The IASME Governance Standard for Information and Cyber Security

Document Number:	iasmestandardv5_0_dgd01.docx
Issue:	5.0
Date:	02 January 2018
Author:	Daniel G. Dresner
Technical Approval:	Jamie Randall
Quality Approval:	Emma Philpott

Modification History

Revision	Date	Revision Description
1.0	1 April 2011	For issue
1.0e	March 2012	Review
1.1	April 2012	Reissue
1.2	August 2012	Minor additions
2.1	December 2012	Alignment with other standards
2.2	March 2013	Inclusion of social media
2.3	March 2013	Conformance statements
3.0	May 2015	Review and update
3.1	October 2015	Review – consistency throughout (such as the objectives and actions matching up) and realignment with the constraints of SMEs (especially with respect to organisational expectations).
3.2	December 2015	Detailed revision. Including correction of the variations in the content and order of the control points in versions 2.3 and 3.0 as the reader progressed through the document.
3.3	February 2016	Updated after IASME Consortium review.
3.4	March 2016	Revised with comments from the certification bodies
4.0	April 2016	For issue
4.1	April 2017	Advisory Board review
5.0	January 2018	For issue

Contents

List of Figures

List of Tables

0. Introduction

0.1. General

Information and data are intangible, yet valuable, business assets that are often neglected in favour of protecting physical assets or attending to cash flow. Information (from hereon in to include data) is often difficult to value and its true worth may only be realised if it becomes unavailable or unreliable. That's why information security – and its subset *cyber security* – is measured in terms of the confidentiality, integrity, and availability of that information.

As the information age has matured, the rate of change – and complexity of business systems – has often left businesses vulnerable to information security breaches. Whereas there can be no guarantees for information safety, there are frameworks available to reduce the associated risks – and their impact – to an acceptable level. However, these frameworks often originate with a focus on large corporations where size and resources give them the wherewithal to implement the protective and contingency measures.

Smaller, dynamic businesses and organisations differ from their larger, more structured counterparts and must deal with information security with greater flexibility and with much smaller budgets. The structure of rigid procedures that support the internal communications in large organisations must give way to the informal cultures of small to medium-sized enterprises (SMEs).

This governance standard, Information Assurance for Small to Medium-sized Enterprises (IASME) is designed as a security benchmark for the SME. The IASME Governance Standard is designed to guide the SME where needed and then assess the level of maturity of an SME's information security. Recognition of this benchmark can be used to assure themselves and their customers that information lodged with them is safe in all practical respects. The IASME Governance Standard can also be scaled up for larger organisations.

0.2. The IASME Governance Standard's objectives

The IASME Governance Standard is an organised way for a business to implement new ways of securing its information, improve existing ones, and be recognised in its sector for having done so. Implementing The IASME Governance Standard creates security-aware workers as part of business as usual.

0.3. How to use this document

Security is a state of assurance which once achieved will need to be maintained. And because it is dependent on the view of risk – which is almost certainly going to vary given the variety of objectives shared across different stakeholders in an organisation (or chain of organisations) – then whether it is achieved or maintained can become subjective. So we have The IASME Governance Standard. It comprises a balance of description and prescription to educate, inform, and give the different stakeholders a common benchmark. The core parts of the standard are formatted in three sections.

0.3.1. Guidance and requirements

The degree to which security activity is engaged needs to be proportionate to the risk involved. When the impact is directly upon people in particular, this may be tragic and irreversible. The guidance section is there to direct you to useful activity to manage the commensurate level of risk.

The requirements subsection sets out the key action that need to be done to have assurance in the security of your information. Your risk profile will steer you beyond these (depending on what it describes).

0.3.2. Typical questions and performance indicators

These subsections set the tone – but not the exhaustive set – of questions that might be asked during an assessment to The IASME Governance Standard. Remember that you are expected to have been able to address all the self-assessment questions first – in line with your risk profile. An assessment may revisit these and go further to assure the state of your security. The examples herein are indicative only to help you and remove the temptation to feel that passing an assessment is a sign to relax!

0.4. Compliance

The minimum benchmark of compliance with this standard is for a company or organisation – regardless of its risk profile – to have met the requirements of The IASME Governance Standard self-assessment which includes the established requirements of the Cyber Essentials Scheme.

Note: A self-assessment is not valid until its compliant completion has been ratified by an accredited IASME certification body.

0.5. Compatibility with other cyber and information security standards

IASME – with The IASME Governance Standard at its core – is a programme of security assurance that has been compiled by SMEs for SMEs with the support of the Technology Strategy Board (now Innovate UK). It provides common ground for SMEs amongst other methods – or standards – which are either not comprehensive or are too prescriptive in their level of complexity for an SME. The IASME Governance Standard creates an equitable approach to cyber and information security for SMEs to work safely in the supply chain with corporate counterparts or customers. To help you keep a sense of perspective, some of these standards are put into context here. Many of them provide detail to particular problems of security and can help to define specific security policies to protect a business and help it recover from information-related loss.

The IASME Governance Standard doesn't expect a company [an SME in particular] to record every policy in a discrete document but does expect the respective policies to be realised consistently for information safety as determined by the company's risk profile. However, if a contract calls for that policy to be documented, The IASME Governance Standard too - which calls for compliance with contractual obligations - would expect it to be documented. (*See Table 4: Explicit and implied information and cyber security policies.*)

0.5.1. Cyber Essentials Scheme (CES)

Both The IASME Governance Standard and the international standard ISO 27001 are based on a risk-led approach, with appropriate treatment. However, day-to-day information and cyber security risks are endemic within a wide range of organisations[1] and it is challenging to set a baseline set of activities that are common to all. Cyber Essentials was created to mitigate the risk from common Internet-based threats based on a significant proportion of the everyday attack paths that lead to all organisations. It is deliberately prescriptive and is aimed to provide a base level of controls before the business even begins to work with computers and other information technology. Cyber Essentials is the starting point of the benchmark against this The IASME Governance Standard.

Cyber Essentials has similarities to the 'MOT' – a test of basic roadworthiness not mechanical assurance. Whereas Cyber Essentials is about the basic technology, The IASME Governance Standard is about the technology, about you, *and about* where and how you work.

The IASME Consortium helped to develop the CES requirements and is one of the Scheme's Accreditation Bodies. The IASME CES requirements are encapsulated into The IASME Governance Standard assessments and can be certified together or separately.

0.5.2. BS ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27001 is the vanguard to a comprehensive set of standards comprising over 35 titles. It sets out the components of an information security management system (ISMS) without giving specific direction on how to tailor the ISMS for the respective business. The IASME Governance Standard was created to bridge the gap between no ISMS and an ISO/IEC 27001-compliant ISMS. An SME which begins with The IASME Governance Standard and migrates to ISO/IEC 27001 is to be commended.

[1] See NCSC (2016) *Common Cyber Attacks: Reducing The Impact*

0.5.3. BS ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27001 is a generic approach to information security that can be applied to cyber security risks. ISO/IEC BS 27032 is a specific set of guidelines addressing the risks usually associated with the idea of cyberspace being an identifiable – but non-physical – environment where people, processes and technology interact. This standard is typical of the growing ISO/IEC 27n library (*see Appendix B*)) which is always open to SMEs who want to adopt a more prescriptive approach to information and cyber security management than The IASME Governance Standard expects.

0.5.4. NCSC 10 Steps to Cyber Security

This is a set of high level awareness guidance that centres on having a board's information risk management regime (step one) and nine things to implement it. All these 10 elements are built into The IASME Governance Standard framework with a round-trip check to make sure that they are being done well enough.

0.5.5. CPNI/SANS 20 Critical Controls for Cyber Defence

This is a catalogue of controls set out by the USA's Center for Internet Security (CIS) and the SANS Institute which have been adopted by the UK's CPNI (part of which is now within NCSC). They comprise a detailed set of activities commensurate with fighting 'most pervasive and dangerous attacks'. For an SME in particular, The IASME Governance Standard provides the foundations for adopting these protective measures for high impact assets such as SCADA systems.

0.5.6. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS compliance is mandated by the payment card suppliers for businesses handling payment card data. Like Cyber Essentials (*see above*) it is essentially risk agnostic and says that if you handle payment card data, you must implement specific controls (as set out in that standard). Like DCPP (*see below*) and The IASME Governance Standard, there is an element of risk profiling regarding the type of processing and storage that goes on in a business.

0.5.7. Defence Cyber Protection Partnership (DCPP) Cyber Risk Profiles

The IASME Governance Standard and the DCPP Cyber Risk Profiles specification (Defence Standard 05-138) have the common ground of basing the expected attention to security on the likely threats that risk the business' confidentiality, integrity, and availability. Matching requirements from this standard are included as footnotes throughout.

0.6. Regulation

The IASME Governance Standard requires attention to the respective laws and regulations that are applicable to the target of evaluation in general and those applicable to information security and safety arising from information collection, storage, processing, and disposal in particular.

