When your organisation needs to be ISO 27001 compliant

Visit: www.pgitl.com
Email: sales@pgitl.com

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT

Protection Group International Ltd
Registered in England & Wales, 07967865

Increasing business opportunities by proving your organisation's commitment to information security

ISO 27001 is the globally recognised information security standard that enables businesses to demonstrate that their current policies and processes meet industry best practice with respect to protecting data. It spans all industries, highlighting best practices for improving the security of information, and minimising risks for businesses.

The benefits of achieving ISO 27001 compliance

Many organisations now require their suppliers to be compliant with the framework before doing business.

The controls required to achieve the ISO 27001 certification will minimise business risk, while demonstrating an ongoing commitment to information security. This is especially important as security breaches pose substantial legal, financial, and reputational risks for businesses.

An ability to show compliance with ISO 27001 instils trust in customers and provides peace of mind to stakeholders, who can be sure that their information is handled, stored, and managed securely.

Many businesses opt for ISO 27001 as the framework is recognised at an international level. It helps organisations to effectively manage their global reputation for best practice information security management and gives them a competitive edge, not only nationally, but in alternative markets.

How PGI can help your organisation achieve ISO 27001 compliance

Our Information Assurance experts will support your organisation at every step of the certification process, including scoping, gap analysis, implementation, internal audit and compliance maintenance.

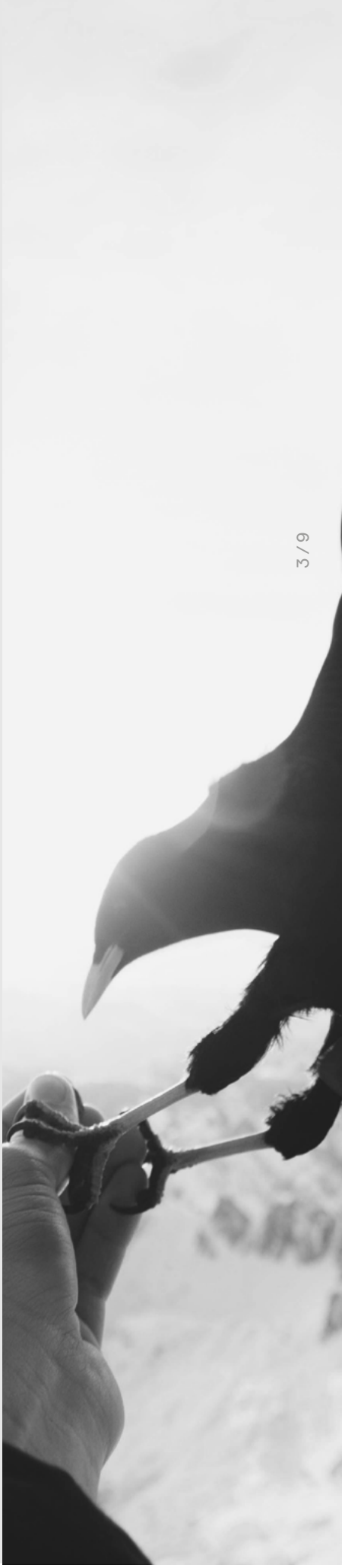
Importantly, we believe that ISO 27001 should be a business enabler, so our team want to help you achieve and maintain compliance in the most cost-effective and efficient way possible.

ISO 27001 grows and changes with your business

In fact, the ISO 27001 framework is designed to grow with your business and exemplifies the importance of taking a flexible approach to information security management.

Your organisation may want to handover the full certification process or your team may only need help with part. Regardless of the areas you need assistance with, we have the skills to help your organisation achieve and maintain compliance.

Our experts can be engaged for singular or multiple-stage ISO 27001 consultancy services, dependent upon what your organisation needs. Please keep reading for an explanation of our consultancy options.



Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865

Why choose PGI

We are a UK-based risk mitigation consultancy empowering organisations to counter digital threats. Our experts help organisations build digital resilience and believe that cyber and information security don't need to be overly complicated, incomprehensible or vastly expensive.

A TAILORED APPROACH

Not every business is the same, so we don't attempt to approach every project in the same way. We get to know your organisation, so we can provide appropriate advice.

PRACTICAL AND AFFORDABLE

Our solutions are affordable because they are proportionate to your needs, not a blanket approach.

CROSS-SECTOR EXPERIENCE

Our team are made up of personnel with backgrounds in security, law enforcement, intelligence, the military and academia and have implemented information security measures across a wide range of industries.

VENDOR-NEUTRAL ADVICE

We are vendor-neutral, so we will always act in your best interests when assessing your risks and offering a solution.

How we can help you with your ISO 27001 certification process

1. Scoping

Scope defines the information, systems and business operations that will be managed under the organisation's Information Security Management System (ISMS) and will be certified to ISO 27001.

WHY IS IT IMPORTANT?

Defining the scope encourages focus on the most critical areas of your business and the risks faced, as well as informing the selection of appropriate controls to tackle these risks.

HOW CAN WE HELP WITH SCOPING?

We can help you establish the context of your ISMS and identify the interested parties and their requirements that must be factored into its design. From this, we can help to define and document an appropriate scope.

