CASE STUDY

The Ideas Distillery

Ideas Distillery smoothes the way to ISO 27001 certification for Camilleri Construction Ltd

Focusing in the domestic and commercial insurance market, Camilleri Construction works with some of the biggest insurance and claims management companies in the UK. With specialist services and its own in-house trade teams, they deal with everything from complete rebuilds to domestic refurbishments. And dealing with blue chip, FTSE 500 companies operating in the financial sector, data security is a must for their target market.

Camilleri Construction needed to achieve ISO 27001 certification in short order to meet the supply chain requirements of their target clients. With the support of the Ideas Distillery's specialist consultancy, Camilleri was able comfortably to meet the requirements of its two-stage audit, despite a demanding timescale.

Background

Insurance industry analysts acknowledge that hackers are increasingly targeting insurance companies with the aim of stealing customer information that they can use for insurance fraud. Interestingly, hackers have identified the insurance industry as one which handles extremely sensitive information but has yet to put in place measures to effectively safeguard itself and its customers from data attacks.

For hackers, the best companies to attack are those with the most consumer data, and insurance companies fit the bill. It's an uphill task for any insurance company to consistently and successfully protect its customers from hackers who only need to be lucky once. In an environment where attacks have increased exponentially, no insurance company would want to find its information breached and its customers' information stolen.

This is prompting insurance companies to secure their entire supply chains, with frontline redevelopment and refurbishment construction firms such as Camilleri a vital part.

Camilleri found itself subject to the same stringent demands as its clients and, in common with other organisations, was experiencing growing pressure to demonstrate good practice in information security.

Camilleri Construction decided to grasp the nettle and certify to ISO 27001, the global best practice standard for information security management.

Requirements

As Camilleri Construction had no existing internal knowledge of ISO 27001 certification, in 2017 it appointed the Ideas Distillery to undertake an initial appraisal of its needs and advise on a course of action. This was also framed against the upcoming GDPR regulations which contained provisions and requirements pertaining to the processing of personally identifiable information of individuals inside the European Union.

As Camilleri Construction's Managing Director Robert Camilleri said, the company was quickly convinced of the Ideas Distillery's expertise in the area: "Through our phone calls and subsequent meeting, it became apparent that the Ideas Distillery had a real depth of expertise in ISO 27001 and practical experience that was very relevant to our situation."

Camilleri also employed the services of an IT company - ITCS - to handle all its IT requirements, and the Ideas Distillery worked with them to ensure that controls were in place which would satisfy the requirements of the ISO 27001 standard.

Process

We identified the key requirements of ISO 27001 for Camilleri Construction and provided a top-level route map for successful ISMS implementation. We outlined a structured approach to implementation based around:

Planning

- ✓ Defining the scope of the ISMS.
- ✓ Undertaking a Gap Analysis to assess their management and IT system requirements and controls currently being implemented.
- ✓ Defining their information security policy.
- ✓ Creating a network map to identify all of the organisation's devices that were connected, as well as their functions.
- ✓ Producing a data map in respect of all personal data held/used by the organisation.
- ✓ Creating a list of relevant risks that would compromise the confidentiality, integrity and availability of their information.
- ✓ Defining a systematic approach to risk assessment.
- ✓ Carrying out risk assessments to identify and evaluate information security risks.
- ✓ Identifying and evaluating options for the treatment of these risks.
- ✓ Selecting, for each risk, the controls to be implemented.
- ✓ Preparing a statement of applicability (SoA).
- ✓ Formulating a risk treatment plan for approval by risk owners.
- ✓ Meeting the organisation's ongoing legal, regulatory and contractual obligations through a Compliance Legal Register.

Doing

- ✓ Helping them with the implementation of the risk treatment plan and planned controls.
- ✓ Helping with staff awareness programmes.
- ✓ Giving advice on managing operations and resources in line with the ISMS.
- ✓ Helping them to implement procedures that enabled prompt detection of, and response to, security incidents.

Checking

- ✓ Helping them with monitoring, reviewing, testing and auditing, particularly in light of a changing risk environment, technology or other circumstances.

ISO 27001 and GDPR

ISO 27001 is a framework for information protection. There are some GDPR requirements that are not directly covered in ISO 27001, such as supporting the rights of personal data subjects: the right to be informed, the right to have their data deleted, and data portability. But, if the implementation of ISO 27001 identifies personal data as an information security asset, then many GDPR requirements will be covered.