The IASME standard predicates itself on good practice and so avoids having to be reissued as legal systems change to deal with new technology or changes in its use.

0.6.1. General Data Protection Regulation (GDPR)

GDPR and the Network Information Security directive have certain nuances – such as the consent issues in GDPR or the breach reporting requirements of both GDPR and NIS. The IASME Governance Standard is about good security practice. Both legal instruments have at their core a requirement to follow good security practice. So, an entity which complies with The IASME Governance Standard passes straight along the line that these governmental requirements set out and have only to concern themselves with the nuances. The IASME Governance Standard prepares a company for this with its requirements to match legal and regulatory expectations and to have the requisite set of policies that defines for itself how it does it (*see Table 4: Explicit and implied information and cyber security policies*).

No one is immune to the consequences of a security incident but The IASME Governance Standard gives you the chance to show that you have used best endeavours.

The core of GDPR enshrines, in law, the basic principle of The IASME Governance Standard– know what you are protecting and understand its relative value to its subjects and so the impact of a security breach. This way, honest protective measures can be put in place and counterbalanced with routes to recovery after an incident.

0.6.2. The Network Information Security (NIS) Directive

To an extent with GDPR – and more explicitly with the definition of critical services of the NIS Directive – is how far down the supply chain the level of risk management will be scrutinised and how the risk profile of arms-length relationships will be considered in the scrutiny of information security. Interpretation of the directive will provide guidance here, but The IASME Governance Standard has always required organisations to consider their most important data and to consider how security requirements should be enforced in contracts with suppliers who handle such data, or the connectivity, or control dependent on it.

1. Scope

1.1. What is The IASME Governance Standard for?

The IASME Governance Standard is a formal information and cyber security methodology that is suitable for any organisation and SMEs in particular. It is sector agnostic and provides a working framework to assure information security against the background of contemporary threats.

The IASME Governance Standard is suitable for the smaller departments of central government and local authorities.

The IASME Governance Standard comprises clear guidance on good information security practices so a business knows where to start taking security measures.

1.2. What are the business drivers for applying The IASME Governance Standard?

The IASME Governance Standard enables businesses to:

- Identify risks to their information.
- Apply adequate barriers or controls to reduce the likelihood or impact of unwanted scenarios.
- Keep information risk at an acceptable level.
- Use a structured self-assessment for the completeness of what they are doing to protect information.
- Proactively verify that the security controls that you implement provide the intended level of information and cyber security.
- Be independently reviewed by an assessor who will be sympathetic to their size and business risk and verify the effectiveness of what they are doing.[2]
- Raise the awareness of information risks in businesses and the wider supply chain of which they may be part.
- Work to a standard of information security within a supply chain regardless of size.
- Give themselves, customers, and their supply chain, a level of assurance akin to ISO/IEC 27001 and similar standards.

[2] H.11 Proactively verify that the security controls are providing the intended level of security.

2. Glossary

Acronyms, and terms	Definitions
Business continuity	The activity of keeping your business operational with your regular expectations of quality and preserving the confidentiality, integrity, of availability of your information assets.
BYOD	Bring Your Own Device
CES	The Cyber Essentials Scheme (*See Cyber Essentials*)
Cloud	A service provided from one or more computers located in a place that is distant from the location in which the service is being used.
CPNI	Centre for the Protection of National Infrastructure. This is part of the Security Service which specialises in protecting essential services for the United Kingdom. See NCSC.
Cyber Essentials	Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. This is also the name of the basic level of certification that can be awarded under this scheme.
Cyber Essentials Plus	Cyber Essentials is a government-backed, industry-supported scheme to help organisations protect themselves against common cyber attacks. Cyber Essentials Plus is a higher level of assurance through the internal and external testing of the organisation's systems for certain vulnerabilities.
Cyber security	The assurance of confidentiality, integrity, and availability of information stored and processed on electronic devices that are usually interconnected.
Data Breach	An incident that leads to a compromise of the confidentiality, integrity, or availability of information. This may be accidental or deliberate.
Disaster recovery	The process of returning to a state of business-as-usual after a significant incident. This may mean a change in working practice as a result of the incident to meet expectations of quality and preserving the confidentiality, integrity, of availability of your information assets.
DMZ	Demilitarised zone. An area between trusted resources and untrusted activities.
HVAC	Heating, ventilation, air conditioning
IASME	The information and cyber security programme for SMEs documented in The IASME Governance Standard.
IASME Bronze	An award showing significant achievement in cyber and information security.

Acronyms, and terms	Definitions
IASME Gold	An award showing that an organisation's achievement in cyber and information security is in line with industry expectations.
IASME Governance	The assurance process for implementing controls to management security in an auditable framework.
IASME Silver	An award showing that an organisation's achievement in cyber and information security will be in line with industry expectations when the external recommendations of the audit body are fully implemented.
ICS	Industrial control systems. *See SCADA.*
Information asset	Processed and unprocessed data and the equipment that is used to store, process, or transmit it, that has value and impact to a business, its stakeholders, its supply chain, or other interested parties. This includes – but not restricted to – your intellectual property.
Information risk	The magnitude, and likelihood, of a loss of information's confidentiality, integrity, and availability.
Information security	A state of confidentiality, integrity, and availability commensurate with the value of the information under scrutiny.
Micro enterprise or organisation	Comprises less than 10 staff and a turnover or balance sheet of ≤ €2 m respectively. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003)
Medium-sized organisation	Comprises between 51 and 250 staff, a turnover of ≤ €50m or a balance sheet total of ≤ €43m. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003.)
NCSC	The National Cyber Security Centre is an arm of GCHQ. NCSC is the national technical authority for information assurance within the UK, providing the definitive voice on the technical aspects of information security across the most critical organisations in the UK, the wider public sector, industry, and SMEs. It was formed from CESG (Communications-Electronics Security Group), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure (CPNI).
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information – information that is governed by respective data protection laws.
Risk	The magnitude, and likelihood of a particular threat event occurring.
Security	A state of grace wherein the assets under scrutiny are adequately protected from the realisation of risks to them.
Security breach	*See security incident.*

Acronyms, and terms	Definitions
Security event	Something that happens contrary to the accepted security policy. An event – or series of events – may lead to a security incident
Security incident	Something that happens that compromises information's confidentiality, integrity, or availability.
Small enterprise or organisation	Comprises between 11 and 49 staff, and a turnover or balance sheet of ≤ €10 m respectively. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003.)
SCADA	Supervisory control and data acquisition. These are mechanisms for collecting and processing data to control processes typically found in industrial control systems (ICS).
SME	Comprises less than 250 staff and a turnover or balance sheet of ≤ €50m or €43m respectively. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003.)
VPN	Virtual Private Network

3. Normative references

- Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks, BIS/14/696
- Ministry of Defence, Defence Standard 05-138, Cyber Security for Defence Suppliers, Issue 1 (21 August 2015)
- IASME Risk Profile Questionnaire and Analysis.

4. How The IASME Governance Standard works

4.1. Understanding your risk profile – and defending it

The IASME Governance Standard is a route map to maintaining a state of information security so that you can focus on your core business objectives. It is these objectives that govern your risk profile. The IASME Governance Standard is a structured catalogue of good practices to increase the likelihood of the successful achievement of your objectives. This is important to keep information security in perspective so that you neither smother your activities in restrictive practices nor leave yourself vulnerable to avoidable losses.

Your risk profile will depend entirely on your objectives – and the threats to them – and the information that you need to achieve them. One person with highly sensitive information assets may have a higher risk profile than a large company handling information with a higher tolerance for its confidentiality, integrity, and availability. You will need to consider any number of threat 'actors'[3] and paths which will vary from all-but invisible technical skulduggery to social engineering. Do they have the capability, the intent, and the opportunity to cause harm? And if they did, would the impact matter? Might you be the conduit to your customers who are the 'high value' targets for the attackers?

Regardless of its risk profile, every candidate business seeking certification to The IASME Governance Standard must be capable of implementing Cyber Essentials and should show that by at least completing the Cyber Essentials self-assessment and having that moderated by an accredited certification body.

The IASME Governance Standard uses a framework to determine your risk profile which considers:

- How are information systems used?
- How outsourced (including 'cloud') facilities are used?
- Whether you and the people you work with use their own equipment for business (BYOD).
- How remote and mobile systems are used?
- Awareness and attitude to the threat environment.
- Estimated value of the business' information assets.
- Estimated value of the business' information technology.

Note: *The IASME Governance Standard strives to stay agnostic of technology strategy so it makes no assumptions about what might be used to assure the confidentiality, integrity, and availability of information. Whatever is used – such as mobile devices, 'BYOD' removable media, cloud or other 'as a service' opportunities – The IASME Governance Standard is concerned with its application to information safety,*

The answers to these questions determine which of the three information risk profiles match your business:

[3] Including – but not restricted to – hacktivists, financial criminals, terrorists, industrial spies, disgruntled insiders, disgruntled former staff, well-intentioned insiders, information security professionals, and script kiddies.