HOW LONG WILL IT TAKE?

This depends on the size of the organisation and the complexity of its systems. Approx. 1 – 2 days.

WHY DO I NEED PGI'S HELP?

We can ensure that the context of the ISMS and requirements of interested parties are appropriately considered and represented, and that the scope is documented to a level suitable to achieve certification. Our consultants can advise on the most appropriate scope for your organisation, which may significantly reduce the scale of your ISMS implementation.

2. Gap analysis

Gap analysis involves comparing what you are currently doing against what you must do to meet the compliance requirements.

WHY IS IT IMPORTANT?

It highlights shortfalls in compliance and where efforts must be concentrated to meet the requirements of the standard.

HOW CAN WE HELP?

The gap analysis provides a view of where effort needs to be concentrated to implement an ISMS and ensure compliance with the standard. It will detail which actions should be prioritised, which can help with project planning, resource forecasting and budgeting.

You will be provided with a Gap Analysis Report, detailing the findings and prioritised recommendations.

HOW LONG WILL IT TAKE?

This depends on the size of the organisation and the scope of its ISMS. Approx. 4 – 8 days.

WHY DO I NEED PGI'S HELP?

Our consultants' expertise in ISO 27001 means they can accurately assess your organisation's current levels of compliance and provide pragmatic recommendations.

Our team can perform a gap analysis more efficiently and effectively than internal staff, who are likely to hold other responsibilities and may not be as familiar with the intricacies of the standard.

Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865

3. Risk management

Risk management identifies your important information and information processing assets, the assessment of security risks related to these assets, and the mechanisms through which these risks are controlled and monitored.

WHY IS IT IMPORTANT?

Risk management is at the core of ISO 27001; organisations must demonstrate that they have taken a risk-based approach to security. This ultimately ensures that resource and investment is prioritised and directed in the most appropriate way to tackle the biggest problems. This can prevent overspend or overcommitment to measures and practices that provide little benefit.

HOW CAN WE HELP?

We can support you in identifying information assets, performing risk assessments and developing a Risk Treatment Plan (RTP) that incorporates cost-effective controls proportionate to the level of risk.

HOW LONG WILL IT TAKE?

This depends on the size of the organisation, the complexity of its operations and the scope of its ISMS. Approx. 2 – 10 days.

WHY DO I NEED PGI'S HELP?

We are recognised as experts in risk management, allowing us to build risk management processes that both fit your organisation and meet the requirements of ISO 27001. Working in partnership with you, our consultants will combine their knowledge of effective risk assessment with your understanding of business operations to accurately assess organisational security risks.

4. Statement of Applicability (SoA)

The SoA is a fundamental part of your ISMS and is one of the mandatory documents required to achieve certification.

WHY IS IT IMPORTANT?

The (SoA) explains which of the controls (as specified in Annex A of ISO 27001) have been selected to tackle risk, which have been omitted and the reasoning.

HOW CAN WE HELP WITH SCOPING?

We can help to populate your SoA with appropriate justification for the inclusion or exclusion of controls. Our team will then review and update the Risk Treatment Plan (RTP), considering any additional controls to be implemented from the SoA.

Alternatively, our experts can provide SoA templates for you to complete and can review the adequacy and suitability of responses upon completion.

HOW LONG WILL IT TAKE?

This depends on the complexity of business operations, the scope of its ISMS and the assessed risks. This will influence the control measures selected as part of the SoA. Approx. 2 – 3 days.

WHY DO I NEED PGI'S HELP?

PGI's expertise in ISO 27001 and experience of ISMS implementation coupled with your familiarity of the business, helps to ensure that your SoA meets appropriate standards to achieve certification.

Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865

5. SoA Gap analysis

A gap analysis is conducted against the controls selected within the SoA. This gap analysis compares the current state of these controls against what must be done to meet compliance requirements.

WHY IS IT IMPORTANT?

It informs where there are shortfalls in control implementation and compliance; and where efforts must be concentrated to improve control measures that mitigate risks. This is a key part of demonstrating compliance.

HOW CAN WE HELP?

The gap analysis details which actions should be prioritised. Following the gap analysis, we will work with you to review the Risk Treatment Plan (RTP) and prioritisation of risk treatment actions. This will support project planning, resource forecasting and budgeting. You will be provided with a Gap Analysis Report, detailing the findings and recommendations.

HOW LONG WILL IT TAKE?

This depends on the size of the organisation, the scope of its ISMS and the Annex A control measures that have been selected and detailed within the SoA. Approx. 4 – 8 days.

WHY DO I NEED PGI'S HELP?

Our consultant's expertise in ISO 27001 and the Annex A control measures allow them to accurately assess your organisation's current levels of compliance and provide pragmatic recommendations.

With the help of our consultants a gap analysis can be performed more efficiently and effectively than by internal staff, who are likely to hold other responsibilities, and may not be as familiar with the intricacies of the standard.

6. Implementation

Implementation involves putting in place the control measures to ensure compliance with ISO 27001.

WHY IS IT IMPORTANT?