So we undertook the following programme alongside ISO 27001 implementation to map out Camilleri Construction's GDPR compliance:

- ✓ Undertaking a Data Mapping exercise
- ✓ Advice on Privacy Governance (Data Protection Officer role)
- ✓ Help with Data Sharing and Service Providers issues (where personal data is shared with third parties)
- ✓ Guidance with Justification for Processing (what data is collected and whether it is needed)
- ✓ Help with Privacy Notices (privacy notices given to applicants, employees and other workers)
- ✓ Advice on Consents and Automated Processing/Profiling (consent as the justification for processing)
- ✓ Help with Privacy by Design and Default (ensuring GDPR compliance is embedded in all processes)
- ✓ Help with Data Protection Impact Assessments (whether any use of personal data could be classed as "high risk")

Andrea Rogerson-Hewett of UKSE's Cardiff Bay Business Centre and Robert Camilleri

Outcome

Camilleri Construction's Stage 1 audit took place in June 2018, when auditors from URS Certification (UKAS accredited to certify the ISO 27001 standard) visited to inspect the company's ISO 27001 documentation. The visit passed off entirely successfully, and Camilleri was advised that it should proceed to a Stage 2 audit in July, when URS would subject the company to far greater scrutiny on how its policies and procedures were applied within the business.

This second audit proved similarly successful, with only two Opportunities For Improvement (OFIs) which were quickly implemented by the company. Camilleri Construction went on to receive its ISO 27001 certification that same month.

Looking back at the project, Managing Director Robert Camilleri says that the Ideas Distillery provided invaluable support to the company: "We would recommend to any company going through the implementation of an Information Security Management System in order to obtain ISO certification.

"Working with the Ideas Distillery has been fantastic. They are tremendously positive and were totally dedicated to helping our company succeed. Without their knowledge and reinforcement, there is no doubt that it would have taken us much longer to achieve our goal and become certified. Their support and commitment made them a pleasure to work with.

"In terms of consulting, we relied heavily on their expertise and knowledge. They fully understood the workings of our company, so that we had an ISMS that truly fitted us.

He also emphasised that the Ideas Distillery's support went further than just enabling a successful certification: "Rather than saying "Let's just get through the audit", the Ideas Distillery approached the certification process from a standpoint of real-world business benefits, and has helped us make it a part of how we approach our work."

Being ISO 27001 certificated has added significant value to Camilleri Construction's business. Not only have the company gained a series of new clients, but, as Robert Camilleri says, "It demonstrates to all our clients that we uphold best practice, and underwrites the quality and integrity of our work."

About the Ideas Distillery

Information is the lifeblood of any business – this is especially true if your clients have entrusted their valuable data to you. Implementing and maintaining an information security management system (ISMS) certified to the internationally recognised data security standard, ISO 27001, is the most effective way of reducing

the risk of suffering a data breach.

An ISMS is a systematic approach to managing the security of sensitive information and is designed to identify, manage and reduce the range of threats to which your information is regularly subjected.

Because of our knowledge, skills and experience, we can guide you and shorten the whole process, and make your information management system works more effectively and efficiently. We'll save you time and money and make sure you avoid the most common mistakes. We'll also make sure you get a system that suits you, not just impose something on you 'to get ISO 27001 certified'.

Using the Ideas Distillery throughout this process means that we will:

- ✓ Bridge the knowledge and resource gap;
- ✓ Bring experience and insight to your management systems project, considerably improving your chance for success for certification first-time by preventing any serious mistakes in development and implementation;
- ✓ Fast-track the development process by effectively planning, supporting and ensuring adequate resources.
- ✓ Save time and money by developing effective systems that realise benefits early and consequently get quicker payback on your project investment.

The major benefits which companies hold ISO 27001 certification are:

- ✓ Demonstrate credibility when tendering for contracts
- ✓ Show you are taking cyber security threats seriously
- ✓ Avoid penalties and financial losses due to data breaches
- ✓ Certification removes the need to complete detailed security questionnaires
- ✓ Give yourself a proven marketing edge against your competitors
- ✓ Meet increasing client demands for greater data security
- ✓ Protect and enhance your reputation
- ✓ Get independently audited proof that your data is secure
- ✓ Meet national and global security laws

The Ideas Distillery provides specialist ISO 27001 consultancy services. We offer our clients help and assistance with the process, producing and implementing Information Security Management Systems that comply with the requirements of the standard.

Contact us for more information:

3B Westfield Road, Cardiff, CF14 1QQ

T: 029 2196 1066 | **E:** info@ideasdistillery.co.uk | www.ideasdistillery.co.uk