macnamara®

SECURITY CERTIFICATION WHITE PAPER

From Cyber Essentials to ISO 27001
How To Pass First Time

Macnamara ICT
Ciaran Kenny MA MSc CITP CEng FBCS

Executive Summary

There are two primary reasons why companies decide to go through the process of security certification.

Sales, Marketing and Commercial

Some customers, such as most government departments or health care providers want specific credentials from their suppliers. Certification can also help with sales and marketing as prospective clients are more likely to do business with a company that takes security seriously.

Security and Compliance

Companies may choose certification to increase the security of their corporate information and financial well-being precisely because they care about security and compliance. Choosing the certification route necessitates a rigorous strategy. Certification can also be used to ensure that a company is in compliance with regulatory and legal duties, such as those imposed by the UK-GDPR.

The two sets of reasons are not mutually exclusive and security certification can produce benefits across both sets at the same time.

This report lays out a certification path for UK based companies, charities and other organisations, beginning with the simplest and progressing through a logically ordered set of certifications to the most time consuming and resource intensive.

The extent to which security certification can positively impact business productivity simply by getting all your information and information processing procedures in order is a benefit of security certification that rarely features in the motivations of those seeking certification but often comes as a pleasant surprise.

Thinking About Certification

Have you considered obtaining a security certification for your company? Perhaps some of the contracts for which you are bidding require certification. This is especially true if you sell to or want to sell to central or local government.

Companies and other organisations are also increasingly checking to see if their suppliers have security or other certifications and giving preference to those who have when granting or renewing contracts.

Without question, getting accredited can enhance your sales and marketing efforts. If nothing else, you will receive some eye-catching badges to display on your website and marketing materials.

What Exactly Is Security Certification?

Holding a security certification demonstrates that your firm complies with a set of security requirements that comprise a security standard. In this paper, we will look at the main security standards that UK firms can be certified against:

Cyber Essentials
Cyber Essentials Plus
IASME Cyber Assurance Level 1
IASME Cyber Assurance Level 2
ISO 27001

Cyber Essentials and Cyber Essentials Plus are government-backed standards in the United Kingdom that are overseen by the IASME (Information Assurance for SMEs) Consortium and established in collaboration with the National Cyber Security Centre (NCSC).

Levels 1 and 2 of IASME Cyber Assurance are based on IASME's own governance and security standard, which can be thought of as a simplified version of ISO 27001.

ISO 27001 is a global standard that establishes a framework for managing information security. It is the most well recognised standard for information security management and is produced by the International Organisation for Standardisation (ISO).

Is It Worth Getting Certified?

Obtaining certification necessitates work. The standards mentioned above are listed in ascending order of difficulty. Your motivation for certification aside, the goal of the security standards is to strengthen your company's security and reduce cybercrime threats to you, your employees, your customers and suppliers, and your company's cash. Aside from lowering risk, a focus on information security can help to guarantee that your company is following legal and regulatory standards such as the UK-GDPR. Consider the following factors when deciding whether certification is worth the expense and effort:

- The security benefits in terms of risk reduction.
- The security benefits in terms of legal and regulatory compliance.
- The sales and marketing benefits.

If your customers, or organisations that you want to be your customers, require certification, it is simply a matter of determining which certification(s) they require and determining whether you value those customers enough to commit the necessary resources to getting certified.

If, on the other hand, your goal is to improve your organisation's security to decrease risk, meet legal or regulatory requirements, or both, the question becomes a little more complicated:

- Is certification the best way to improve security?
- Which certifications will yield the best improvement for the least cost and effort?

For most businesses, the stark separation between sales, marketing, and security is inaccurate. Of course, you can benefit in both ways. However, it is likely that your major motivation is one of the two.

Isn’t Certification Just A Box Ticking Exercise?

Yes, it certainly can be. It depends on you. From here on we will assume, even if you are primarily motivated by sales and marketing goals, you are pleased to get the security benefits. This being the case, the box ticking exercise criticism can be flipped on its head: yes, it is a box ticking exercise and, if you can honestly tick all the boxes, you are going to get a significant security uplift. Box ticking or not, if our goal is to improve security a standard will help.

When it comes to security, you may ask if you really need a badge. Why not just focus on increasing security and ignore these bureaucratic standards? This position is not unreasonable; however, there is more than a touch of reinventing the wheel here.