Table 1: The IASME Governance Standard business risk profiles	
Low	The footprint of the organisation's business is small enough to present a small attack surface. The compromise of confidentiality, integrity, and availability would have low impact results because of the relatively low value information assets. Threat agents may not be greatly motivated, resourced, or persistent.
Intermediate	The footprint of the organisation's business has a significant number of associational paths but not enough to lead inevitably to high-impact compromise of information (at least in part because the relative value of the information is not high). Threat agents are likely to be tailored and targeted to specific information assets to loss of confidentiality, integrity, and availability.
Complex	The footprint of the organisation's business is a sufficiently sized surface as to risk vulnerabilities to the information handled with high impact results if compromised. The information held by the organisation will have particular sensitivity for it or its customers. Threat agents are likely to be well resourced and sufficiently motivated to make persistent efforts to exfiltrate data and reduce or suspend operational integrity.

Businesses that have successfully completed their first assessment are re-assessed at least annually, or when their risk profile changes significantly. It is commendable to not only attend to security with a policy of continuous improvement but also to take opportunities to innovate in the methods used for information assurance.

4.2. Implementation, orchestration, and adjustment

The risk profile of your business will guide the decisions made about the information and cyber security controls required to keep the business safe and resilient. These controls are the practical measures that you put in place to protect your business information. Each control addresses one or more aspects of information security, such as:

- Asset identification and classification
- Risk impact assessment and protection
- Detection and deterrence
- Response and recovery

The IASME Governance Standard encourages these controls to be built into business processes so that security operates in harmony with the business and is indistinguishable from it as much as possible.

Controls are selected based on the risk to your business information and not the size of your business. Adjustments can be made at any time as the risk changes.

4.3. Showing customers, suppliers…and yourself

The IASME Governance Standard is about assessing risk to your business information and keeping that risk at an acceptable level to you, your customers, and supply chain. The IASME Governance Standard assesses and measures your security controls. The process is documented, objective, and repeatable and scalable to what you do. The IASME Governance Standard is about continuous assessment, with an initial cycle leading to your first certification, and continuing with intermediate assessments annually and comprehensive re-assessment after three years.

The IASME Governance Standard was designed for SMEs and recognises that SMEs thrive on their agility. Therefore The IASME Governance Standard expects only a fitting amount of guiding documentation and evidence of good information and cyber security practices to give assurance. The

IASME Governance Standard is designed to show a balance of proactive measures and the capability to be resilient in the face of accidental or deliberate information and cyber security incidents.

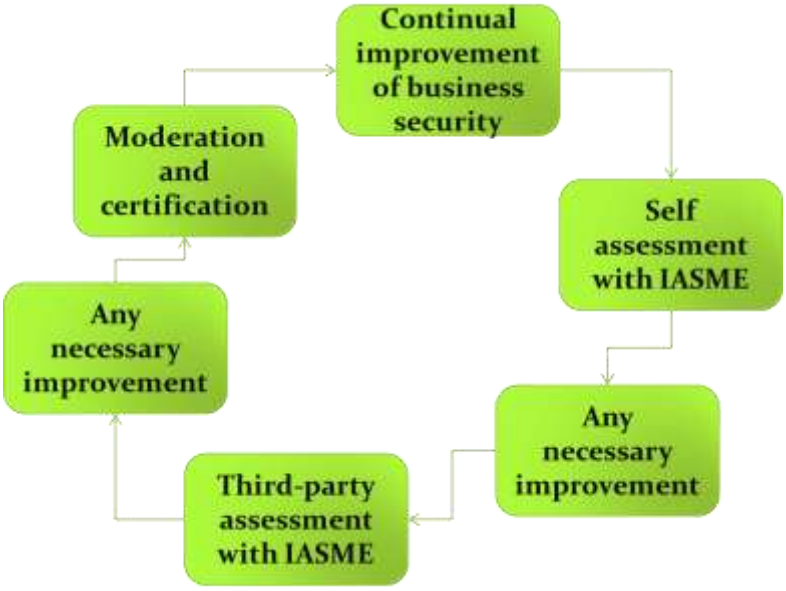

Figure 1: Round-tripping with The IASME Governance Standard's initial cycle

The IASME Governance Standard wants business documentation that is right-sized for you and that is useful for maintaining a visible commitment to managing information security well. You will use the documentation to show commitment at the highest level, clear accountability, and responsibility, as well as it helping to benchmark your certification.

4.4. Who watches the watchmen?

The integrity of the IASME Governance Standard is scrutinised by an advisory board and updated as a result of changes to the threat landscape. Companies that engage with the assessment process are assured of its quality throughout the assessment process that supports the standard. The IASME Consortium engages assessors, who are experienced security professionals with auditing skills, and use their experience to make a decision about the suitability of the security measures of a business. This is part of the ongoing risk-profiling that, although done at the beginning of the process, only really comes together and ends with the assessor's recommendation to the moderator.

The moderators act as custodians of consistency and quality for The IASME Governance Standard assessment process. Assessors act as a proxy for the moderators and, as part of the audit process, visit the relevant sites of the organisation. Even a home office has its vulnerabilities. Part of the added value of The IASME Governance Standard are the inspirational recommendations for improvement that are picked up in attendance.

The challenge for The IASME Governance Standard (or any standard) is to provide a level playing field in its assessment of a business to provide a comparable benchmark. That's why we insist on the visit. The moderators are there to make informed judgements and protect The IASME Governance Standard programme from being compromised.

4.5. Businesses in more than one location

If a business is located in more than one location, then the assessor will consider the sampling that must take place. A key deciding factor is the likelihood that one site mirrors another.

If a site is not visited then it:

- Must be engaged in the same type of business as one that has been, and apply the same tools, techniques, and policies. If it has its own way of doing things then it remains out of scope until audited.
- Must not be engaged in any activities that are out of scope which could compromise the information security model established for the in-scope activities. For example, sharing space or work with other businesses may have an effect.
- Must account for the distribution in the risk profiling and be assessed accordingly
- Must be subject to internal checks that will be available for inspection at one of the audited site(s).

Franchises, agents, and resellers need their own scope and certification.

5. Investing in cyber and information security with The IASME Governance Standard

Investment in cyber security requires judging risks and taking positive actions to control them.

It is split into four main categories:

- **Asset identification** (of what needs to be secure – which may include hardware and software, personal records, business data from diaries to financial plans and report, intellectual property such as designs and know-how, or control data).
- **Risk impact assessment and protection** (to make it as secure as possible within the risk profile).
- **Detection** (of defects in business processes, accidental or deliberate security incidents) **and deterrence** (of attacks).
- **Response and recovery** from incidents (in tune with the level of resilience needed by the business).

There is no complete distinction between the last two categories. Many protective measures have elements of detection and may assist recovery; some recovery measures may lead to better protection and so on. In the table below, they are organised by their main impact on maintaining a state of information and cyber security.

Table 2: The IASME Governance Standard's business information security overview

Cycle	Security aspect	What you must achieve…
Identify and classify	Planning	What is the appropriate state of security for the stakeholders in your business? Build right-sized security into all your business activities. Consider the security impact of change on your staff, customers and other stakeholders, your working practices, hardware, and software.
	Organisation	Who has the rights to make decisions that affect your information security? Who is responsible for making information safe and who is accountable when incidents happen? Who provides the leadership if there's a dispute? What is the escalation path through that leadership? Segregate work – and access to the resources needed – to match these responsibilities. Manage the information resources which you own or have a duty of care to, and those affected by relations with partners or your supply chain. Manage those relationships. Define the responsibility of directors and their direct involvement of setting levels of risk acceptance.
	Assets	Know what you need to protect. What information have you got to lose? Understand the value of your information assets and your physical assets; acquire and dispose of them securely. Have a good picture of how the assets in your business estate both fit together yet remain shared amongst those who have the privilege to use them acceptably. Be clear about how to handle information securely.

