

ISO27001 - Gap Analysis



What is it?

The **norm**. ISO27001 Gap analysis allows your organisation to ascertain how far it is from ISO27001 compliance.

This information can be used to provide a plan of how to achieve certification, provide assurance ahead of an external audit or simply to assess your organisation's security posture using ISO27001 as a framework for best practice.

The purpose of the Gap Analysis service is simple:

- * To assess your documentation and ensure it aligns with the ISO27001 standard.
- * To assess your current working practices, with interviews, to ensure they align with the standard and your own policies.
- * To provide an overview of whether your organisation is compliant with ISO27001 or how far you are from compliance.
- * To deliver a list of actions which, if completed, will bring your organisation into compliance with the standard.

Why now?

As security incidents become increasingly common, even amongst the world's largest companies, maintaining the security and privacy of your organisations and its customers data is a growing area of concern for businesses and the IT organisations that support them. Furthermore, customers are becoming more diligent when choosing which suppliers to use. Holding an ISO27001 certification may simplify procurement processes or be a mandatory customer requirement.

Certain industries are mandated to deploy systems and controls to protect the security and privacy of sensitive data. While doing so inevitably incurs a cost, it also brings significant benefits. Even if your organisation is not required to do so by law, adhering to compliance standards delivers many advantages.

A gap analysis helps you understand and reduce operational risks and increase revenue generating opportunities.

Can you afford to expose your business to financial, operational, and reputational risk?

What's included?

- * An assessment of your organisation's information security documentation.
- * A holistic assessment of your organisation's people, organisational, technological, and physical security controls with respect to information security.
- * An overview of how far your organisation is from ISO27001 compliance.
- * A list of actions and level of effort estimate which, if completed, will bring your organisation into compliance with ISO27001.



Want more detail?

For the full Service Description of our GAP Analysis Service [<<ClickHere>>](#).
To register your interest and get one of the team to call you [<<ClickHere>>](#)
or just give us a call on **+44 (0)20 385 55242**.

In a nutshell...

Demonstrating your commitment to meeting regulatory and best practice standards is a direct reflection on the integrity and sustainability of your business. While customers procurement processes or investor requirements are often some of the main drivers for embarking on compliance initiatives, the benefits are far greater in terms of fostering long-term relationships with customers, suppliers and partners and contributing to the bottom line. The **norm.** ISO27001 Gap analysis service is designed to provide customers with a clear picture of where their organisation stands and exactly what needs to be done to achieve compliance.

What are the business benefits?

Having your organisation formally accredited to these compliance standards provides numerous business benefits including, but not limited to;

- * Reduced direct and indirect operational risks from a cyber-attack or data breach
- * Re-enforcing customer and supplier trust
- * Opening new markets and revenue streams
- * Improving the company's value to shareholders and investors
- * Reduced corporate insurance premiums
- * Reduced likelihood of industry fines from regulatory infringements

How does it work?

Once you sign up to the service, a member of our customer experience team will be assigned as your project lead. They will arrange a welcome call with you to run you through the process, outlining who is responsible for each element of the assessment. We will then:

- * Introduce you to your fully qualified Information Security consultant who will be responsible for conducting the assessment and to provide any additional background information.
- * Your consultant will provide a list of documentation required for review and a mechanism of sharing that documentation will be agreed.
- * A workshop plan will be provided, so that working practices can be validated against ISO27001 and your business policies.
- * **norm.** will report on whether you are compliant with ISO27001, provide a list of actions needed to reach compliance, including level of effort estimate, and highlight any other risks noted during the gap analysis.

FAQs...

What is ISO27001?

ISO27001 is the international standard focused on information security. Which means it aims to preserve the confidentiality, integrity, and availability of information in all its forms. This is achieved by the implementation of an information security management system, underpinned by risk management processes, and supported by 93 security controls. These security controls are split into 4 themes: Organisational, People, Technological, and Physical. The intended outcome of all of this is a holistic and self-improving system which is tailored to your organisational needs.

How long will a Gap analysis take?

The shortest amount of elapsed time you can expect a gap analysis to take, availability permitting, is around 2.5 – 3 weeks. Split as follows:

- * 1 week to review documentation.
- * 1 week to perform workshops.
- * 0.5 - 1 week to write up the findings.

This means the “time cost” for your organisation is 1 week to attend workshops and however long it takes for your staff to locate and share documentation.

What if my organisation does not have the documentation required for the initial review?

If your organisation is missing the documentation required for review do not worry, just provide anything you do have or that you think is related. The absence of this documentation will be noted in the report and advice will be provided on how to write any missing policies.

Once we understand the gaps to compliance, can norm. assist with gaining certification?

Absolutely! A Gap Analysis is essential to understand how far away your organisation is from being able to pass a Stage 2 ISO27001 external audit and gain certification. The real work and effort, however, starts with the remediation and closure of the gaps identified and the implementation of an effective Information Security Management System (ISMS) that will be required to demonstrate to an auditor that the business is operated in accordance with the requirements of the ISO27001 standard. **Norm.** can assist organisations to successfully navigate this journey to the extent you require us to, from fully managing the implementation and establishment of the ISMS and ongoing operation, to simply providing ad hoc guidance and oversight to complement and provide qualified independent advice to your existing internal information security team to ensure you are fully prepared for external audit. For further details of this service, please refer to **norm.**'s ISO27001 Readiness Service.

norm.