If you wish to increase security, why not use the work that has been done to create the standards as an instruction manual or framework to guide your efforts? Otherwise, it can be very difficult to know where to start. After that, you might as well seek certification to ensure that you did everything correctly.

Is There A Downside To Using A Standard?

Except for ISO 27001, which costs roughly £200 (for the document), all the standards covered here can be obtained for free. So cost is not an issue.

The biggest disadvantage of using a standard is that they are all assembled by expert committees. As a result, some clauses may be perplexing. It can be tough to grasp exactly what you are being asked to do at times. These periodic misunderstandings result from the necessity for compromise and consensus on committees.

These issues are uncommon and can easily be sorted out by asking someone who knows or spending some time on Google. There is relatively minimal risk in exploiting professional work that has already been completed. Without a standard, it can be hard to know where to start or where you are.

The Certification Journey

The security certification journey can be compared to a tube line running from Cyber Essentials to ISO 27001. You can either take the entire journey or get off at an intermediate stop. Your destination is decided by your objectives in security, compliance, sales, or marketing. If done correctly, covering the whole line will take a couple of years, but you may not need to go all the way to the end of the line. Let's take a look at that journey.

CYBER ESSENTIALS

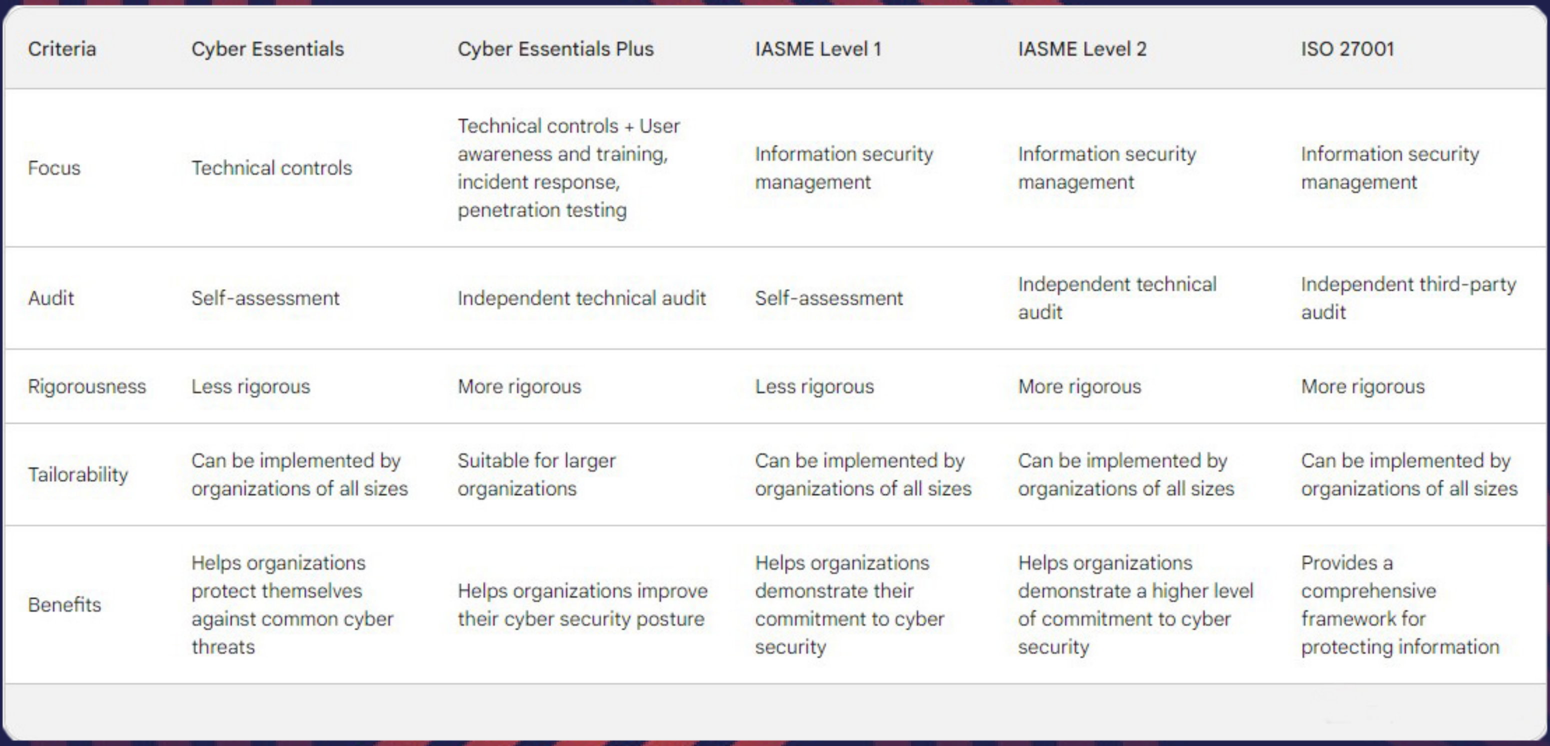
CYBER ESSENTIALS PLUS

IASME CYBER ASSURANCE LEVEL ONE

AUDITED IASME CYBER ASSURANCE LEVEL TWO

Information Security Management ISO 27001 Certified

Each certification has different controls, audit methodology, and benefits:



Criteria	Cyber Essentials	Cyber Essentials Plus	IASME Level 1	IASME Level 2	ISO 27001
Focus	Technical controls	Technical controls + User awareness and training, incident response, penetration testing	Information security management	Information security management	Information security management
Audit	Self-assessment	Independent technical audit	Self-assessment	Independent technical audit	Independent third-party audit
Rigorousness	Less rigorous	More rigorous	Less rigorous	More rigorous	More rigorous
Tailorability	Can be implemented by organizations of all sizes	Suitable for larger organizations	Can be implemented by organizations of all sizes	Can be implemented by organizations of all sizes	Can be implemented by organizations of all sizes
Benefits	Helps organizations protect themselves against common cyber threats	Helps organizations improve their cyber security posture	Helps organizations demonstrate their commitment to cyber security	Helps organizations demonstrate a higher level of commitment to cyber security	Provides a comprehensive framework for protecting information