Table 2: The IASME Governance Standard's business information security overview		
Cycle	**Security aspect**	**What you must achieve…**
	Assessing risks	Consider information risk in the business context and determine your business' risk appetite so that you can manage that risk accordingly. Extend that risk management to customers, partners, and suppliers. Maintain vigilant oversight of your risk profile. Keep abreast of emerging threats and countermeasures so that your risk assessment is always contemporary. Consider insurance to manage the level of residual risk you face after your control measures are in place and an incident occurs.
	Legal and regulatory landscape	Establish legal and regulatory requirements, management direction and communications. With which legislation do you need to comply? Know what is required, monitor compliance, and do what needs to be done to counter deviations. Establish the working practices to enable the principle of information-related legislation such as requirements to retain or delete data, or release it to its owners or the authorities.
	People	Profile your people and educate your staff, colleagues, contractors, partners, and co-workers in the risks and responsibilities associated with the information systems they use. Know whom you're hiring. Remind them of the value of the data – include the written and spoken word. Make the culture of information security business as usual. Deter misuse of information assets. If the worst comes to the worst, make sure that you've a path for redress such as disciplinary action. Your direct colleagues – and the people in your supply chain – are almost certainly going to form part of your front line defences, reporting and recovery from incident. Directly – or indirectly – education about appropriate behaviours with information must be embedded.
Protect	Policy realisation	Create a comprehensive and right-sized set of information and cyber security policies that keep the decisions about how you manage security at your fingertips. Don't expect everyone to know every policy, but do distribute them as needed. Support the implementation of these policies and check that they are not only being implemented but that they still satisfy your risk appetite pragmatically.
	Physical and environmental protection	Protect your information assets from physical threats and environmental harm. Lock away confidential information that isn't in use, keep it out of sight from those unauthorised to see it when it is.

Table 2: The IASME Governance Standard's business information security overview		
Cycle	**Security aspect**	**What you must achieve…**
	Secure business operations	Nurture the way that business is done so that it is done securely. Manage and monitor your information systems effectively, keeping them up to date with contemporary software patches and upgrades. [4] Encrypt sensitive information carefully to keep information confidential for those who need it. Make sure that encryption is set up correctly – that it is not vulnerable through some other work around and that it can only be decrypted in the right place at the right time so that it offers the expected level of security and accessibility to legitimate users.
	Access control	Control whom, and what, can access your information. Prefer a 'need to know' way of working.
Detect and Deter	Malware and technical intrusion	Install reliable anti-malware software on all devices where this prevention tool is available. Keep your anti-malware software up to date. Pay attention to its warnings and reports and take actions according to the risks it informs you about. Deploy other technical tools including intrusion detection and prevention methods.
	Monitoring, review, and change	Make sure that the policies that you set to protect information and recover from a security incident are effective and remain supportive of your business objectives. Know which business systems and processes you need to track and monitor for acceptable activity – according the information safety policies that you have set - and how you will identify the unacceptable. Keep an eye on who is trying to access your information and where they are trying to access it from. Be prepared and ready to act on the intelligence your monitoring provides. Keep information which is forensically sound from a legal perspective.

[4] M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.

Table 2: The IASME Governance Standard's business information security overview		
Cycle	**Security aspect**	**What you must achieve…**
Respond and Recover	Backup and restore	Back up as frequently as you can stand versus the amount of rework you can afford to do. Maintain at least one of the back-ups off-site and at some distance from the working version of the data. Ensure backup copies are kept appropriately secured for the data they contain.
	Incident management	Ensure breaches of confidentiality, integrity, or availability of your data are detected and dealt with. Make them easy to report to a responsible entity without blame. Set out a policy with clear responsibilities for reporting incidents as required by law and decency to customers and the respective external authorities. Learn the lessons.[5]
	Business continuity, disaster recovery, and resilience	Be ready to keep working through, and recover from, the effects of deliberate attack, accidental damage, and natural disasters. Make sure that you can transform, renew, and recover in timely response from a partial or total loss of information assets. Be true to the Cyber Security Essentials by making sure that the security requirements that they define are 'business as usual' across your information systems.

[5] L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.

6. Identify

You can't protect what you don't know that you have. If you don't know what you're protecting – and how information systems should behave in different situations – you are likely to miss that you are being attacked or that information has already been lost or damaged. Information or data may have been altered inappropriately or malicious programs loaded without detection. You may only become aware of the value of your assets and the cost to your business when you try to recover from an attack or insider carelessness.

Note: This has much in common with 8.2 Monitoring.

6.1. Planning

Planning	What is the appropriate state of security for the stakeholders in your business? Build right-sized security into all your business activities. Consider the security impact of change on your staff, customers, and other stakeholders, your working practices, hardware, and software.[6]

6.1.1. Guidance

Planning is the action of taking decisions in advance. As a result of information security planning you will get to understand what you can define in day-to-day activities, special 'project' activities which may be bound to a particular time, and activities that will only need to take place if and when trigger events take place.

6.1.2. Requirements

What needs to be done to have assurance in the security of your information?

Make provisions for information and cyber security as part of your business planning so that it doesn't become a surprise – possibly a very expensive one. This is certainly to be considered during procurement, contracting, supply, and organising yourself, partners, and dealing with other interested parties. Make achievable, time-bound plans to implement the information and cyber security measures that you need.

6.1.3. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

What is the risk profile of the business under scrutiny?

What is the appropriate state of security for the stakeholders in the business under scrutiny?

How does the business build right-sized security into all of its business activities?

How does the business consider the security impact of change on its staff, customers and other stakeholders, its working practices, hardware and software?

How does the business design, implement, and maintain its information systems – both electronic networks and paper systems?

With the identification of assets and risk assessment, has the business identified its risk appetite?

[6] H.06 Define and implement a policy to control installations of and changes to software on any systems on the network.

6.2. Organisation[7]

Organisation	Who has the rights to make decisions that affect your information security? Who is responsible for making information safe and who is accountable when incidents happen? Who provides the leadership if there's a dispute? What is the escalation path through that leadership? Segregate work[8] – and access to the resources needed – to match these responsibilities. Manage the information resources which you own or have a duty of care to, and those affected by relations with partners or your supply chain.[9] Manage those relationships. . Define the responsibility of directors and their direct involvement of setting levels of risk acceptance.

6.2.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Essential steps in protecting a business involve:

- Ensuring commitment and funding for information and cyber security activities from the top.
- Appointing a well-informed leader with authority to coordinate and act on information and cyber security activities. It is preferable to make that commitment tangible by appointing a director to the role[10].
- Assign the ownership of risks and their treatment to those who have the best understanding of outcomes and potential impact.
- Forming a group – or a network of people – from across the organisation to coordinate and implement information and cyber security activities.[11]
  - Manage the cost of the group by assigning responsibilities to existing posts.
  - Make responsibilities clear. If you have a system of staff appraisal, include the information and cyber security work within objectives.
- Review your information and cyber security activities with your directors so that they can exercise their responsibility for assuring the appropriate governance of risk.
- Maintain knowledge of emerging threats and countermeasures using expert advice.

6.2.2. Key questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Who has the rights to make decisions that affect the business' information security?
Who is responsible for making information secure and who is accountable when incidents happen?
Who provides the leadership if there's a dispute?
What is the escalation path through that leadership?
How does the business segregate work to match these responsibilities?

[7] L.01 Define and assign information security relevant roles and responsibilities.
[8] L.07 Define and implement a policy to control access to information and information processing facilities.
[9] L.02 Define and implement a policy that addresses information security risks within supplier relationships.
[10] Strive to avoid assigning too much responsibility for information and cyber security activities to the person responsible for IT in your business. They may well be responsible to implementing security technologies but it's not fair to expect them to have the understanding of all the business processes that the technology supports.
[11] Micro organisations can do this informally; larger organisations require a more formal structure to preserve the communication channels.

How does the business manage the information resources which it owns or has a duty of care to and those affected by relations with partners or its supply chain? How does the business manage those relationships?

6.3. Assets

Assets	Know what you need to protect. What information have you got to lose? Understand the value of your information assets and your physical assets; acquire and dispose of them securely. Have a good picture of how the assets in your business estate both fit together yet remain shared amongst those who have the privilege to use them acceptably. Be clear about how to handle information securely.

6.3.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Risk assessment and recovery from information and cyber security incidents – a data breach for example – both rely on having a good understanding of your key information assets. Only then can you appreciate your attack surface and what you've got to lose.

Are your assets on a local computer, 'cloud' storage, on social media, a member of staff's computer, or in a filing cabinet? These are just examples. Know the medium and the location. Know when they are moved around and be sure that they are suitably cleared when you dispose of them.

With the proliferation of so much recordable media – including memory cards, mobile telephones, 'USB sticks', and tablets, and the distribution of intellectual property across private and public 'cloud' computing resources – this is a task requiring meticulous attention.[12]

The most severe information and cyber security incidents may be where they impact assets which are critical to business operations. You need to understand the relative values of your information assets so that you can spend your security budget effectively and – in the case of an incident – know the order of priority in which to recover your assets.

You need to know the relative value and impact of your information assets to your business so that you can apply adequate protection for them through their life cycle from creation or acquisition through to safe disposal (which may include erasure, shredding, or other methods of destruction).

6.3.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business know what it needs to protect? What information has the business got to lose? How does the business understand the value of its information assets; acquire and dispose of them securely? How does the business have a good picture of how the assets in its business estate fit together? Is the business clear about how to handle information securely?

[12] L.09 Define and implement a policy to control the exchanging of information via removable media.