Failure to implement the controls necessary to mitigate risk means the organisation will not be compliant with ISO 27001. This could increase the likelihood of a data breaches and subsequent fines or penalties, as well as significant reputational damage.

HOW CAN WE HELP?

With our support your organisation can be assured that the control measures implemented are pragmatic and provide the appropriate levels of assurance. As an example, our team can apply their expertise to develop best practice, ISO 27001 compliant policies and procedures, allowing your workforce to focus efforts on other implementation activities.

Our wider team can also perform penetration tests and vulnerability assessments to identify vulnerabilities and demonstrate review and continuous improvement as required by ISO 27001.

HOW LONG WILL IT TAKE?

This is heavily dependent on the organisation's current levels of compliance. Establishing a timescale can be very difficult, which is why we recommends performing a Gap Analysis against the controls selected within the SoA. The findings of the Gap Analysis can be used in project planning and resource forecasting. Approx. 3 – 10 months.

WHY DO I NEED PGI'S HELP?

It may be the case that your organisation is best placed to perform much of the implementation. However, where necessary, we can provide support and advice where specialist expertise is necessary, or where your organisation lacks the appropriate resource.
Engaging with PGI allows an independent and unbiased view of the suitability of the controls being implemented.

Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865

7. Internal audit

Internal audit involves reviewing the implemented controls to ensure they are working effectively to manage risk and meet the requirements of ISO 27001.

WHY IS IT IMPORTANT?

Performing audits is a key aspect of ISO 27001 compliance and supports the principle of review and continuous improvement of security that is pivotal to compliance.

HOW CAN WE HELP?

Our consultants are qualified ISO 27001 Lead Auditors and can act as your internal audit function. Performing internal audits shows the performance of your security controls, including areas of noncompliance and opportunities for improvement.

Upon conclusion of any audit, you will be provided with a report detailing the findings and recommendations to improve compliance where necessary.

We can help to define an appropriate audit schedule that fits with your company and covers all areas necessary to maintain certification.

HOW LONG WILL IT TAKE?

The number of audits to be performed is dependent on the size of the organisation, the scope of the ISMS and the controls that have been selected to address risks. The length of each audit can vary depending on which control measures are under review. Approx. 2 - 4 days per audit.

WHY DO I NEED PGI'S HELP?

As qualified ISO 27001 Lead Auditors, you can be assured that our consultants will perform thorough and professional audits that cover all aspects required to maintain certification.

By engaging our experts as your internal audit capability, audits can be performed more efficiently and effectively than by internal staff, who are likely to hold other responsibilities and may not be as familiar with the intricacies of the standard and best practices for information security audits.

8. Certification readiness (review and audit support)

A guiding hand through your certification audits. Our consultants will help to ensure all required documentation is up to date and in place (for the stage 1 audit) and demonstrates all aspects of your ISMS to the external auditor (stage 2 audit).

WHY IS IT IMPORTANT?

Engaging our team help to guide you through the external audit will offer the best chance of achieving certification. We have significant experience with the ISO 27001 certification and understand the key aspects that will be inspected as part of the audit process.

HOW CAN WE HELP?

We will attend both stage 1 and stage 2 certification audits to help discuss and demonstrate to the auditor the effective ISMS that has been implemented. Our consultants will support you in answering questions from the auditor, providing appropriate evidence of compliance and, where necessary, challenge any findings that are felt to be unrepresentative of security management within the organisation.

HOW LONG WILL IT TAKE?

This is impacted by two key factors:
- The number of days required to perform a full certification audit of your ISMS (as determined by the external auditor).
- The level of PGI support you would prefer during the certification audit.

WHY DO I NEED PGI'S HELP?

Using our consultants' knowledge of the ISO 27001 standard and the expectations of external auditors, gives you the best chance of achieving certification. Those who are less familiar with the standard and the audit process may offer less detailed explanations of compliance, potentially resulting in non-conformities. These non-conformities can jeopardise certification of your ISMS.

Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865

9. Continuous improvement

Continuous improvement focuses on maintaining your compliance with ISO 27001. This is done by regularly reviewing the performance of the ISMS and enhancing measures where required.

WHY IS IT IMPORTANT?

After achieving certification, organisations are subject to regular surveillance audits from their external auditor. These surveillance audits occur approximately every 6-12 months. They are performed to monitor the organisation's ongoing commitment to security and compliance with ISO 27001.

Organisations must demonstrate that they have reviewed and, where necessary, improved security measures. Any business changes that impact security must be factored into the ISMS to ensure security measures remain robust.

HOW CAN WE HELP?

We can provide ongoing compliance support, including providing expertise on how to improve security controls and reviewing any business changes and their impact to your ISMS and certification to ISO 27001.

Our teams can also provide:
- Regular security audits
- Penetration Testing
- Vulnerability Assessment
- Security awareness and education

HOW LONG WILL IT TAKE?

For all ongoing support, PGI will provide clear timescales, considering the size of the organisation and the scope of its ISMS.

WHY DO I NEED PGI'S HELP?

Our people's expertise and experience can help you devise an effective continuous improvement programme that is suitable for your business. PGI consultants provide you with specialist knowledge and resource capacity, enabling your workforce to concentrate on their core operations.

Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865