Cyber Essentials

CYBER ESSENTIALS

Despite being an entry-level standard, Cyber Essentials is appropriate for enterprises of all sizes and provides protection against all the most frequent cyber-attacks.

Cyber Essentials focuses on technological security controls in five main areas:

- Secure configuration of IT systems and software
- Boundary firewalls and Internet gateways
- Access control
- Patch management
- Malware protection

To obtain Cyber Essentials certification, you must first complete an online self-assessment. Your answers are then evaluated by a qualified assessor, who may either grant a pass or fail or (more likely) request additional information.

The self-assessment questions can be downloaded here: Free Download of Cyber Essentials Self Assessment Questions - Iasme and a full explanation of the standard here: Cyber Essentials Requirements for IT Infrastructure v3.1 April 2023 (published January 2023) (ncsc.gov.uk).

The NCSC has also provided a Cyber Essentials Readiness Toolkit which you can access here: Readiness | (iasme.co.uk).

Passing Cyber Essentials

The key to passing Cyber Essentials first time is:

- Read the Requirements for IT Infrastructure document
- Make any necessary changes to your environment (based on the document)
- Write any necessary policies or procedures (based on the document)
- Contact Macnamara, another certification body or IASME directly to setup your online assessment.
- Complete the assessment as you would an exam, i.e., read the questions carefully and answer them in full without adding any additional information.
- Do not submit your answers until you have double checked them, making sure:
    - No answers contradict other answers
    - You have provided additional information where it is required
    - You have not included any unsupported equipment in inventory details.
    - You understand all the questions and all your answers.

One frequently asked question concerning Cyber Essentials is:

"Given that it is a self-assessment, can't I just put whatever answers I want, even if they are not true?"

The answer, of course, is yes. But, aside from the necessity that the most senior person in your firm certify the responses as truthful, it is a meaningless exercise.

Cyber Essentials is the very minimum that each responsible firm should do in terms of cyber security. Making the decision not to do so while pursuing a security certification appears to be a self-defeating strategy. It's also worth mentioning that the interconnected nature of some of the questions can make it clear if you do decide to go down this path.

As well as providing an uplift to your company’s security, Cyber Essentials should be viewed as an educational exercise aimed at raising awareness inside your firm. It must be repeated once a year to keep the certificate valid.