6.4. Assessing risks

Assessing risks	Consider information risk in the business context and determine your business' risk appetite so that you can manage that risk accordingly. Extend that risk management to customers, partners, and suppliers. Maintain vigilant oversight of your risk profile. Keep abreast of emerging threats and countermeasures so that your risk assessment is always contemporary.

6.4.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Maintain vigilant oversight of your risk profile by maintaining a contemporary risk assessment:[13]

- Keep up to date with the risks to your business objectives and understand how those risks can affect the information you need to deliver those objectives effectively.
- Consider information risk in the business context and determine your business' risk appetite so that you can manage that risk accordingly.
- Extend that risk assessment to customers, partners and suppliers.[14]
- Separate the risk assessment from the risk treatment so that you will be able to focus on the risks and potential impact, and then take a balanced suite of counter measures to protect your information.
- Be aware of other business risks being addressed at director level such as:
  - Environmental risk
  - Legal and regulatory risk
  - Market risk
  - Operational risk
  - People risk
- Integrate your information risk assessment with the risk management of other business risks that will be being addressed at director level.
- Keep abreast of emerging threats – and their risk to your business – and the constant, background risks which remain steadfast.
- Use your risk assessment to guide the practicality of how you may use – if at all – information resources including (but not restricted to):
  - BYOD
  - Portable storage media
  - Public, private, and hybrid cloud computing resources.
  - Social media

An assessment to The IASME Governance Standard is a method for assessing the thoroughness of your risk assessment and making sure that it is fit for your business. A risk assessment that is compatible with The IASME Governance Standard manifests in a comprehensive view of risk (including people issues) and a balanced set of relevant policies to make information and cyber security business as usual.

[13] M.03 Define and implement a policy that provides for repeatable information security risk assessments.
[14] L.02 Define and implement a policy that addresses information security risks within supplier relationships.

6.4.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business maintain vigilant oversight of its risk profile?
How does the business consider information risk in the business context and determine your business' risk appetite so that it can manage that risk accordingly?
How does the business extend that risk management to customers, partners and suppliers?
How does the business keep abreast of emerging threats and countermeasures so that its risk assessment is always contemporary?

6.5. Legal and regulatory landscape

Legal and regulatory landscape	Establish legal and regulatory requirements, management direction and communications. With which legislation do you need to comply? Know what is required, monitor compliance, and do what needs to be done to counter deviations. Establish the working practices to enable the principle of information-related legislation such as requirements to retain or delete data, or release it to its owners or the authorities.

6.5.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Every business has certain legally enforceable obligations associated with company registration, accounting, managing customers and other business processes. Make sure that you are aware of your obligations and have the support in your business processes for fulfilling them.

Make a clear list[15]. IASME expects you to include areas special to your business – for example PCI DSS if you handle credit card data or the General Data Protection Regulations if you hold personally identifiable information – but other legal and regulatory items for consideration and implementation may include (but not be restricted to):

Table 3 A sample of information-related legislation which may be relevant to respective businesses

Civil Contingencies Act 2004	Communications Act 2003	Companies (Audit, Investigations and Community Enterprise) Act 2004
Companies (Trading Disclosures) Regulations 2008	Companies Act 2006	Computer Misuse Act 1990
Consumer Credit Act 1974 and 2006	Consumer Protection (Distance Selling) Regulations 2000	Consumer Protection from Unfair Trading Regulations 2008
Copyright (Computer Programs) Regulations 1992	Copyright and Rights in Databases Regulations 1997	Copyright, Designs and Patents Act 1988
Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002	Data Protection Act 1998	Data Retention (EC Directive) Regulations 2009

[15] This may be appropriate in your documented security policy.

Table 3 A sample of information-related legislation which may be relevant to respective businesses		
Defamation Act 2006	Digital Economy Act 2010	Electronic Commerce (EC Directive) Regulations 2002
Electronic Communications Act 2000	Electronic Signatures Regulations 2002	Equality Act 2010
General Data Protection Regulation (EU) 2016/679	Health and Safety (Display Equipment) Regulations 1992	Health and Safety at Work etc. Act 1974
Human Rights Act 1998	Malicious Communications Act 1988	Mobile Telephone (Re-Programming) Act 2002
Patents Act 1977 and 2004	Privacy and Electronic Communications (EC Directive) Regulations 2003 and 2011	Protection from Harassment Act 1977
Regulation of Investigatory Powers Act 2000	Sale and Supply of Goods Act 1994	Sale and Supply of Goods to Consumers Regulations 2002
Sale of Goods Act 1979	Supply of Goods and Services Act 1982	Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000
Trade Marks Act 1994	Waste Electrical and Electronic Equipment Regulations 2006	

Identify your business' legal, statutory, regulatory and contractual obligations and security requirements for the use of information, intellectual property rights and legal use of software and other products

Ensure that your business records are protected from loss, destruction or falsification in accordance with legal and other obligations. This may include – but not be restricted to – internal and external audit information. You may need to draw up a retention schedule to keep track of these.

6.5.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Has the business established the legal and regulatory requirements of its management direction and communications? How does the business know what is required and monitor compliance?

6.6. People

People	Profile your people and educate your staff, colleagues, contractors, partners, and co-workers in the risks and responsibilities associated with the information systems they use. Know whom you're hiring[16]. Remind them of the value of the data – include the written and spoken word. Make the culture of information security business as usual. Deter misuse of information assets. If the worst comes to the worst, make sure that you've a path for redress such as disciplinary action[17]. Your direct colleagues – and the people in your supply chain – are almost certainly going to form part of your front line defences, reporting and recovery from incidents. Directly – or indirectly – education about appropriate behaviours with information must be embedded.

6.6.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

People can be both the front line and the last line of protection for your information. They need to be trained to deliver the work you expect from them and to appreciate the risks to themselves and the business that are associated with the information systems to which they will have access.

Look at the roles across your business and make sure that staff receive the appropriate instruction and training. This may range from training courses – in person or on-line – literature ranging from on-screen reminders to 'how tos' and good practice guides. Make this part of induction and give sensibly spaced reminders – at least annually. Be aware of new threats and increased risks. Keep abreast of current incidents and use examples to reinforce the risks and the actions to be taken to avoid them occurring in your business.

Clearly assign specific roles – and the respective responsibilities – relating to information governance to named individuals. Examples include the titular Data Protection Officer and (in health care) the Caldicott Guardian.

Ensure that everyone who has access to the data on your information systems:[18] [19]

- Are suitable[20] from a security viewpoint before and during employment. References and screening may be necessary for some roles.[21]
- Are aware of, and adequately trained in, their security responsibilities. Include reporting of incidents – without blame – and
- Are only given access to what they need for their work.
- Are only granted the privileges to read, change, or delete information as appropriate to their roles and responsibilities.

[16] L.13 Define and implement a policy for verifying an individual's credentials prior to employment.
[17] L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.
[18] L.04 Define employee (including contractor) responsibilities for information security.
L.05 Define and implement a policy to provide employees and contractors with information security training.
M.02 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.
[19] L.07 Define and implement a policy to control access to information and information processing facilities.
M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.
[20] L.13 Define and implement a policy for verifying an individual's credentials prior to employment.
[21] M.14 Define and implement a policy for applying security vetting checks to employees.

- Are aware of current threats, including those arising from manipulation of social media, infected websites, use of personal devices and others,
- Are suitably debriefed and privileges removed on termination of employment.[22]
- Are contractually obligated:
  - To respect and implement your security policies as related to the work that they do.
  - Leave intellectual property ownership with the business unless some other explicit arrangement exists.

This includes – but is not restricted to – permanent and temporary staff, whether full or part time, on contract, paid or unpaid.

Establish your rules for the acceptable use of your company assets – be explicit as to whether any personal use is allowed. These rules will include what can or can't be said about your business and the people involved in it in e-mail and on social media.

Have a structured programme of checks in place to make sure that privileges are still relevant and have not been abused.

On termination of employment, access privileges should be immediately withdrawn and the employee de-briefed on their post-employment confidentiality responsibilities.

6.6.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business profile its people and educate all its staff, colleagues, contractors, partners, and co-workers in the risks associated with their responsibilities and the computing power of the devices available?
How does the business know whom it's hiring?
How does the business remind them of the value of the data – include the written and spoken word wherever they may manifest?
How does the business make the culture of information security business as usual?
If the worst comes to the worst, is there a clear path for redress? How is it used?

[22] M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.

7. Protect

7.1. Policy realisation[23]

Policy realisation	Create a comprehensive and right-sized set of information and cyber security policies that keep the decisions about how you manage security at your fingertips. Don't expect everyone to know every policy but do distribute them as needed. Support the implementation of these policies and check that they are not only being implemented but that they still satisfy your risk appetite pragmatically.

