE FOR MAKING THE AUDIT PROCESS AS SMOOTH AS POSSIBLE?

“Be organised and transparent. Have all the required documents ready and be open to questions from the auditor. Good preparation and clear communication will make the audit much easier. An ‘audit cheat sheet’ can be very helpful.”

05. HOW IMPORTANT IS MANAGEMENT’S COMMITMENT TO THE SUCCESS OF AN ISMS?

“It’s absolutely crucial. Without visible and measurable commitment from top management, the necessary support for effectively implementing and maintaining the ISMS is often missing. Audits can quickly reveal if management’s commitment is genuine or only superficial.”

Conclusion.

In this Quick Start Guide, I have outlined the key steps to achieving ISO 27001 certification and provided you with practical insights into the certification audit.

Use this document as a professional guide to help you navigate the path to ISO success and achieve your goals on the first attempt.

Need support? We are happy to hear from you!

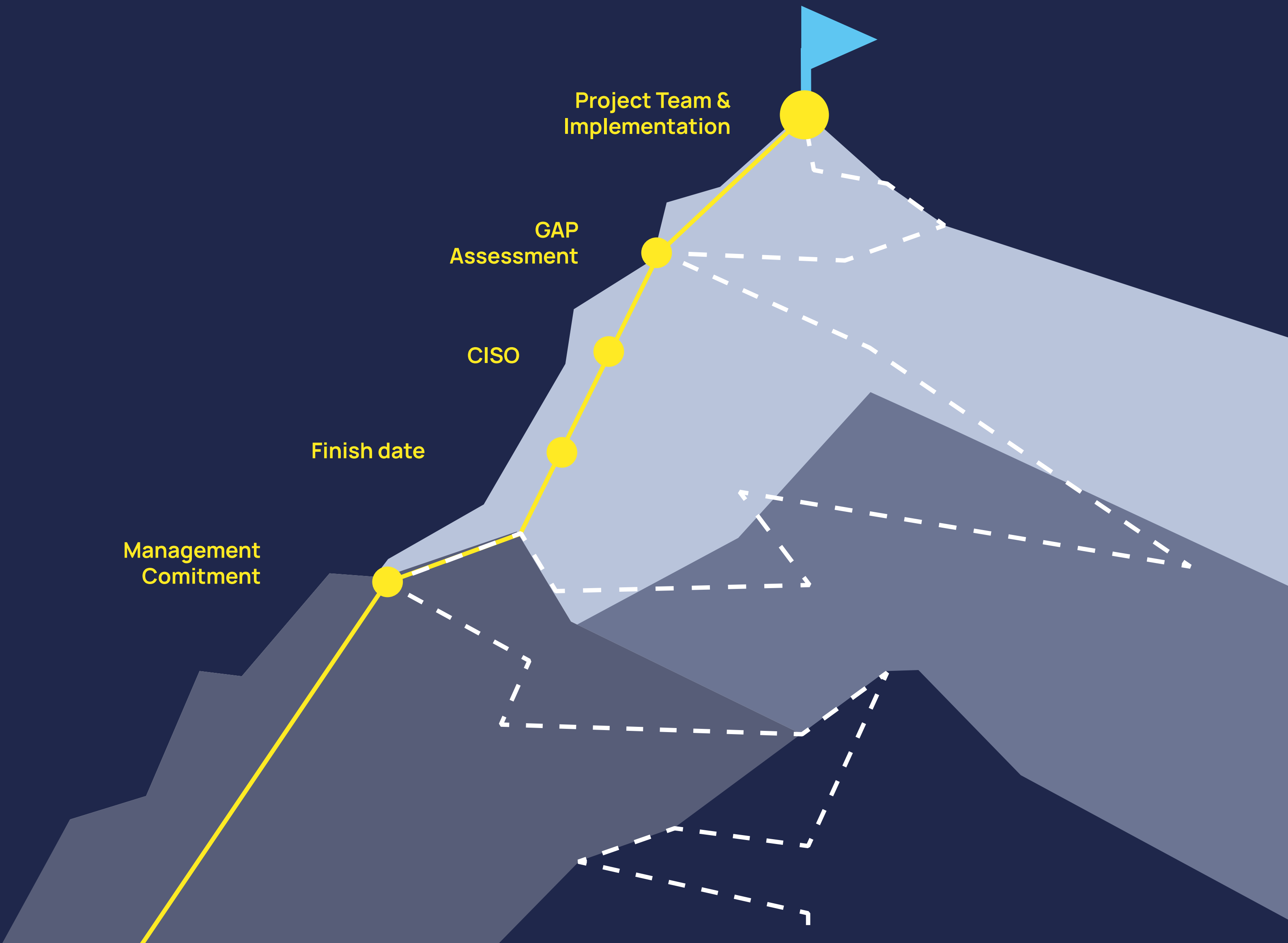
Questions or feedback?

I am happy to answer them in a personal meeting. Feel free to schedule an appointment.

Yours, Fabian Weber

BOOK YOUR FREE CONSULTATION HERE

THE TWO PATHS TO ISO 27001 CERTIFICATION



Public
Cloud
Group

About PCG.

Public Cloud Group (PCG) supports companies in their digital transformation through the use of public cloud solutions.

With a product portfolio designed to accompany organisations of all sizes in their cloud journey and competence that is a synonym for highly qualified staff that clients and partners like to work with, PCG is positioned as a reliable and trustworthy partner for the hyperscalers, relevant and with repeatedly validated competence and credibility.

We have the highest partnership status with the three relevant hyperscalers (Amazon Web Services, Google Cloud und Microsoft Cloud) As experienced providers, we advise our customers independently with cloud implementation, application development, and managed services.

Contact.

MAIL	germany@pcg.io
TEL	+49 (0) 7159 497920

More information at

www.pcg.io