Cyber Essentials Plus

Cyber Essentials Plus builds on Cyber Essentials, i.e. a successful Cyber Essentials self-assessment is a prerequisite, by adding the following controls:

- User awareness and training
- Incident response
- Penetration testing

The primary distinction between Cyber Essentials and Cyber Essentials Plus is that Cyber Essentials Plus includes an independent technical audit of your IT systems to ensure that appropriate controls are in place.

While Cyber Essentials is a good starting point for organisations new to cyber security because it is relatively simple to implement and maintain and can help protect your organisation from common cyber threats, Cyber Essentials Plus is a more comprehensive scheme that is appropriate for organisations looking to improve their cyber security posture. It requires more effort to implement and maintain, but it provides greater assurance that your organisation is secure from cyber threats.

You can download the Cyber Essentials Plus test specification from the NCSC here: Cyber Essentials Plus Illustrative Test Specification v3.1 April 2023 (ncsc.gov.uk)

The Cyber Essentials Plus test includes:

- External vulnerability scan and internal vulnerability scan of end user devices, servers and cloud services
- Check if device patching is up to date
- Check protection against malware
- Check that Multi Factor Authentication is enabled on all cloud services
- Check that user accounts do not have administrative privileges

The assessor will also consider, and perhaps verify, the answers provided on the Cyber Essentials self-assessment.

To pass the first time, download the above-mentioned test specification, perform the tests yourself, and make any necessary modifications before applying for the assessment. Before completing the assessment, the assessor will provide feedback and allow you to make changes.

To keep your certification valid, you must retake the evaluation every year.

You can get more information about both tiers of Cyber Essentials from the NCSC here: Cyber Essentials Frequently asked questions (FAQ) - NCSC.GOV.UK and from Macnamara here Cyber Essentials: is it worth it? - Macnamara ICT

IASME Cyber Assurance Level 1

IASME Cyber Assurance approaches information security quite differently than Cyber Essentials, though Cyber Essentials is a precondition for IASME Cyber Assurance. IASME Cyber Assurance is expressly designed to be a simplified version of ISO 27001 that may be attained by smaller enterprises without the resources required by ISO 27001.

The standard can be downloaded here: IASME Cyber Assurance Standard v6.0.

IASME describes the certification as:

> *“an award demonstrating an organisation’s proactivity towards maintaining a reasoned state of cyber and information security”*

The IASME standard provides significantly more guidance than Cyber Essentials and focuses far more on governance and people, based on the notion that technical measures alone will not keep you safe.

IASME Cyber Assurance is based on risk and the implementation of controls appropriate to the risks identified. The standard is divided into thirteen themes as follows:

- Planning information security
- Organisation
- Assets
- Legal and regulatory landscape
- Assessing and treating risks
- Physical and environmental protection
- People
- Policy realisation
- Managing access
- Technical intrusion
- Backup and restore
- Secure business operations, monitoring, review and change management
- Resilience: business continuity, incident management and disaster recovery

For each theme, detailed advice and explanation is included in the standard and in many cases, where documentation is required, templates are available here: IASME Cyber Assurance Helpful Templates

IASME Cyber Assurance is more difficult to complete than Cyber Essentials since it requires a significant amount of documentation, and while many of the policies and procedures you need may already exist, there is a good chance they haven't been documented.

To successfully pass IASME Cyber Assurance Level 1 first time, start by downloading the standard from the link above:

- Read it in detail to identify where you are likely to fall short.
- Conduct a risk assessment as outlined in the standard and base the rest of your work on that assessment, e.g. to determine whether you need a separate policy for a specific area, review the risks associated with that area.
- Download the question set from here: IASME-Cyber-Assurance-Question-Set_V12e-Hartnell
- Work through the question considering your risk assessment and risk treatment.
- Prepare the necessary policies, procedures and evidence, such as log files.
- Publish policies and procedures and verify that all staff have read and understood them.
- Contact Macnamara, another certification body or IASME directly to setup your online assessment.
- Complete the assessment as you would an exam, i.e., read the questions carefully and answer them in full without adding any additional information.
- Do not submit your answers until you have double checked them.
- Your answers will be checked by an IASME assessor.

You will get a pass / fail result or request for more information within 72 hours. The online self-assessment must be repeated annually to maintain a valid certification.