7.1.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Policies are all the decisions you make about how you want your business to run and the protective and recovery methods that you're prepared to invest in information and cyber security. They may manifest as a setting on a laptop, permission to use a particular brand of tablet computer, the size of strips in a paper shredder, whether or not there are bars on a window or an additional padlock on a filing cabinet. They are not random decisions; they are the thoughtful result of your risk assessment. Policies set out:

- How you will identify your business's security needs.
- How you will protect your business according to those needs.
- How you will detect security problems and deal with them.
- How you will respond to security incidents and recover from potential business interruptions.

Get the right balance of consistent good practice through habit with the need to write down and refer to the policies that define how you approach and implement those protective measures. Write policies down wherever practical. Such documentation is a method of communicating and a way of recording a benchmark for when you need to check whether you have done your best either before, during, or after the inevitable information security incident.

You will need an overall security policy setting out your commitment to information and cyber security and how you go about it. Whether it is *all* written down or not, the people responsible for implementing the policy should be able know – and be able to explain to others:

- The purpose of the policy – why does the business need it and what's the risk of not having it?
- Scope – what does the policy apply to, and what – if anything – is excluded?
- What the policy actually is – a clear, pithy, and imperative description of the controls which contribute to the security of information in your business.
- How it's monitored to make sure that it's implemented correctly and is working for the business.
- What happens if the policy is breached? Security incidents are inevitable. Be prepared with a business continuity element in every policy.
- What to do to enforce it – technology, awareness, or a mix of both. Don't just rely on the last resort of disciplinary action.
- When will the policy be reviewed for its continued fit to the business – perhaps after a fixed interval or an event or incident which may affect the policy?

The table below shows the reality of the information security challenge in contemporary business. Whether you need to define and implement an information security policy from this table is governed by your risk profile and the first question in the bullet points above: why does the business need it and what's the risk of not having it?

[23] L.10 Define and implement an information security policy, related processes and procedures.

This is a substantial list and even if you do find that you need to document all your policies you don't usually need to have one document per policy. Items may standalone or be usefully combined for easy reference. 'BYOD' may be such a policy. You will usually find that many of your policy decisions are documented in various practical places such as business plans, a contract with a supplier,[24] or a staff contract. Ask yourself, can I convincingly show someone that this is my regular practice, or remember precisely what we decided was the safest practice for the business?

7.1.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Has the business created a comprehensive and right-sized set of policies that keep the decisions about how it manages security at its fingertips?

How does the business distribute policies on a need-to-know basis?

How does the business support the implementation of these policies and check that they are not only being implemented but that they still satisfy its risk appetite pragmatically?

Table 4: Explicit and implied information and cyber security policies

Type	Policy	Areas covered
Policies about Asset Management	Intellectual property	How intellectual property should be managed and how to comply with relevant legislation
	Classification of information	How information should be prioritised and marked in terms of risk to the business[25]
	Ownership and responsibilities	Who owns different information and physical assets
	Physical security	Keeping assets safe from physical loss or damage
	Clear desk policy	Ensuring that office environment is regulated and controlled
	Acquisition of hardware, software and services	How such items are evaluated, directed, monitored, accepted and licensed/registered[26]
	Handling and disposal of computer equipment and information assets	Details how to transport and securely dispose of computer equipment, how to handle information assets, and how to securely destroy information[27]
	Media handling	How to store and handle media containing information
	Data sharing and exchange	Regulate which information can be shared and how

[24] L.02 Define and implement a policy that addresses information security risks within supplier relationships.
[25] L.06 Define and implement a policy for ensuring that sensitive information is clearly identified.
[26] M.11 Define and implement a policy to control the use of authorised software.
[27] M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.

Table 4: Explicit and implied information and cyber security policies		
Type	**Policy**	**Areas covered**
Policies about people	Governance	Detailing management commitment to policies, governance and organisation of policy, authority for enforcing policies and management review. Expectations of the level of contractual detail in the assurance of complementary information security policies with second and third parties in your supply chain need to be set.
	Acceptable use of computers	Covering topics such as personal use, BYOD and social media
	Data and account access	For permanent staff, temporary staff and contractors detailing new starter data access, data access for leavers, modifications and access privilege review and management[28] [29]
	Data protection	How the business will comply with Data Protection Act
	Remote working	Covering how staff should act when working remotely/teleworking [30]
	Third-party services	Detailing how agreements are to be set with third parties
	Training and awareness	How training commensurate with roles and responsibilities is provided and end-user guidance to security issues
	Risk management	How risk is assessed, acceptable levels, treatment[31], business continuity and resilience including disaster recovery
	Passwords and key management	Management of cryptographic keys and passwords that provide access to information[32]
	Remote access (such as VPN)	Criteria for allowing remote access[33]
	Change Management	New Installations and Change Management Procedures including data quality and integrity, backup and storage
	Incident and event management	How incidents are to be managed including points of escalation and incident logging
	E-commerce and credit card handling	Compliance with e-commerce legislation and credit card standards such as PCI
	Assessment	Auditing of the company including internal and external

[28] L.07 Define and implement a policy to control access to information and information processing facilities.
[29] L.12 Define and implement a policy to manage the access rights of user accounts.
[30] M.10 Define and implement a policy to control remote access to networks and systems.
[31] Prevention, reduction, outsource/transfer of treatment, acceptance
[32] M.13 Define and implement a policy to maintain the confidentiality of passwords.
[33] M.10 Define and implement a policy to control remote access to networks and systems.

Table 4: Explicit and implied information and cyber security policies		
Type	**Policy**	**Areas covered**
	Legal and regulatory compliance	How the company will comply with relevant legislation and regulations
	Social media	Who and what may be posted on social media, forums, and websites. Consider what may cause offence or attract unwanted attention (religion, politics, libel, customer details, journeys, locations) especially where several pieces of information may come together to disclose information. Make clear the responsibilities of staff in their personal use and the disciplinary or legal consequences. Record this in contracts.
Policies about technology	Configuration management	How to keep configuration of systems secure including vulnerability management/ patching[34]
	Architecture	How systems are managed and deployed including data centres, cloud both private and public
	Internet Connection	Topics relating to internet access, permitted protocols, content filtering, firewall, internet facing services, DMZ, routers and switches
	Communications	How telecoms are managed such as VOIP, wireless communication, mobile phones
	Internal server security	What is the appropriate set up for internal servers so that they support the work done with adequate flexibility?
	Mobile devices	Specific requirements for portable devices such as laptop computers, tablets, and portable storage[35].
	Protection against malicious software	How the company protects against virus, Trojan, worm, adware and spyware
	Testing	How the Demonstration/Testing/ Sandbox Facility is to be setup and configured
	Monitoring	Topics such as Intrusion detection/prevention, non-repudiation and log management[36]
	Encryption	Management of cryptographic communications

Note: Not every business – and certainly not all staff within a business – will find that every policy in the table is applicable to them.

[34] L.11 Record and maintain the scope and configuration of the information technology estate.
[35] Although not specific to mobile devices, questions of ownership, malware protection, remote wiping and acceptable use will need to be considered.
[36] M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.

7.2. Physical and environmental protection

Physical and environmental protection	Protect your information assets from physical threats and environmental harm. Lock away confidential information that isn't in use, keep it out of sight from those unauthorised to see it when it is.

7.2.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Protection of your information and cyber security extends to the physical protection of information assets, to prevent theft, loss, or damage and their impact on the availability of your business information and associated resources. This may only require the basic measures expected by your insurance policy which may include, but not be restricted to, door (5-lever mortise) and window locks, window bars, or video surveillance – all appropriate to the places that your business operates from.

Special attention is likely to be required as you take equipment or papers into public places – or work from home, or work away overnight (in hotels for example) and so on. Your risk assessment should support your decision as to the suitability – from a security perspective – of where you work. Beware of people 'looking over your shoulder' in these circumstances when working in unprotected places. Be careful where you put your equipment in vulnerable places like the queue in a restaurant or a luggage rack.

In some cases, physical protection – like other security requirements – may be dictated by your customers[37] or just the practical compliance with legal requirements such as data protection (which you must apply to the records you keep about your staff). The measures you take – such as smoke and fire detection and suppression, intruder alarms (all installed and maintained by a regulated firm) – will be traceable to your risk assessment. This will similarly cover common sense actions such as placing equipment off the ground to avoid water damage (in the event of flood, leak or burst pipe). Policy decisions will need to cover portable devices such as what to do with them while travelling. For example, if equipment is left unattended in a car it must be locked away out of sight. Policies must cope with potential conflicts like rules about checking equipment into aircraft holds.

If your equipment requires any particular working conditions – such as heating, ventilation, or air conditioning (HVAC) – be careful to maintain these within the guidelines set out by the respective manufacturers. Your risk assessment will tell you what monitoring and redundancy are expected from these measures.

7.2.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Does the business protect its information assets from the exposure and realisation of physical threats and environmental harm?

How does the business lock away confidential information that isn't in use, keep it out of sight from those unauthorised to see it when it is.

[37] Some government contracts will be a good example.

7.3. Secure business operations

Secure business operations	Nurture the way that business is done so that it is done securely. Manage and monitor your information systems effectively, keeping them up to date with contemporary software patches and upgrades.[38] Encrypt sensitive information carefully to keep information confidential for those who need it. Make sure that encryption is set up correctly – that it is not vulnerable through some other work around and that it can only be decrypted in the right place at the right time so that it offers the expected level of security and accessibility to legitimate users.

7.3.1. Guidance

Be aware of how the business of your activities, particularly when under pressure, can open attack vectors that might have been avoided with more time, care, and attention.

7.3.2. Requirements

What needs to be done to have assurance in the security of your information?

Secure business operations means the orchestration of security activities in a 'business-as-usual' way. So, as well as carrying out all the other direction in this standard to match your risk profile, there are particular activities which lay the foundations for people and technology to take up their roles in business processes to assure the continuing security of what you do.

This will mean that you will:

- Be aware of your fixed business architecture and the 'end point' devices which may change more often.
- Avoid the use of unauthorised hardware and software.
- Make sure that all the relevant changes are made to software to keep it up to date with newly fixed vulnerabilities (usually from the suppliers of the software you use). Apply these updates – or patches – and make sure that the installation is successful on all applicable devices. This will include:
  - Operating systems.
  - Application software and 'apps'.
  - E-commerce facilities.
- Keep control over the use of portable storage (including 'USB' sticks and memory cards, devices like tablets, phones, and games consoles which can be used for portable storage):
  - Consider whether certain types of information just should not be on certain types of devices (or certain types of devices when they are taken to certain places).
  - Vary your safe storage policy as necessary to fit on-premises working, mobile working, working from home, and working abroad.

  Make sure that where personal equipment (BYOD) is used for business that protective measures for equipment are commensurate with your risk assessment.
- Usually install security and other critical updates immediately.
- Keep service level agreements relevant and up to date with (amongst others):
  - Agencies and agency staff.
  - Service suppliers including, but not restricted to[39]:

[38] M.11 Define and implement a policy to control the use of authorised software.
[39] L.02 Define and implement a policy that addresses information security risks within supplier relationships.

- Data centre and cloud service providers.
- e-commerce and payment service providers.
- Hardware and software support services.
- Maintenance services (such as alarm systems, fire suppressants, HVAC).

Use encryption based on what your risk assessment recommends. Remember:

- You will need to retrieve your data so you must be able to decrypt it for use. Be organised in how you store and protect your encryption keys[40].
- To consider the arrangements for communications (such as e-mail) and ensure that the encryption is consistently applied throughout the business process.
- To manage the encryption of portable devices and media like memory cards, USB sticks, and discs.

Encrypt by default where Personally Identifiable Information (PII) is located.

Prefer automated methods of encryption over ones which require some manual action.

7.3.3. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business nurture the way that business is done so that it is done securely?
How does the business manage and monitor its information systems effectively, keeping them up to date with contemporary software patches and upgrades?
Does the business encrypt sensitive information carefully to keep information confidential for those who need it? How does it make sure that the way that information is encrypted is set up competently – that it is not vulnerable through some other work around and that it can be decrypted in the right place at the right time?

7.4. Access control

Access control	Control whom, and what, can access your information. Prefer a 'need to know' way of working.

7.4.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Give users access to all the resources and data necessary for their roles, but no more. This applies equally to data stored on computer equipment as to the respective parts of the premises where you do business. This is also applicable to a micro-business with one employee: you should not be carrying out day-to-day tasks such as invoicing or dealing with e-mail whilst logged on as a user with administrator privileges which allow significant changes to the way your computer systems work. You may also consider establishing – and implementing - your access control policies with restrictions as to the locations access may made from.

Give adequate consideration to full and part-time staff, contractors, volunteers, and visitors.

Make sure that the access privileges that are required for one computer or program to access information from another are also set up with these access control principles.

Make sure that privileges to access information can be revoked in a timely manner when someone changes roles (and no longer needs access) or is leaving your business.

[40] Don't lose access because someone leaves, dies, or forgets how to access the encryption key(s).

You may well contract with expertise outside your business to set up access to your technology. Make sure that you have non-disclosure agreements in place and can revoke the privileges that your suppliers may have been given.

This policy is referred to as 'least privilege' or 'need to know' and the decisions to grant access comes from your understanding of your risk profile. Certain privileges bring with them an increased risk of deliberate or accidental damage which can cause significant disruption. Consider – as applicable to your business – the need to access:

- Customer information.
- Databases – in whole or in part.
- Information about employees and contractors.
- Management information.
- Monitoring systems.
- Operating system files.
- Applications and other software programs
- Software source code.

7.4.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business control whom and what can access its information? Does the business prefer a 'need to know' way of working? If not, why not?

8. Detect and Deter

8.1. Malware and technical intrusion

Malware and technical intrusion	Install reliable anti-malware software on all devices where this prevention tool is available. Keep your anti-malware software up to date. Pay attention to its warnings and reports and take actions according to the risks it informs you about. Deploy other technical tools including intrusion detection and prevention methods.[41]

8.1.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Malware is malicious code that is designed to affect data confidentiality, integrity, or availability. It may:

- Come through e-mail (often as a specific branch of social engineering called 'phishing'), portable media, poisoned websites – especially 'blogs' and social media – and documents.
- Obtain intelligence about what you do or what you do for your customers.
- Steal saleable information such as know-how, plans, or financial information.
- Disrupt your working facilities by denying access and leave you exposed to blackmail to regain them.
- Form the vanguard of a bigger, more sustained attack on your business or a more valuable target in the supply chain which you provide the path to.

Malware is continually evolving to avoid detection so anti-malware must be kept up to date to enable it to detect malware and take action to block or delete it.

Prefer anti-malware software which:

- Has facilities to remove an infection if need be.
- Also blocks websites which are likely to pass on malicious content.

Set up[42]:

- Protective 'boundary' measures – such as firewalls – on devices that have the capability to host them.
- Ways of detecting unauthorised activity. These may include – but not be restricted to – tools and appliances for intrusion detection, data loss prevention, and honey pots or traps to distract attackers.

Review the settings on all your technology periodically to ensure that they are commensurate with contemporary threats.

8.1.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business deploy anti-malware and other technical tools including intrusion detection and prevention methods?

[41] H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.
[42] M.12 Define and implement a policy to control the flow of information through network borders.

8.2. Monitoring, review, and change – for healthy systems and unauthorised activity[43]

Monitoring, review, and change[44]	Make sure that the policies that you set to protect information and recover from a security incident are effective and remain supportive of your business objectives. Know which business systems and processes you need to track and monitor for acceptable activity – according the information safety policies that you have set - and how you will identify the unacceptable. Keep an eye on who is trying to access your information and where they are trying to access it from. Be prepared and ready to act on the intelligence your monitoring provides. Keep information which is forensically sound from a legal perspective.

8.2.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Be prepared to follow these basic directions for forensic readiness for when an information or cyber security incident occurs:

- Know how to access any logging information which your operating systems and applications provide to show how and by whom information is accessed.
- Pay attention to the reporting mechanisms provided with your security software such as firewalls and anti-malware.
- Have the ability to trace who has access to particular information (such strategic or personally identifiable information.
- If your risk assessment shows you need CCTV, make sure that cameras are suitably positioned and record adequate quality for playback and time analysis.
- Protect access to your monitoring systems and preserve the records they produce according to a suitable retention schedule.
- Make sure that employees are aware of any monitoring that may take place.

8.2.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Which business scenarios does the business track and monitor for acceptable activity and how does it identify the unacceptable. How does the business keep an eye on who is trying to access its information and where they are trying to access it from? How does the business keep information which is forensically sound from a legal perspective?

[43] H.11 Proactively verify that the security controls are providing the intended level of security.
[44] M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.

9. Respond and Recover

No security measures can be fully effective all the time, so investment in ways to respond to security incidents and recover from losses is essential. This includes a considered level of cyber liability insurance commensurate with the risk assessment.

9.1. Backup and restore

Backup and restore	Back up as frequently as you can stand versus the amount of rework you can afford to do. Maintain at least one of the back-ups off-site and at some distance from the working version of the data. Ensure backup copies are kept appropriately secured for the data they contain.

9.1.1. Guidance…

Regularly backing up (and having the ability to restore the backup) may be most effective method of protecting your business from the effects of accidental or malicious tampering such as deleting data, hardware failure, or ransomware.

9.1.2. …Requirements

What needs to be done to have assurance in the security of your information?

Secure the integrity and availability of information and information processing facilities with a backup and restore capability.

Key information should be backed up regularly and one copy of the backup(s) kept in a secure location away from the business premises. The backups must be tested regularly to be certain that they can be used to restore systems or information.