IASME Cyber Assurance Level 2

IASME describes its Level 2 certification as:

> *“an award independently confirming that an organisation’s achievement in cyber and information security is in line with industry expectations.”*

IASME Cyber Assurance Level 1 is a prerequisite for Level 2. Level 2 involves an independent audit of the processes, procedures and controls required by the standard as covered in Level 1.

The audit is conducted by an IASME Certification Body Assessor and is a non-technical audit usually involving interviews with members of staff and a review of documentation and system configurations.

How To Be Audited

Being ready for the assessor and making their life easier will help you to have a successful audit:

- Organise facts and evidence in advance, i.e., know the locations of key documentation and verify that you have the necessary access.
- During the meeting try to provide thoughtful and detailed answers but be concise.
- Do not volunteer information that has not been requested, only answer the questions asked and do not introduce new or associated topics. Stick to facts in your answers and do not express your opinions.
- When asked for examples, give real life examples rather than ideal or desirable situations.
- Be friendly and helpful and remember the audit is not a test that you can fail if you give the wrong answer. The auditor has been employed to help us achieve certification.

Prepare your staff for the audit, auditees must be familiar with the policies and procedures relating to their areas of responsibility. They must also know:

- Where the information security policies can be accessed
- How to raise a security incident
- Who is responsible for information security and how to contact them

The IASME Cyber Assurance Level 2 certification is valid for one year but is automatically renewed in years two and three if you successfully complete IASME Cyber Assurance Level 1. Year four renewal requires a full audit as in year one.

ISO 27001

With IASME Cyber Assurance Level 2 under your belt, you are well on the way to obtaining the gold standard in information security, ISO 27001. ISO 27001 is a global standard that establishes a framework for managing information security. It is the best recognised standard for information security management and is produced by the International Organisation for Standardisation (ISO).

ISO 27001 is a more stringent standard than Cyber Essentials and covers a broader range of topics than IASME Cyber Assurance.

You may read a portion of the standard here: ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection – Information security management systems – Requirements. You will have to purchase a full copy from the same location to embark on a certification project.

ISO 27001 defines the structure of an information security management system as well as 114 security controls that can be adapted to an organisation's needs. Unlike IASME Cyber Assurance, ISO 27001 provides little direction on how controls should be implemented; this is up to you depending on your own needs and the requirements of the standard.

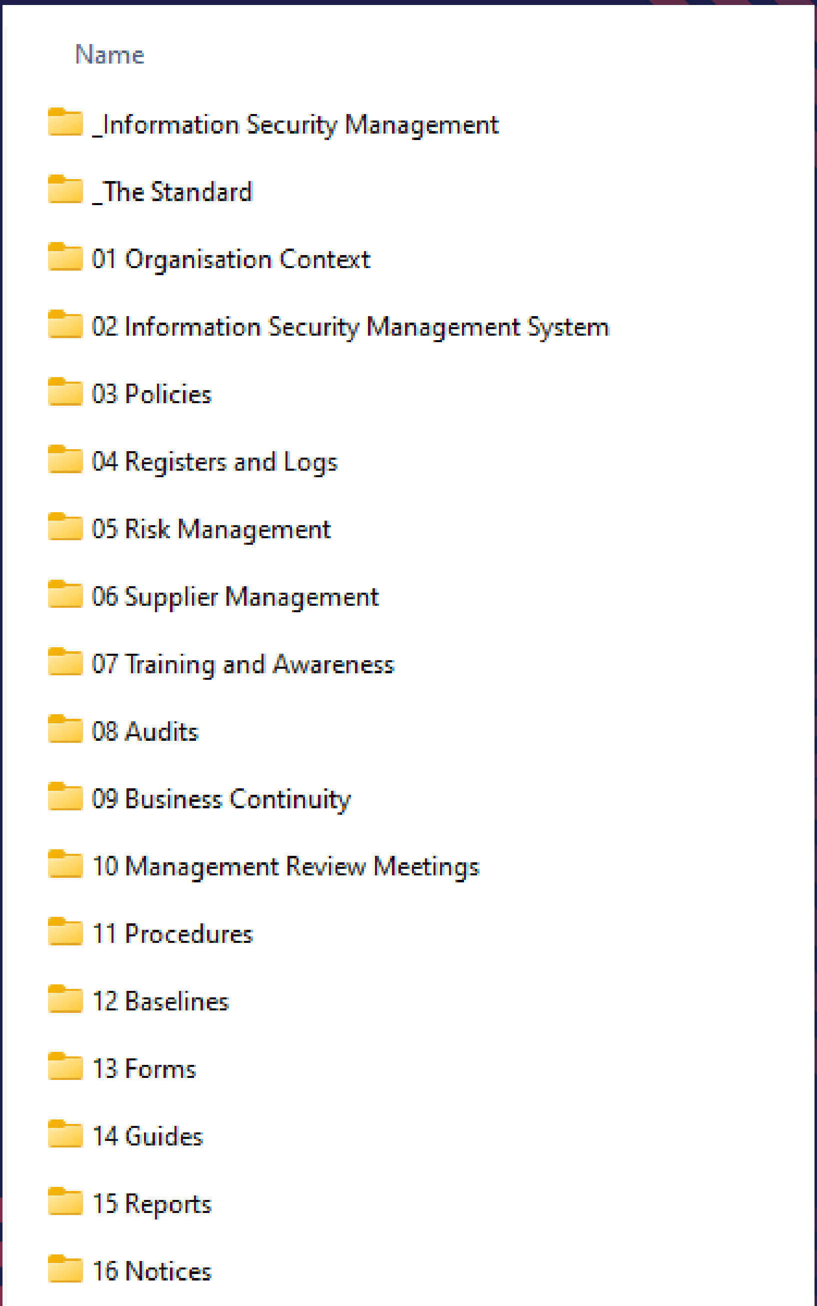
However, if you do need more guidance than is directly provided in the standard there are a substantial set of documents in the ISO 27000 range which provide this guidance, and many of the same areas are covered by the detailed guidance given in the IASME Cyber Assurance standard.