The IASME Governance Standard recommends three copies of your information:

- The day-to-day working copy
- A master back up (which may be the copy you store off-site away from the operational systems).
- A local back up for easy retrieval

– but all tuned by the expectations of your business continuity or disaster recovery plan.

9.1.3. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Does the business back up as frequently as it can stand versus the amount of rework it can stand or afford to do?

Does the business maintain at least one of the back-ups off-site and (well away from the working version of the data)?

How does the business secure backup copies to a degree commensurate with the risk to the data they contain?

Can the business show its confidence in the restoration of backups to complete, operational capability?

9.2. Incident management

Incident management[45]	Ensure breaches of confidentiality, integrity, or availability of your data are detected and dealt with. Make them easy to report to a responsible entity without blame. Set out a policy with clear responsibilities for reporting incidents as required by law and decency to customers and the respective external authorities. Learn the lessons.[46]

9.2.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Record breaches of confidentiality, integrity or availability of your systems, deal with them, and learn and apply the lessons. Analyse your records for:

- Recurring problems.
- How effective you were in dealing with an incident. How disruptive was it?
- The effectiveness of your risk assessment – did you get it right?

View incidents as learning experiences. Use them to educate yourself and your staff.

Update your risk assessment and the security measure it recommends with the intelligence gathered following an incident. Update you policies accordingly.

Preserve any information which may be required from a legal standpoint – consider if it will be needed for disciplinary action[47].

Make sure that people you work with know how to, and to whom, to report incidents. Make it clear who has the authority to invoke any necessary contingency measures.

Know your legal reporting obligations too and make it clear who is – and is not – allowed to talk about incidents outside the business.

9.2.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

How does the business ensure breaches of confidentiality, integrity or availability of it data are detected and dealt with?

Are staff, contractors, and partners able to report security incidents without blame?

How does the business show that it learns and applies the lessons of incidents to prevent their reoccurrence or reduce their impact?

[45] L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.
[46] L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.
[47] Note that digital forensics – like other forensics – is a specialist discipline. Digital information is volatile and subject to corruption that can make it misleading and inadmissible evidence of what went on.

9.3. Business continuity, disaster recovery, and resilience

Business continuity, disaster recovery, and resilience	Be ready to keep working through, and recover from, the effects of deliberate attack, accidental damage, and natural disasters. Make sure that you can transform, renew, and recover in timely response from a partial or total loss of information assets. Be true to the Cyber Security Essentials by making sure that the security requirements that they define are 'business as usual' across your information systems.

9.3.1. Guidance and requirements

What needs to be done to have assurance in the security of your information?

Make sure you can recover quickly from partial or total loss of keyinformation assets. Use the decisions in your risk assessment to prepare a plan about how you will deal with the loss of confidentiality, integrity, or availability of the critical information assets:

- Make sure everyone knows their responsibilities in the event of a break in business-as-usual.
- Make sure that authorities and responsibilities for disclosure of a data breach are allocated explicitly and that these can be realised when required.
- Plan for how you will maintain the ongoing confidentiality, integrity, and availability in unusual circumstances.
- Consider industrial action and natural phenomena such as flooding
- Include useful contact numbers, licence and service level agreement information in your plan.
- Exercise your plan from time to time so that you know it works – and keep it up to date to account for changes to your business.
- Involve any external services that you may need to.
- Consider – and act on – any marketing or public relations implications.

Learn the lessons from the event(s) and update your risk assessment and the security measure it recommends with the intelligence gathered. Update your information and cyber security policies accordingly.

9.3.2. Typical questions and performance indicators

A selection – but not exhaustive set – of tests that you will need to pass.

Is the business ready to keep working through, and recover from, the effects of deliberate attack, accidental damage, and natural disasters? How will the business make sure you it transform, renew, and recover in timely response from partial or total loss of information assets? Is the business true to the Cyber Security Essentials? (Not just 'ticking boxes' but meeting the Cyber Essentials Scheme requirements as part of its security strategy.)

Appendix A. DCPP Criteria

Good Governance

L.01 Define and assign information security relevant roles and responsibilities.
L.02 Define and implement a policy that addresses information security risks within supplier relationships.
M.01 Define and implement a policy that provides for regular, formal information security related reporting.

Culture and Awareness

L.03 Define and implement a policy that ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.
L.04 Define employee (including contractor) responsibilities for information security.
L.05 Define and implement a policy to provide employees and contractors with information security training.
M.02 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.

Risk Management

M.03 Define and implement a policy that provides for repeatable information security risk assessments.

Information

L.06 Define and implement a policy for ensuring that sensitive information is clearly identified.
L.07 Define and implement a policy to control access to information and information processing facilities.
M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.
M.05 Define and implement a policy for data loss prevention.
M.06 Ensure that the organisation has identified asset owners and that asset owners control access to their assets.

Technology and Services

L.08 Maintain Cyber Essentials Scheme Plus Certification.
L.09 Define and implement a policy to control the exchanging of information via removable media.
L.10 Define and implement an information security policy, related processes and procedures.
L.11 Record and maintain the scope and configuration of the information technology estate.
L.12 Define and implement a policy to manage the access rights of user accounts.
M.07 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.
M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.
M.09 Define and implement a policy to monitor user account usage and to manage changes of access rights.
M.10 Define and implement a policy to control remote access to networks and systems.
M.11 Define and implement a policy to control the use of authorised software.
M.12 Define and implement a policy to control the flow of information through network borders.
M.13 Define and implement a policy to maintain the confidentiality of passwords.
H.01 Maintain patching metrics and assess patching performance against policy.
H.02 Ensure that wireless connections are authenticated.
H.03 Deploy network monitoring techniques that complement traditional signature-based detection.
H.04 Place application firewalls in front of critical servers to verify and validate the traffic going to the server.
H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.
H.06 Define and implement a policy to control installations of and changes to software on any systems on the network.
H.07 Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines.

H.08 Undertake administration access over secure protocols, using multi-factor authentication.
H.09 Design networks incorporating security countermeasures, such as segmentation or zoning.
H.10 Ensure Data Loss Prevention (DLP) at network egress points to inspect the contents of and, where necessary, block information being transmitted outside of the network boundary.

Personnel Security

L.13 Define and implement a policy for verifying an individual's credentials prior to employment.
L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.
L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.
M.14 Define and implement a policy for applying security vetting checks to employees.
M.15 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.
M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.

Preparing for and Responding to Security Incidents

L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.
H.11 Proactively verify that the security controls are providing the intended level of security.

Appendix B. ISO 27n standards

The information security standards associated with ISO/IEC 27001 are legion (see below). The IASME Governance Standard continues to support SMEs by being the spine point of good information security practice that is scalable and effective.

- ISO/IEC 27000:2014 – Glossary
- ISO/IEC 27001:2013 – ISMS requirements
- ISO/IEC 27002:2013 – ISMS controls…a code of practice
- ISO/IEC 27003:2010 – ISMS implementation guidance
- ISO/IEC 27004:2009 – Security metrics
- ISO/IEC 27005:2011 – Risk management
- ISO/IEC 27006:2011 – ISMS certification
- ISO/IEC 27007:2011 – ISMS auditing
- ISO/IEC TR 27008:2011 – Controls auditing guide
- ISO/IEC 27009:TBA – Sector-specific ISMS
- ISO/IEC 27010:2012 – Information security management for inter-sector and inter-organisational communications
- ISO/IEC 27011:2008 (ITU X.1051) – Information security management for telecommunications
- ISO/IEC 27013:2015 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014:2013 – Information security governance
- ISO/IEC TR 27015:2012 – Information security management for financial services
- ISO/IEC TR 27016 – Information security management economics
- ISO/IEC 27017 – Information security controls for cloud computing
- ISO/IEC 27018 – Personal identifiable information on public cloud computing services
- ISO/IEC TR 27019:2013 – Information security for process control
- in the energy industry SCADA
- ISO/IEC 27031:2011 – ICT readiness for business continuity
- ISO/IEC 27032:2012 – Cyber security
- ISO/IEC 27033:2009 – IT network
- ISO/IEC 27034:2011 – Application security
- ISO/IEC 27035:2011 – Information security incident management
- ISO/IEC 27036:2013 – Supplier relationship management
- ISO/IEC 27037:2012 – Digital forensics
- ISO/IEC 27038 – Digital redaction
- ISO/IEC 27039 – Intrusion detection and prevention systems
- ISO/IEC 27040 – Storage security
- ISO/IEC 27041 – Suitability and adequacy of incident investigative methods
- ISO/IEC 27042 – Analysis and interpretation of digital evidence
- ISO/IEC 27043 – Incident investigation
- ISO/IEC 27044 – Security Incident and Event Management (SIEM)
- ISO/IEC 27050 – Electronic discovery
- ISO 27799:2008 – ISMS in the health sector