Like IASME Cyber Assurance, ISO 27001 requires organisations to implement a risk-based approach to information security. This means that you need to assess your risks and implement controls that are proportionate to those risks.

The key concepts of ISO 27001 are:

- Risk assessment: This is the process of identifying, evaluating, and mitigating risks to information security.
- Information security controls: These are the measures that organisations put in place to protect their information assets.
- Risk treatment: This is the process of taking steps to reduce the likelihood or impact of risks to information security.
- Information security management system (ISMS): This is the framework that organisations use to manage their information security.
- Continuous improvement: This is the process of continually improving the ISMS to meet the organisation's changing needs.

A comprehensive ISO 27001 Information Security Management System will look something like this:



Name

_Information Security Management

_The Standard

01 Organisation Context

02 Information Security Management System

03 Policies

04 Registers and Logs

05 Risk Management

06 Supplier Management

07 Training and Awareness

08 Audits

09 Business Continuity

10 Management Review Meetings

11 Procedures

12 Baselines

13 Forms

14 Guides

15 Reports

16 Notices

How Long Does It Take?

This is determined by the resources available for the project and whether templates are used to meet the documentation needs.

There are firms that will walk you through everything in three months, but to get the most out of the process, you should do it yourself using a licensed template pack and, if necessary, consulting specialists. Nothing in the standard requires in-depth technical knowledge, and it is a frequent misconception that security standards should be left in the hands of technical people.

Internal and external audits are required by the standard, with a full internal audit cycle of the system and its controls accomplished before an external audit can take place. Attempting to implement and fully audit the system in less than six months is unrealistic, at least if you want to achieve a real security uplift. One year is a reasonable time frame for achieving certification and reaping the security benefits of a worthwhile deployment.

An emphasis on evidence to verify that controls are applied over time distinguishes ISO 27001 from both Cyber Essential and IASME Cyber Assurance. The previous two are very much point-in-time assessments, i.e. certification that the standard was fulfilled on the day of assessment, whereas ISO 27001 certification comes closer to demonstrating that the standard was met at the time of audit and for a discernible period prior to the audit.

It is not useful to try to encapsulate the keys to success with ISO 27001 in a paragraph because the standard itself contains everything you need to know; however, you may want to contact Macnamara or another source of knowledge for advice on interpreting the standard.

The ISO 27001 certification is granted after a successful Certification Audit conducted by an ISO 27001 Certification Body. It is not uncommon for a first audit to fail and for the audit report to be used to prepare for a second effort.

The ISO 27001 accreditation is valid for three years and is subject to a continuous internal audit covering the information security management system and all controls every 12 months, as well as an external Surveillance Audit in years two and three to verify the system's and controls' continued operation. In year four, an external audit for recertification is required.

Other Security Standards And Certifications

ISO 27001 is by far the most well-known and widely recognised information security standard, but there are many others: some defined for specific applications, such as IEC 62433 for Industrial Automation and Control Systems (IACS), others applicable in specific countries or territories, such as Australia's Essential Eight, and some with limited and tightly defined applicability, such as ETSI EN 303 645, which provides a set of baseline security requirements for consumer electronic devices making up the Internet of Things.

The US National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is used by larger US businesses, is perhaps the most directly comparable in breadth to ISO 27001.

You may come across another couple that appear to be standards or certificates but are, in fact, something else:

SOC (System and Organisation) Reports

The American Institute of Certified Public Accountants (AICPA) created SOC reports. A SOC report is an audit report that covers information security, availability, processing integrity, confidentiality, and privacy safeguards. SOC 2 reports are frequently issued, subject to NDA, to demonstrate an organisation's commitment to information security.

SOC 3 is more general, whereas SOC 1 is more focused on financial systems. A SOC for Cybersecurity report may also be made available. These reports are not security certifications, but they can be quite helpful when evaluating a potential supplier.

PCI-DSS (Payment Card Industry - Data Security Standard)

PCI-DSS appears to be a security standard because it is one. However, unlike the other standards discussed in this study, it is a private standard produced by a consortium of payment card and payment service industry groups, including Visa, Mastercard, and American Express.

PCI-DSS does not have an associated certification; rather, it is used to protect payment card service providers from fraud and determine the fees charged to their customers, such as retail stores, restaurants, and so on, based on the extent to which they are compliant with the standard, as determined by a questionnaire they complete, or a test administered by the provider. The standards discussed in this report provide a way of complying with PCI-DSS which is necessary if you handle payment cards.

Conclusion

Whether you are interested in security certifications due to a concern for security, a desire to meet compliance obligations, commercial requirements, or simply because the badge would look good on your website, there is a straightforward path that leads from Cyber Essentials to ISO 27001, with plenty of stops along the way.

Both levels of Cyber Essentials make up the entry level to certification and are relatively simple to implement. Together, they eliminate most of the cyber risks faced by businesses. IASME Cyber Assurance goes substantially further by covering risk, people, policies and procedures. While IASME Cyber Assurance is more demanding than Cyber Essentials, IASME provides a huge amount of guidance, templates and material to help you through the process.

ISO 27001 is the gold standard and not especially easy to obtain as very little guidance is given. However, if you follow the path set out in this report and use IASME Cyber Assurance as a steppingstone to ISO 27001 you will find that you are 70% of the way there when you start. The remaining 30% will take work and may require expert assistance but it is very achievable and not different in kind to the work already done for IASME Cyber Assurance.

Were you to start with ISO 27001, it can be depressing to embark on a project that will not produce results for a year or more; on top of that, convincing management to support such a long-term initiative can be difficult.

By following the steps outlined in this report, you will be able to create results rapidly while also delivering many certifications along the road. Sales and marketing personnel will be pleased when you supply new tools and badges as you steadily increase your organisation's security. You will also see a consistent increase in business productivity as employees become accustomed to working in a structured manner, according to specified protocols for everyday activities, understanding where information is stored, who has access to it, and what security incidents look like.

Whatever your motivations, if you want to bring tangible benefits to your business in the areas of security, compliance, sales, marketing, and productivity, going on the security certification journey is one of the best and most cost-effective ways to do it.

What Next?

If we've aroused your interest and you want to learn more, Macnamara are security and certification experts. Ciaran Kenny, our security lead and company founder, would be glad to speak with you.

And don't worry, it's true: you can do it all on your own. We're here to help if you need it, but there's nothing stopping you from doing it yourself.

Ciaran Kenny | Director & Security Lead
ciaran@macnamara.co.uk
020 8132 5803

Geoff Courts | Managing Director
geoff@macnamara.co.uk
020 8132 5804

Macnamara ICT
enquiries@macnamara.co.uk
020 3443 9820

Macnamara ICT Ltd, The Clarence Centre, 6 St George's Circus, London, SE1 6FE

https://macnamara.co.uk